Distribution Agreement

In presenting this thesis or dissertation as a partial fulfillment of the requirements for an advanced degree from Emory University, I hereby grant to Emory University and its agents the non-exclusive license to archive, make accessible, and display my thesis or dissertation in whole or in part in all forms of media, now or hereafter known, including display on the world wide web. I understand that I may select some access restrictions as part of the online submission of this thesis or dissertation. I retain all ownership rights to the copyright of the thesis or dissertation. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

Signature:

_____ _____

Michael Cerchia Date

Topics in Abelian Varieties

By

Michael Cerchia
Doctor of Philosophy

Mathematics

David Zureick-Brown, Ph.D.
Advisor

Parimala Raman, Ph.D.
Committee Member

Suresh Venapally, Ph.D.
Committee Member

Accepted:

Kimberly Jacob Arriola, PhD
Dean of the James T. Laney School of Graduate Studies

Date

Topics in Abelian Varieties

By

Michael Cerchia
B.A., SUNY Geneseo, NY, 2012
M.A., Wake Forest University, NC, 2019

Advisor: David Zureick-Brown, Ph.D.

An abstract of
A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Mathematics
2024

Abstract

Topics in Abelian Varieties
By Michael Cerchia

We prove theorems and present progress on problems in the broad category of abelian varieties. The flavor of these problems and the techniques used to solve them vary, but a common theme is the use of geometric techniques (and in particular moduli theory) to solve concrete questions from arithmetic. The first two problems involve section rings of algebraic varieties. These rings are classical objects of study and play a central role in the minimal model program. In the first of these problems, we describe the section ring of elliptic curves for arbitrary divisors, and give a complete description when the underlying divisor is supported by up to two points. In the second, we investigate canonical rings of moduli stacks of principally polarized abelian varieties, with particular focus on the $g = 2$ case. These have additional arithmetic significance: the canonical ring of modular curves, when equipped with the structure of an algebraic stack, gives rise to rings of modular forms. By considering this higher dimensional analogue, we can determine explicit presentations for rings of Siegel modular forms. After these problems, we present progress on classifying torsion subgroups for elliptic curves over quartic fields, extending work of Mazur and Merel. Finally, we investigate under what conditions a Weil polynomial of degree 2g occurs as the characteristic polynomial of Frobenius for a simple abelian variety of dimension g over a given finite field, and give an answer for the $g = 7$ case.

Topics in Abelian Varieties

By

Michael Cerchia
B.A., SUNY Geneseo, NY, 2012
M.A., Wake Forest University, NC, 2019

Advisor: David Zureick-Brown, Ph.D.

A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Mathematics
2024

Acknowledgments

First, thanks to my advisor David Zureick-Brown for his generous and consistent support throughout my time at Emory. In addition to suggesting some of the problems that comprise this thesis, he has made many invaluable suggestions and has patiently taught me a lot of math over the years. I also thank my committee members, Parimala and Suresh, for taking the time to read this and listen to me talk about it over the summer while traveling abroad. Next, thanks to everyone else who taught me at Emory, including Michelangelo Grigni, Brooke Ullery, Shanshuang Yang, and my teaching mentor Juan Villeta-Garcia. I'm also grateful to David Borthwick, Terry Ingram, and Jim Nagy for smoothly running a supportive department. Finally, I want to thank everyone who I worked on math with over the years – I am lucky to have found kind and fun collaborators in Evan O'Dorney, Jesse Franklin, and Alexis Newton (who I also thank for watching my cats).

Contents

Chapter 1

Section rings of Q-Divisors on elliptic curves

1.1 Introduction and Background

Let X be a variety defined over a field k (which we may assume to be algebraically closed), and let D be a divisor on X. Throughout this chapter and the next, we will investigate the *section ring* of X and D:

$$R(X, D) := \bigoplus_{i=0}^{\infty} H^0(X, iD),$$

where we use the abbreviated notation $H^0(X, D) := H^0(X, \mathcal{O}(D))$ to denote the global sections of the sheaf $\mathcal{O}(D)$ on X.

In this chapter, we will continue to restrict to the case of curves. Quotients $X\backslash\Gamma$ of the upper half-plane by torsion-free cocompact Fuchsian groups $\Gamma \leq \mathrm{PSL}_2(\mathbb{R})$ are in bijective correspondence with compact Riemann surfaces of genus $g \geq 2$. The latter can be given the structure of a nonsingular projective algebraic curve over $\mathbb{C}$ via the canonical map $X \to \mathbb{P}^{g-1}$, constructed from global sections of the sheaf Ω_X

of holomorphic differential 1-forms on X. As Ω is ample, the *canonical ring*

$$R = R(X) = \bigoplus_{d \geq 0} H^0(X, \Omega^{\otimes d})$$

satisfies $X \cong \operatorname{Proj} R$. We observe that if K_X (equivalently Ω) is very ample, then we can apply the Proj functor to the natural multiplication map

$$\operatorname{Sym} H^0(X, K) \hookrightarrow R(X, K)$$

to get the canonical embedding

$$X \cong \operatorname{Proj} R(X, K) \to \operatorname{Proj}(\operatorname{Sym} H^0(X, K)/I) \cong \mathbb{P}^N,$$

where I here is the kernel of the multiplication map above.

This canonical ring is central to the minimal model program (where finite generation of the canonical ring of a variety is a main theorem) and is a classical object of study: By a theorem of Enriques and Babbage, which is commonly referred to as Petri's theorem, if X is neither hyperelliptic, trigonal (possessing a degree 3 map to $\mathbb{P}^1$), nor a plane curve of degree 5 (and genus 6), then $R(X) \cong \mathbb{C}[x_1, \ldots, x_g]/I$ is generated in in degree 1 with relations in degree 2. Petri further provides explicit quadratic relations defining I given in terms of a basis $x_1, \ldots x_g$ for $H^0(X, \Omega)$ as well as syzygies among the relations.

This classical result has been generalized in various ways. For instance, we can give any quotient $\Gamma\backslash\mathcal{H}$ with finite area the structure of a Riemann surface, but only if we now account for the points with nontrivial stabilizer groups. If we do this by adjusting the atlas in the neighborhoods of these points, then the resulting surface no longer corresponds to an algebraic curve, but rather to a *stacky curve*, where we now account for the finite number of points with a nontrivial (finite) stabilizer group.

In this setting, Voight and Zureick-Brown [12] extend Petri's Theorem by providing an explicit presentation of the canonical ring for a tame log stacky curve: They show that the canonical ring

$$R(\mathcal{X}, \Delta) = \bigoplus_{d \geq 0} H^0(\mathcal{X}, \Omega(\Delta)^{\otimes d}),$$

where $\Delta = \sum_i P_i$ is an effective divisor of distinct points, is generated as a $\mathbb{C}$-algebra by elements of degree at most $3e$ with relations of degree at most $6e$, where e is the maximum of 1 and the orders of the stabilizer groups. An important application of this result is that it provides generators and relations for rings of modular forms. Indeed, for any $N \geq 1$, the ring

$$M(\Gamma_0(N)) = \bigoplus_{k \in 2\mathbb{Z}_{\geq 0}} M_k(\Gamma_0(N)) = \bigoplus_{k \geq 0} H^0(X_0(N), \Omega^1(\Delta)^{\otimes k/2})$$

of modular forms is generated as a $\mathbb{Z}$-algebra in degree at most 3, with relations of degree at most 6 (and where Δ is the divisor of cusps).

Since log-canonical divisors on stacks are specific $\mathbb{Q}$-rational divisors, a natural question is whether we can say anything about canonical rings for general $\mathbb{Q}$-divisors for specific classes of curves. O'Dorney [9] gives a complete description of the section ring for $\mathbb{Q}$-divisors on $\mathbb{P}^1$ for the cases when D is supported by up to two points, and he gives tight bounds on the degrees of the generators and relations in the general case. In the rest of this chapter, we will extend these results to genus 1 curves; here, we will have to be sensitive to the group structure and to the fact that elliptic curves do not admit a rational function of degree one.

1.2 One-point support

1.3 The one-point case

Fix an elliptic curve C with a marked point ∞. We denote by t_i a function on C whose polar divisor is $i(\infty)$. We recall that t_i exists for $i \in \mathbb{Z}_{\geq 2} \cup \{0\}$; if C is given by a Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, then we may take

$$t_i = \begin{cases} x^{i/2}, & i \text{ even} \\ x^{(i-3)/2}y, & i \text{ odd.} \end{cases}$$

In this section, we take a divisor $D = \alpha(\infty)$ and study the generators and relations of the resulting section ring $R(C, D)$. Observe that there must be at least three generators and one relation (if $R(C, D)$ were freely generated, it would yield a birational isomorphism of C to some $\mathbb{P}^n$, which is impossible).

Example 1.3.1. Let $D = (\infty)$ consist of a single point with multiplicity 1. Then $R(C, D)$ has generators u, $x = u^2t_2$, $y = u^3t_3$ in degrees 1, 2, and 3, respectively, and a single degree 6 relation

$$y^2 + a_1uxy + a_3u^3y = x^3 + a_2u^2x^2 + a_4u^4x + a_6u^6,$$

a homogenization of the usual Weierstrass equation of the elliptic curve C. These generators are shown diagrammatically in Figure 1.1, where we plot degree on the horizontal axis and pole order on the vertical axis. We use bullets for generators, open dots for other elements of $R(X, D)$, and +'s to emphasize the nonexistence of elements in $R(X, D)$ having a simple pole at ∞.

In the following, we use without comment the following well-known characterization of the principal divisors on an elliptic curve C: ([10, Corollary III.3.5]) A divisor

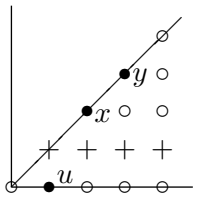

Figure 1.1: The section ring of $D = (P)$, which has three generators

$D = \sum n_P(P)$ on an elliptic curve is a principal divisor if and only if $\sum n_P = 0$ (as integers) and $\sum(n_P P) = 0$ (in the elliptic curve group law).

1.3.1 Generators

Theorem 1.3.2. *Let $D = \alpha(\infty)$ be a $\mathbb{Q}$-divisor on an elliptic curve C supported at a single point ∞. Let*

$$0 = \frac{c_0}{d_0} < \frac{c_1}{d_1} < \cdots < \frac{c_r}{d_r} = \alpha$$

be the nonnegative best approximations to α. Then $R(X, D)$ has a minimal generating set consisting of functions $f = t_c u^d$ for the following pairs (d, c):

(*a*) $(d, c) = (d_i, c_i)$ *for $i \neq 1$ (observe that c_1/d_1 is always the unique best lower approximation with numerator 1, and therefore inadmissible here);*

(*b*) $(d, c) = (d_{(\mathrm{b})}, c_{(\mathrm{b})}) = (\lceil 2/\alpha \rceil, 2)$ *if* $\{-1/\alpha\} \in [0, 1/2)$*;*

(*c*) $(d, c) = (d_{(\mathrm{c})}, c_{(\mathrm{c})}) = (\lceil 3/\alpha \rceil, 3)$ *if* $\{-1/\alpha\} \in [0, 1/3)[1/2, 2/3)$*;*

(*d*) $(d, c) = (d_{(\mathrm{d})}, c_{(\mathrm{d})}) = (d_1 + d_2, c_1 + c_2)$ *if* $\{-1/\alpha\} \in (0, 1/2)$.

We denote each relevant lattice point by $v_i = (d_i, c_i)$, and the corresponding generator of the section ring by $f_i = t_{c_i} u^{d_i}$, where i ranges over an index set I containing $\{0, 2, 3, \ldots, r\}$ as well as the special symbols (b), (c), and (d) in the cases in which they appear.

Proof. First, we transform the problem to finding generators for a certain semigroup.

Observe that a $\Bbbk$-basis for $R(X, D)$ is given by

$$\{t_c u^d : (d, c) \in M\} \tag{1.1}$$

where M is the monoid

$$M = \{(d, c) \in \mathbb{Z}^2 : 0 \leq c \leq \alpha d, c \neq 1\}.$$

For $v = (d, c) \in M$ a vector, let $f_v = t_c u^d$ be the corresponding element of $R(X, D)$. We cannot construct an isomorphism of $R(X, D)$ with the monoid ring $\Bbbk[M]$ in this way, but the objects are closely related, and we will use the combinatorial structure of M to probe the algebraic structure of $R(X, D)$.

Note that, owing to the grading by d, M is an **atomic** monoid, that is, every element is a (not necessarily unique) sum of irreducibles. Consequently, M has a unique minimal generating set, namely the irreducibles. Suppose that the following combinatorial lemmas about M are proved:

Lemma 1.3.3. *The irreducibles of M are exactly the pairs (d, c) in the statement of the theorem.*

Lemma 1.3.4. *Let (d, c) be an irreducible of M. Then any element $(d, c') \in M$ with $c' > c$ has a unique atomic decomposition.*

Let us show that these two lemmas imply the statement of the theorem. Let $\mathcal{P}$ be the set of irreducibles of M. Since $\mathcal{P}$ generates M, the corresponding generating set $\{f_v : v \in \mathcal{P}\}$ generates a subring $S' \subseteq R(X, D)$ containing elements $t_c^{(d)} u^d$ for all $(d, c) \in M$ (where $t_c^{(d)}$ is a function on C with a pole of order c at ∞, possibly depending on d). These elements span $R(X, D)$ as a $\Bbbk$-vector space, so $S' = R(X, D)$.

Now we show that each generator $f_v = t_c u^d$ is necessary. Let $S' \subseteq R(X, D)$ be the subring generated by the $f_{v'}$, $v' \neq v$, and suppose for the sake of contradiction

that $f_v \in S'$. Write

$$f_v = a_1 f_1 + \cdots + a_k f_k,$$

where $a_i \in \Bbbk$ and the $f_i \in S'_{\deg=d}$ are distinct products of the generators of S'. Since $v \in M$ is irreducible, no f_i can have a pole of order exactly c, so two of them, say f_1 and f_2, must have a common larger order $c' > c$ to cancel the poles out. But by Lemma 1.3.4, this is impossible. □

Proof of Lemma 1.3.3. To understand the structure of M, we compare it to the simpler monoid

$$M_0 = \{(d, c) \in \mathbb{Z}^2 : 0 \leq c \leq \alpha d\}$$

in which the condition $c \neq 1$ has been omitted. This monoid controls the structure of the section ring for the corresponding situation in genus zero, and in the course of proving [9, Theorem 4], it was shown that the irreducibles of M_0 are precisely the vectors (d_i, c_i) determined by the best lower approximations c_i/d_i.

Since $M \subset M_0$, all such vectors remain irreducible in M if they lie in M. Thus the vectors of type (a) in Theorem 1.3.2 are irreducible. For types (b) and (c), note that these are the simplest vectors in M with c-coordinate 2 and 3, respectively, and cannot be decomposed, since M has no elements with c-coordinate 1. Thus they must be added unless they already appeared in type (a). For type (b), we have that $c/d = 2/\lceil 2/\alpha \rceil$ is a best lower approximation (necessarily the second one c_2/d_2) if and only if

$$\begin{aligned}
\frac{2}{\lceil 2/\alpha \rceil} &> \frac{1}{\lceil 1/\alpha \rceil} \\
2\left\lceil \frac{1}{\alpha} \right\rceil &> \left\lceil \frac{2}{\alpha} \right\rceil \\
\frac{2}{\alpha} + 2\left\{ -\frac{1}{\alpha} \right\} &> \frac{2}{\alpha} + \left\{ -\frac{2}{\alpha} \right\} \\
2\left\{ -\frac{1}{\alpha} \right\} &> \left\{ -\frac{2}{\alpha} \right\}.
\end{aligned} \tag{1.2}$$

Since

$$\{2x\} = \begin{cases} 2\{x\} & \{x\} < 1/2 \\ 2\{x\} - 1 & \{x\} \geq 1/2, \end{cases}$$

the inequality (1.2) holds exactly when $\{-1/\alpha\} \geq 1/2$, so the generator of type (b) is needed whenever $\{-1/\alpha\} < 1/2$. For type (c), an analogous computation shows that $\{-1/\alpha\}$ must lie in the range $[0, 1/3)[1/2, 2/3)$ for $3/\lceil 3/\alpha \rceil$ not to have already appeared as a best lower approximation.

Finally, for type (d), note that if $-1/\alpha$ is an integer, then there is no c_2/d_2 because $c_1/d_1 = \alpha$ is the last approximation; while if $\{-1/\alpha\} \geq -1/2$, then $c_2 = 2$ as we found above, so $c_1 + c_2 = 3$, which pole order was already covered in types (a) and (c). So we only need to consider type (d) in the case $\{-1/\alpha\} \in (0, 1/2)$. Here $c_2 \geq 3$ and c_3 (if it exists) is greater than $1 + c_2$, so the only irreducibles that could possibly appear in a decomposition of $v = (d_1 + d_2, c_1 + c_2)$ are

$$(d_0, c_0) = (1, 0), \quad (\lceil 2/\alpha \rceil, 2), \quad (\lceil 3/\alpha \rceil, 3), \quad (d_2, c_2).$$

The last generator (d_2, c_2) may be eliminated immediately since the difference $v - (d_2, c_2) = (d_1, 1)$ lies outside M. That leaves three generators lying in the submonoid

$$\angle v_0 v_1 = \langle (1, 0), (d_1, 1) \rangle = \langle (d_0, c_0), (d_1, c_1) \rangle = \left\{ (d, c) \in \mathbb{Z}^2 : 0 \leq c \leq \frac{c_1}{d_1} d \right\}$$

of M_0 determined by the first two best lower approximations of α. But v lies outside $\angle v_0 v_1$ since $c_2/d_2 > c_1/d_1$, so v is irreducible in M. This completes the proof that the claimed generators are irreducible and distinct.

It remains to prove that there are no other irreducibles, that is, any nonzero vector $v \in M$ not among the ones listed is reducible in M. As an element of M_0, any v lies in

some angle $\angle v_i v_{i+1}$ and so can be decomposed as a positive integer linear combination

$$v = a(d_i, c_i) + b(d_{i+1}, c_{i+1})$$

of two consecutive generators of M_0. If $i \geq 2$, then these are also generators of M, so we only need to consider two cases:

Case 1. *$i = 0$. Then $(d_0, c_0) = (1, 0)$ is already a generator of M. We must have $b \neq 1$ since $v \in M$, so b can be written as a sum of 2's and 3's, which yields an expression for v in terms of the generators of types (a), (b), and (c).*

Case 2. *$i = 1$, so*

$$v = a(d_1, c_1) + b(d_2, c_2). \tag{1.3}$$

We may assume that a and b are nonzero, or else we could have taken $i = 0$ or $i = 2$ respectively (in the latter case, allowing a zero coefficient on a possibly nonexistent (d_3, c_3)). If $a \neq 1$, note that each term individually belongs to M, so v is reducible. So $a = 1$ and $b \geq 1$, and

$$v = (d_1 + d_2, c_1 + c_2) + (b - 1)(d_2, c_2)$$

is either reducible or a generator of type (d). □

Proof of Lemma 1.3.4. Now let $v = (d, c)$ be an irreducible of M. We wish to prove that any element $v' = (d, c') \in M$ lying above v has a unique atomic decomposition. By the previous lemma, v is of one of the four types in Theorem 1.3.2; we handle each type in turn. In Figure 1.2, we illustrate the various cases that can occur.

In type (a), c/d is a best lower approximation to α. Then c'/d must also be a best lower approximation to α, so v' is also irreducible (note that this can only occur if $d = 1$ and $\alpha \geq 3$).

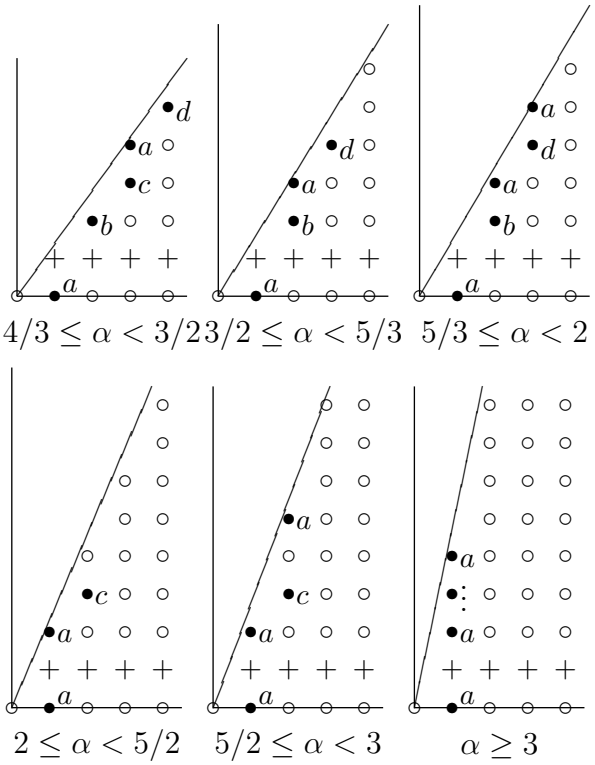

Figure 1.2: Cases covered by Lemma 1.3.4, where a generator of M has a point of M directly above it. The bullets indicate generators, annotated with their type (items a–d of Theorem 1.3.2).

In type (b), for there to be even one point $v' = (\lceil 2/\alpha \rceil, 3)$ in M above the given point $v = (\lceil 2/\alpha \rceil, 2)$, we must have the inequality

$$\frac{3}{\alpha} \le \left\lceil \frac{2}{\alpha} \right\rceil . \tag{1.4}$$

As the ceiling augments its argument by less than 1, we must have $\alpha > 1$, so v is either $(1, 2)$ or $(2, 2)$. The first case can be excluded as v is of type (a) rather than (b). There remains the possibility that $v = (2, 2)$ and $v' = (2, 3)$, which appears for $3/2 \le \alpha < 2$ and is also irreducible (of type (a)). (Points with $c' \ge 4$ cannot occur here, as then we would have had $\alpha \ge 2$ and $(1, 2) \in M$.)

In type (c), we analogously find that $\alpha > 1$ and v is either $(2, 3)$ or $(3, 3)$. Then:

- If $v = (2, 3)$, we must have $2 \le \alpha < 3$, and v' is either $(2, 4)$ or $(2, 5)$. The vector $v' = (2, 4) = 2(1, 2)$ has a unique atomic decomposition. If $\alpha \ge 5/2$,

then $v' = (2, 5)$ is also admissible and irreducible (of type (a)).

- If $v = (3, 3)$, we must have $4/3 \leq \alpha < 3/2$ to get the unique possible $v' = (3, 4) \in M$; this v' is irreducible (of type (a)).

For type (d), we first note that, since c_2/d_2 is the best lower approximation following $c_1/d_1 = 1/d_1$, we have

$$\frac{c_2}{d_2} = \frac{c_2}{c_2 d_1 - 1} \leq \alpha < \frac{c_2 - 1}{(c_2 - 1)d_1 - 1}. \tag{1.5}$$

For a point $v' = (d_1 + d_2, c_1 + c_2 + 1)$ to appear above v in M, we must have

$$\alpha \geq \frac{c_1 + c_2 + 1}{d_1 + d_2} = \frac{c_2 + 2}{d_1(c_2 + 1) - 1}. \tag{1.6}$$

Combining (1.5) and (1.6) yields

$$\frac{c_2 + 2}{d_1(c_2 + 1) - 1} < \frac{c_2 - 1}{(c_2 - 1)d_1 - 1}$$

which simplifies to

$$(c_2 - 1)d_1 < 3.$$

Accordingly, c_2 and d_1 must have their minimum possible values $c_2 = 2$ and $d_1 = 1$. We have $v = (3, 4)$, $5/3 \leq \alpha < 2$, and $v' = (3, 5)$, which is irreducible of type (a), completing the proof. □

1.3.2 Relations

We turn our attention to understanding a set of relations for the section ring $R(X, D)$. We again begin by looking at the genus 0 case. In this case, we have $\binom{r}{2}$ relations

among the $r+1$ generators, each led by a different quadratic monomial. These form a minimal basis for the relation ideal, as well as a Gröbner basis with respect to several of the commonly used term orders, including the **grevlex** order chosen by default in programs such as Sage and also used in the literature, such as in [12]. Having a Gröbner basis is desirable for computations, especially if the Gröbner basis is also minimal.

In the genus 1 case, as one might expect, things are a bit more involved, and it is good to choose the term order judiciously so that the Gröbner basis is as nearly minimal as possible. The term order we use is as follows:

Definition. Let $\{v_i\}_{i\in I}$ be the generators of M as computed in Theorem 1.3.2, and let $\{f_i\}_{i\in I}$ be the corresponding generators of $R(X,D)$. Order the index set I in increasing degree d and, within each degree, ordered in increasing pole order c; the order of the generators is therefore

$$\begin{aligned}
&f_0 \prec f_{(\mathrm{b})} \prec f_{(\mathrm{c})}, && \{-1/\alpha\} = 0\\
&f_0 \prec f_{(\mathrm{b})} \prec f_{(\mathrm{c})} \prec f_2 \prec f_{(\mathrm{d})} \prec f_3 \prec \cdots, && \{-1/\alpha\} \in (0,1/3)\\
&f_0 \prec f_{(\mathrm{b})} \prec f_2 \prec f_{(\mathrm{d})} \prec f_3 \prec \cdots, && \{-1/\alpha\} \in [1/3,1/2)\\
&f_0 \prec f_2 \prec f_{(\mathrm{c})} \prec f_3 \prec \cdots, && \{-1/\alpha\} \in [1/2,2/3)\\
&f_0 \prec f_2 \prec f_3 \prec \cdots, && \{-1/\alpha\} \in [2/3,1).
\end{aligned}$$

Given two distinct monomials

$$m^{(1)} = \prod_i v_i^{a_i^{(1)}} \quad \text{and} \quad m^{(2)} = v_i^{a_i^{(2)}},$$

where i ranges over the indices of all the generators in Theorem 1.3.2, we declare that either $m^{(1)}$ is lower than $m^{(2)}$, written $m^{(1)} \prec m^{(2)}$, or the reverse $m^{(1)} \succ m^{(2)}$ as follows:

1. First we compare degrees: if

$$\sum_i a_i^{(1)} d_i < \sum_i a_i^{(2)} d_i,$$

then $m^{(1)} \prec m^{(2)}$.

2. Then we compare pole orders: if the degrees are equal but

$$\sum_i a_i^{(1)} c_i < \sum_i a_i^{(2)} c_i,$$

then $m^{(1)} \prec m^{(2)}$.

3. If the degrees and pole orders are equal, we compare exponents of the generators, starting from the highest: if $a_i^{(1)} < a_i^{(2)}$ but $a_j^{(1)} = a_j^{(2)}$ for $f_j \succ f_i$, then $m^{(1)} \prec m^{(2)}$.

We can now state our main theorem. As in [12], we cannot list the relations in full detail, but at least we can provide the leading terms.

Theorem 1.3.5. *Let $D = \alpha(\infty)$ be a 1-point divisor. Denote the generators of type (a) in Theorem 1.3.2 by*

$$f_i = u^{d_i} t_{c_i}, \quad i = 0, 2, 3, \ldots, r,$$

and denote the exceptional generators of type (b), (c), and (d) by $f_{(\mathrm{b})}$, $f_{(\mathrm{c})}$, and $f_{(\mathrm{d})}$, respectively. Then a Gröbner basis of the relations of $R(X, D)$ has the following leading terms:

1. *All products $f_i f_j$, where $3 \leq i \leq r, 0 \leq j \leq i-2, j \neq 1$, except possibly $f_3 f_0$ (see below);*

2. *All products* $f_i f_{(\mathrm{b})}$, $f_i f_{(\mathrm{c})}$, *and* $f_i f_{(\mathrm{d})}$, *where* $3 \leq i \leq r$, *if these exceptional generators exist;*

3. *Additional relations, according to the value of* $\{-1/\alpha\}$ *which also controls the generators:*

$\{-1/\alpha\} \in$	*Exc. gens.*	*Leading terms of relations*
$\{0\}$	$f_{(\mathrm{b})}, f_{(\mathrm{c})}$	$f_{(\mathrm{c})}^2$
$(0, 1/3)$	$f_{(\mathrm{b})}, f_{(\mathrm{c})}, f_{(\mathrm{d})}$	$f_{(\mathrm{c})}^2, f_{(\mathrm{b})}f_{(\mathrm{d})}, f_{(\mathrm{c})}f_{(\mathrm{d})}, f_{(\mathrm{d})}^2, f_0 f_{(\mathrm{d})}, f_0 f_2$
$[1/3, 1/2)$	$f_{(\mathrm{b})}, f_{(\mathrm{d})}$	$\boxed{f_0^2 f_2^2}, f_0 f_{(\mathrm{d})}, f_{(\mathrm{b})}f_{(\mathrm{d})}, f_{(\mathrm{d})}^2$
$[1/2, 2/3)$	$f_{(\mathrm{c})}$	$f_{(\mathrm{c})}^2$
$[2/3, 1)$	—	$\boxed{f_0 f_3^2}$, *omit* $f_0 f_3$

Moreover, the relations comprising the Gröbner basis are all minimal, with the possible exception of the two cases with a non-quadratic leading term (boxed):

- *The relation with the quartic leading term* $f_0^2 f_2^2$ *is never minimal.*
- *The relation with the cubic leading term* $f_0 f_3^2$ *is minimal if and only if* $\{-1/\alpha\}$ *belongs to the subinterval* $[2/3, 3/4)$.

The relations for $R(X, D)$ are closely connected with those of the associated monoid M. Recall from the previous subsection that M has a minimal generating set $\{v_i\}_{i \in I}$. Let F be the free commutative monoid on $|I|$ generators $\{\tilde{v}_i\}_{i \in I}$ (isomorphic to $\mathbb{Z}_{\geq 0}^{|I|}$), and let π be the projection map

$$\pi : F \to M$$

$$\tilde{v}_i \mapsto v_i.$$

To complete a presentation of M is to find a (preferably finite) list of relations

$$R_j \colon e_j \sim e'_j$$

such that $M = F/\{R_j\}_j$, that is, such that the relation generated by the R_j is precisely

$$e \sim e' \iff \pi(e) = \pi(e').$$

To do this systematically, we make the following definition:

Definition. If $v \in M$, the **minimal decomposition** of v is the sum

$$\mathrm{MD}(v) = \sum_i a_i \tilde{v}_i \in F$$

such that $\pi(\mathrm{MD}(v)) = v$ and $\mathrm{MD}(v)$ is minimal with respect to the order from Definition 1.3.2 on elements of F.

Remark. It is evident from the d-grading on M that only finitely many such decompositions exist. Also, since v is fixed, the first two steps of Definition 1.3.2 may be skipped when comparing decompositions.

Definition. The **Gröbner basis** of M consists of the relations

$$v \sim \mathrm{MD}(\pi(v))$$

for all vectors v satisfying the following two conditions:

1. $v \neq \mathrm{MD}(\pi(v))$;
2. If $w <_F v$ (that is, $v = w + z$ with $0 \neq z \in F$), then $w = \mathrm{MD}(\pi(w))$.

Such a vector $v \in F$ is called a **relation leader** for M.

Remark. It is easy to see that the Gröbner basis forms a presentation of M as a quotient of F. Indeed, the relation leaders give the leading terms of a Gröbner basis of the monoid algebra $\Bbbk[M]$ as a quotient of the free algebra $\Bbbk[F]$ (adapting Definition 1.3.2 appropriately to define a term order on $\Bbbk[F]$).

The proof of Theorem 1.3.5 rests on the following combinatorial lemma:

Lemma 1.3.6. *The relation leaders for M are exactly the vectors $v = \sum_{i \in I} a_i \tilde{v}_i$ corresponding to each of the monomials $\prod_{i \in I} f_i$ claimed to be a leading term of a relation for $R(X, D)$ in Theorem 1.4.2.*

Given this lemma, the proof of the theorem is not so hard:

Proof of Theorem 1.3.5. Given a relation leader $v \in F$, let

$$v = \sum_i a_i \tilde{v}_i \quad \text{and} \quad \mathrm{MD}(\pi(v)) = \sum_i b_i \tilde{v}_i.$$

We get that $\prod_i f_i^{a_i}$ and $\prod_i f_i^{b_i}$ have the same degree and pole order, so their difference (after suitably scaling) has a pole of lower order and can be written in terms of the other generators to get a relation r_v in the relation ideal of $R(X, D)$. Since we compare monomials with reference to their pole orders, the leading term of r_v is $\prod_i f_i^{a_i}$.

Now, given any element $f \in R(X, D)$ expressed as a polynomial in the generators f_i, we can apply monomial multiples of the relations r_v to remove any relation leaders from the leading term, until either the entire sum vanishes (verifying that $f = 0$ in $R(X, D)$) or the leading term is a minimal decomposition $\mathrm{MD}((d, c))$, verifying that f is a nonzero element of leading degree d with a pole of order c. This shows that the r_v form a Gröbner basis.

It remains to determine which of the relations in the Gröbner basis are minimal. Note that if $v = \tilde{v}_i + \tilde{v}_j$ has Hamming weight 2, then r_v, which has a quadratic leading term $f_i f_j$, must be minimal because there are no relations with a term of f_i or f_j alone to generate this relation (or else f_i, respectively f_j, would not be a generator).

This leaves the two boxed relations. The relation with quartic leading term $f_0^2 f_2^2$, in case $\{-1/\alpha\} \in [1/3, 1/2)$, has the form

$$f_0^2 f_2^2 = f_{(\mathrm{b})}^3 + \text{lower-order poles},$$

but since

$$2v_0 + 2v_2 = v_0 + v_{(\mathrm{b})} + v_{(\mathrm{d})} = 3v_{(\mathrm{b})},$$

this relation can be derived by subtracting those led by $f_{(\mathrm{b})} f_{(\mathrm{d})}$ and $f_0 f_{(\mathrm{d})}$ after multiplying by f_0 and $f_{(\mathrm{b})}$ respectively to cancel the $f_0 f_{(\mathrm{b})} f_{(\mathrm{d})}$ term. Hence this relation is never minimal.

We now turn to the relation with cubic leading term $f_0 f_3^2$. The corresponding relation in M is

$$v_0 + 2v_3 = 3v_2 \tag{1.7}$$

If $\{-1/\alpha\} \in [3/4, 1)$, then there is a vector $v_4 = 2v_3 - v_2 \in M$, and the relation (1.7) is not minimal, even in M:

$$v_0 + 2v_3 = v_0 + v_2 + v_4 = 3v_2.$$

Translating from M to $R(X, D)$, we find correspondingly that the relation with leading term $f_0 f_3^2$ can be generated by the relations led by $f_2 f_4$ and $f_0 f_4$.

On the other hand, if $\{-1/\alpha\} \in [2/3, 3/4)$, then $2v_3 - v_2 \notin M$, and there are no relations having a term of f_3^2 or $f_0 f_3$, hence no way to decompose the relation with leading term $f_0 f_3^2$. □

Proof of Lemma 1.3.6. Let $v = (d, c) \in M$. If $v \in \angle v_i v_{i+1}$ for $i \geq 2$, then we have a decomposition $v = a_i v_i + a_{i+1} v_{i+1}$ with $a_j \geq 0$. We claim that this is a minimal decomposition. Suppose not; let $v = \sum_j b_j v_j$ be a lesser one. We must have $b_j = 0$ for $j \leq i + 1$. If $b_{i+1} < a_{i+1}$, then the difference $v - b_{i+1} v_{i+1}$ would be outside $\angle v_0 v_i$ and

thus not expressible as a sum of generators preceding v_{i+1}, all of which are within that angle. So $b_{i+1} = a_{i+1}$. Similarly, if $b_i < a_{i+1}$, then the difference $v - b_{i+1}v_{i+1} - b_iv_i$ would be outside $\angle v_0v_i$ and thus not expressible as a sum of generators preceding v_{i+1}, all of which are within that angle. So $b_i = v_i$ and hence all other b_i are 0.

We now compute the minimal decompositions of vectors in $\angle v_0v_2$. The generators needed are some subset of

$$v_0, v_{(\mathrm{b})}, v_{(\mathrm{c})}, v_2, v_{(\mathrm{d})}, v_3$$

in the various cases. The resulting minimal decompositions are shown in Table **??**. Each individual decomposition is not hard to prove minimal. The pattern of the decompositions is as follows: the generating sets $\{v_0, v_{(\mathrm{b})}\}$, $\{v_{(\mathrm{b})}, 2\}$, or (if $\{-1/\alpha\} \geq 1/2$) $\{v_0, v_2\}$ generates a sublattice of index 2 inside the appropriate angle. If the desired vector v lies in this sublattice as tested by the parity of a_1, its minimal decomposition is an integer combination of those two generators; otherwise there is need for a single copy of $v_{(\mathrm{c})}$, $v_{(\mathrm{d})}$, or v_3.

Looking over the minimal decompositions that we have found, we immediately see that the sums $v_i + v_j$, where $i \geq 3$ and $0 \leq j \leq i-2$, do not appear and therefore are relation leaders, with one exception: if $\{-1/\alpha\} \in [2/3, 1)$, then $v_0 + v_3$ is the minimal decomposition of $v_1 + v_2$. The same argument applies to the sums $v_i + v_j$ where $i \geq 3$ and j is one of the special symbols (b), (c), and (d). It remains only to check sums of v_0, $v_{(\mathrm{b})}$, $v_{(\mathrm{c})}$, $v_{(\mathrm{d})}$, v_2, and (if $\{-1/\alpha\} \in [2/3, 1)$) v_3, and in each case we get the desired result:

- For $\{-1/\alpha\} = 0$, as the only generators are f_0, $f_{(\mathrm{b})}$, and $f_{(\mathrm{c})}$, there will only be one relation leader, namely $2v_{(\mathrm{c})}$. Any decomposition with at most one copy of $v_{(\mathrm{c})}$ is minimal by our computations.

- For $\{-1/\alpha\} \in (0, 1/3)$, any decomposition not containing the relation leaders

$2v_{(\mathrm{c})}$, $v_{(\mathrm{b})} + v_{(\mathrm{d})}$, $v_{(\mathrm{c})} + v_{(\mathrm{d})}$, $2v_{(\mathrm{d})}$, $v_0 + v_{(\mathrm{d})}$, or $v_0 + v_2$ is of one of the forms

$$a_0 v_0 + a_{(\mathrm{b})} v_{(\mathrm{b})}, \quad a_0 v_0 + a_{(\mathrm{b})} v_{(\mathrm{b})} + v_{(\mathrm{c})},$$
$$a_{(\mathrm{b})} v_{(\mathrm{b})} + a_2 v_2, \quad a_{(\mathrm{b})} v_{(\mathrm{b})} + a_2 v_2 + v_{(\mathrm{c})}, \quad a_2 v_2 + v_{(\mathrm{d})}$$

and hence is minimal.

- For $\{-1/\alpha\} \in [1/3, 1/2)$, any decomposition not containing the relation leaders $2v_{(\mathrm{c})}$, $v_{(\mathrm{b})} + v_{(\mathrm{d})}$, $v_{(\mathrm{c})} + v_{(\mathrm{d})}$, $2v_{(\mathrm{d})}$, $v_0 + v_{(\mathrm{d})}$, or $2v_0 + 2v_2$ is of one of the forms

$$a_0 v_0 + a_{(\mathrm{b})} v_{(\mathrm{b})}, \quad a_0 v_0 + a_{(\mathrm{b})} v_{(\mathrm{b})} + v_2,$$
$$a_{(\mathrm{b})} v_{(\mathrm{b})} + a_2 v_2, \quad a_{(\mathrm{b})} v_{(\mathrm{b})} + a_2 v_2 + v_0, \quad a_2 v_2 + v_{(\mathrm{d})}$$

and hence is minimal.

- For $\{-1/\alpha\} \in [1/2, 2/3)$, any decomposition not containing the relation leader $2v_{(\mathrm{c})}$ is of one of the forms

$$a_0 v_0 + a_2 v_2, \quad a_0 v_0 + a_2 v_2 + v_{(\mathrm{c})}$$

and hence is minimal.

- For $\{-1/\alpha\} \in [2/3, 1)$, any decomposition not containing the relation leader $v_0 + 2v_3$ is of one of the forms

$$a_0 v_0 + a_2 v_2, \quad a_0 v_0 + a_2 v_2 + v_3, \quad a_2 v_2 + a_3 v_3$$

and hence is minimal.

This completes the proof of the lemma. □

1.4 The effective two-point case

Let $D = \alpha^{(1)}(P^{(1)}) + \alpha^{(2)}(P^{(2)})$ be an effective $\mathbb{Q}$-divisor on an elliptic curve C supported on two points $P^{(k)}$. In this section, we study the structure of the associated section ring $R(X, D)$. We may assume that $\alpha^{(1)} \geq \alpha^{(2)}$ since the roles of the points $P^{(k)}$ may be interchanged.

1.4.1 Generators

For $c \in \mathbb{Z}_{\geq 0}$, $c \neq 1$, and for $i \in \{1, 2\}$, denote by $t_c^{(k)}$ a function on C whose polar divisor is $c(P^{(i)})$. Also, let w be the function on C whose polar divisor is $P^{(1)} + P^{(2)}$. (Such a function is unique up to scaling and adding constants.) Note the following:

Lemma 1.4.1. *Let $D = a^{(1)}(P^{(1)}) + a^{(2)}(P^{(2)})$ be a nonzero effective $\mathbb{Z}$-divisor supported at two points. The linear system of functions $H^0(D)$ has dimension $a^{(1)} + a^{(2)}$, with a basis as follows:*

- $\{1, t_2^{(1)}, \ldots, t_{a^{(1)}}^{(1)}\}$ *if* $a^{(1)} > a^{(2)} = 0$;
- $\{1, t_2^{(2)}, \ldots, t_{a^{(2)}}^{(2)}\}$ *if* $a^{(2)} > a^{(1)} = 0$;
- $\{1, w, t_2^{(1)}, \ldots, t_{a^{(1)}}^{(1)}, t_2^{(2)}, \ldots, t_{a^{(2)}}^{(2)}\}$ *if* $a^{(1)}$ *and* $a^{(2)}$ *are positive.*

Proof. The dimension of $H^0(D)$ is given by the Riemann–Roch theorem. We check that the claimed functions are linearly independent because they have different orders at ∞, so they must form a basis. □

We now state the generators of the section ring. Our description generalizes the one-point case (Theorem 1.3.2):

Theorem 1.4.2. *Let $D = \alpha^{(1)}(P^{(1)}) + \alpha^{(2)}(P^{(2)})$ be an effective $\mathbb{Q}$-divisor on an elliptic curve C supported on two points $P^{(k)}$, with $\alpha^{(1)} \geq \alpha^{(2)}$. Let*

$$0 = \frac{c_0^{(k)}}{d_0^{(k)}} < \frac{c_1^{(k)}}{d_1^{(k)}} < \cdots < \frac{c_{r^{(k)}}^{(k)}}{d_{r^{(k)}}^{(k)}} = \alpha^{(k)}$$

be the best lower approximations to $\alpha^{(k)}$*. Notice that the denominators*

$$d_1^{(k)} = \lceil 1/\alpha^{(k)} \rceil$$

satisfy $d_1^{(1)} \leq d_1^{(2)}$*.*

Then $R(X, D)$ *has a minimal system of generators of the following forms:*

(*a*) $f_i^{(k)} = t^{(k)}_{c_i^{(k)}} u^{d_i^{(k)}}$ *for* $k \in \{1, 2\}$ *and* $i = 0, 2, 3, \ldots, r^{(k)}$ *(including* $f_0 = u$ *for* $i = 0$*)*

(*b*) $f_{(\mathrm{b})} = t_2^{(1)} u^{\lceil 2/\alpha^{(1)} \rceil}$ *if* $\{-1/\alpha^{(1)}\} \in [0, 1/2)$*;*

(*c*) $f_{(\mathrm{c})} = t_3^{(1)} u^{\lceil 3/\alpha^{(1)} \rceil}$ *if* $\{-1/\alpha^{(1)}\} \in [0, 1/3)[1/2, 2/3)$ *and* $\lceil 1/\alpha^{(2)} \rceil > \lceil 1/\alpha^{(1)} \rceil$*;*

(*d*) $f_{(\mathrm{d})} = t^{(1)}_{c_1^{(1)} + c_2^{(2)}} u^{d_1^{(1)} + d_2^{(1)}}$*, if* $\{-1/\alpha^{(1)}\} \in (0, 1/2)$ *and* $\lceil 1/\alpha^{(2)} \rceil > \lceil 1/\alpha^{(1)} \rceil$*;*

(*e*) $f_w = w u^{d_1^{(2)}}$*.*

Proof. Lemma 1.4.1 suggests the following strategy. Write $D = D^{(1)} + D^{(2)}$ where

$$D^{(k)} = \alpha^{(k)} P^{(k)}.$$

Then, as a $\Bbbk$-vector space,

$$R(X, D) = R(X, D^{(1)}) + R(X, D^{(2)}) + \Bbbk[u] u^{d_1^{(2)}} w, \tag{1.8}$$

because w is the only basis element for any graded piece $u^n H^0(nD)$ of $R(X, D)$ that does not already appear in either $R(X, D^{(1)})$ or $R(X, D^{(2)})$, and it first appears in degree $\lceil 1/\alpha^{(2)} \rceil = d_1^{(2)}$. Hence we can get a generating set for $R(X, D)$ by aggregating generating sets for $R(X, D^{(1)})$ and $R(X, D^{(2)})$ and adjoining the single added generator $u^{d_1^{(2)}} w$. We must then pare this set down to a minimal generating set. From the general theory of graded algebras, the *degrees* of the minimal generators are uniquely

determined; but the generators themselves and their pole orders at the $P^{(k)}$) are not. Observe that the generator $wu^{d_1^{(2)}}$ is minimal, as it is the lowest-degree element in $R(X, D)$ that does not lie in the subring $R(X, D^{(1)})R(X, D^{(2)})$ generated by functions with poles at only one of the two given points $P^{(k)}$.

A generator of type (a) in each $R(X, D^{(k)})$ (the labeling coming from Theorem 1.3.2) will always remain minimal in $R(X, D)$, as there is no way to get a pole of order $c_j^{(k)}$ by combining elements of lower degrees, by definition of best lower approximation. We consider the other types in turn.

We first claim that the generators of types (b), (c), and (d) in $R(X, D^{(2)})$, if any, are *never* minimal in $R(X, D)$ and can be removed. By the proof of Theorem 1.3.2, all of these correspond to vectors (d, c) that are minimal generators of the monoid

$$M^{(2)} = \{(d, c) \in \mathbb{Z}^2 : 0 \leq c \leq \alpha^{(2)}d, c \neq 1\}$$

but not of the simpler monoid

$$M_0^{(2)} = \{(d, c) \in \mathbb{Z}^2 : 0 \leq c \leq \alpha^{(2)}d\}.$$

But $R(X, D)$, unlike $R(X, D^{(2)})$, contains homogeneous elements f achieving every vector

$$(d, c) = (\deg f, -\mathrm{ord}_{P^{(2)}} f)$$

in $M_0^{(2)}$: take wu^d if $c = 1$, and otherwise take the appropriate element of $R(X, D^{(2)})$. Consequently, given a generator $g \in R(X, D)$ whose associated vector $(d, c) = (\deg g, -\mathrm{ord}_{P^{(2)}} g)$ is reducible in $M_0^{(2)}$, we can multiply elements of $R(X, D)$ of lower degrees to achieve the pole order c and subtract this from g to leave a pole of lower order. This lower order can again be achieved by a product of generators besides g (note that generators of types (b), (c), and (d) always appear in distinct degrees, referring to Lemma 1.3.4

and Figure 1.2), and continuing this way, we arrive at a function with no pole at $P^{(2)}$, that is, an element of $R(X, D^{(1)})$. Hence g is a polynomial in the other generators of $R(X, D)$.

We now investigate under what conditions the generators of types (b), (c), and (d) in $R(X, D^{(1)})$ remain minimal in $R(X, D)$. For (b), the generator $f_{(\mathrm{b})} = t_2^{(1)} u^{\lceil 2/\alpha^{(1)} \rceil}$ of degree $d = \lceil 2/\alpha^{(1)} \rceil$ is the first appearance in $R(X, D)$ of a function with a double pole at $P^{(1)}$. By assumption, there is no other generator of $R(X, D^{(1)})$ with a double pole in this degree, so the only way to eliminate it is to multiply two functions of lower degree with simple poles at $P^{(1)}$. The first function of this sort is

$$f_w^2 = w u^{\lceil 1/\alpha^{(2)} \rceil} \cdot w u^{\lceil 1/\alpha^{(2)} \rceil} \tag{1.9}$$

of degree

$$2 \left\lceil \frac{1}{\alpha^{(2)}} \right\rceil \geq 2 \left\lceil \frac{1}{\alpha^{(1)}} \right\rceil \overset{*}{=} \left\lceil \frac{2}{\alpha^{(1)}} \right\rceil = d,$$

the starred equality holding since $\{-1/\alpha^{(1)}\} \in [0, 1/2)$. So the only way that this generator can be non-minimal is if equality holds, and in particular, $R(X, D^{(1)})$ and $R(X, D^{(2)})$ look alike up to degree d. But the unique product (1.9) in this degree has double poles at both $P^{(1)}$ and $P^{(2)}$, and since we already threw out the generator $t_2^{(2)} u^d$ of type (b) in $R(X, D^{(2)})$, there is no way to cancel out the double pole at $P^{(2)}$. Hence the generator $f_{(\mathrm{b})}$, if it appears in $R(X, D^{(1)})$, always remains minimal in $R(X, D)$, as claimed.

Next, we look at type (c). Here we have a generator $f_{(\mathrm{c})} = t_3^{(1)} u^{\lceil 3/\alpha^{(1)} \rceil}$ of degree $d = 3/\lceil 3/\alpha^{(1)} \rceil$, which is the least degree in which there appears a triple pole at $\alpha^{(1)}$. To cancel out this pole, we must multiply two elements of lower degree with a single

and a double pole at $P^{(1)}$. The first function of this sort is

$$wu^{\lceil 1/\alpha^{(2)} \rceil} \cdot t_2^{(1)} u^{\lceil 2/\alpha^{(1)} \rceil} = \begin{cases} f_w f_{(\mathrm{b})}, & \{-1/\alpha^{(1)}\} \in [0, 1/2) \\ f_w f_2^{(1)}, & \{-1/\alpha^{(1)}\} \in [1/2, 1) \end{cases} \tag{1.10}$$

of degree

$$\left\lceil \frac{1}{\alpha^{(2)}} \right\rceil + \left\lceil \frac{2}{\alpha^{(1)}} \right\rceil \geq \left\lceil \frac{1}{\alpha^{(1)}} \right\rceil + \left\lceil \frac{2}{\alpha^{(1)}} \right\rceil \overset{*}{=} \left\lceil \frac{3}{\alpha^{(1)}} \right\rceil = d, \tag{1.11}$$

the starred equality holding since $\{-1/\alpha^{(1)}\} \in [0, 1/3)[1/2, 2/3)$. Again, the generator is therefore minimal unless equality holds. If equality holds, then the function (1.10) has a triple pole at $P^{(1)}$ as well as a simple pole at $P^{(2)}$ which can be canceled by adding the appropriate multiple of wu^d, yielding an element of $R(X, D^{(1)})$ with the desired triple pole. Accordingly, the generator g of type (c) is minimal if and only if equality does *not* hold in (1.11), as claimed.

Finally, suppose $R(X, D^{(1)})$ has a generator of type (d), which is of the form $f_{(\mathrm{d})} = t_c^{(1)} u^d$ where

$$d = d_1^{(1)} + d_2^{(1)}, \quad c = c_1^{(1)} + c_2^{(1)} = 1 + c_2^{(1)}$$

Note that this is only the second degree, after $d_2^{(1)}$, in which $R(X, D)$ is strictly larger than the subring $S' = R(X, 1/d_1^{(1)} P^{(1)} + \alpha^{(2)} P^{(2)}))$ where the pole order at $P^{(1)}$ is limited by the first best lower approximation $1/d_1^{(1)}$. To eliminate $f_{(\mathrm{d})}$, we must multiply two elements of lower degree at least one of which lies outside S'. Hence we must use

$$f = t_{c_2^{(1)}} u^{d_2^{(1)}},$$

a generator of $R(X, D^{(1)})$ of type (a). We must multiply it by an element h of degree $d_1^{(1)}$ with at least a simple pole at $P^{(1)}$. But a double pole at $P^{(1)}$ does not appear until degree $\lceil 2/\alpha^{(1)} \rceil \geq 2d_1^{(1)} - 1$, which is too high unless $d_1^{(1)} = 1$ and $\alpha^{(1)} \geq 2$, and

here there cannot be a generator of type (d), because then the generator $t_3^{(1)}u^2$ is of type (a) or (c) rather than (d). So h must have a simple pole at $P^{(1)}$, which only happens when the generator $h = wu^{d_1^{(2)}}$ has low enough degree, namely when

$$\left\lceil \frac{1}{\alpha^{(2)}} \right\rceil = \left\lceil \frac{1}{\alpha^{(1)}} \right\rceil . \tag{1.12}$$

We can then multiply $f \cdot h$ to get a function in degree d with the desired pole order c at $P^{(1)}$ and a simple pole at $P^{(2)}$, which can be canceled by adding the appropriate multiple of wu^d. Accordingly, the generator $f_{(\mathrm{d})}$ is minimal if and only if equality does *not* hold in (1.12), as claimed. □

1.4.2 Relations

In this section we state and prove the relations among the generators in the effective two-point case. It will be noted that, in Theorem 1.4.2, the form of the generators is quite different depending on whether (1.12) holds or not. This bifurcation in turn affects the term order we choose and the form of the relations, and hence we divide the statement and proof into two.

The unequal ceilings case

In this section we assume that

$$\left\lceil \frac{1}{\alpha^{(2)}} \right\rceil < \left\lceil \frac{1}{\alpha^{(1)}} \right\rceil . \tag{1.13}$$

Definition. Let $D = \alpha^{(1)}P^{(1)} + \alpha^{(2)}P^{(2)}$ be an effective $\mathbb{Q}$-divisor on C supported at two points, and assume (1.13). We order the generators of $R(X, D)$

(1) first by pole order at $P^{(2)}$,

(2) then by degree,

(3) then by pole order at $P^{(1)}$.

We order the monomials in the generators of $R(X, D)$

(1) first by pole order at $P^{(2)}$,

(2) then by degree,

(3) then by pole order at $P^{(1)}$,

(4) then by the exponents of the generators, starting with the highest generator.

Remark. By sorting first by pole order at $P^{(2)}$, we ensure that the generators of the subring $R(X, D^{(1)})$, and monomials therein, appear first in the ordering, and in the same order as in the 1-point case (Definition 1.3.2). For instance, if $\{-1/\alpha^{(1)}\} \in (0, 1/3)$, the ordering of the generators is

$$u = f_0 \prec f_{(\mathrm{b})} \prec f_{(\mathrm{c})} \prec f_2^{(1)} \prec f_{(\mathrm{d})} \prec f_3^{(1)} \prec \cdots \prec f_{r^{(1)}}^{(1)} \prec f_w \prec f_2^{(2)} \prec \cdots \prec f_{r^{(2)}}^{(2)}.$$

Theorem 1.4.3. *With this term order, a Gröbner basis for the relation ideal of $R(X, D)$ has the following leading terms:*

1. *The same leading terms of the relations among the $f_i^{(1)}$, $f_{(\mathrm{b})}$, $f_{(\mathrm{c})}$, and $f_{(\mathrm{d})}$ that obtain in the one-point case for $R(X, D^{(1)})$ in Theorem 1.3.5;*
2. *$u \cdot f_i^{(2)}$, $i \geq 2$;*
3. *$f_w \cdot f_i^{(2)}$, $i \geq 3$;*
4. *$f_i^{(2)} \cdot f_j^{(2)}$, $i \geq j + 2$;*
5. *All products $f^{(1)} f^{(2)}$ where $f^{(1)}$ is of one of the forms $f_i^{(1)}$ ($i \geq 2$), $f_{(\mathrm{b})}$, $f_{(\mathrm{c})}$, or $f_{(\mathrm{d})}$ and $f^{(2)}$ is of one of the forms $f_j^{(2)}$ ($j \geq 2$) or f_w.*

Proof. Because we ordered the generators of $R(X, D^{(1)})$ (the "old" generators) before all others (the "new" generators), the Gröbner basis for the relations among the old generators is unchanged from the one-point case. We call these the "old" relations.

A $\Bbbk$-basis for the quotient space $R(X, D)/R(X, D^{(1)})$ consists of one function $f^{(2)}_{(d,c)}$ of degree d having pole order c at $P^{(2)}$, for each (d, c) with $1 \leq c \leq \alpha^{(2)}d$. Note that $c = 1$ need not be excluded now. Consequently, the relations between the new generators closely parallel the genus zero case. For (d, c) in the angle $\angle v^{(2)}_i v^{(2)}_{i+1}$, the minimal monomial achieving degree d and pole order c is a product of the appropriate powers of the two consecutive generators $f^{(2)}_i$ and $f^{(2)}_{i+1}$, where $f^{(2)}_1$ must be replaced by f_w. Consequently, any product of two nonconsecutive new generators, or of a new and an old generator, is the leading term of a relation (a "new" relation).

The new relations are all minimal because their leading terms are quadratic. It remains to consider whether an old, minimal relation can become non-minimal when the new generators and relations are added. (An old, non-minimal relation obviously remains non-minimal here.) Referring to Theorem 1.3.5, there was only one case where a relation with a non-quadratic leading term was nonetheless minimal: the case $\{-1/\alpha^{(1)}\} \in [2/3, 3/4)$. Here there are generators $u = f_0, f^{(1)}_2, f^{(1)}_3$ corresponding to best lower approximations

$$\frac{c_0}{d_0} = 1, \quad \frac{c_2}{d_2} = \frac{2}{2n-1}, \quad \frac{c_3}{d_3} = \frac{3}{3n-2}$$

(letting $n = d_1 = \lceil 1/\alpha^{(1)} \rceil$). The relation in question has leading term $u{f^{(1)}_3}^2$, so if it is not minimal, then some other relation must have a term of $uf^{(1)}_3$ or ${f^{(1)}_3}^2$ to cancel it out. We claim there is no relation having either of these terms. This is clear for ${f^{(1)}_3}^2$ because its pole order of 6 at $P^{(1)}$ is the largest possible in degree $6n-4$, except possibly $\mathrm{ord}_{P^{(1)}}(f^{(1)}_4) = -7$ when $n = 1$, and no other monomial achieves this pole order. As to uf_3, we observe that the only possible monomials in degree $3n-1$ having

a pole of order at least 3 at $P^{(1)}$ are

$$uf_3, \quad {f_2^{(1)}}^2, \quad f_2^{(1)} f_3^{(1)}, \quad {f_3^{(1)}}^2, \quad f_4^{(1)}. \tag{1.14}$$

(since $f_2^{(1)} f_w$, the first monomial of this sort outside $R(X, D^{(1)})$, has degree at least $(2n-1)+(n+1) > 3n-1$). The functions (1.14) have poles of distinct orders $3, 4, 5, 6, 7$ at $P^{(1)}$ and thus cannot figure in any relation, completing the proof. □

The equal ceilings case

In this section we assume that

$$\left\lceil \frac{1}{\alpha^{(1)}} \right\rceil = \left\lceil \frac{1}{\alpha^{(2)}} \right\rceil. \tag{1.15}$$

Definition. Let $D = \alpha^{(1)} P^{(1)} + \alpha^{(2)} P^{(2)}$ be an effective $\mathbb{Q}$-divisor on C supported at two points, and assume (1.15). We order the generators of $R(X, D)$ in the following way:

$$u = f_0 \prec f_w \prec \left[f_{(\mathrm{b})}\right] \prec f_2^{(1)} \prec \cdots \prec f_{r^{(1)}}^{(1)} \prec f_2^{(2)} \prec \cdots \prec f_{r^{(2)}}^{(2)},$$

with the brackets because $f_{(\mathrm{b})}$ appears only when $\{-1/\alpha^{(1)}\} \in [0, 1/2)$. We order monomials in the generators by the exponents of the generators, largest first (i.e. lex order).

Remark. Note the absence of comparison of degrees or pole orders in this term order, in contrast to Definition 1.4.2. It would be desirable to use a more uniform term order for all effective two-point divisors, but this leads to difficulties such as a profusion of cases and a heightened number of non-minimal relations in the Gröbner basis.

Theorem 1.4.4. *With this term order, a Gröbner basis for the relation ideal of $R(X, D)$ has the following leading terms:*

(*a*) *If $\{-1/\alpha^{(1)}\} \in [0, 1/2)$:*

1. $f_{(\mathrm{b})}^2$;
2. $uf_i^{(k)}$, $i \geq 2$, $k \in \{1,2\}$;
3. $f_w f_i^{(k)}$, $i \geq 3$, $k \in \{1,2\}$;
4. $f_{(\mathrm{b})} f_i^{(k)}$, $i \geq 2$, $k \in \{1,2\}$;
5. $f_i^{(k)} f_j^{(k)}$, $i \geq j+2$, $k \in \{1,2\}$;
6. $f_i^{(1)} f_j^{(2)}$, $i \geq 2$, $j \geq 2$.

(*b*) *If* $\{-1/\alpha^{(1)}\} \in [1/2, 1)$*:*

1. $\boxed{f_2^{(1)} f_w^2}$;
2. $uf_i^{(1)}$, $i \geq 3$;
3. $uf_i^{(2)}$, $i \geq 2$;
4. $f_w f_i^{(k)}$, $i \geq 3$, $k \in \{1,2\}$;
5. $f_i^{(k)} f_j^{(k)}$, $i \geq j+2$, $k \in \{1,2\}$;
6. $f_i^{(1)} f_j^{(2)}$, $i \geq 2$, $j \geq 2$.

Moreover, the relations comprising the Gröbner basis are all minimal, with the possible exception of the one with a cubic leading term (boxed), which is minimal if and only if

$$\{-1/\alpha^{(1)}\} \in [1/2, 2/3) \quad \textit{and} \quad \{-1/\alpha^{(2)}\} \in [0, 1/2).$$

Proof. The proof of this theorem is somewhat different from the preceding ones owing to the different term order. Let $n = \lceil 1/\alpha^{(1)} \rceil = \lceil 1/\alpha^{(2)} \rceil$, and define the subdivisors

$$D' = \frac{2}{\lceil 2/\alpha^{(1)} \rceil} P^{(1)} + \frac{1}{n} P^{(2)} = \begin{cases} \frac{1}{n} P^{(1)} + \frac{1}{n} P^{(2)}, \{-1/\alpha^{(1)}\} \in [0, 1/2) \\ \frac{2}{2n-1} P^{(1)} + \frac{1}{n} P^{(2)}, \{-1/\alpha^{(1)}\} \in [1/2, 1) \end{cases}$$

$$D'' = \frac{2}{\lceil 2/\alpha^{(1)} \rceil} P^{(1)} + \alpha^{(2)} P^{(2)}.$$

The significance of the resulting filtration of the section rings $R(X, D') \subseteq R(X, D'') \subseteq R(X, D)$ is that

(a) $R(X, D')$ is generated by the lowest three generators: u, f_w, and either $f_{(\mathrm{b})}$ ($\{-1/\alpha^{(1)}\} \in [0, 1/2)$) or $f_2^{(1)}$ ($\{-1/\alpha^{(1)}\} \in [1/2, 1)$);

(b) $R(X, D'')$ is generated by $R(X, D')$ and the remaining generators $f_i^{(1)}$;

(c) $R(X, D)$ is generated by $R(X, D'')$ and the remaining generators $f_i^{(2)}$.

These claims are not hard to show. For brevity, we focus on the case $\{-1/\alpha^{(1)}\} \in [1/2, 1)$, the other being analogous. Here $R(X, D)$ has a relation because the element $f_2^{(1)} f_w^2$, with degree and pole orders $(d, c^{(1)}, c^{(2)}) = (4n-1, 4, 2)$, can be expressed as a linear combination of terms ${f_2^{(1)}}^2 u$ $(4n-1, 4, 0)$, $f_w^2 u^{2n-1}$ $(4n-1, 2, 2)$, and elements with lower pole orders (namely $f_2^{(1)} f_w u^n$, $f_2^{(1)} u^{2n}$, $f_w u^{3n-1}$, and u^{4n-1}). Applying this relation, we can express any polynomial in the first three generators as a linear combination of terms $f_w^i u^j$, ${f_2^{(1)}}^i u^j$, and ${f_2^{(1)}}^i f_w u^j$. Specifically, in degree $d \geq n$, we have the elements

$$\begin{aligned} & f_w^i u^{d-ni}, && 0 \leq i \leq \frac{d}{n} \\ & {f_2^{(1)}}^i u^{d-(2n-1)i}, && 1 \leq i \leq \frac{d}{2n-1} \\ & {f_2^{(1)}}^i f_w u^{d-(2n-1)i}, && 1 \leq i \leq \frac{d-n}{2n-1}. \end{aligned} \tag{1.16}$$

Comparing pole orders shows these are all linearly independent, and the number of them is

$$\begin{aligned} 1 + \left\lfloor \frac{d}{n} \right\rfloor + \left\lfloor \frac{d}{2n-1} \right\rfloor + \left\lfloor \frac{d-n}{2n-1} \right\rfloor &= 1 + \left\lfloor \frac{d}{n} \right\rfloor + \left\lfloor \frac{d}{2n-1} \right\rfloor + \left\lfloor \frac{d-n+1/2}{2n-1} \right\rfloor \\ &= \left\lfloor \frac{d}{n} \right\rfloor + \left\lfloor \frac{d}{2n-1} \right\rfloor + \left\lfloor \frac{d}{2n-1} + \frac{1}{2} \right\rfloor \\ &= \left\lfloor \frac{d}{n} \right\rfloor + \left\lfloor \frac{2d}{2n-1} \right\rfloor \\ &= \dim(R(X, D'))_{\deg=d}, \end{aligned}$$

so in fact (1.16) are a basis for $R(X, D')$, so there are no more generators or relations needed.

The generation of the quotient spaces $R(X, D'')/R(X, D')$ and $R(X, D)/R(X, D')$ follows the genus zero case: a $\Bbbk$-basis is indexed by combinations $(d, c^{(k)})$ of degree and pole order at the respective point with

$$\frac{2}{\lceil 2/\alpha^{(1)} \rceil} d < c^{(1)} \leq \alpha^{(1)} d, \quad k = 1 \text{ (for } R(X, D'')/R(X, D')\text{)}$$
$$\frac{1}{n} d < c^{(2)} \leq \alpha^{(2)} d, \quad k = 2 \text{ (for } R(X, D)/R(X, D'')\text{)},$$

and each $(d, c^{(k)})$ is minimally achieved by a product of consecutive generators ${f_i^{(k)}}^a {f_{i+1}^{(k)}}^b$, where f_w stands in for both $f_1^{(1)}$ and $f_1^{(2)}$. Consequently, any product of two generators not of this type is the leading term of a relation, as claimed.

It remains to determine whether the relation with the cubic, boxed leading term $f_2^{(1)} f_w^2$ (degree $4n-1$) is minimal. We divide into cases by the values of the $\{-1/\alpha^{(i)}\}$, as claimed in the theorem.

If $\{-1/\alpha^{(1)}\} \in [2/3, 1)$, that is, $\alpha^{(1)} \geq 3/(3n-2)$, there is a best lower approximation $c_3^{(1)}/d_3^{(1)} = 3/(3n-2)$ giving a generator $f_3^{(1)}$ in degree $3n-2$ with a triple pole at $P^{(1)}$. Using the relations

$$R_1 = f_3^{(1)} u + \cdots$$
$$R_2 = f_3^{(1)} f_w + \cdots,$$

we take a linear combination $R = f_w R_1 - u R_2$, causing the leading terms $f_3^{(1)} f_w u$ to cancel. Observe that R_1 has a term $f_2^{(1)} f_w$, the only possible monomial in degree $4n-1$ with a triple pole at $P^{(1)}$ below $f_3^{(1)} u$ in the term ordering. So R has a term $f_2^{(1)} f_w^2$. All other terms of $f_w R_1$ and $u R_2$, except the leading terms which cancel, are lower in the term ordering (namely $f_2^{(1)} f_w u^n$, $f_2^{(1)} u^{2n}$, $f_w u^{3n-1}$, and u^{4n-1}). So we have

achieved a relation R with the desired leading term, showing that the boxed Gröbner basis element is not minimal.

Similarly, if $\{-1/\alpha^{(2)}\} \in [1/2, 1)$, that is, $\alpha^{(2)} \geq 2/(2n-1)$, there is a best lower approximation $c_2^{(2)}/d_2^{(2)} = 2/(2n-1)$ giving a generator $f_2^{(2)}$ in degree $2n-1$ with a double pole at $P^{(2)}$. Using the relations

$$R_1 = f_2^{(2)} u + \cdots$$
$$R_2 = f_2^{(2)} f_2^{(1)} + \cdots,$$

we form a combination

$$R = f_2^{(1)} R_1 - u R_2 - c u^{2n-1} R_1,$$

where the first two terms have canceling leading terms $f_2^{(2)} f_2^{(1)} u$, and the constant c is chosen to cancel out the term $f_2^{(2)} u^{2n}$ which may appear in uR_2. The highest remaining term is $f_2^{(1)} f_w^2$, which must appear with a nonzero coefficient because f_w^2 is the only other term in R_1 that can have a double pole at $P^{(1)}$. So, again, the boxed Gröbner basis element is not minimal.

Finally, if $\{-1/\alpha^{(1)}\} \in [1/2, 2/3)$ and $\{-1/\alpha^{(2)}\} \in [0, 1/2)$, we claim that the boxed Gröbner basis element is minimal. If not, it arises by canceling the leading terms of other relations, so there must be a monomial in the generators of degree $4n-1$ divisible by two different leading terms of relations. We have $\deg f_2^{(2)} \geq 3n-1$, $\deg f_3^{(2)} \geq 4n-2$, and $\deg f_3^{(1)} \geq 5n-3$, so we can restrict our sights to u, f_w, $f_2^{(1)}$, and $f_2^{(2)}$. The only relations among these have leading terms $u f_2^{(2)}$, $f_w f_2^{(2)}$, and $f_2^{(1)} f_w^2$, all of which have degree at least $4n-1$, so this is impossible. □

Remark. The structure of the ring is somewhat simpler in this case and much more nearly symmetric between $\alpha^{(1)}$ and $\alpha^{(2)}$.

1.5 The subtle behavior of the ineffective two-point case

It would be desirable to extend the results of this paper to ineffective two-point divisors D having positive multiplicity at one point and negative at the other. However, in this situation, the section ring depends on the choice of curve C and divisor D in a much more subtle way.

Example. Let $D = 4P^{(1)} - P^{(2)}$. In degree 1, we have three generators t_2u, t_3u, t_4u. In degree 2, the question arises of whether the six pairwise products $u^2t_it_j$ of the generators fill the six-dimensional space

$$(R(X,D))_{\deg=2} = u^2 \cdot \langle t_3, t_4, t_5, t_6, t_7, t_8 \rangle .$$

In fact they do. If there were a linear relation among these products, a consideration of zero and pole orders at the $P^{(k)}$ shows that it would have to have the form

$$t_3^2 = ct_2t_4, \quad c \in \Bbbk,$$

but the two sides do not have the same divisor. Hence degree 1 generates degree 2, and in particular t_3 is a linear combination of the products t_it_j, $2 \le i \le j \le 4$. In fact, we can be more explicit:

Taking $y = t_3$ and $x = t_2$ as coordinates, we get a Weierstrass equation of the curve

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $P^{(1)}$ is the point at ∞ and $P^{(2)}$ is the origin $(0,0)$. We must have

- $a_6 = 0$ since $(0,0)$ lies on C;
- $a_4 = 0$ since y has a double zero at $(0,0)$;

- $a_3 \neq 0$ since C is nonsingular at $(0,0)$;
- $a_2 \neq 0$ or else y would have a triple zero at $(0,0)$.

Then

$$t_4 = x^2 - \frac{a_3}{a_2} y,$$

and the curve's equation can be written as

$$t_3 = \frac{1}{a_3}\left(t_2 t_4 - \frac{a_3}{a_2} t_2 t_3 + a_2 t_2^2 - t_3^2\right),$$

showing that indeed $t_3 \in \langle t_2 t_4, t_3^2, t_2 t_3, t_2^2 \rangle$. Note that t_3's pole of order 3 at $P^{(1)}$ arises from canceling functions with poles of order 6, 6, 5, and 4.

Example. Let p and q be coprime positive integers. By the Euclidean algorithm, there are positive integers a and b such that $aq - bp = 1$. Let $P^{(1)}$ and $P^{(2)}$ be points whose difference is not torsion, and consider the divisor

$$D = \frac{a}{p} P^{(1)} - \frac{b}{q} P^{(2)}$$

of degree $1/(pq)$. For $d > 0$, the dimension of $(R(X,D))_{\deg=d}$ is

$$\dim(R(X,D))_{\deg=d} = \max\left\{0, \left\lfloor \frac{ad}{p} \right\rfloor - \left\lceil \frac{bd}{q} \right\rceil - 1\right\}.$$

We recognize the right side as the number of ways of writing $d - pq$ in the form $xp + yq$ where $x, y \in \mathbb{Z}_{\geq 0}$. The least degree in which there is any element is $d = pq$. For $pq \leq d < 2pq$, the degrees in which $R(X,D)$ is nonzero are of the form $d = pq + k$ where k belongs to the Frobenius (symmetric, two-generated) semigroup

$$\langle p, q \rangle = \{xp + yq : x, y \in \mathbb{Z}_{\geq 0}\},$$

and due to the degree bound $pq \leq d < 2pq$, none of these can generate each other. This yields an intricate pattern of generators and relations.

1.5.1 A conjecture on generators

Suppose that $P^{(1)}$ and $P^{(2)}$ are two points on C such that $P^{(1)} - P^{(2)}$ is not a torsion class in the Picard group (the generic case). For $c \geq 0$, let t_c denote the unique function (up to scaling) on C with

$$\div(t_c^{(1)}) = -c(P^{(1)}) + (c-1)(P^{(2)}) + (cP^{(1)} \oplus (1-c)P^{(2)}),$$

where $\oplus$ denotes addition in the group law on C, as opposed to formal addition of divisors. Observe that if $c \geq 2$, then

$$\operatorname{ord}_{P^{(1)}} t_c = -c \quad \text{and} \quad \operatorname{ord}_{P^{(2)}} t_c = c - 1.$$

Lemma 1.5.1. *Let $D = \alpha^{(1)}(P^{(1)}) - \alpha^{(2)}(P^{(2)})$ be a $\mathbb{Z}$-divisor on an elliptic curve supported at two points, where $\alpha^{(1)} > \alpha^{(2)} \geq 0$. Then $H^0(D)$ has dimension $\alpha^{(1)} - \alpha^{(2)}$ with a basis consisting of the functions*

- $\{1, t_2, \ldots, t_{\alpha^{(1)}}\}$ *if* $\alpha^{(2)} = 0$*;*
- $\{t_{\alpha^{(2)}+1}, \ldots, t_{\alpha^{(1)}}\}$ *if* $\alpha^{(2)} > 0$.

Proof. Since $\deg D = \alpha^{(1)} - \alpha^{(2)} \geq 1$, the Riemann-Roch theorem gives us the dimension $h^0(D)$. We check that the claimed functions belong to $H^0(D)$ and have different pole orders at $P^{(1)}$, so they must form a basis. □

Let $D = \alpha^{(1)}(P^{(1)}) - \alpha^{(2)}(P^{(2)})$ be a $\mathbb{Q}$-divisor supported at the two points $P^{(k)}$, and suppose that $\alpha^{(1)} > \alpha^{(2)} > 0$ so that $R(X, D)$ is non-trivial. Since $P^{(1)} - P^{(2)}$ is not torsion, $H^0(dD)$ does not contain any function f of degree d with $\operatorname{ord}_{P^{(1)}}(f) = \lceil d\alpha^{(2)} \rceil$.

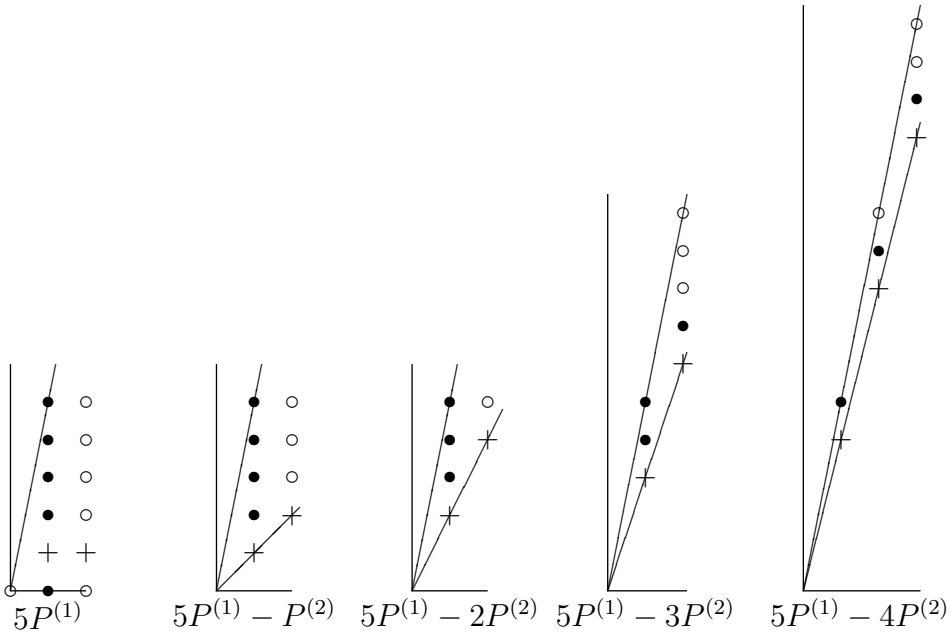

Figure 1.3: Example bases for $R(X, D)$ with D as in Lemma 1.5.1

Accordingly, we mark the points $(d, \lceil d\alpha^{(2)} \rceil)$ in the monoid $M' = \{(d, c) \in \mathbb{Z}^2 : d\alpha^{(2)} \leq c \leq d\alpha^{(1)}\}$ by a '+' in our examples.

Conjecture. Let $D = \alpha^{(1)}(P^{(1)}) - \alpha^{(2)}(P^{(2)})$ be an ineffective ($\alpha^{(1)} > \alpha^{(2)} > 0$) $\mathbb{Q}$-divisor on an elliptic curve C supported at two points $P^{(k)}$, where $P^{(1)} - P^{(2)}$ is not a torsion class in the Picard group (the generic case). Let

$$0 = \frac{c_0^{(1)}}{d_0^{(1)}} < \frac{c_1^{(1)}}{d_1^{(1)}} < \cdots < \frac{c_r^{(1)}}{d_r^{(1)}} = \alpha^{(1)};\ 0 = \frac{c_0^{(2)}}{d_0^{(2)}} > \frac{c_1^{(2)}}{d_1^{(2)}} > \cdots > \frac{c_s^{(2)}}{d_s^{(2)}} = \alpha^{(2)}$$

be the best lower approximations to $\alpha^{(1)}$ and the best upper approximations to $\alpha^{(2)}$ respectively. Let $M = \{(d, c) \in \mathbb{Z}^2 : d\alpha^{(2)} + 1 \leq c \leq d\alpha^{(1)}\}$.

Then $R(X, D)$ has a minimal system of generators of the following forms:

(a) $t_{c_j^{(1)}} u^{d_j^{(1)}}$, for $j = s^{(2)} + 1, \ldots, r^{(1)}$ if $c_j^{(1)} > \lceil d_j^{(2)} \alpha^{(2)} \rceil$ for some j;

(b) $t_{c_j^{(2)}+1} u^{d_j^{(2)}}$, for $j = 2, \ldots, s^{(2)}$ if such a generator has not already appeared and no $(d_j^{(2)}, c_j^{(2)} + n) \in M$ with $n \geq 2$ is (at least) two distinct nonnegative linear combinations of $(d, c) \in M$ with $d < d_j^{(2)}$;

(c) $t_{c_j^{(2)}+2}u^{d_j^{(2)}}$, for $j = 3, \ldots, s^{(2)}$ if all of the following conditions are met:

- $c_j^{(2)} + 2 \leq d_j^{(2)}\alpha^{(1)}$,
- $(d_j^{(2)}, c_j^{(2)} + 2)$ is not a nonnegative linear combination of any $(d, c) \in M$ with $d < d_j^{(2)}$, and
- no point $(d_j^{(2)}, c_j^{(2)} + n) \in M$ for $n \geq 3$ is (at least) two distinct nonnegative linear combinations of $(d, c) \in M$ with $d < d_j^{(2)}$.

Remark. Each type of generator in Conjecture 1.5.1 is minimal because of how we have defined them. As in [9], Theorems 1.3.2 and 1.4.2 and [8], no best lower approximation to $\alpha^{(1)}$ comes from combining functions in lower degrees, and by definition no generator of type (b) or (c) corresponds to a linear combination of other generators, nor some difference of functions as in the proof of Theorem 1.4.2. For examples of D with sufficiently large degrees we can use Magma to determine the degrees of minimal generators for $R(X, D)$ including Example 1.5.1 which has the subtle behavior of Example 1.5, and generators from Conjecture 1.5.1 seem to give a basis.

However, it is difficult to verify this conjecture rigorously, especially in cases such as Example 1.5 with small degree, as Magma needs to check for generators in such large degrees as to be computationally prohibitive. Even if Conjecture 1.5.1 is true, the question remains of whether we can find a simpler description of the generators which does not rely on manually working out every possible linear combination of vectors in the monoid M while successively adding generators in the order indicated by Definition 1.3.2.

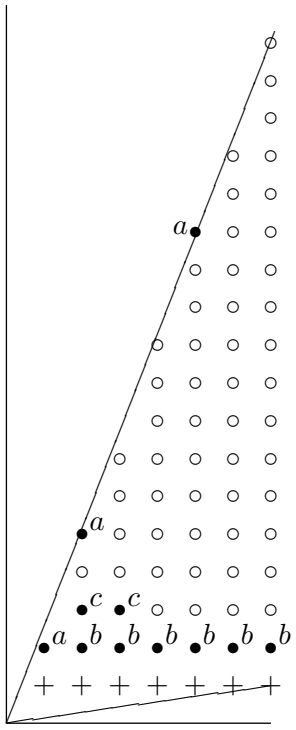

Figure 1.4: Generators for $R(X, D)$ labeled according to Conjecture 1.5.1 when $D = \frac{13}{5}P^{(1)} - \frac{1}{7}P^{(2)}$.

Example. Let $D = \frac{2}{3}P^{(1)} - \frac{3}{5}P^{(2)}$. This is an example of the behavior discussed in Example 1.5. Up to degree 60, Magma computes generators for $R(X, D)$ in degrees:

$$15, 18, 20, 21, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 37.$$

1.6 Arbitrary effective $\mathbb{Q}$-divisors

For divisors supported by more than two points, generators and relations often occur in high degrees, and it is difficult to explicitly describe the canonical ring. Thanks to [8] we are able to determine inductive presentations of such rings for effective $\mathbb{Q}$-divisors, similar to the main inductive theorem in Voight–Zureick-Brown [12, 8.3.1].

Example. As in [12, Example 5.7.7] let $D' = \frac{1}{2}P_1 + \frac{1}{2}P_2$, and following [12, Example 5.7.9] let $D = D' + \frac{1}{2}P_3 = \frac{1}{2}P_1 + \frac{1}{2}P_2 + \frac{1}{2}P_3$. Then $\deg D = 3/2$. By the Generalized

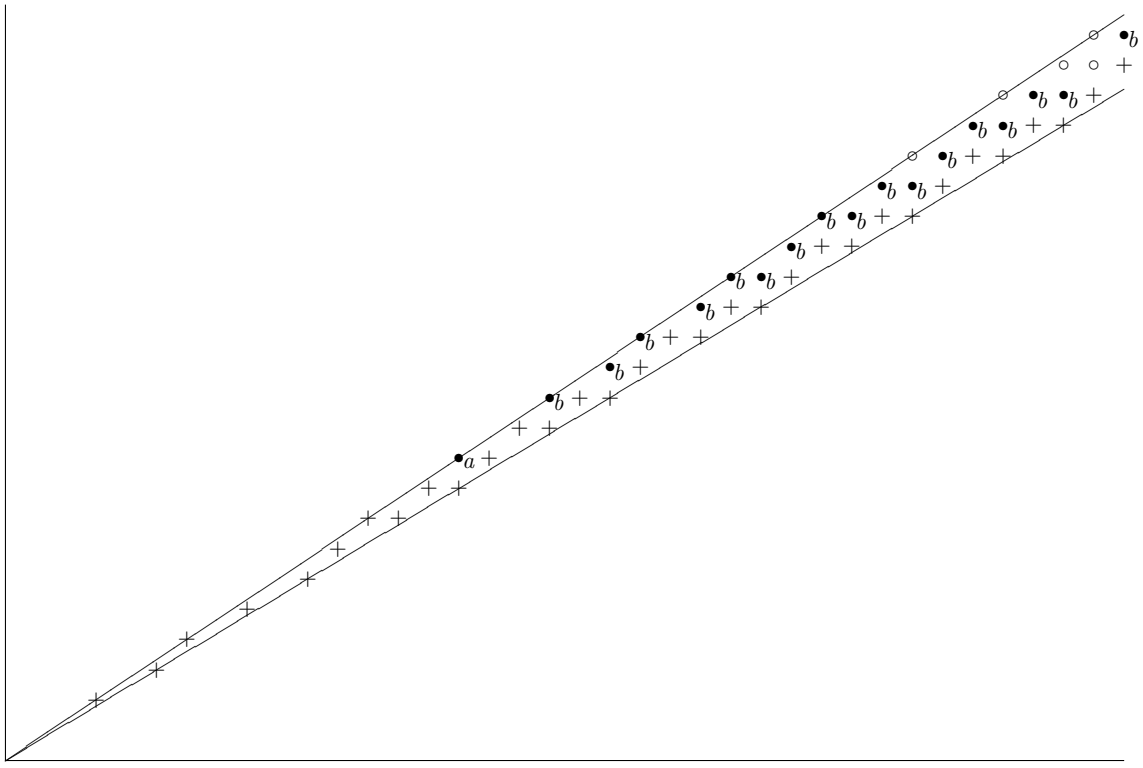

Figure 1.5: Generators for $R(X, D)$ labeled according to Conjecture 1.5.1 where $D = \frac{2}{3}P^{(1)} - \frac{3}{5}P^{(2)}$.

Max Noether Theorem [12, Lemma 3.1.4], $H^0(C, 2D) \otimes H^0(C, (d-2)D) \to H^0(C, dD)$ is surjective for $d > 5$, so all generators occur in degree < 5.

More precisely, in [12] it is computed that $R(X, D')$ is generated in degrees 1, 2, and 4 while $R(X, D)$ is generated in degrees 1, 2, and 2. The square of the last degree-2 generator of $R(X, D)$ is the degree-4 generator for $R(X, D')$.

So the minimal presentations have the form $R(X, D) = \Bbbk[u, x_1, x_2]/I_D$ and $R(X, D') = \Bbbk[u, x_1, x_2^2]/I_{D'}$, where I_D, $I_{D'}$ are the relation ideals. In particular, $R(X, D)$ is generated over $R(X, D')$ by x_2.

A powerful result which allows one to compute an inductive presentation of the section ring of a general $\mathbb{Q}$-divisor on an elliptic curve is [8, Lemma 4.4]. We paraphrase the result, which is of independent interest, in the terminology of this document for reference. We then use it to prove Theorem 1.6.2 by verifying that our general $\mathbb{Q}$-divisors satisfy the hypotheses of the lemma.

If D is a divisor on a curve C, P is a point on C, and f is a rational function on C, we define, following [8],

$$\operatorname{ord}_P^D(f) = \operatorname{ord}_P(f) + \operatorname{ord}_P(D),$$

so that $f \in H^0(D)$ if and only if $\operatorname{ord}_P^D(f) \geq 0$ for all points P.

Lemma 1.6.1 ([8, Lemma 4.4])**.** *Let C be a curve (of any genus) and let D' be an effective $\mathbb{Q}$-divisor on C. Suppose that P is not a basepoint of dD' for any $d \in \mathbb{N}$, i.e. we can choose generators $u = f_0, f_1, \ldots, f_m$ of $R(X, D')$ with $\deg(u) = 1$, and $\operatorname{ord}_P^{D'}(f_i) = 0$ for $0 \leq i \leq m$.*

Suppose that $D = D' + \dfrac{a}{b}P$ for some $a, b \in \mathbb{N}$ such that $\frac{a}{b}$ is reduced and

$$h^0(C, dD) = h^0(C, dD') + \left\lfloor d \cdot \frac{a}{b} \right\rfloor \quad \text{for all } d \in \mathbb{N}. \tag{1.17}$$

Then

(*a*) *$R(X, D)$ is generated over $R(X, D')$ by some elements $g_1, \ldots, g_n$ whose degrees $d_i = \deg(g_i)$ and pole orders $c_i = -\mathrm{ord}_P^{D'}(g_i)$ satisfy $c_i \leq c_{i+1} \leq a$ and $d_i \leq d_{i+1} \leq b$ for all i.*

(*b*) *Choose a monomial ordering $\prec$ on $\Bbbk[u = f_0, f_1, \ldots, f_m]$ such that*

$$\mathrm{ord}_u(f) < \mathrm{ord}_u(h) \Rightarrow f \prec h.$$

Equip $\Bbbk[f_0, \ldots, f_m]$ with the graded P-lexicographic order from [8, Definition 4.2] and equip $\Bbbk[g_1, \ldots, g_n] \otimes \Bbbk[f_0, \ldots, f_m]$ with the block order from [8, Definition 2.19]. Let I' denote the ideal of relations of

$$\Bbbk[f_0, \ldots, f_m] \to R(X, D')$$

and let I denote the ideal of relations of

$$\Bbbk[f_0, \ldots, f_m, g_1, \ldots, g_n] \to R(X, D).$$

Then

$$\mathrm{in}_\prec(I) = \mathrm{in}_\prec(I')\Bbbk[f_0, \ldots, f_m, g_1, \ldots, g_n] + \langle U_i : 1 \leq i \leq n \rangle + \langle V \rangle,$$

where $V = \{f_i g_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ and U_i is the set of monomials of the form $\prod_{j=1}^{i} g_j^{e_j}$ with $e_j \in \mathbb{N}_{\geq 0}$ such that

(a) $\sum_{j=1}^{i} e_j c_j \leq c_{i+1}$,

(b) there does not exist $(e'_1, \ldots, e'_i) \neq (e_1, \ldots, e_i)$ with all $e'_j \leq e_j$ and $\sum_{j=1}^{i} e'_j c_j \geq c_{i+1}$, and

(c) there does not exist some $r < i$ such that $\sum_{j=1}^{r} e_j c_j > c_{r+1}$.

(c) *Let $\tau = \max_i \deg f_i$. Then $R(X, D)$ is generated over $R(X, D')$ in degrees up to b, with I generated over I' in degrees up to $\max\{2b, b + \tau\}$.*

Remark. Note that the condition $h^0(C, D') \geq 1$ from the original statement of [8, Lemma 4.4] is automatic any for effective $\mathbb{Q}$-divisor D on a genus 1 curve C since we have $h^0(C, D) = \max\{\deg D, 1\}$. Also, for u we can take the usual u in the definition of the section ring.

Finally, as a corollary to Lemma 4.4(c) of [8], we obtain a bound on the generator and relation degrees for arbitrary effective $\mathbb{Q}$-divisors:

Theorem 1.6.2. *Let*

$$D = \sum_{i=1}^{n} \alpha^{(i)}(P^{(i)})$$

be an effective divisor on a genus 1 curve C, with the coefficients $\alpha^{(i)} = a^{(i)}/b^{(i)}$ in reduced form and the distinct points $P^{(i)}$ ordered so that

$$\alpha^{(1)} \geq \cdots \geq \alpha^{(n)}.$$

Then the section ring S_D is generated in degrees at most

$$B = \max\{3b^{(1)}, b^{(2)}, \ldots, b^{(n)}\},$$

with relations in degrees at most $2B$.

These bounds are achievable: see Examples 1.3.1 and 1.6.

Proof of Theorem 1.6.2. Now let

$$D = \sum_{i=1}^{n} \frac{a^{(i)}}{b^{(i)}}\big(P^{(i)}\big)$$

be an effective divisor, with $\alpha^{(1)} \geq \cdots \geq \alpha^{(n)}$. We prove that the section ring $R(X, D)$ is generated in degrees at most

$$B = \max\{3b^{(1)}, b^{(2)}, \ldots, b^{(n)}\},$$

with relations in degrees at most $2B$.

In the base case $n = 1$, we are claiming that the section ring $R(X, D)$ of a divisor $D = (a/b)P$ is generated in degrees at most $B = 3b$ with relations in degrees at most $6b$. The generator bound follows from Theorem 1.3.2, observing that the exceptional generator (c) has degree at most $\lceil 3b/a \rceil \leq 3b$. The relation bound is automatic for relations with quadratic leading terms. By Theorem 1.3.5, the only other minimal relation has leading term $f_0 f_3^2$ and degree $1 + 2d_3 \leq 3b < 6b$, completing the proof of the base case.

To prove the induction step, we must verify that the subdivisor

$$D' = \sum_{i=1}^{n-1} \frac{a^{(i)}}{b^{(i)}} \left(P^{(i)}\right)$$

and the point $P = P^{(n)}$ satisfy the hypotheses of Lemma 1.6.1. That P is not a basepoint of dD' is automatic for us, because either

- $dD' = 0$, and the constant $1 \in H^0(dD')$ has no basepoints, or
- $\deg dD' = 1$, and the constant $1 \in H^0(dD')$ has a basepoint $P_i \neq P$, or
- $\deg dD' \geq 2$, and the linear system $H^0(dD')$ is basepoint-free by Fact 1.3.

As to (1.17), the hypothesis $\alpha_1 \geq \cdots \geq \alpha_n$ ensures that $dD = 0$ exactly when $d < \lceil 1/\alpha_1 \rceil$. If this condition holds, then (1.17) reduces to $1 = 1 + 0$, which is true. Otherwise, (1.17) reduces to

$$\deg dD - 1 = (\deg dD' - 1) + \deg \left\lfloor d \cdot \frac{a}{b} \cdot P \right\rfloor,$$

which is also true. Thus Lemma 1.6.1 applies.

By induction, $R(X, D')$ is generated in degrees at most

$$B' = \max\{3b^{(1)}, b^{(2)}, \ldots, b^{(n-1)}\},$$

with relations in degrees at most $2B'$. Accordingly, $R(X, D)$ is generated over $R(X, D')$ in degrees at most $b^{(n)}$, so generated over $\Bbbk$ in degrees at most

$$\max\{B', b^{(n)}\} = B.$$

The relation ideal I is generated over its counterpart I' in degrees at most

$$\max\{2b^{(n)}, b^{(n)} + \tau\} \leq \max\{2b^{(n)}, b^{(n)} + B'\},$$

and since I' is generated in degrees at most $2B'$, the degrees of all relations are bounded by

$$\max\{2b^{(n)}, b^{(n)} + B', 2B'\} = 2B,$$

as desired. □

Chapter 2

The Canonical Ring of $\mathcal{A}_g$

2.1 Introduction, Background, and Setup

We will now investigate the canonical ring of $\mathcal{A}_g$, the moduli space of principally polarized abelian varieties of dimension g. The main application of this problem is to provide explicit generators and relations for rings of classical Siegel modular forms. Indeed, we have the following identification:

$$M(\Gamma_g) \cong \bigoplus_{d \geq 0} H^0(\mathcal{A}_g, K_{\mathcal{A}_g}),$$

where $K_{\mathcal{A}_g}$ is the canonical divisor of the corresponding space. Such rings have been described in the cases $g = 2$ and $g = 3$ by Igusa [7] and Tsuyumine [11], but they did not use geometric methods (for one, the notion of an algebraic stack had not been developed by the time of those publications). Rather the tools they used were analytic, and they worked more directly with modular forms.

In this chapter, we propose a geometric approach to the problem for g up through 6 (the last genera for which $\mathcal{A}_g$ is not of general type), and describe the progress made so far. This will build off of the work of Voight and Zureick-Brown [12] who solved the $g = 1$ case (and much more) by studying canonical rings of *stacky curves*.

We will focus mostly on the $g = 2$ case, but we expect the approach to generalize, making appropriate adjustments, to higher dimensions. What makes the $g = 2$ case special is that most abelian varieties of dimension 2 come from jacobians of curves, and this in turn allows us to identify the moduli space as a certain open subset of a weighted projective space. Because weighted projective spaces are toric varieties, we end up with a collection of combinatorial tools that allow us to compute log-canonical rings of a broader class of varieties. This will in turn enable us to generalize results of Landesman et. al. [8], who compute section rings of $\mathbb{Q}$-divisors of $\mathbb{P}^n$ and Hirzebruch surfaces.

2.1.1 Siegel Modular Forms

We compile some definitions and facts regarding Siegel modular forms.

Let $g \geq 1$ be an integer, and let $J := \left(\begin{smallmatrix} 0 & I_g \\ -I_g & 0 \end{smallmatrix}\right)$ We define the *symplectic group* to be

$$\Gamma_g := \mathrm{Sp}_{2g}(\mathbb{Z}) = \{\gamma \in_{2g} (\mathbb{Z}) \mid {}^t\gamma\, J\gamma = J\}$$

and the *Siegel upper half space* to be

$$\mathcal{H}_g := \{\tau \in \mathrm{Mat}_{g\times g}(\mathbb{C}) \mid {}^t\tau = \tau, \mathrm{Im}(\tau) > 0\}.$$

We can define a natural action of Γ_g on $\mathcal{H}_g$ via

$$\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)\tau := (A\tau + B)(C\tau + D)^{-1}.$$

When $g = 1$, this action is equivalent to the action of $\mathrm{SL}_2(\mathbb{Z})$ on the complex upper half plane via linear fractional transformation, as we would expect. The quotient space $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ is in bijective correspondence with elliptic curves over the complex numbers up to isomorphism. One would hope for a uniformization theorem for all

abelian varieties of higher dimension, but we don't get so lucky: A point $\tau \in \mathcal{H}_g$ determines a torus $\mathbb{C}^g/\mathbb{Z}^g + \mathbb{Z}^g\tau$, but we do not get all complex g-dimensional tori this way.

To rectify this, we recall

Lemma 2.1.1. *The following conditions on a complex torus $X = V/\Lambda$ are equivalent:*

1. *X admits an embedding into a complex projective space;*
2. *X is the complex manifold associated to an algebraic variety;*
3. *There is a positive definite Hermitian form H on V such that $\mathrm{Im}(H)$ takes integral values on $\Lambda \times \Lambda$.*

If a complex torus satisfies these requirements, it is called a complex *abelian variety*. It is further called *principally polarized* if the map $\mathrm{Im}(H) : \Lambda \times \Lambda \to \mathbb{Z}$ is unimodular.

We have a canonical bijection between the set of isomorphism classes of principally polarized abelian varieties of dimension g and the orbit space $\Gamma_g \setminus \mathcal{H}_g$. For details, see [1].

2.1.2 The $g = 2$ case

The moduli stack $\mathcal{A}_g$ can be conveniently described in terms of $\mathcal{M}_g$, the moduli stack of smooth curves of genus g, and its Deligne-Mumford compactification, $\overline{\mathcal{M}_g}$, which parametrizes stable curves of genus g. The boundary divisors of $\overline{\mathcal{M}_g}$ (respectively in M_g, the coarse space) are denoted

$$\delta_0, \ldots, \delta_{\lfloor g/2 \rfloor} \text{ (resp. } \Delta_0, \ldots \Delta_{\lfloor g/2 \rfloor}).$$

There is a natural morphism $Q : \overline{\mathcal{M}_g} \to \mathcal{M}_g$, which satisfies

$$Q * \Delta_i = \delta_i \ i \neq 1, \ Q^* \Delta_1 = 2\delta_1.$$

When $g = 2$, the boundary divisors are Δ_0 and Δ_1, which (generically) parametrize genus 1 curves with a node and two genus one curves intersecting, respectively.

We recall that a smooth genus two curve C has a sheaf of differentials ω_C that gives us the canonical morphism

$$j : C \to \mathbb{P}(H^0(C, \omega_C)) \cong \mathbb{P}^1$$

which is a finite map of degree two. By Riemann-Hurwitz, j is branched over 6 distinct points, and we can construct a binary sextic form vanishing at these six points, which is unique up to a scalar multiple. If we have, conversely, a binary sextic form F with distinct zeros $b_1, \ldots, b_6 \in \mathbb{P}^1$, we can construct a unique degree two cover of $\mathbb{P}^1$ that is branched over these points. Ultimately, this gives us a bijection

$$\{\text{Genus two curves up to isomorphism}\} \longleftrightarrow \{\text{Binary sextic forms with distinct zeros}\}/\operatorname{GL}_2 .$$

In order to construct $\mathcal{A}_2$, we must consider the following *Igusa invariants* [7]. These arise from looking at the natural action of GL_2 on a general binary sextic of the form

$$F = ax^6 + 6bx^5y + 15cx^4y^2 + 20dx^3y^3 + 15ex^2y^4 + 6fxy^5 + gy^6$$

given by

$$F \mapsto (M, F) := (\det M)^{-2} F(xm_{11} + ym_{21}, xm_{12} + ym_{22}),$$

where the m_{ij} are the entries of the two-by-two matrix M.

If $\zeta_i, \dots \zeta_6$ are the roots of our binary sextic form, we use the shorthand (ij) to denote $\zeta_i - \zeta_j$. The Igusa invariants are then given by

$$A = a^2 \sum_{\text{fifteen}} (12)^2(34)^2(56)^2$$

$$B = a^4 \sum_{\text{ten}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2$$

$$C = a^6 \sum_{\text{sixty}} (12)^2(23)^2(31)^2(45)^2)(56)^2(64)^2(14)^2(25)^2(36)^2$$

$$D = a^{10} \prod_{i,j} (ij)^2$$

$$E = a^{15} \prod_{\text{fifteen}} ((14)(36)(52) - (16)(32)(54))$$

If we define

$$X := \operatorname{Proj} R = \operatorname{Proj} k[A, B, C, D, E]/(E^2 - G(A, B, C, D)),$$

where G is a weighted homogeneous polynomial of degree 30 giving us a unique relation among the invariants $E^2 = G(A, B, C, D)$ (see [2]), then we have the following from work of Igusa.

Theorem 2.1.2 (Igusa)**.** *[7]*

1. $X \cong \operatorname{Proj} k[A, B, C, D] \cong \mathbb{P}(2, 4, 6, 10) \cong \mathbb{P}(1, 2, 3, 5)$.

2. *A binary sextic with a zero of multiplicity three, admitting a nonvanishing invariant of positive degree, is mapped to* $p := [1, 0, 0, 0, 0] \in X$.

Further, we have that the moduli scheme M_2 can be identified with $X \setminus \{D = 0\}$, where D is the discriminant. (See [5] for more details.)

The next step is to arrive at a nice description of $\mathcal{A}_2$, which involves blowing up the invariant-theory quotient described above. We recall that the Torelli morphism

$t : M_g \hookrightarrow A_g$ associates to each curve its Jacobian. Now for $g = 2$, we have from the above paragraph that M_2 is an open subset of X, and so we may extend it to a rational map

$$\tau : X \dashrightarrow \overline{A}_2.$$

From inclusion and the Torelli map, we get $M_2 \hookrightarrow \tilde{X} = \overline{\mathrm{Graph}(\tau)} \subset X \times \overline{A}_2$, and it follows that $\tilde{X}$ compactifies M_2. Further, from [7], we have that the indeterminacy of τ is the point $p = [1, 0, 0, 0, 0] \in X$ corresponding to binary sextic forms with a zero of multiplicity three, and that τ is resolved by a weighted blow-up centered at p

$$b : \tilde{X} \to X.$$

The exceptional divisor is mapped isomorphically to the locus of principally polarized abelian surfaces that decompose as a product of two elliptic curves. It then follows from the proof of Proposition 2.10 in [5] that we have an identification

$$A_2 \cong \overline{M}_2 \setminus \Delta_0.$$

We note that the right side can be identified with an open set of a blow-up of a weighted projective space. To get a description of the canonical divisor, we have a ramification formula due to Hassett in Proposition 3.5 of [5]:

$$K_{\mathcal{M}_2} + \alpha\delta \equiv Q^*(K_{\overline{M}_2} + \alpha\Delta_0 + \frac{1+\alpha}{2}\Delta_1 + \frac{1}{2}\Xi),$$

where Ξ is the closure of the space of smooth curves admitting a bielliptic involution.

Now, since A_2 can be interpreted in terms of a weighted projective space, we can use tools from toric geometry to complete the task of computing its canonical ring. In particular, what we have to do is

1. Determine how to interpret the open set $\overline{M}_2 \setminus \Delta_0$ as a toric variety.

2. Find a way to compute canonical rings of toric varieties with stack structure.

In either case, a necessary prerequisite is to compute the log canonical ring of $\mathbb{P}(1,2,3,5)$ (or for the broadest possible class of toric varieties). Luckily, we have some tools at our disposal.

For a toric variety X_Σ corresponding to a fan Σ and a divisor $D = \sum_\rho D_\rho$ (where D_ρ denotes the divisor corresponding to the ray ρ in the fan), we define the polyhedron

$$P_D = \{m \in M_\mathbb{R} \mid \langle m, u_\rho \rangle \geq -a_\rho \text{ for all rays } \rho\},$$

where u_ρ denotes a generator of ρ. From page 190 of [3], we have a convenient tool for computing global sections of the sheaf associated to a torus-invariant Weil divisor D on $X_\sum$:

$$H^0(X_\sum, D) = \bigoplus_{m \in P_D \cap \mathbb{Z}^n} \mathbb{C} \cdot \lambda^m,$$

and we further have that $P_{lD} = lP_D$.

We can use this to compute some examples of log-canonical rings of toric varieties. However, the stacky setting remains elusive.

Example 2.1.3. We shall compute log-canonical rings of $X := \mathbb{P}^1_k \times \mathbb{P}^1_k$ (with respect to bidegree) using the toric description. First note that we have an exact sequence given by

$$0 \to \mathbb{Z}^n \to \mathrm{Div}_{T_N}(X) \cong \bigoplus_\rho D_\rho \to \mathrm{Cl}(X) \to 0,$$

where the second map is given by $m \to \sum_\rho \langle x, u_\rho \rangle D_\rho$ (see [3] for details). Since a toric fan for X is given by $\langle (1,0), (-1,0), (0,1), (0,-1) \rangle$ in $\mathbb{R}^2$, it follows from the exact sequence that $\mathrm{Cl}(X) = \langle D_1, D_2 \rangle \cong \mathbb{Z}^2$. The canonical divisor of X is given by $K_X \sim -D_1 - D_2 - D_3 - D_4 \sim -2D_1 - 2D_2$. In degree 0, we get that the canonical

ring is k. For any divisor with non-negative bidegree, it follows from the definition of P_D that the canonical ring is a double Veronese-embedding. For instance, when the bidegree of D $(2,2)$, the log-canonical ring is (the homogenized version of)

$$R_D = k[x_1, x_2, y_1, y_2]/(x_2 - x_1^2, y_2 - y_1^2).$$

This is what we expect since the log-canonical ring of $\mathbb{P}^1$ is given by Veronese embeddings (one can see this from the toric description or from direct computations. This is worked out fully in [12]).

Chapter 3

Quartic Torsion

3.1 Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. The watershed 1978 paper by Mazur tells us what the possible torsion subgroups of $E(\mathbb{Q})$ are: $E(\mathbb{Q})_{tors}$ is isomorphic to one of $\mathbb{Z}/N\mathbb{Z}$ (for $1 \leq N \leq 10$ or $N = 12$) or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$ (for $1 \leq N \leq 4$). To do this, Mazur packaged elliptic curves along with torsion data into appropriate modular curves and studied those.

We let $Y_1(N)$ be the curve paramaterizing (E, P), where P is a point of exact order N on E, and let $Y_1(M, N)$ (with $M|N$) be the curve paramaterizing E/K such that $E(K)_{tors}$ contains the subgroup $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$. Both of these types of modular curves may be thought of as Riemann surfaces arising from smooth compactifications of quotients of the (extended) upper half plane $\mathcal{H}^* = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\} \cup \{\mathbb{Q}\} \cup \{i\infty\}$ by the congruence subgroups

$$\Gamma_1(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod{N}\}$$

and

$$\Gamma_1(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod{N}\ M|b\},$$

respectively, and where the *cusps* are the equivalent classes of $\{\mathbb{Q}\} \cup \{i\infty\}$ under the action of each group. Note that by setting $M = 1$, we get $X(1, N) = X(N)$.

We can then reinterpret Mazur's theorem as the statement that $X_1(M, N)(\mathbb{Q})$ has no non-cuspidal rational points for (M, N) outside of the set $\{(1, N)|1 \leq N \leq 10 \text{ or } N = 12\} \cup \{(2, 2N)|1 \leq N \leq 4\}$.

In the following decades, a full classification has been completed for elliptic curves over quadratic and cubic as well. In the 1980s, Kamienny-Kenku-Momose proved that if E be an elliptic curve over a quadratic number field K, then $E(K)_{tors}$ is one of the following groups:

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z}, &\qquad \text{for } 1 \leq N \leq 16 \text{ or } N = 18, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, &\text{ for } 1 \leq N \leq 6, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z}, &\text{ for } 1 \leq N \leq 2, \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. & \end{aligned}$$

In particular, the corresponding curves $X_1(M, N)$ all have $g \leq 2$, which guarantees that they have infinitely many quadratic points.

About a decade later, Merel proved that for every integer $d \geq 1$, there is a constant $N(d)$ such that for all $K/\mathbb{Q}$ of degree at most d and all E/K, $\#E(K)_{tors} \leq N(d)$. This invites us to consider the following task: Fix $d \geq 1$. Classify all groups which can occur as $E(K)_{tors}$ for K/Q of degree d. Which of these occur infinitely often?

The next case considered was $d = 3$, which was only completed in 2020 by Derickx–Etropolski–Morrow–van Hoeij–Zurieck-Brown [4], who proved that if $K/\mathbb{Q}$ is a cubic extension and E/K an elliptic curve, then $E(K)_{tors}$ is isomorphic to one of the fol-

lowing 26 groups:

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z} \qquad & \text{with } 1 \leq N \leq 21, N \neq 17, 19, \text{ and} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} \; & \text{with } 1 \leq N \leq 7. \end{aligned}$$

This case differs from the degree 1 and 2 cases in that there is a *sporadic point*, corresponding to the elliptic curve **162b1** over $\mathbb{Q}(\zeta_9)^+$ for $N = 21$. This is unusual, because $\mathbb{Z}/21\mathbb{Z}$ only occurs for *one* elliptic curve up to isomorphism (instead of infinitely many).

The next case is quartic torsion, which is the focus of the rest of this chapter. Previous work by Jeon–Kim–Park in 2006 tells us which torsion subgroups for elliptic curves over quartic fields occur for infinitely many elliptic curves up to isomorphism: If K varies over all quartic number fields and E varies over all elliptic curves over K, the group structures which appear infinitely often as $E(K)_{tors}$ are exactly the following:

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z} \qquad & \text{with } 1 \leq N \leq 24, N \neq 19, 23, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} \; & \text{with } 1 \leq N \leq 9, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z} \; & \text{with } 1 \leq N \leq 3, \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4N\mathbb{Z} \; & \text{with } 1 \leq N \leq 2, \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, & \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, & \end{aligned}$$

What we want to prove is that these are the *only* possible subgoups – that there is no sporadic quartic torsion.

3.2 Strategy

We wish to rule out non-cuspidal quartic points on all the modular curves $X(N)$, restricting to the cases where the Jacobian of the curve is rank zero.

For a curve X and an integer $d \geq 1$, we define the d^{th}-symmetric power of X to be $X^{(d)} := X^d/S_d$, where S_d is the symnmetric group on d letters. The K-points of $X^{(d)}$ correspond to effective K-rational divisors on X of degree d. And a point of degree d gives rise to a divisor of degree d, which can be thought of as a point in $X^{(d)}(K)$.

If $X^{(d)}(K)$ is non-empty, then a fixed K-rational divisor E of degree d gives rise to an Abel-Jacobi map

$$f_{d,E} : X^{(d)} \to J_X,\ D \mapsto D - E.$$

By the Mordell-Weil theorem for abelian varieties, we know that $J_X(K)$ is a finitely-generated abelian group, and so

$$J(K) \cong \mathbb{Z}^r \oplus J(K)_{\text{tors}},$$

where $J(K)_{\text{tors}}$ is a finite group called the *torsion subgroup* of $J(K)$. We say that a point $P \in X(K)$ is a *torsion point* if $f_{d,E}(P) \in J(K)_{\text{tors}}$. In what follows, we focus on cases where the rank $r = 0$.

3.2.1 Direct Analysis

When $X(N)$ has gonality at least 5 and the rank of $J_1(N)$ is zero, we can compute the finitely many preimages of the Abel-Jacobi map $\iota : X_1(N)^{(4)}(\mathbb{Q}) \to J_1(N)(\mathbb{Q})$. If the size of the Jacobian is relatively small and the genus of $X_1(\mathbb{Q})$ is small (usually less than 10) then it might be computationally feasible to work directly over $\mathbb{Q}$. Otherwise, we can reduce by a prime of good reduction and work over a finite field.

Either way, we fix a base point $\infty \in X_1(N)(\mathbb{Q})$ and note that a divisor $D \in J_1(N)(\mathbb{Q})$ is in the image of the Abel-Jacobi map $E \mapsto E - 4\infty$ if and only if the linear system $|D = 4\infty| \neq \emptyset$, which can be computed in Magma. If $|D + 4\infty| = \emptyset$, we move on; otherwise, it will contain a single effective divisor E of degree 4. As we let D range over $J_1(N)(\mathbb{Q})$, we compute all effective degree 4 divisors in this way, and therefore we will have computed the entire image of Abel-Jacobi. Since this analysis over $\mathbb{Q}$ can be computationally slow, we can sometimes reduce by an appropriate prime to speed up the process. Consider the diagram

$$\begin{array}{ccc} X^{(4)}(\mathbb{Q}) & \xhookrightarrow{\iota} & J_X(\mathbb{Q}) \\ \big\downarrow{\scriptstyle \mathrm{red}_X} & & \big\downarrow{\scriptstyle \mathrm{red}_J} \\ X^{(4)}(\mathbb{F}_p) & \xhookrightarrow{\iota_p} & J_X(\mathbb{F}_p) \end{array}$$

This is commutative, and the injectivity of the maps holds if we assume that X has gonality at least 5. Thus the image of ι_p contains the reduction of the image of ι, and so the strategy is to

1. compute the image of ι_p,
2. compute the preimage of $\operatorname{im} \iota_p$,
3. compute the elements of $\mathrm{red}_J^{-1}(\mathrm{im}(\iota_p))$.

So far, using this strategy as is has ruled out the existence of non-cuspidal torsion points on $X_1(26)$. This curve has genus 10 with torsion subgroup $\mathbb{Z}/133\mathbb{Z} \times \mathbb{Z}/1995\mathbb{Z}$. There are 12 rational cusps and zero quadratic, cubic, or quartic cusps, and we use reduction mod 3.

We note that when the genus of $X_1(N)$ and the size of $J_1(N)$ are large, direct analysis is not computationally feasible, even with reduction. In these cases, we use the strategy of mapping to a quotient curve. In these cases, we attempt to map to a quotient before attempting direct analysis ($N = 25$ and $N = 28$ work this way).

Level	$X_1(N)$ Genus	X_H Curve Genus	X_H Gonality ≥ 5	Method	Level	$X_1(N)$ Genus	X_H Curve Genus	X_H Gonality ≥ 5	Method
25	12	12	Y	Direct analysis on a quotient	62	91	7	N	
26	13	13	Y	Direct Analysis on $X_1(26)$	64	93	13	Y	
27	10	13			66	81	9	N	
28	10	10	Y	Direct analysis on a quotient	68	105	13		
30	9	9			69	133	13		
31	26	6	N		70	97	9	N	
32	17	17			72	97	9	Y	
33	21	11	Y		75	145	9	N	
34	21	9	Y		76	136	8	Y	
35	25	9	Y		78	121	11	N	Maps to a previous case
36	17	17	N		81	190	10	Y	
38	28	10	Y		84	133	21		
39	33	9	Y		87	225	9	N	
40	25	9	Y		90	153	11	Y	
42	25	9	Y		94	231	11	N	
44	36	8	Y		96	193	17		
45	41	9	Y		98	235	7	N	
46	45	45			100	231	7	N	
48	37	13			108	250	10	Y	
49	69	19			110	281	15		
50	48	22			119	481	11	N	
51	65	9	Y		120	289	73		
52	55	9	Y	Maps to a previous case	132	381	39		
54	52	17			140	457	39		
55	81	9	N		150	489	19		
56	61	9	Y		168	625	97		
60	57	15			180	705	53		

Noting that quartic torsion points do not exist of prime order $p > 17$, the remaining values of N that we need to rule out are $\{26, 27, 29, 30, 31, 32, 33, 34, 35, 36, 38, 39, 40, 42, 44, 45, 46, 48, 49, 50, 51, 52, 54, 62, 64, 66, 68, 69, 70, 72, 75, 76, 78, 81, 84, 87, 90, 94, 96, 98, 100, 108, 110, 119, 120, 132, 140\}$. See the above table for the remaining cases, the gonality and genera of the corresponding modular curves, and methods used so far.

Chapter 4

Weil polynomials of abelian varieties over finite fields

4.1 Introduction

Let A be an abelian variety of dimension g over a finite field $\mathbb{F}_q$, where $q = p^n$ is a prime power. Let $T_\ell(A)$ be the ℓ-adic Tate module of A and $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. For $\ell \neq p$, we define the characteristic polynomial of the Frobenius endomorphism Frob_A of A as

$$\chi_A(t) = \det(\mathrm{Frob}_A - tI \mid V_\ell(A)),$$

which is a monic polynomial of degree $2g$ with integer coefficients independent of the choice of the prime ℓ. Moreover, $\chi_A(t)$ can be written as

$$\chi_A(t) = t^{2g} + a_1 t^{2g-1} + a_g t^g + q a_{n-1} t^{g-1} + \cdots + q^{g-1} a_1 t + q^g$$

and its set of roots has the form $\{\omega_1, \cdots, \omega_g, \omega_1, \cdots, \omega_g\}$, where ω_i is *q-Weil number* for $i \in \{1, \ldots g\}$. We recall that a *q-Weil number* ω is an algebraic integer such that $|\sigma(\omega)| = \sqrt{q}$ for any embedding $\sigma : \mathbb{Q}(\omega) \to \mathbb{C}$. Moreover, a *q-Weil polynomial* is a

monic integer polynomial whose roots are q-Weil numbers. Thus the characteristic polynomial of Frobenius, $\chi_A(t)$ is a Weil polynomial.

A standard result in the field due to Tate asserts that the characteristic polynomial is an isogeny invariant. More precisely, given two abelian varieties A and B defined over $\mathbb{F}_q$, Tate's Theorem says that A is $\mathbb{F}_q$-isogenous to B if and only if $\chi_A(t) = \chi_B(t)$. Any abelian variety can be decomposed into simple abelian varieties and the characteristic polynomial is compatible with this decomposition. To see this, let A be an abelian variety defined over $\mathbb{F}_q$. It is well known that A is isogenous to the product

$$A \sim A_1^{r_1} \times \ldots \times A_m^{r_m},$$

where each A_i is a simple abelian variety over $\mathbb{F}_q$ such that $A_i \not\sim A_j$ for $i \neq j$, and $r_i \geq 1$ is an integer. If χ_{A_i} is the characteristic polynomial of the Frobenius endomorphism of A_i, we have that

$$\chi_A(t) = \chi_{A_1}(t)^{r_1} \ldots \chi_{A_m}(t)^{r_m}.$$

Therefore understanding $\chi_A(t)$ for abelian varieties A over finite fields of dimension g reduces to understanding $\chi_A(t)$ of simple abelian varieties A of $\dim(A) \leq g$. An essential property of $\chi_A(t)$ for $\mathbb{F}_q$-simple abelian varieties A over $\mathbb{F}_q$ is that

$$\chi_A(t) = m_A(t)^e$$

where $m_A(t)$ is an irreducible polynomial and $e \geq 1$ an integer. We call e *the multiplicity* of A and we note that $e \mid 2\dim(A)$. We want to know under what conditions a given Weil polynomial of degree $2g$ occurs as the characteristic polynomial of Frobenius for a simple abelian variety of dimension g over a given finite field, and we answer this question for $g = 7$.

4.2 Answer for $g = 7$

In this subsection, we answer the above question for $g = 7$.

In this section we let A be a simple abelian variety of dimension g over $\mathbb{F}_q$ with $q = p^n$, for a prime p and integer $n \geq 1$. We denote by Frob_A the q-th power Frobenius endomorphism of A and $\chi_A(t)$ the characteristic polynomial of Frob_A as viewed inside $V_l(A)$, for an $l \neq p$ as described in the previous section. We recall that

$$\chi_A(t) = m_A(t)^e, \tag{4.1}$$

where $m_A(t)$ is an irreducible polynomial, and $e \geq 1$ an integer called the multiplicity of A. From this equality, it follows that $e|2\dim(A)$. As discussed in the introduction, it is always the case that $\chi_A(t)$ is a Weil polynomial. However the converse is not always true. In the following theorem, we next answer the question of when the converse holds in the case of $g = 7$.

Theorem 4.2.1. *Let $f(t) = t^{14}+a_1t^{13}+a_2t^{12}+\ldots+a_2q^5t^2+a_1q^6t+q^7$ be an irreducible Weil polynomial. Then the polynomial $f(t)$ is the characteristic polynomial of a simple abelian variety of dimension 7 over $\mathbb{F}_q$ if and only if one of the following conditions holds:*

1. *$v_p(a_1) \geq \frac{1}{2}n, v_p(a_2) \geq n, v_p(a_3) \geq \frac{3}{2}n, v_p(a_4) \geq 2n, v_p(a_5) \geq \frac{5}{2}n, v_p(a_6) \geq 3n, v_p(a_7) \geq \frac{7}{2}n$ and $f(t)$ has no root of valuation $\frac{1}{2}n$ nor irreducible factors of degree 3 or 5 or 7 in $\mathbb{Q}_p[t]$.*

2. *$v_p(a_1) = 0, v_p(a_2) \geq \frac{1}{2}n, v_p(a_3) \geq n, v_p(a_4) \geq \frac{3}{2}n, v_p(a_5) \geq 2n, v_p(a_6) \geq \frac{5}{2}n, v_p(a_7) \geq 3n$ and $f(t)$ has no root of valuation $\frac{1}{2}n$ nor irreducible factors of degree 3 or 5 in $\mathbb{Q}_p[t]$.*

3. *$v_p(a_1) = 0, v_p(a_2) \geq \frac{1}{3}n, v_p(a_3) \geq \frac{2}{3}n, v_p(a_5) \geq \frac{3}{2}n, v_p(a_4) = n, v_p(a_6) \geq 2n, v_p(a_7) \geq \frac{5}{2}n$ and $f(t)$ has no root of valuation $\frac{1}{3}n, \frac{1}{2}n$ or $\frac{2}{3}n$ and has exactly 2 degree 3 irreducible factors in $\mathbb{Q}_p[t]$.*

4. $v_p(a_1) = 0, v_p(a_2) \geq \frac{1}{4}n, v_p(a_3) \geq \frac{1}{2}n, v_p(a_4) \geq \frac{3}{4}n, v_p(a_5) = n, v_p(a_6) \geq \frac{3}{2}n, v_p(a_7) \geq 2n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{4}n, \frac{1}{2}n$ *or* $\frac{3}{4}n$ *and has at most* 2 *degree* 2 *irreducible factors in* $\mathbb{Q}_p[t]$.

5. $v_p(a_1) = 0, v_p(a_2) \geq \frac{2}{5}n, v_p(a_3) \geq \frac{4}{5}n, v_p(a_4) \geq \frac{6}{5}n, v_p(a_5) \geq \frac{8}{5}n, v_p(a_6) = 2n, v_p(a_7) \geq \frac{5}{2}n$ *and* $f(t)$ *has no root of valuation* $\frac{2}{5}n, \frac{1}{2}n$ *or* $\frac{3}{5}n$ *nor degree* 3 *irreducible factors in* $\mathbb{Q}_p[t]$.

6. $v_p(a_1) = 0, v_p(a_2) \geq \frac{1}{5}n, v_p(a_3) \geq \frac{2}{5}n, v_p(a_4) \geq \frac{3}{5}n, v_p(a_5) \geq \frac{4}{5}n, v_p(a_6) = n, v_p(a_7) \geq \frac{3}{2}n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{5}n, \frac{1}{2}n$ *or* $\frac{4}{5}n$ *nor degree* 3 *irreducible factors in* $\mathbb{Q}_p[t]$.

7. $v_p(a_1) = 0, v_p(a_2) \geq \frac{1}{3}n, v_p(a_3) \geq \frac{2}{3}n, v_p(a_4) \geq n, v_p(a_5) \geq \frac{4}{3}n, v_p(a_6) \geq \frac{5}{3}n, v_p(a_7) = 2n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{3}n$ *or* $\frac{2}{3}n$ *nor degree* 2 *irreducible factors in* $\mathbb{Q}_p[t]$.

8. $v_p(a_1) = 0, v_p(a_2) \geq \frac{1}{6}n, v_p(a_3) \geq \frac{1}{3}n, v_p(a_4) \geq \frac{1}{2}n, v_p(a_5) \geq \frac{2}{3}n, v_p(a_6) \geq \frac{5}{6}n, v_p(a_7) = n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{6}n$ *or* $\frac{5}{6}n$ *nor irreducible factors of degree* 2 *or* 3 *in* $\mathbb{Q}_p[t]$.

9. $v_p(a_1) \geq 0, v_p(a_2) = 0, v_p(a_3) \geq n/2, v_p(a_4) \geq n, v_p(a_5) \geq 3n/2, vp(a_6) \geq 2n, v_p(a_7) \geq 5n/2$ *and* $f(t)$ *has no root of valuation*$\frac{1}{2}n$ *nor irreducible factors of degree* 3 *or* 5 *in* $\mathbb{Q}_p[t]$.

10. $v_p(a_1) \geq 0, v_p(a_2) = 0, v_p(a_3) \geq n/3, v_p(a_4) \geq 2n/3, v_p(a_5) \geq n, v_p(a_6) \geq 3n/2, v_p(a_7) \geq 2n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{2}n, \frac{1}{3}n, \frac{2}{3}n$*over* $\mathbb{Q}_p[t]$.

11. $v_p(a_1) \geq 0, v_p(a_2) = 0, v_p(a_3) \geq n/4, v_p(a_4) \geq n/2, v_p(a_5) \geq 3n/4, v_p(a_6) \geq n, v_p(a_7) \geq 5n/4$ *and* $f(t)$ *has no root of valuation*$\frac{1}{2}n, \frac{3}{4}n, \frac{1}{4}n$ *and we cannot have more than 3 irreducible factors of degree 2.*

12. $v_p(a_1) \geq 0, v_p(a_2) = 0, v_p(a_3) \geq \frac{1}{5}n, v_p(a_4) \geq \frac{2}{5}n, v_p(a_5) \geq \frac{3}{5}n, v_p(a_6) \geq \frac{4}{5}n, v_p(a_7) = n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{5}n$ *or* $\frac{4}{5}n$ *and has no irreducible factors of degree*

3 in $\mathbb{Q}_p[t]$.

13. $v_p(a_1) \geq 0, v_p(a_2) = 0, v_p(a_3) \geq \frac{2}{5}n, v_p(a_4) \geq \frac{4}{5}n, v_p(a_5) \geq \frac{6}{5}n, v_p(a_6) \geq \frac{8}{5}n, v_p(a_7) = 2n$ *and* $f(t)$ *has no root of valuation* $\frac{2}{5}n$ *or* $\frac{3}{5}n$ *and has no irreducible factors of degree 3 in* $\mathbb{Q}_p[t]$.

14. $v_p(a_1) \geq 0, v_p(a_2) \geq 0, v_p(a_3) = 0, v_p(a_4) \geq \frac{1}{2}n, v_p(a_5) \geq n, v_p(a_6) \geq \frac{3}{2}n, v_p(a_7) \geq 2n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{2}n$ *nor irreducible factors of degree* 3 *in* $\mathbb{Q}_p[t]$.

15. $v_p(a_1) \geq 0, v_p(a_2) \geq 0, v_p(a_3) = 0, v_p(a_4) \geq \frac{1}{3}n, v_p(a_5) \geq \frac{2}{3}n, v_p(a_6) = n, v_p(a_7) \geq \frac{3}{2}n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{3}n$, $\frac{1}{2}n$ *or* $\frac{2}{3}n$ *in* $\mathbb{Q}_p[t]$.

16. $v_p(a_1) \geq 0, v_p(a_2) \geq 0, v_p(a_3) = 0, v_p(a_4) \geq \frac{1}{4}n, v_p(a_5) \geq \frac{1}{2}n, v_p(a_6) \geq \frac{3}{4}n, v_p(a_7) = n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{4}n$ *or* $\frac{3}{4}n$ *and has at most* 2 *irreducible factors of degree* 2 *in* $\mathbb{Q}_p[t]$.

17. $v_p(a_1) \geq \frac{1}{3}n, v_p(a_2) \geq \frac{2}{3}n, v_p(a_3) = 0, v_p(a_4) \geq \frac{3}{2}n, v_p(a_5) \geq 2n, v_p(a_6) \geq \frac{5}{2}n, v_p(a_7) \geq 3n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{3}n$, $\frac{1}{2}n$ *or* $\frac{2}{3}n$ *and has at most* 2 *irreducible factors of degree* 3 *in* $\mathbb{Q}_p[t]$.

18. $v_p(a_1) \geq \frac{1}{4}n, v_p(a_2) \geq \frac{1}{2}n, v_p(a_3) \geq \frac{3}{4}n, v_p(a_4) = n, v_p(a_5) \geq \frac{3}{2}n, v_p(a_6) \geq 2n, v_p(a_7) \geq \frac{5}{2}n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{4}n, \frac{1}{2}n$ *or* $\frac{3}{4}n$ *and has no irreducible factors of degree* 3 *and* $f(t)$ *has at most* 3 *irreducible factors of degree 2 in* $\mathbb{Q}_p[t]$.

19. $v_p(a_1) \geq \frac{1}{4}n, , v_p(a_2) \geq \frac{1}{2}n, , v_p(a_3) \geq \frac{3}{4}n, , v_p(a_4) = nv_p(a_5) \geq \frac{4}{3}n, v_p(a_6) \geq \frac{5}{3}n, v_p(a_7) = 2n$ *and* $f(t)$ *has no root of valuation* $\frac{3}{4}n, \frac{2}{3}n, \frac{1}{3}n, \frac{1}{4}n$ *in* $\mathbb{Q}_p$, *nor a factor of degree 2 in* $\mathbb{Q}_p[t]$.

20. $v_p(a_1) \geq 0, , v_p(a_2) \geq 0, , v_p(a_3) \geq 0, v_p(a_4) = 0, v_p(a_5) \geq \frac{1}{2}n, , v_p(a_6) \geq n, , v_p(a_7) \geq \frac{3}{2}n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{2}n$ *in* $\mathbb{Q}_p$, *nor a factor of degree 3 in* $\mathbb{Q}_p[t]$.

21. $v_p(a_1) \geq 0, \quad v_p(a_2) \geq 0, \quad v_p(a_3) \geq 0, \quad v_p(a_4) = 0, v_p(a_5) \geq \frac{1}{3}n, v_p(a_6) \geq \frac{2}{5}n, v_p(a_7) = n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{3}n, \frac{2}{3}n$ *in* $\mathbb{Q}_p$.

22. $v_p(a_1) \geq 0, v_p(a_2) \geq 0, v_p(a_3) \geq 0, v_p(a_4) \geq 0, v_p(a_5) \geq 0, v_p(a_6) \geq \frac{1}{2}n, v_p(a_7) \geq n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{2}n$ *in* $\mathbb{Q}_p[t]$.

23. $v_p(a_1) \geq \frac{1}{5}n, v_p(a_2) \geq \frac{2}{5}n, v_p(a_3) \geq \frac{3}{5}n, v_p(a_4) \geq \frac{4}{5}n, v_p(a_5) \geq 0, v_p(a_6) \geq \frac{3}{2}n, v_p(a_7) \geq 2n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{5}n$, $\frac{1}{2}n$ *or* $\frac{4}{5}n$ *nor degree* 3 *irreducible factors in* $\mathbb{Q}_p[t]$.

24. $v_p(a_1) \geq \frac{2}{5}n, v_p(a_2) \geq \frac{4}{5}n, v_p(a_3) \geq \frac{6}{5}n, v_p(a_4) \geq \frac{8}{5}n, v_p(a_5) \geq 0, v_p(a_6) \geq \frac{5}{2}n, v_p(a_7) \geq 3n$ *and* $f(t)$ *has no root of valuation* $\frac{2}{5}n$, $\frac{1}{2}n$ *or* $\frac{3}{5}n$ *nor degree* 3 *irreducible factors in* $\mathbb{Q}_p[t]$.

25. $v_p(a_1) \geq 0, v_p(a_2) \geq 0, v_p(a_3) \geq 0, v_p(a_4) \geq 0, v_p(a_5) \geq 0, v_p(a_6) \geq 0, v_p(a_7) \geq \frac{1}{2}n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{2}n$ *in* $\mathbb{Q}_p[t]$.

26. $v_p(a_1) \geq \frac{1}{6}n, v_p(a_2) \geq \frac{1}{3}n, v_p(a_3) \geq \frac{1}{2}n, v_p(a_4) \geq \frac{2}{3}n, v_p(a_5) \geq \frac{5}{6}n, v_p(a_6) \geq 0, v_p(a_7) \geq \frac{3}{2}n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{6}n, \frac{1}{2}n$ *or* $\frac{5}{6}n$ *nor irreducible factors of degree* 3 *and* $f(t)$ *has exactly* 1 *irreducible factor of degree 2 in* $\mathbb{Q}_p[t]$.

27. $v_p(a_1) \geq \frac{1}{3}n, v_p(a_2) \geq \frac{2}{3}n, v_p(a_3) \geq n, v_p(a_4) \geq \frac{4}{3}n, v_p(a_5) \geq \frac{5}{3}n, v_p(a_6) \geq 0, v_p(a_7) \geq \frac{5}{2}n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{3}n, \frac{1}{2}n$ *or* $\frac{2}{3}n$ *and has exactly* 1 *irreducible factor of degree 2 in* $\mathbb{Q}_p[t]$.

28. $v_p(a_1) \geq 0, v_p(a_2) \geq 0, v_p(a_3) \geq 0, v_p(a_4) \geq 0, v_p(a_5) \geq 0, v_p(a_6) \geq 0, v_p(a_7) \geq \frac{1}{2}n$.

29. $v_p(a_1) \geq \frac{1}{7}n, v_p(a_2) \geq \frac{2}{7}n, v_p(a_3) \geq \frac{3}{7}n, v_p(a_4) \geq \frac{4}{7}n, v_p(a_5) \geq \frac{5}{7}n, v_p(a_6) \geq \frac{6}{7}n, v_p(a_7) \geq \frac{3}{2}n$ *and* $f(t)$ *has no root of valuation* $\frac{1}{7}n$ *or* $\frac{6}{7}n$ *nor irreducible factors of degree* 2 *and* 3.

30. $v_p(a_1) \geq \frac{2}{7}n, v_p(a_2) \geq \frac{4}{7}n, v_p(a_3) \geq \frac{6}{7}n, v_p(a_4) \geq \frac{8}{7}n, v_p(a_5) \geq \frac{10}{7}n, v_p(a_6) \geq \frac{12}{7}n, v_p(a_7) \geq \frac{5}{2}n$ *and* $f(t)$ *has no root of valuation* $\frac{2}{7}n$ *or* $\frac{5}{7}n$ *nor irreducible factors of degree* 2 *and* 3.

31. $v_p(a_1) \geq \frac{3}{7}n, v_p(a_2) \geq \frac{6}{7}n, v_p(a_3) \geq \frac{9}{7}n, v_p(a_4) \geq \frac{12}{7}n, v_p(a_5) \geq \frac{15}{7}n, v_p(a_6) \geq \frac{18}{7}n, v_p(a_7) \geq \frac{5}{2}n$ *and* $f(t)$ *has no root of valuation* $\frac{3}{7}n$ *or* $\frac{4}{7}n$ *nor irreducible factors of degree* 2 *and* 3.

We collect a few theoretical results from Hayashisa's [6] which we will use to prove the theorem.

Lemma 4.2.2. *Let* A *be a simple abelian variety over* $\mathbb{F}_q$ *with* $q = p^n$ *elements and* $\chi_A(t)$ *the characteristic polynomial of Frob*$_A$*. Suppose that* $\chi_A(t)$ *has a real root. Then we have*

- *if* n *is even, then* $\dim(A) = 1$,
- *if* n *is odd, then* $\dim(A) = 1$.

Proof. This is Lemma 2.4. in [6]. □

Corollary 4.2.3. *Suppose that the dimension of* A *is a prime number* $l \geq 3$*. Then* $e = 1$ *or* $e = l$*.*

Proof. Since e divides $2l$ and l is a prime, we have either $e \in \{1, 2, l, 2l\}$. Suppose $e = 2$ or $e = 2l$. Then $m_A(t)$ is an irreducible polynomial of odd degree. Hence the polynomial $m_A(t)$ has a real root. This contradicts $l \geq 3$ by Lemma 4.2.2. □

We note that $e = l$ is covered in the following theorem. So we are left with studying $e = 1$, i.e. the irreducible case.

Theorem 4.2.4. *Let* $a, b \in Z$ *and* $2 < g \in Z$*. Set* $f(t) = (t^2 + at + b)^g \in Z[t]$*. Then the polynomial* $f(t)$ *is the characteristic polynomial of a simple abelian variety of*

dimension g over $\mathbb{F}_q$ with $q = p^n$ elements if and only if g divides n, $b = q$, $|a| < 2\sqrt{q}$ and $a = kq^{s/g}$, where k, s are integers satisfying $\gcd(k, p) = 1, \gcd(s, g) = 1$ and $1 \leq s < g/2$.

Proof. This is Theorem 1.2. in [6]. □

Theorem 4.2.5. *An irreducible Weil polynomial $f(t)$ of degree $2g$ is the characteristic polynomial of a simple abelian variety of dimension g over $\mathbb{F}_q$ (i.e. $e = 1$) if and only if $f(t)$ has no real root and the following condition holds*

$$\frac{v_p(f_i(0))}{n} \in \mathbb{Z}, \text{ for all } f_i \text{ monic irreducible factors of } f(t) \in \mathbb{Q}_p[t]. \tag{4.2}$$

Proof. This is Corollary 3.2. in [6]. □

We next prove Theorem 4.2.1

Proof. Following Hayashida's proof of [6, Theorem 1.3.] we let $f(t)$ be an irreducible Weil polynomial of degree 14. It is the characteristic polynomial of a simple abelian variety A of dimension 7 over $\mathbb{F}_q$ if and only if the conditions in Theorem 4.2.5 hold. First, note that if $f(t)$ had a real root that came from a simple abelian variety A, then Lemma 4.2.2 gives that $\dim(A)$ is 1 or 2, a contradiction. To check the second condition, we employ Newton Polygons. Let $\mathcal{NP}(f)$ be the Newton Polygon of f. Then $\mathcal{NP}(f)$ has 14 possible vertices

$$(0, 7n), (1, 6n+v_p(a_1)), (2, 5n+v_p(a_2)), (3, 4n+v_p(a_3)), (4, 3n+v_p(a_4)), (5, 2n+v_p(a_5)),$$

$$(6, n + v_p(a_6)), (7, v_p(a_7)), (8, v_p(a_6)), (9, v_p(a_5)), (10, v_p(a_4)), (11, v_p(a_3)), (12, v_p(a_2)),$$

$$(13, v_p(a_1)), (14, 0).$$

These give rise to 31 possible Newton Polygons, sandwiched between the two boundary cases of an ordinary simple abelian variety and a supersingular one. Hayashida

notes that if one of these points is a vertex, then the point must be a lattice point belonging to $\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$. By symmetry of $\mathcal{NP}(f)$, it is sufficient to classify cases according to whether either of $(0,7n),(1,6n+v_p(a_1)),(2,5n+v_p(a_2)),(3,4n+v_p(a_3)),(4,3n+v_p(a_4)),(5,2n+v_p(a_5)),(6,n+v_p(a_6)),(7,v_p(a_7))$, is a vertex of not. The rest of the proof consists in describing these cases.

Case 0: Assume there is no vertex. This is the ordinary case. Then

$$\begin{cases} 6n+v_p(a_1)\geq \frac{13}{2}n \\ 5n+v_p(a_2)\geq 6n \\ 4n+v_p(a_3)\geq \frac{11}{2}n \\ 3n+v_p(a_4)\geq 5n \\ 2n+v_p(a_5)\geq \frac{9}{2}n \\ n+v_p(a_6)\geq 4n \\ v_p(a_7)\geq \frac{7}{2}n \end{cases} \Rightarrow \begin{cases} v_p(a_1)\geq \frac{1}{2}n \\ v_p(a_2)\geq n \\ v_p(a_3)\geq \frac{3}{2}n \\ v_p(a_4)\geq 2n \\ v_p(a_5)\geq \frac{5}{2}n \\ v_p(a_6)\geq 3n \\ v_p(a_7)\geq \frac{7}{2}n \end{cases}.$$

In this case, we have

$$(t-\alpha_1)\cdots(t-\alpha_{14})\in\mathbb{Q}_p[t]$$

with

$$v_p(\alpha_1)=\cdots=v_p(\alpha_{14})=\frac{1}{2}n.$$

Thus Theorem 4.2.5 holds if and only if

$f(t)$ has no root of valuation $\frac{1}{2}n$ nor irreducible factors of degree 3 or 5 or 7 in $\mathbb{Q}_p[t]$.

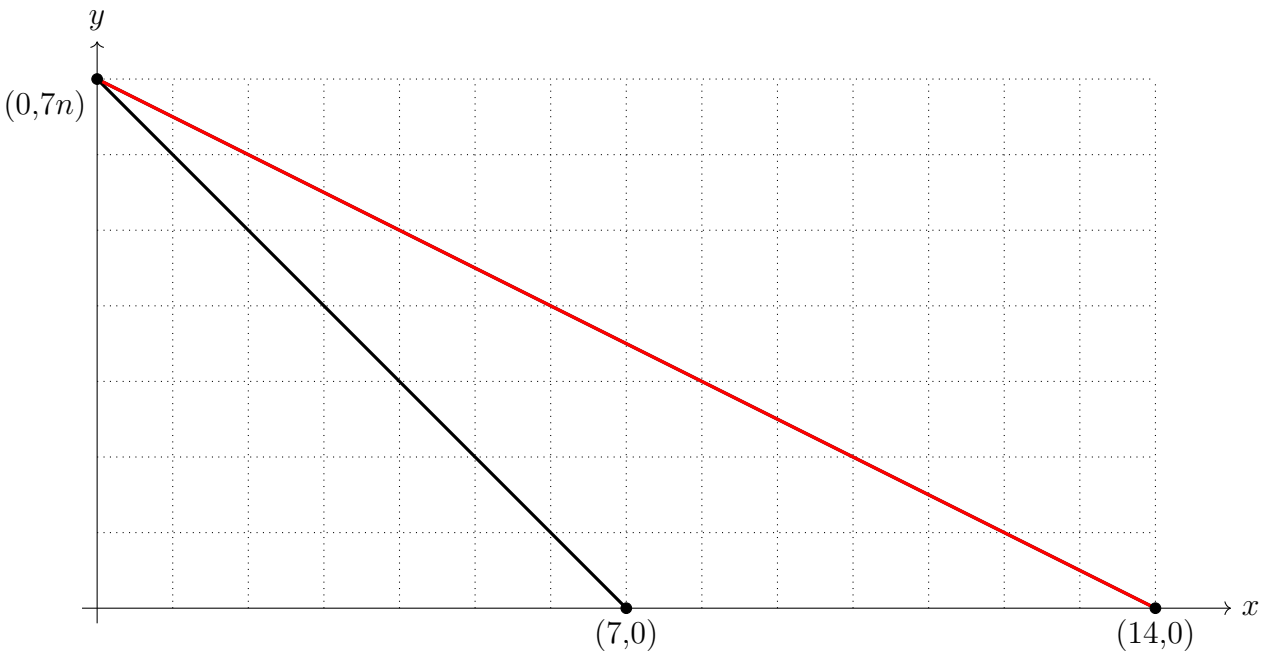

Figure 4.1: The Newton polygon for case 0.

Case 1: Assume the first vertex is $(1, 6n+v_p(a_1))$. In this case the only possibility is $(1, 6n + v_p(a_1)) = (1, 6n)$ and $v_p(a_1) = 0$.

(1-1) $(1, 6n + v_p(a_1)) = (1, 6n)$ is the sole vertex. Then

$$\begin{cases} 5n + v_p(a_2) \geq \frac{11}{2}n \\ 4n + v_p(a_3) \geq 5n \\ 3n + v_p(a_4) \geq \frac{9}{2}n \\ 2n + v_p(a_5) \geq 4n \\ n + v_p(a_6) \geq \frac{7}{2}n \\ v_p(a_7) \geq 3n \end{cases} \Rightarrow \begin{cases} v_p(a_2) \geq \frac{1}{2}n \\ v_p(a_3) \geq n \\ v_p(a_4) \geq \frac{3}{2}n \\ v_p(a_5) \geq 2n \\ v_p(a_6) \geq \frac{5}{2}n \\ v_p(a_7) \geq 3n \end{cases}.$$

In this case, we have

$$t-\alpha_1, (t-\alpha_2)\cdots(t-\alpha_{13}), t-\alpha_{14} \in \mathbb{Q}_p[t]$$

with

$$\begin{aligned} v_p(\alpha_1) &= n, \\ v_p(\alpha_2) &= \cdots = v_p(\alpha_{13}) = \frac{1}{2}n, \\ v_p(\alpha_{14}) &= 0. \end{aligned}$$

Thus Theorem 4.2.5 holds if and only if

$f(t)$ has no root of valuation $\dfrac{1}{2}n$ nor irreducible factors of degree 3 or 5 in $\mathbb{Q}_p[t]$.

(1-2) $(1, 6n + v_p(a_1)) = (1, 6n)$ and $(4, 3n + v_p(a_4)) = (4, 4n)$ are vertices. Then $v_p(a_4) = n$ and

$$\begin{cases} 5n + v_p(a_2) \geq \frac{16}{3}n \\ 4n + v_p(a_3) \geq \frac{14}{3}n \\ 2n + v_p(a_5) \geq \frac{7}{2}n \\ n + v_p(a_6) \geq 3n \\ v_p(a_7) \geq \frac{5}{2}n \end{cases} \Rightarrow \begin{cases} v_p(a_2) \geq \frac{1}{3}n \\ v_p(a_3) \geq \frac{2}{3}n \\ v_p(a_5) \geq \frac{3}{2}n \\ v_p(a_6) \geq 2n \\ v_p(a_7) \geq \frac{5}{2}n \end{cases} .$$

In this case, we have

$$t-\alpha_1, (t-\alpha_2)\cdots(t-\alpha_4), (t-\alpha_5)\cdots(t-\alpha_{10}), (t-\alpha_{11})\cdots(t-\alpha_{13}), t-\alpha_{14} \in \mathbb{Q}_p[t]$$

with

$$\begin{aligned} v_p(\alpha_1) &= n, \\ v_p(\alpha_2) = \cdots = v_p(\alpha_4) &= \frac{2}{3}n, \\ v_p(\alpha_5) = \cdots = v_p(\alpha_{10}) &= \frac{1}{2}n, \\ v_p(\alpha_{11}) = \cdots = v_p(\alpha_{13}) &= \frac{1}{3}n, \\ v_p(\alpha_{14}) &= 0. \end{aligned}$$

Thus Theorem 4.2.5 holds if and only if $f(t)$ has no root of valuation $\frac{1}{3}n, \frac{1}{2}n$ or $\frac{2}{3}n$ and has exactly 2 degree 3 irreducible factors in $\mathbb{Q}_p[t]$.

(1-3) $(1, 6n + v_p(a_1)) = (1, 6n)$ and $(5, 2n + v_p(a_5)) = (5, 3n)$ are vertices. Then $v_p(a_5) = n$ and

$$\begin{cases} 5n + v_p(a_2) \geq \frac{21}{4}n \\ 4n + v_p(a_3) \geq \frac{9}{2}n \\ 3n + v_p(a_4) \geq \frac{15}{4}n \\ n + v_p(a_6) \geq \frac{5}{2}n \\ v_p(a_7) \geq 2n \end{cases} \Rightarrow \begin{cases} v_p(a_2) \geq \frac{1}{4}n \\ v_p(a_3) \geq \frac{1}{2}n \\ v_p(a_4) \geq \frac{3}{4}n \\ v_p(a_6) \geq \frac{3}{2}n \\ v_p(a_7) \geq 2n \end{cases} .$$

In this case, we have

$$t-\alpha_1, (t-\alpha_2)\cdots(t-\alpha_5), (t-\alpha_6)\cdots(t-\alpha_9), (t-\alpha_{10})\cdots(t-\alpha_{13}), t-\alpha_{14} \in \mathbb{Q}_p[t]$$

with

$$\begin{aligned} v_p(\alpha_1) &= n, \\ v_p(\alpha_2) = \cdots = v_p(\alpha_5) &= \frac{3}{4}n, \\ v_p(\alpha_6) = \cdots = v_p(\alpha_9) &= \frac{1}{2}n, \\ v_p(\alpha_{10}) = \cdots = v_p(\alpha_{13}) &= \frac{1}{4}n, \\ v_p(\alpha_{14}) &= 0. \end{aligned}$$

Thus Theorem 4.2.5 holds if and only if $f(t)$ has no root of valuation $\frac{1}{4}n, \frac{1}{2}n$ or $\frac{3}{4}n$ and has at most 2 degree 2 irreducible factors in $\mathbb{Q}_p[t]$.

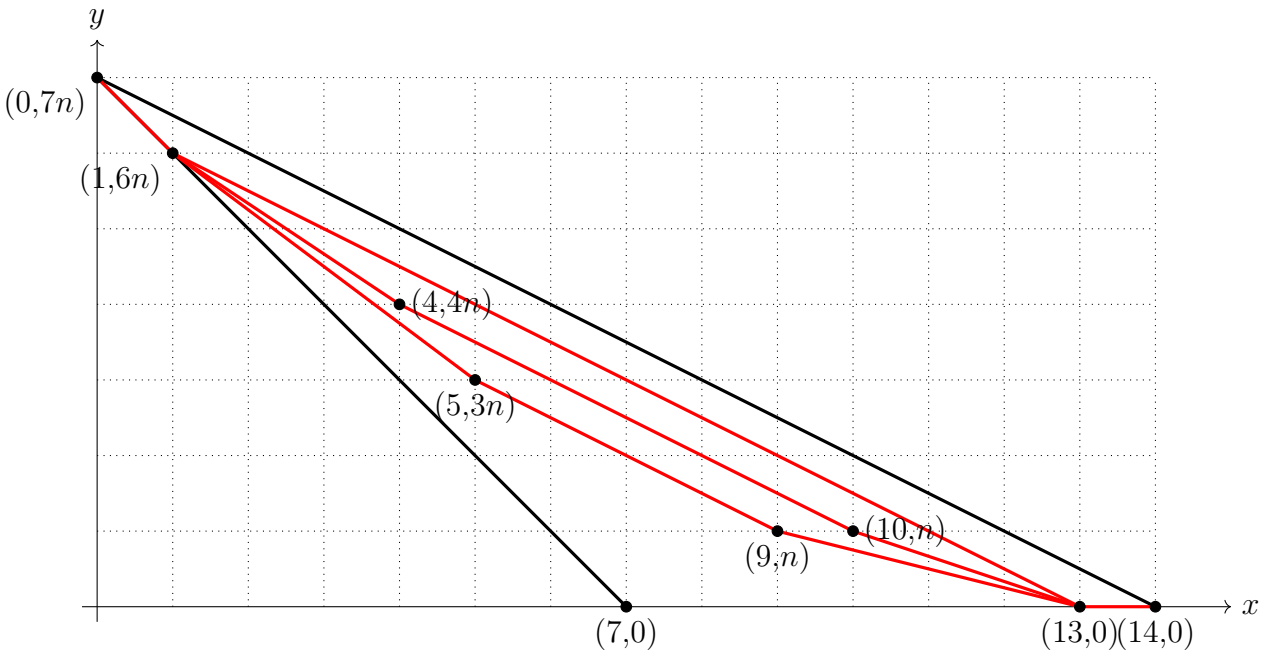

Figure 4.2: The Newton polygon for case (1-1), (1-2) and (1-3).

(1-4) $(1, 6n + v_p(a_1)) = (1, 6n)$ and $(6, n + v_p(a_6)) = (6, 3n)$ are vertices. Then

$v_p(a_6) = 2n$ and

$$\begin{cases} 5n + v_p(a_2) \geq \frac{27}{5}n \\ 4n + v_p(a_3) \geq \frac{24}{5}n \\ 3n + v_p(a_4) \geq \frac{21}{5}n \\ 2n + v_p(a_5) \geq \frac{18}{5}n \\ v_p(a_7) \geq \frac{5}{2}n \end{cases} \Rightarrow \begin{cases} v_p(a_2) \geq \frac{2}{5}n \\ v_p(a_3) \geq \frac{4}{5}n \\ v_p(a_4) \geq \frac{6}{5}n \\ v_p(a_5) \geq \frac{8}{5}n \\ v_p(a_7) \geq \frac{5}{2}n \end{cases} .$$

In this case, we have

$$t - \alpha_1, (t - \alpha_2) \cdots (t - \alpha_6), (t - \alpha_7)(t - \alpha_8), (t - \alpha_9) \cdots (t - \alpha_{13}), t - \alpha_{14} \in \mathbb{Q}_p[t]$$

with

$$\begin{aligned} v_p(\alpha_1) &= n, \\ v_p(\alpha_2) &= \cdots = v_p(\alpha_6) = \frac{3}{5}n, \\ v_p(\alpha_7) &= v_p(\alpha_8) = \frac{1}{2}n, \\ v_p(\alpha_9) &= \cdots = v_p(\alpha_{13}) = \frac{2}{5}n, \\ v_p(\alpha_{14}) &= 0. \end{aligned}$$

Thus Theorem 4.2.5 holds if and only if

$f(t)$ has no root of valuation $\frac{2}{5}n, \frac{1}{2}n$ or $\frac{3}{5}n$ nor degree 3 irreducible factors in $\mathbb{Q}_p[t]$.

(1-5) $(1, 6n + v_p(a_1)) = (1, 6n)$ and $(6, n + v_p(a_6)) = (6, 2n)$ are vertices. Then

$v_p(a_6) = n$ and

$$\begin{cases} 5n + v_p(a_2) \geq \frac{26}{5}n \\ 4n + v_p(a_3) \geq \frac{22}{5}n \\ 3n + v_p(a_4) \geq \frac{18}{5}n \\ 2n + v_p(a_5) \geq \frac{14}{5}n \\ v_p(a_7) \geq \frac{3}{2}n \end{cases} \Rightarrow \begin{cases} v_p(a_2) \geq \frac{1}{5}n \\ v_p(a_3) \geq \frac{2}{5}n \\ v_p(a_4) \geq \frac{3}{5}n \\ v_p(a_5) \geq \frac{4}{5}n \\ v_p(a_7) \geq \frac{3}{2}n \end{cases}.$$

In this case, we have

$$t - \alpha_1, (t - \alpha_2) \cdots (t - \alpha_6), (t - \alpha_7)(t - \alpha_8), (t - \alpha_9) \cdots (t - \alpha_{13}), t - \alpha_{14} \in \mathbb{Q}_p[t]$$

with

$$\begin{aligned} v_p(\alpha_1) &= n, \\ v_p(\alpha_2) &= \cdots = v_p(\alpha_6) = \frac{4}{5}n, \\ v_p(\alpha_7) &= v_p(\alpha_8) = \frac{1}{2}n, \\ v_p(\alpha_9) &= \cdots = v_p(\alpha_{13}) = \frac{1}{5}n, \\ v_p(\alpha_{14}) &= 0. \end{aligned}$$

Thus Theorem 4.2.5 holds if and only if

$f(t)$ has no root of valuation $\frac{1}{5}n, \frac{1}{2}n$ or $\frac{4}{5}n$ nor degree 3 irreducible factors in $\mathbb{Q}_p[t]$.

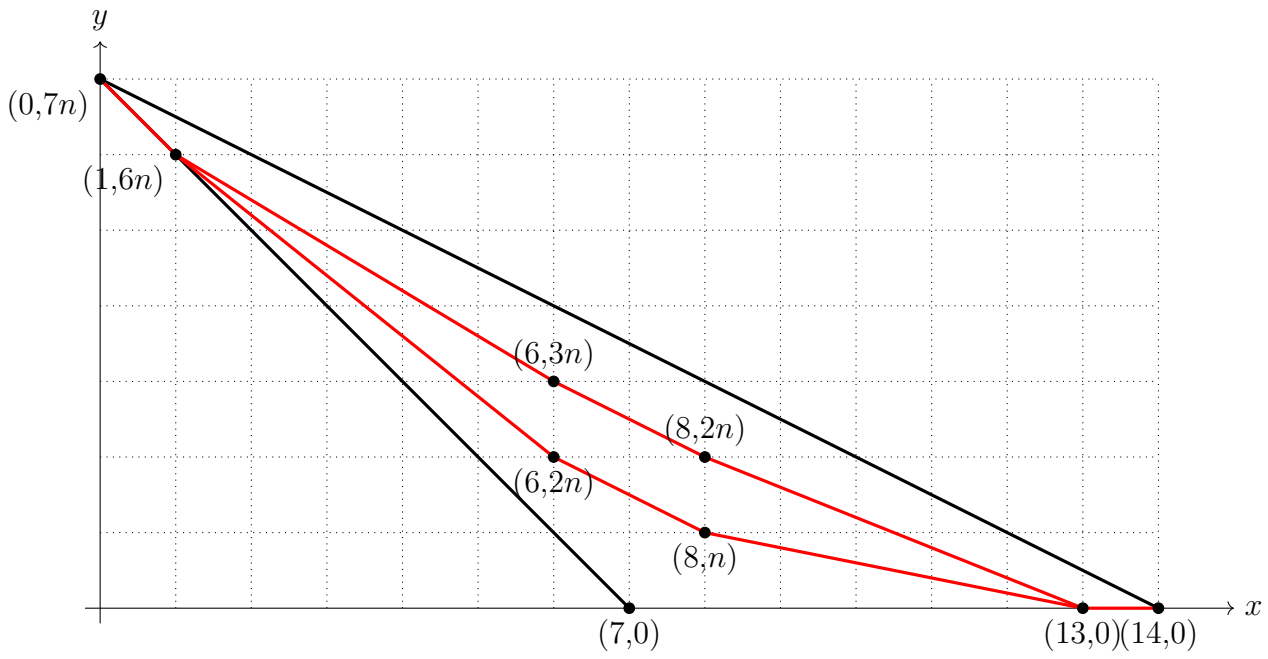

Figure 4.3: The Newton polygon for case (1-4) and (1-5).

(1-6) $(1, 6n+v_p(a_1)) = (1, 6n)$ and $(7, v_p(a_7)) = (7, 2n)$ are vertices. Then $v_p(a_7) = 2n$ and

$$\begin{cases} 5n + v_p(a_2) \geq \frac{16}{3}n \\ 4n + v_p(a_3) \geq \frac{14}{3}n \\ 3n + v_p(a_4) \geq 4n \\ 2n + v_p(a_5) \geq \frac{10}{3}n \\ n + v_p(a_6) \geq \frac{8}{3}n \end{cases} \Rightarrow \begin{cases} v_p(a_2) \geq \frac{1}{3}n \\ v_p(a_3) \geq \frac{2}{3}n \\ v_p(a_4) \geq n \\ v_p(a_5) \geq \frac{4}{3}n \\ v_p(a_6) \geq \frac{5}{3}n \end{cases} .$$

In this case, we have

$$t - \alpha_1, (t - \alpha_2) \cdots (t - \alpha_7), (t - \alpha_8) \cdots (t - \alpha_{13}), t - \alpha_{14} \in \mathbb{Q}_p[t]$$

with

$$\begin{aligned} v_p(\alpha_1) &= n, \\ v_p(\alpha_2) &= \cdots = v_p(\alpha_7) = \frac{2}{3}n, \\ v_p(\alpha_8) &= \cdots = v_p(\alpha_{13}) = \frac{1}{3}n, \\ v_p(\alpha_{14}) &= 0. \end{aligned}$$

Thus Theorem 4.2.5 holds if and only if

$f(t)$ has no root of valuation $\frac{1}{3}n$ or $\frac{2}{3}n$ nor degree 2 irreducible factors in $\mathbb{Q}_p[t]$.

(1-7) $(1, 6n + v_p(a_1)) = (1, 6n)$ and $(7, v_p(a_7)) = (7, n)$ are vertices. Then $v_p(a_7) = n$ and

$$\begin{cases} 5n + v_p(a_2) \geq \frac{31}{6}n \\ 4n + v_p(a_3) \geq \frac{13}{3}n \\ 3n + v_p(a_4) \geq \frac{7}{2}n \\ 2n + v_p(a_5) \geq \frac{8}{3}n \\ n + v_p(a_6) \geq \frac{11}{6}n \end{cases} \Rightarrow \begin{cases} v_p(a_2) \geq \frac{1}{6}n \\ v_p(a_3) \geq \frac{1}{3}n \\ v_p(a_4) \geq \frac{1}{2}n \\ v_p(a_5) \geq \frac{2}{3}n \\ v_p(a_6) \geq \frac{5}{6}n \end{cases}.$$

In this case, we have

$$t - \alpha_1, (t - \alpha_2) \cdots (t - \alpha_7), (t - \alpha_8) \cdots (t - \alpha_{13}), t - \alpha_{14} \in \mathbb{Q}_p[t]$$

with

$$\begin{aligned} v_p(\alpha_1) &= n, \\ v_p(\alpha_2) = \cdots = v_p(\alpha_7) &= \frac{5}{6}n, \\ v_p(\alpha_8) = \cdots = v_p(\alpha_{13}) &= \frac{1}{6}n, \\ v_p(\alpha_{14}) &= 0. \end{aligned}$$

Thus Theorem 4.2.5 holds if and only if

$f(t)$ has no root of valuation $\frac{1}{6}n$ or $\frac{5}{6}n$ nor irreducible factors of degree 2 or 3 in $\mathbb{Q}_p[t]$.

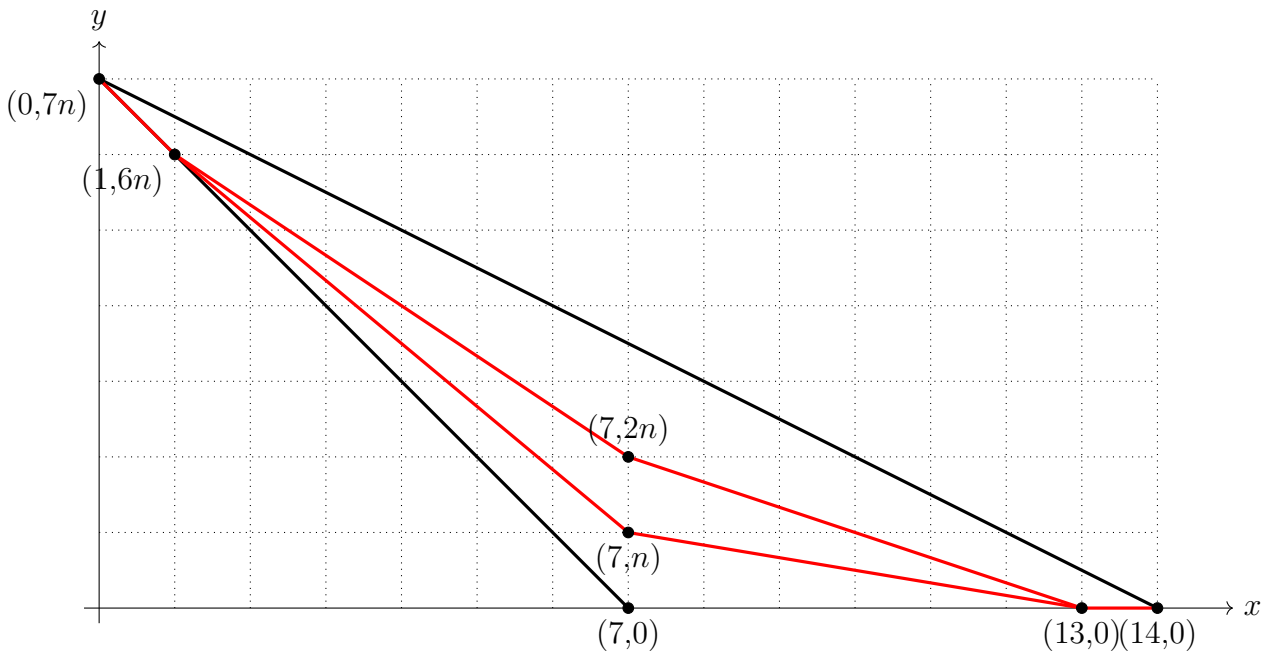

Figure 4.4: The Newton polygon for case (1-6) and (1-7).

The other cases follow similarly, and this completes the proof of the theorem. □

Bibliography

[1] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004. ISBN 3-540-20488-1. doi: 10.1007/978-3-662-06307-1. URL https://doi.org/10.1007/978-3-662-06307-1.

[2] A. Clebsch. Zur Theorie der binären algebraischen Formen. *Math. Ann.*, 3 (2):265–267, 1870. ISSN 0025-5831. doi: 10.1007/BF01443987. URL https://doi.org/10.1007/BF01443987.

[3] David A. Cox, John B. Little, and Henry K. Schenck. *Toric varieties*, volume 124 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2011. ISBN 978-0-8218-4819-7. doi: 10.1090/gsm/124. URL https://doi.org/10.1090/gsm/124.

[4] Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown. Sporadic cubic torsion. *Algebra Number Theory*, 15(7):1837–1864, 2021. ISSN 1937-0652. doi: 10.2140/ant.2021.15.1837. URL https://doi.org/10.2140/ant.2021.15.1837.

[5] Brendan Hassett. Classical and minimal models of the moduli space of curves of genus two. In *Geometric methods in algebra and number theory*, volume 235

of *Progr. Math.*, pages 169–192. Birkhäuser Boston, Boston, MA, 2005. doi: 10.1007/0-8176-4417-2_8. URL https://doi.org/10.1007/0-8176-4417-2_8.

[6] Daiki Hayashida. The characteristic polynomials of abelian varieties of higher dimension over finite fields. *J. Number Theory*, 196:205–222, 2019. ISSN 0022-314X. doi: 10.1016/j.jnt.2018.09.014. URL https://doi.org/10.1016/j.jnt.2018.09.014.

[7] Jun-ichi Igusa. On Siegel modular forms of genus two. *Amer. J. Math.*, 84:175–200, 1962. ISSN 0002-9327. doi: 10.2307/2372812. URL https://doi.org/10.2307/2372812.

[8] Aaron Landesman, Peter Ruhm, and Robin Zhang. Section rings of $\mathbb{Q}$-divisors on minimal rational surfaces. *Math. Res. Lett.*, 25(4):1329–1357, 2018. ISSN 1073-2780. doi: 10.4310/MRL.2018.v25.n4.a13. URL https://doi.org/10.4310/MRL.2018.v25.n4.a13.

[9] Evan O'Dorney. Canonical rings of $\mathbb{Q}$-divisors on $\mathbb{P}^1$. *Ann. Comb.*, 19(4):765–784, 2015. ISSN 0218-0006. doi: 10.1007/s00026-015-0280-y. URL https://doi.org/10.1007/s00026-015-0280-y.

[10] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. ISBN 978-0-387-09493-9. doi: 10.1007/978-0-387-09494-6. URL https://doi-org.ezproxy.uvm.edu/10.1007/978-0-387-09494-6.

[11] Shigeaki Tsuyumine. On Siegel modular forms of degree three. *Amer. J. Math.*, 108(4):755–862, 1986. ISSN 0002-9327. doi: 10.2307/2374517. URL https://doi.org/10.2307/2374517.

[12] John Voight and David Zureick-Brown. The canonical ring of a stacky curve.

Mem. Amer. Math. Soc., 277(1362):v+144, 2022. ISSN 0065-9266. doi: 10.1090/memo/1362. URL https://doi.org/10.1090/memo/1362.