Algorithmic Aspects of Hyperelliptic Curves and their Jacobians

An essay submitted in total fulfilment of the requirements of the degree of
Doctor of Philosophy in Pure Mathematics
under a Jointly-Awarded PhD Program between
The University of Sydney, Australia, and
l'Université d'Aix-Marseille, France,

by

Hamish Ivey-Law

under the direction of

David Kohel and Claus Fieker

School of Mathematics and Statistics
University of Sydney
Australia

and through the cotutelle scheme

Institut de Mathématiques de Luminy
Université d'Aix-Marseille
France

December, 2012

UNIVERSITÉ D'AIX-MARSEILLE
Faculté des Sciences de Luminy

THÈSE

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ D'AIX-MARSEILLE
et, dans le cadre d'une Cotutelle, de PhD de l'Université de Sydney

École Doctorale en Mathématiques et Informatique de Marseille
Discipline: Mathématiques

présentée et soutenue publiquement par

Hamish IVEY-LAW

le 14 décembre 2012

Titre:

Algorithmic Aspects of Hyperelliptic Curves and their Jacobians

Les directeurs de thèse: David KOHEL et Claus FIEKER
Les rapporteurs: Kamal KHURI-MAKDISI et Michael STOLL

JURY:

Dr. Claus FIEKER	Directeur de thèse
Dr. Florian HESS	Examinateur
Dr. David KOHEL	Directeur de thèse
Dr. David LUBICZ	Examinateur
Dr. Christophe RITZENTHALER	Examinateur
Dr. Michael STOLL	Rapporteur

Abstract (English)

The contribution of this thesis is divided naturally into two parts. In Part I we generalise the work of Khuri-Makdisi [22] on algorithms for divisor arithmetic on curves over fields to more general bases. We prove that the natural analogues of the results of Khuri-Makdisi [22] continue to hold for relative effective Cartier divisors on projective schemes which are smooth of relative dimension one over an arbitrary affine Noetherian base scheme and that natural analogues of the algorithms remain valid in this context for a certain class of base rings. We introduce a formalism for such rings, which are characterised by the existence of a certain subset of the usual linear algebra operations for projective modules over these rings.

Part II of this thesis is concerned with a type of Riemann-Roch problem for divisors on certain algebraic surfaces. Specifically we consider algebraic surfaces arising as the square or the symmetric square of a hyperelliptic curve of genus at least two over an (almost) arbitrary field. The main results are a decomposition of the spaces of global sections of certain divisors on such surfaces and explicit formulæ for the dimensions of the spaces of sections of these divisors. In the final chapter we present an algorithm which generates a basis for the space of global sections of such a divisor.

We now explain the content of each part of the thesis in more detail.

Relative curves and their Jacobians

Khuri-Makdisi [22] introduced a means to perform arithmetic with divisors on curves over fields which represents a divisor as a subspace of the space of global sections of some power of given very ample divisor. On the basis of two principal theoretical results, he shows that many natural operations on divisors can be reduced to relatively simple linear algebra over the base field. Chapters 2 and 3 of this thesis are concerned with the generalisation of the results of Khuri-Makdisi [22].

Let $S = \mathrm{Spec}(R)$ be an affine Noetherian scheme and let X/S be a projective S-scheme which is smooth of relative dimension one over S; we

call X/S a *relative curve*. In Section 2.1 we show that the modules of sections of a relative effective Cartier divisor on X are projective. In Section 2.2 we describe conditions for very ampleness and normal generation of invertible sheaves. In particular we show that the usual relationships between very ampleness and normal generation can be lifted from the fibres, as can the familiar result that a divisor of degree at least $2g+1$ is normally generated and hence very ample. In Section 2.3 we prove the two principal results that underlie the algorithms for performing arithmetic with divisors:

Proposition 2.3.5. *Let $S = \mathrm{Spec}(R)$, let X/S be a relative curve and let $\mathscr{M}$ and $\mathscr{N}$ be normally generated sheaves on X. Then*

$$\mu : H^0(X, \mathscr{M}) \otimes H^0(X, \mathscr{N}) \to H^0(X, \mathscr{M} \otimes \mathscr{N})$$

is surjective.

Proposition 2.3.7. *Let X/S be a relative curve of genus g and let $\mathscr{M}$ and $\mathscr{N}$ be invertible sheaves on X, each of degree at least $2g+1$. Then for any relative effective Cartier divisor D on X of degree at most $\deg(\mathscr{M})-(2g+1)$, we have*

$$H^0(X, \mathscr{M}(-D)) = \Big(H^0(X, \mathscr{M} \otimes_{\mathscr{O}_X} \mathscr{N}(-D)) : H^0(X, \mathscr{N})\Big)_\mu$$

with respect to the canonical homomorphism μ of Proposition 2.3.5.

In Chapter 3 we demonstrate that Propositions 2.3.5 and 2.3.7 allow us to derive algorithms for arithmetic of divisors which are analogous to those presented by Khuri-Makdisi [22]. We reprove a selection of his algorithms in this more general context; in particular, we give algorithms that allow addition of divisor classes in $\mathrm{Pic}^0_X(S)$.

Spaces of sections on algebraic surfaces

Let C be a hyperelliptic curve of genus $g \geqslant 2$, and let $\mathrm{Sym}^2(C)$ be the symmetric product of C. Let $\infty \in C(\overline{k})$ be a Weierstrass point over an algebraic closure of the base field k and set $D_\infty = 2(\infty)$. Let $p_i : C \times C \to C$ for $i = 1, 2$ be the two projection maps. Let $F = p_1^*(D_\infty) + p_2^*(D_\infty)$ be the fibral divisor on $C \times C$ and let ∇ be the antidiagonal divisor on $C \times C$. Set $\gamma = g - 1$ and let $m > \gamma$ and $r \geqslant 0$. The main results of Chapter 4 are the following. In Theorem 4.5.11 we prove that, under mild conditions, there is a decomposition

$$H^0(C \times C, mF + r\nabla) \cong H^0(C^2, mF) \oplus \bigoplus_{i=1}^{r} H^0(C, (2m - \gamma i)D_\infty).$$

As a corollary we obtain formulæ for the dimension of this space as a function of m and r. For example, when $2m - \gamma r > \gamma$, we obtain

$$\dim H^0(C \times C, mF + r\nabla) = (2m - \gamma)^2 + 4mr - \gamma r(r + 2).$$

Similarly, in Theorem 4.6.12 we prove under mild conditions that we have a decomposition

$$H^0(\mathrm{Sym}^2(C), 2m\Theta_S + r\nabla_S) \cong H^0(\mathrm{Sym}^2(C), 2m\Theta_S) \oplus \bigoplus_{i=1}^{r} H^0(\mathbb{P}^1, (2m - \gamma i)(\infty))$$

where $2\Theta_S$ is the image of F and ∇_S is the image of ∇ under the quotient map $C \times C \to \mathrm{Sym}^2(C)$. As a corollary we obtain formulæ for the dimension of this space in terms of m and r. For example, when $2m - \gamma r > 0$, we obtain

$$\dim H^0(\mathrm{Sym}^2(C), 2m\Theta_S + r\nabla_S) = \binom{2m - \gamma + 1}{2} + r(2m + 1) - \gamma\binom{r + 1}{2}.$$

We have been unable to prove the results above in the case $2m - \gamma r = 0$, though we conjecture that the results hold in this case too. Indeed, the algorithm developed in Chapter 5 allows us to test the conjecture in any particular case.

In Chapter 5 we describe a decomposition of $H^0(C \times C, mF)$ with respect to the eigenspaces of the action of permuting coordinates and use this information to develop an algorithm to generate an explicit basis for the space $H^0(\mathrm{Sym}^2(C), 2m\Theta_S + r\nabla_S)$. We show that the algorithm reproduces, modulo projective linear transformation, the well-known basis of Cassels [7] and Flynn [12] describing the embedding of the Jacobian of curve of genus two in $\mathbb{P}^{15}$ and we show that it confirms the dimension formulæ of Chapter 4 in several cases. We finish with a brief discussion of potential applications to coding theory on surfaces of the form $C \times C$ and $\mathrm{Sym}^2(C)$.

Résumé (français)

Ce travail se divise en deux parties. Dans la première partie, nous généralisons le travail de Khuri-Makdisi [22] qui décrit des algorithmes pour l'arithmétique des diviseurs sur une courbe sur un corps. Nous montrons que les analogues naturelles de ses résultats se vérifient pour les diviseurs de Cartier relatifs effectifs sur un schéma projectif, lisse et de dimension relative un sur un schéma affine noetherien quelconque, et que les analogues naturelles de ses algorithmes se vérifient pour une certaine classe d'anneaux de base. Nous présentons un formalisme pour tels anneaux qui sont caractérisés par l'existence d'un certain sous-ensemble des opérations standards de l'algèbre linéaire pour les modules projectifs sur ces anneaux.

Dans la deuxième partie de ce travail, nous considérons un type de problème de Riemann-Roch pour les diviseurs sur certaines surfaces algébriques. Plus précisément, nous analysons les surfaces algébriques qui émanent d'un produit ou d'un produit symétrique d'une courbe hyperelliptique de genre supérieur à un sur un corps (presque) arbitraire. Les résultats principaux sont une décomposition des espaces de sections globales de certains diviseurs sur telles surfaces et des formules explicites qui décrivent les dimensions des espaces de sections de ces diviseurs. Dans le dernier chapitre, nous présentons un algorithme qui produit une base pour l'espace de sections globales d'un tel diviseur.

À présent, nous décrivons de manière plus détaillée le contenu de chaque partie de la thèse.

Courbes relatives et leurs jacobiennes

Khuri-Makdisi [22] a présenté un moyen de calculer certaines opérations arithmétiques avec les diviseurs sur une courbe sur un corps fini qui représente un diviseur comme un sous-espace de sections globales d'une puissance d'un diviseur donné très ample. À partir de deux résultats théoriques principaux, il a montré que plusieurs opérations naturelles sur les diviseurs peuvent être réduites à l'algèbre linéaire sur le corps de base. Les Chapitres 2 et 3 sont

consacrés à la généralisation des résultats de Khuri-Makdisi [22].

Soient $S = \mathrm{Spec}(R)$ un schema affine noetherien et X/S un S-schema projectif, lisse de dimension relatif un sur S; on appelle X/S une *courbe relative*. Dans la Section 2.1, nous montrons que les modules de sections d'un diviseur de Cartier relatif effectif sur X sont projectifs. Dans la Section 2.2, nous décrivons les conditions pour qu'un faisceau inversible soit très ample ou engendré normalement. En particulier, nous montrons que les relations attendues entre les propriétés d'être très ample ou d'être engendré normalement se relèvent des fibres. Dans la Section 2.3, nous montrons les deux résultats principaux qui sous-tendent les algorithmes pour calculer les opérations arithmétiques sur les diviseurs :

Proposition 2.3.5. *Soient $S = \mathrm{Spec}(R)$ et X/S une courbe relative, et soient $\mathscr{M}$ et $\mathscr{N}$ deux $\mathscr{O}_X$-modules qui sont engendrés normalement. Alors*

$$\mu : H^0(X, \mathscr{M}) \otimes H^0(X, \mathscr{N}) \to H^0(X, \mathscr{M} \otimes \mathscr{N})$$

est surjective.

Proposition 2.3.7. *Soit X/S une courbe relative de genre g et soient $\mathscr{M}$ et $\mathscr{N}$ deux faisceaux inversibles sur X, chacun de degré au moins $2g+1$. Alors tout diviseur de Cartier relatif effectif D sur X de degré au plus $\deg(\mathscr{M}) - (2g+1)$ satisfait l'équation*

$$H^0(X, \mathscr{M}(-D)) = \left(H^0(X, \mathscr{M} \otimes_{\mathscr{O}_X} \mathscr{N}(-D)) : H^0(X, \mathscr{N})\right)_\mu$$

par rapport à l'homomorphisme canonique μ de Proposition 2.3.5.

Dans le Chapitre 3 nous montrons que les Propositions 2.3.5 et 2.3.7 nous permettent de décrire des algorithmes pour l'arithmétique des diviseurs qui sont analogues à ceux présentés par Khuri-Makdisi [22]. Nous dérivons à nouveau une sélection de ses algorithmes dans ce contexte plus général ; en particulier nous donnons un algorithme qui calcule la somme de deux classes de diviseurs dans $\mathrm{Pic}^0_X(S)$.

Espaces de sections sur une surface algébrique

Soient C une courbe hyperelliptique de genre $g \geqslant 2$ et $\mathrm{Sym}^2(C)$ le produit symétrique de C. Soient $\infty \in C(\overline{k})$ un point Weierstrass sur une clôture algébrique du corps de base k et $D_\infty = 2(\infty)$. Soient $p_i : C \times C \to C$ pour $i = 1, 2$ les deux applications de projection. Soient $F = p_1^*(D_\infty) + p_2^*(D_\infty)$ le diviseur fibral sur $C \times C$ et ∇ le diviseur anti-diagonal sur $C \times C$. Notons

$\gamma = g - 1$ et soient $m > \gamma$ et $r \geqslant 0$. Les résultats principaux du Chapitre 4 sont les suivants. Dans le Théorème 4.5.11, nous montrons, sous certaines conditions légères, qu'il existe une décomposition

$$H^0(C \times C, mF + r\nabla) \cong H^0(C^2, mF) \oplus \bigoplus_{i=1}^{r} H^0(C, (2m - \gamma i)D_\infty).$$

On obtient comme corollaire des formules qui décrivent la dimension de cet espace comme une fonction de m et r. Par exemple, lorsque $2m - \gamma r > \gamma$, on obtient

$$\dim H^0(C \times C, mF + r\nabla) = (2m - \gamma)^2 + 4mr - \gamma r(r + 2).$$

D'une façon similaire, dans le Théorème 4.6.12 nous montrons, sous certaines conditions légères, qu'il existe une décomposition

$$H^0(\mathrm{Sym}^2(C), 2m\Theta_S + r\nabla_S) \cong H^0(\mathrm{Sym}^2(C), 2m\Theta_S) \oplus \bigoplus_{i=1}^{r} H^0(\mathbb{P}^1, (2m - \gamma i)(\infty))$$

où $2\Theta_S$ et ∇_S sont les images de F et ∇ sous la projection canonique $C \times C \to \mathrm{Sym}^2(C)$. Comme corollaire, on obtient des formules qui décrivent la dimension de cet espace en fonction de m et r. Par exemple, lorsque $2m - \gamma r > 0$, on obtient

$$\dim H^0(\mathrm{Sym}^2(C), 2m\Theta_S + r\nabla_S) = \binom{2m - \gamma + 1}{2} + r(2m + 1) - \gamma\binom{r + 1}{2}.$$

Nous ne pouvons montrer les résultats dans le cas où $2m - \gamma r = 0$. Néanmoins, nous conjecturons que les résultats se vérifient aussi dans ce cas. En effet, l'algorithme présenté dans le Chapitre 5 nous permet de vérifier la conjecture dans chaque cas particulier.

Dans le Chapitre 5, nous décrivons une décomposition de $H^0(C \times C, mF)$ par rapport aux espaces propres de l'action de la permutation de coordonnées et nous nous en servons pour développer un algorithme qui produit une base explicite pour l'espace $H^0(\mathrm{Sym}^2(C), 2m\Theta_S + r\nabla_S)$. Nous montrons que l'algorithme reproduit, modulo une transformation projective linéaire, la base bien connue de Cassels [7] et Flynn [12] qui décrit le plongement de la jacobienne d'une courbe de genre deux dans $\mathbb{P}^{15}$. Nous montrons de plus qu'il vérifie les formules de dimension du Chapitre 4 dans plusieurs cas. On conclut avec une discussion brève des applications potentielles à la théorie des codes sur les surfaces de la forme $C \times C$ et $\mathrm{Sym}^2(C)$.

Acknowledgements

First and foremost I would like to thank my supervisor, David Kohel, for his direction, support, and limitless patience. To have had his guidance during my journey towards mathematical maturity has been a great privilege and a great pleasure.

I would like to thank the examiners Kamal Khuri-Makdisi and Michael Stoll for the many improvements they suggested.

Over the course of my candidature, many people have generously contributed some of their time to help improve my understanding and presentation of mathematics generally, and in particular many aspects of the present work have benefited from these conversations. In this spirit I would like to thank Peter Bruin, Xavier Caruso, Virgile Ducet, Bas Edixhoven, Stephen Enright-Ward, Claus Fieker, David Gruenewald, Qing Liu, and Ben Smith.

I would like to thank Traian Muntean and Robert Rolland for their generous support as well as the opportunity for profitable collaboration with the team at eRISCS.

I would like to thank my colleagues at IML for providing such a convivial work environment.

I would like to thank my friends and family for their moral support over the last few years. To my friends in Marseille, thank you for making the move to this strange foreign land a pleasure, and to those friends in various parts of Australia and the rest of the globe, thank you for tenaciously keeping contact.

Last, but far from least, I would like to thank Céline for her unwavering companionship, support and patience; you have enriched my life beyond measure.

Dedicated to the memory of
Phyllis M. Ivey
1923–2010

Contents

Chapter 1

Geometric preliminaries

In this chapter we recall the background material and notation necessary for the subsequent chapters. Most of the material presented in this chapter can be found in Hartshorne [17], Liu [26] or Mumford [32].

1.1 Divisors and invertible sheaves

Let $(X, \mathscr{O}_X)$ be a scheme and let $\mathscr{K}_X$ be the sheaf of total quotient rings (also called the sheaf of stalks of meromorphic functions) on X. We denote by $\mathscr{K}_X^*$ the sheaf of multiplicative groups of invertible elements of the sheaf of rings $\mathscr{K}_X$. Similarly, we denote by $\mathscr{O}_X^*$ the sheaf of groups of invertible elements of the sheaf of rings $\mathscr{O}_X$. For any sheaf $\mathscr{F}$ on X, we will denote the global sections of $\mathscr{F}$ by $\Gamma(X, \mathscr{F})$.

A *Cartier divisor* on X is a global section of the sheaf $\mathscr{K}_X^*/\mathscr{O}_X^*$. A Cartier divisor can therefore be given as a system $\{(U_i, f_i)\}_{i\in I}$ where $\{U_i\}_{i\in I}$ is an open covering of X and the functions f_i are sections of $\Gamma(U_i, \mathscr{K}_X^*)$ such that for all $(i, j) \in I \times I$, we have $f_i/f_j \in \Gamma(U_i \cap U_j, \mathscr{O}_X^*)$; that is, the ratio f_i/f_j is a non-zero regular function on $U_i \cap U_j$. Two such systems $\{(U_i, f_i)\}_{i\in I}$ and $\{(V_j, g_j)\}_{j\in J}$ define the same Cartier divisor if $f_i/g_j \in \mathscr{O}_X^*(U_i \cap V_j)$ for all $(i, j) \in I \times J$.

The set of Cartier divisors $\Gamma(X, \mathscr{K}_X^*/\mathscr{O}_X^*)$ on X will be denoted by $\mathrm{Div}(X)$; it has a group structure defined as follows. Let $D_1 = \{(U_i, f_i)\}_{i\in I}$ and $D_2 = \{(V_j, g_j)\}_{j\in J}$ be two Cartier divisors on X. Then the sum $D_1 + D_2$ is given by $\{(U_i \cap V_j, f_i g_j)\}_{(i,j)\in I\times J}$, the negative $-D_1$ is given by $\{(U_i, f_i^{-1})\}_{i\in I}$, and the identity element is $\{(X, 1)\}$.

The image of a non-zero rational function $f \in \Gamma(X, \mathscr{K}_X^*)$ in $\Gamma(X, \mathscr{K}_X^*/\mathscr{O}_X^*)$ is called a *principal Cartier divisor* and will be denoted by $\mathrm{div}(f)$. Two Cartier divisors D_1 and D_2 are said to be *rationally equivalent* if their differ-

ence $D_1 - D_2$ is a principal Cartier divisor, in which case we write $D_1 \sim_{\mathrm{rat}} D_2$. The group of classes of Cartier divisors modulo the relation of rational equivalence will be denoted by $\mathrm{CaCl}(X)$.

A Cartier divisor $D = \{(U_i, f_i)\}_{i \in I}$ is said to be *effective* if $f_i \in \Gamma(U_i, \mathscr{O}_X)$ for all $i \in I$.

Lemma 1.1.1. *Let X be a Noetherian scheme of dimension 1. Given an arbitrary Cartier divisor D, there exist non-zero effective divisors E_1 and E_2 such that $D = E_1 - E_2$*

Proof. See Liu [26, Lemma 7.3.6]. □

An *invertible sheaf* on X is a locally free $\mathscr{O}_X$-module of rank one. To a Cartier divisor $D = \{(U_i, f_i)\}_{i \in I}$ we can associate an invertible subsheaf $\mathscr{O}_X(D)$ of $\mathscr{K}_X$, defined, for each $i \in I$, by

$$\mathscr{O}_X(D)|_{U_i} = f_i^{-1} \mathscr{O}_X|_{U_i}.$$

A divisor D is effective if and only if $\mathscr{O}_X(-D) \subseteq \mathscr{O}_X$. If D is effective, we denote by $(D, \mathscr{O}_D)$ the closed subscheme of X associated to the invertible sheaf of ideals $\mathscr{O}_X(-D)$. For any invertible sheaf $\mathscr{L}$, we denote by $\mathscr{L}(D)$ the invertible sheaf $\mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{O}_X(D)$.

Let X be a smooth algebraic curve over a field k and let $D = \{(U_i, f_i)\}_{i \in I}$ be a Cartier divisor on X. As X is smooth, the local ring $\mathscr{O}_{X,x}$ at a point x of X is a discrete valuation ring. The *order of D at x*, denoted by $\mathrm{ord}_x(D)$, is defined as follows. For an open set U_i containing x, we set $\mathrm{ord}_x(D) = \mathrm{ord}_x(f_i)$, where $\mathrm{ord}_x(f_i)$ is the valuation of f_i in $\mathscr{O}_{X,x}$. One can check that $\mathrm{ord}_x(D)$ is independent of the choice of (U_i, f_i). The *degree* of D, denoted by $\deg(D)$, is the integer

$$\deg(D) = \sum_x \mathrm{ord}_x(D)[k(x) : k]$$

where the sum is over the closed points of X and $k(x)$ denotes the residue field $\mathscr{O}_{X,x}/\mathfrak{m}_x$ at x.

Proposition 1.1.2. *Let X be a curve over a field k and let D be an effective Cartier divisor on X. Then the degree of D satisfies*

$$\deg(D) = \dim \Gamma(D, \mathscr{O}_D).$$

Proof. See Liu [26, Lemma 7.3.5]. □

Proposition 1.1.3. *Let X be a curve over a field k and let D be a divisor on X. If $\Gamma(X, \mathscr{O}_X(D)) \neq 0$, then $\deg(D) \geqslant 0$. Furthermore, if $\dim \Gamma(X, \mathscr{O}_X(D)) \neq 0$ and $\deg(D) = 0$, then $\mathscr{O}_X(D) \cong \mathscr{O}_X$.*

Proof. See Hartshorne [17, Lemma IV.1.2]. □

1.2 Cohomology of sheaves

Let X be a scheme and let $\mathscr{F}$ be a sheaf on X. We denote by $H^i(X, \mathscr{F})$ the *ith cohomology group of* $\mathscr{F}$. The definition of $H^i(X, \mathscr{F})$ is beyond the scope of this work; see Hartshorne [17, Chapter III] or Liu [26, Chapter 5] for the definition. We will collect here the main properties of the cohomology groups of coherent sheaves on projective varieties.

Proposition 1.2.1. *Let X be a scheme and let $\mathscr{F}$ be a sheaf on X. Then*

$$H^0(X, \mathscr{F}) \cong \Gamma(X, \mathscr{F}).$$

Proof. See Hartshorne [17, Section III.2] or Liu [26, Proposition 5.2.6]. □

Proposition 1.2.2. *Let X be a scheme and let*

$$0 \to \mathscr{F}' \to \mathscr{F} \to \mathscr{F}'' \to 0$$

be a short exact sequence of sheaves on X. Then for all $i \geqslant 0$ there exist coboundary maps

$$\delta^i : H^i(X, \mathscr{F}'') \to H^{i+1}(X, \mathscr{F}')$$

giving a long exact sequence of cohomology groups

$$\begin{aligned} 0 \to H^0(X, \mathscr{F}') \to H^0(X, \mathscr{F}) \to H^0(X, \mathscr{F}'') \\ \xrightarrow{\delta^0} H^1(X, \mathscr{F}') \to H^1(X, \mathscr{F}) \to H^1(X, \mathscr{F}'') \xrightarrow{\delta^1} \cdots \end{aligned} \tag{1.1}$$

Proof. See Hartshorne [17, Section III.2]. □

Theorem 1.2.3. *Let X be a projective scheme over a Noetherian ring A and let $\mathscr{F}$ be a coherent sheaf on X. Then $H^i(X, \mathscr{F})$ is a finitely generated A-module for all $i \geqslant 0$.*

Proof. See Hartshorne [17, Theorem III.5.2(a)]. □

Theorem 1.2.4. *Let X be a projective variety of dimension n over an algebraically closed field k and let $\mathscr{F}$ be a coherent sheaf on X. Then*

(i) $\dim_k H^i(X, \mathscr{F}) = 0$ *for $i > n$.*

(ii) (Serre Duality) Suppose moreover that X is nonsingular and that $\mathscr{F}$ is locally free; write $\mathscr{F}^\vee = \operatorname{Hom}_{\mathscr{O}_X}(\mathscr{F}, \mathscr{O}_X)$. Then for all i, there is a natural isomorphism

$$H^i(X, \mathscr{F}) \cong H^{n-i}(X, \mathscr{F}^\vee \otimes_{\mathscr{O}_X} \omega_X)^\vee$$

where $\omega_X = \Omega_X^n = \bigwedge^n \Omega_X^1$ denotes the canonical sheaf on X, and $V^\vee$ denotes the dual of a finite vector space V.

Proof. See Hartshorne [17, Theorem III.2.7] for (i) and Hartshorne [17, Corollary III.7.7 and Corollary III.7.12] for (ii). □

We will often write $h^i(X, \mathscr{F}) = \dim_k H^i(X, \mathscr{F})$ when the base field is clear from the context.

Theorem 1.2.5 (Künneth Formula)**.** *Let X and Y be projective varieties and let $\mathscr{F}$ and $\mathscr{G}$ be quasi-coherent sheaves on X and Y respectively. Then for all $i \geqslant 0$,*

$$H^i(X \times Y, p_1^*\mathscr{F} \otimes p_2^*\mathscr{G}) \cong \bigoplus_{j+k=i} H^j(X, \mathscr{F}) \otimes H^k(Y, \mathscr{G})$$

where $p_1 : X \times Y \to X$ and $p_2 : X \times Y \to Y$ are the projection maps.

Proof. See Kempf [21, Proposition 9.2.4]. □

Recall that a morphism $f : X \to Y$ of schemes is called *affine* if there exists a covering of Y by open affine sets $\{V_i\}$ such that $f^{-1}(V_i) \subseteq X$ is affine for all i; this is equivalent to the condition that, for *any* open affine subset $V \subseteq Y$, the open set $f^{-1}(V)$ is affine (see Hartshorne [17, Exercise II.5.17(a)]).

Proposition 1.2.6. *Let $f : X \to Y$ be a morphism of schemes and let $\mathscr{F}$ be a sheaf on X. For all $i \geqslant 0$, there is a canonical homomorphism*

$$H^i(Y, f_*\mathscr{F}) \to H^i(X, \mathscr{F})$$

which is an isomorphism if $\mathscr{F}$ is quasi-coherent and either (i) X is separated, and f is affine, or (ii) f is a closed immersion.

Proof. See Liu [26, Exercise 5.2.3]. □

Let X be a projective variety over a field k and let $\mathscr{F}$ be a coherent sheaf on X. The *Euler-Poincaré characteristic* of $\mathscr{F}$ is defined to be

$$\chi(\mathscr{F}) = \sum_{i \geqslant 0} (-1)^i h^i(X, \mathscr{F}).$$

By Theorems 1.2.3 and 1.2.4(i the Euler-Poincaré characteristic is always finite. In particular, if X is a curve, then Theorem 1.2.4(i)

$$\chi(\mathscr{F}) = h^0(X, \mathscr{F}) - h^1(X, \mathscr{F}).$$

If $\mathscr{L} = \mathscr{O}_X(D)$ for some divisor D on X, then we will write $\chi(D)$ for $\chi(\mathscr{L})$.

Theorem 1.2.7 (Riemann-Roch)**.** *Let X be a projective curve over a field k and let $\mathscr{L}$ be an invertible sheaf on X. Then there exists an integer* $\deg(\mathscr{L})$ *such that*

$$\chi(\mathscr{L}) = \deg(\mathscr{L}) + \chi(\mathscr{O}_X) = \deg(\mathscr{L}) + 1 - g.$$

Proof. See Liu [26, Theorem 7.3.17 and Theorem 7.3.26] or Hartshorne [17, Theorem IV.1.3]. □

Let X be a projective curve over a field k. The *degree* of an invertible sheaf $\mathscr{L}$ on X is defined to be the integer

$$\deg(\mathscr{L}) = \chi(\mathscr{L}) - \chi(\mathscr{O}_X).$$

Note that, if $\mathscr{L} = \mathscr{O}_X(D)$ for a divisor D on X, then $\deg(\mathscr{L}) = \deg(D)$.

Corollary 1.2.8. *Let X be a projective curve over a field k and let $\mathscr{L}$ be an invertible sheaf on X. If* $\deg(\mathscr{L}) > 2g - 2$*, then*

$$\dim \Gamma(X, \mathscr{L}) = \deg(\mathscr{L}) + 1 - g.$$

Proof. See Liu [26, Remark 7.3.33]. □

1.3 Embeddings in projective space

Let $S = \bigoplus_{d\in\mathbb{Z}} S_d$ be a graded ring and let $X = \operatorname{Proj}(S)$. For any integer n, let $S(n)$ denote the twisted module $\bigoplus_{d\in\mathbb{Z}} S_{d+n}$. The $\mathscr{O}_X$-module $\mathscr{O}_X(n)$ is defined to be the sheaf associated to the graded module $S(n)$. When $n = 1$, we call $\mathscr{O}_X(1)$ the *twisting sheaf* of Serre. For an arbitrary $\mathscr{O}_X$-module $\mathscr{F}$, we define the *nth twist of* $\mathscr{F}$ to be $\mathscr{F}(n) = \mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{O}_X(n)$. For simplicity, for any sheaf $\mathscr{F}$, we will write $\mathscr{F}^n$ for $\mathscr{F}^{\otimes n} = \mathscr{F} \otimes \cdots \otimes \mathscr{F}$ (n times) throughout this work.

Proposition 1.3.1. *Let $S = \bigoplus_{d\in\mathbb{Z}} S_d$ be a graded ring which is generated by S_1 as an S_0-algebra and let $X = \operatorname{Proj}(S)$. Then we have the following:*

(i) The sheaf $\mathscr{O}_X(n)$ is invertible on X for all n.

(ii) For all m and n,

$$\mathscr{O}_X(m) \otimes_{\mathscr{O}_X} \mathscr{O}_X(n) \cong \mathscr{O}_X(m+n).$$

In particular, for any sheaf of $\mathscr{O}_X$-modules $\mathscr{F}$

$$\mathscr{F}(m) \otimes_{\mathscr{O}_X} \mathscr{O}_X(n) \cong \mathscr{F}(m+n).$$

(iii) Let $T = \bigoplus_{d\in\mathbb{Z}} T_d$ be another graded ring which is generated by T_1 as a T_0-algebra and let $Y = \mathrm{Proj}(T)$. Let $\varphi : S \to T$ be a homomorphism of graded rings (so degrees are preserved), let $U \subseteq Y$ be the maximal open subset of Y such that $f : U \to X$ is a morphism determined by φ. Then

$$f^*(\mathscr{O}_X(n)) \cong \mathscr{O}_Y(n)|_U \qquad \text{and} \qquad f_*(\mathscr{O}_Y(n)|_U) \cong (f_*\mathscr{O}_U)(n).$$

Proof. See Hartshorne [17, Proposition II.5.12]. □

The graded S-module associated to an $\mathscr{O}_X$-module $\mathscr{F}$ is defined to be the group

$$\Gamma_*(\mathscr{F}) = \bigoplus_{n\in\mathbb{Z}} \Gamma(X, \mathscr{F}(n)).$$

This group is given the structure of a graded S-module as follows. Any element $s \in S_d$ determines a global section $s \in \Gamma(X, \mathscr{O}_X(d))$. Then given any global section $t \in \Gamma(X, \mathscr{F}(n))$, the product $s \cdot t \in \Gamma(X, \mathscr{F}(n+d))$ is given by the image of $s \otimes t$ under the isomorphism $\mathscr{F}(n) \otimes_{\mathscr{O}_X} \mathscr{O}_X(d) \cong \mathscr{F}(n+d)$ of Proposition 1.3.1(ii). In particular, for any ring A, we have $\Gamma_*(\mathscr{O}_{\mathbb{P}^r_A}) = A[x_0, \ldots, x_r]$ (see Hartshorne [17, Proposition II.5.13]).

Let $\mathscr{L}$ be an invertible sheaf on a Y-scheme $X \to Y$. Then $\mathscr{L}$ is said to be *very ample* with respect to Y if there is an immersion $\iota : X \to \mathbb{P}^r_Y$ for some $r \geqslant 1$ such that $\iota^*(\mathscr{O}_{\mathbb{P}^r_Y}(1)) \cong \mathscr{L}$. If $\mathscr{L}$ and $\mathscr{M}$ are very ample sheaves on X with respect to Y, then $\mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{M}$ is also very ample (see Hartshorne [17, Exercise II.5.12]).

Let $\mathscr{F}$ be an $\mathscr{O}_X$-module on a scheme X. Then $\mathscr{F}$ is said to be *generated by global sections* if there is a set of global sections

$$\{s^{(i)}\}_{i\in I} \subseteq \Gamma(X, \mathscr{F})$$

such that, for all $x \in X$, the stalk $\mathscr{F}_x$ of $\mathscr{F}$ at x is generated as an $\mathscr{O}_{X,x}$-module by $\{s^{(i)}_x\}$, where $s^{(i)}_x$ denotes the image of $s^{(i)}$ in $\mathscr{F}_x$. For example, if $S = \bigoplus_{d\in\mathbb{Z}} S_d$ is a graded ring which is generated by S_1 as an S_0-algebra, and if $X = \mathrm{Proj}(S)$, then $\mathscr{O}_X(1)$ is generated by $S_1 \subseteq \Gamma(X, \mathscr{O}_X(1))$ (see Hartshorne [17, Example II.5.16.3]).

Let X be a projective scheme over a Noetherian ring A and let $\mathscr{L}$ be an invertible sheaf on X. Then $\mathscr{L}$ is said to be *ample* if, for every coherent $\mathscr{O}_X$-module $\mathscr{F}$, there is an integer n_0 such that, for all $n \geqslant n_0$, the sheaf $\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{L}^n$ can be generated by a finite number of global sections.

Theorem 1.3.2 (Serre)**.** *Let $\mathscr{L}$ be a very ample sheaf on a projective scheme X over a Noetherian ring A. Then $\mathscr{L}$ is ample.*

Proof. See Hartshorne [17, Theorem II.5.17]. □

Theorem 1.3.3. *Let X be a scheme of finite type over a Noetherian ring A and let $\mathscr{L}$ be an invertible sheaf on X. Then $\mathscr{L}$ is ample if and only if $\mathscr{L}^m$ is very ample over* $\mathrm{Spec}(A)$ *for some $m > 0$.*

Proof. See Hartshorne [17, Theorem II.7.6]. □

Theorem 1.3.4. *Let A be a ring, let X be an A-scheme, and let $\mathbb{P}^r_A = \mathrm{Proj}(A[x_0, \ldots, x_r])$ be projective r-space over A.*

(i) If $\varphi : X \to \mathbb{P}^r_A$ is a morphism of A-schemes, then $\varphi^*(\mathscr{O}_{\mathbb{P}^r_A}(1))$ is an invertible sheaf on X which is generated by the global sections $s_i = \varphi^*(x_i)$ for $i = 0, \ldots, r$.

(ii) Conversely, suppose $s_0, \ldots, s_r \in \Gamma(X, \mathscr{L})$ are global sections which generate an invertible sheaf $\mathscr{L}$ on X. Then there exists a unique morphism $\varphi : X \to \mathbb{P}^r_A$ of A-schemes such that $\mathscr{L} \cong \varphi^*(\mathscr{O}_{\mathbb{P}^r_A}(1))$ and $s_i = \varphi^*(x_i)$.

Proof. See Hartshorne [17, Theorem II.7.1]. □

Corollary 1.3.5. *A very ample sheaf is generated by global sections.*

Proof. This follows directly from Theorem 1.3.4. □

Proposition 1.3.6. *Let X be a smooth projective curve of genus g over a field k. Let $\mathscr{L}$ be an invertible sheaf on X.*

(i) If $\deg(\mathscr{L}) \geqslant 2g$, then $\mathscr{L}$ is generated by global sections.

(ii) If $\deg(\mathscr{L}) \geqslant 2g + 1$, then $\mathscr{L}$ is very ample.

Proof. See Hartshorne [17, Corollary IV.3.2]. □

Proposition 1.3.7. *Let A be a ring.*

(i) If Y is a closed subscheme of $\mathbb{P}^r_A$, then there is a homogeneous ideal $I \subseteq A[x_0, \ldots, x_r]$ such that Y is the closed subscheme determined by I.

(ii) A scheme Y over $\mathrm{Spec}(A)$ *is projective if and only if it is isomorphic to* $\mathrm{Proj}(S)$ *for some graded ring $S = \bigoplus_{d \in \mathbb{Z}} S_d$, where $S_0 = A$ and S is finitely generated by S_1 as an S_0-algebra.*

Proof. See Hartshorne [17, Corollary II.5.16]. □

Let A be a ring and let X be a closed subscheme of $\mathbb{P}^r_A$. The *homogeneous coordinate ring* $S(X)$ of X for the given embedding is defined to be

$$S(X) = A[x_0, \ldots, x_r]/I$$

where I is the homogeneous ideal $\Gamma_*(\mathscr{I}_X)$ associated to the ideal sheaf $\mathscr{I}_X$ of X. A scheme X is *normal* if its local rings are integrally closed domains. A closed subscheme $X \subseteq \mathbb{P}^r_A$ is *projectively normal* for the given embedding if its homogeneous coordinate ring $S(X)$ is an integrally closed domain.

Let $\mathscr{L}$ be an ample invertible sheaf on a scheme X. Then $\mathscr{L}$ is said to be *normally generated* if

$$\Gamma(X, \mathscr{L})^{\otimes n} \to \Gamma(X, \mathscr{L}^{\otimes n})$$

is surjective for all $n \geqslant 1$. This is equivalent to the condition that

$$\Gamma(X, \mathscr{L}^{\otimes i}) \otimes_k \Gamma(X, \mathscr{L}^{\otimes j}) \to \Gamma(X, \mathscr{L}^{\otimes (i+j)})$$

is surjective for all $i, j \geqslant 1$.

Theorem 1.3.8. *Let X be smooth, complete curve of genus g over an algebraically closed field k. Let $\mathscr{M}$ and $\mathscr{N}$ be invertible sheaves on X such that $\deg(\mathscr{M}) \geqslant 2g+1$ and $\deg(\mathscr{N}) \geqslant 2g$. Then the map*

$$\Gamma(X, \mathscr{M}) \otimes_k \Gamma(X, \mathscr{N}) \to \Gamma(X, \mathscr{M} \otimes_{\mathscr{O}_X} \mathscr{N})$$

is surjective.

Proof. See Mumford [31, Theorem 2.6]. □

Corollary 1.3.9. *Let X be a smooth, complete curve of genus g over an algebraically closed field k. If $\mathscr{L}$ is an invertible sheaf on X of degree $\deg(\mathscr{L}) \geqslant 2g+1$, then $\mathscr{L}$ is normally generated.*

Proof. See Mumford [31, Corollary to Theorem 2.6]. □

1.4 The Picard group

Proposition 1.4.1. *If $\mathscr{L}$ and $\mathscr{M}$ are invertible sheaves on a ringed space X, then so is $\mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{M}$. Let $\mathscr{L}$ be an invertible sheaf on X and define*

$$\mathscr{L}^{-1} = \mathrm{Hom}_{\mathscr{O}_X}(\mathscr{L}, \mathscr{O}_X)$$

(this is the dual sheaf of $\mathscr{L}$). Then $\mathscr{L}^{-1}$ is an invertible sheaf on X and

$$\mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{L}^{-1} \cong \mathscr{O}_X.$$

Proof. See Hartshorne [17, Proposition II.6.12]. □

Let X be a ringed space. We define the *Picard group* of X, denoted by $\mathrm{Pic}(X)$, to be the set of isomorphism classes of invertible sheaves on X. Proposition 1.4.1 shows that $\mathrm{Pic}(X)$ is in fact a group under the operation of tensor product of $\mathscr{O}_X$-modules with identity element $\mathscr{O}_X$.

Proposition 1.4.2. *Let X be a scheme. Then we have the following:*

(i) For any Cartier divisor D, the sheaf $\mathscr{O}_X(D)$ is invertible. There is a bijection between $\mathrm{Div}(X)$ and the set of invertible subsheaves of $\mathscr{K}$ given by $D \mapsto \mathscr{O}_X(D)$.

(ii) For any two Cartier divisors D_1 and D_2 on X,

$$\mathscr{O}_X(D_1 - D_2) \cong \mathscr{O}_X(D_1) \otimes_{\mathscr{O}_X} \mathscr{O}_X(D_2)^{-1}.$$

(iii) Let D_1 and D_2 be two Cartier divisors on X. Then $D_1 \sim_{\mathrm{rat}} D_2$ if and only if $\mathscr{O}_X(D_1) \cong \mathscr{O}_X(D_2)$ as invertible sheaves.

Proof. See Hartshorne [17, Proposition II.6.13]. □

Theorem 1.4.3. *Let X be a scheme and define a map*

$$\varphi : \mathrm{CaCl}(X) \to \mathrm{Pic}(X) \qquad \text{by} \qquad D \mapsto \mathscr{O}_X(D).$$

Then φ is an injective homomorphism. If X is integral, then φ is an isomorphism.

Proof. See Hartshorne [17, Corollary II.6.14, Proposition II.6.15]. □

If X is a projective, flat S-scheme with integral geometric fibres, then the Picard group of X has the structure of a scheme (see Kleiman [24, Theorem 4.8]). We denote by $\mathrm{Pic}^0(X)$ the union of the connected components of the identity of $\mathrm{Pic}(X_s)$ for $s \in S$.

Theorem 1.4.4. *Let k be an algebraically closed field and let X be a smooth projective variety over k. Then $\mathrm{Pic}^0(X)$ is an abelian variety. If X is a curve, then $\mathrm{Pic}^0(X)$ is dual to the Jacobian of X.*

Proof. See Kleiman [24, Remarks 5.24, 5.25 and 5.26]. □

A morphism of schemes $f : X \to Y$ induces a homomorphism

$$f^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$$

sending $\mathscr{M}$ on Y to $f^*\mathscr{M}$ on X, which in turn induces a homomorphism

$$f^* : \mathrm{Pic}^0(Y) \to \mathrm{Pic}^0(X).$$

In particular, for any invertible sheaves $\mathscr{L}$ and $\mathscr{M}$ on Y,

$$f^*(\mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{M}) \cong f^*\mathscr{L} \otimes_{\mathscr{O}_Y} f^*\mathscr{M}. \tag{1.2}$$

1.5 Quotient varieties

Theorem 1.5.1. *Let X be an variety over an algebraically closed field k and let G be a finite subgroup of $\mathrm{Aut}(X)$. Suppose that, for any $x \in X$, the orbit of x is contained in an affine open subset of X. Then there is a variety Y and a morphism $\pi : X \to Y$ satisfying the following properties:*

(i) As a topological space, Y is the quotient of X for the action of G; that is, $Y = X/G$ as a set and $U \subset Y$ is open if and only if $\pi^{-1}(U)$ is open.

(ii) For any open affine set $U \subset Y$, we have

$$\Gamma(U, \mathscr{O}_Y) = \Gamma(\pi^{-1}(U), \mathscr{O}_X)^G$$

where $\Gamma(\pi^{-1}(U), \mathscr{O}_X)^G$ denotes the elements of $\Gamma(\pi^{-1}(U), \mathscr{O}_X)$ fixed by the action of G.

These conditions determine the pair (Y, π) up to isomorphism. The morphism π is finite, surjective and separable. If X is affine, then so is Y.

Proof. See Mumford [32, Theorem 7.1]. □

The pair (Y, π) appearing in Theorem 1.5.1 is called the *geometric quotient* of X by G.

Let $G \subseteq \mathrm{Aut}(X)$ be a finite group acting on X, let $\pi : X \to X/G$ be the quotient, and let $\mathscr{F}$ be a coherent sheaf on X/G. For any $g \in G$, we have $\pi = \pi \circ g$ and it follows that g induces an automorphism $g^* : \pi^*\mathscr{F} \to \pi^*\mathscr{F}$. Hence G acts on $\pi^*\mathscr{F}$ in a manner compatible with the action on X. We define a coherent *G-sheaf* on X to be a coherent $\mathscr{O}_X$-module on X on which G acts in a manner compatible with the action on X.

Let $\mathscr{F}$ be a sheaf on X. Recall that the direct image of $\mathscr{F}$ is defined by $\Gamma(V, \pi_*\mathscr{F}) = \Gamma(\pi^{-1}(V), \mathscr{F})$ for all open $V \subseteq X/G$. If $\mathscr{F}$ is a G-sheaf on X, then, for all open $V \subseteq X/G$, the group G acts on $\Gamma(\pi^{-1}(V), \mathscr{F})$ and hence $\pi_*\mathscr{F}$ is a G-sheaf on X/G since G acts trivially on X/G. For any G-sheaf $\mathscr{F}$ on X we denote by $\pi_*(\mathscr{F})^G$ the sheaf on X/G defined by

$$V \mapsto \Gamma(V, \pi_*\mathscr{F})^G = \Gamma(\pi^{-1}(V), \mathscr{F})^G.$$

The following result is a modification of Mumford [32, Proposition 7.2] where we have removed the condition that G act freely, but we impose the condition that $\mathscr{L}$ be locally free.

Proposition 1.5.2. *Let $\pi : X \to X/G$ be the geometric quotient of a variety X by a finite group of automorphisms G, and let $\mathscr{L}$ be a locally free sheaf on X/G. Then $\mathscr{L} \cong \pi_*(\pi^*\mathscr{L})^G$ and, in particular,*

$$\Gamma(X/G, \mathscr{L}) \cong \Gamma(X, \pi^*\mathscr{L})^G.$$

Proof. We first reduce to the affine case as in the proof of Mumford [32, Theorem 7.1]. For any x in X, let U' be an open affine subset of X containing the orbit Gx of x. Then $U = \bigcap_{g\in G} gU'$ is an affine open subset of X containing x which is stable under the action of G. Thus X has a covering of G-stable affine open sets U. If the proposition holds for X and X/G affine, then $\mathscr{L}(U) \cong \pi_*(\pi^*\mathscr{L})^G(U)$ for this covering and consequently $\mathscr{L} \cong \pi_*(\pi^*\mathscr{L})^G$.

Now assume $X = \mathrm{Spec}(A)$ is affine, so $X/G = \mathrm{Spec}(B)$ with $B = A^G$, and let $\Gamma(X/G, \mathscr{L}) = M$. We have

$$\Gamma(X/G, \pi_*(\pi^*\mathscr{L})^G) = \Gamma(X, \pi^*\mathscr{L})^G \cong (M \otimes_B A)^G \cong M^G,$$

so it suffices to prove that $M = M^G$. As M is locally free, we can assume that B is local and M is free, in which case the result follows from the fact that $(B^r)^G = (B^G)^r = B^r$ for any $r \geqslant 1$. □

Let X be a variety. The symmetric group $\mathfrak{S}_n$ in n letters acts on the n coordinates of the n-fold product $X^n = X \times \cdots \times X$ by permutation. We define the *nth symmetric product* of X, denoted by $\mathrm{Sym}^n(X)$, to be the geometric quotient of X^n by $\mathfrak{S}_n$; the symmetric product exists by Theorem 1.5.1. If X is a smooth curve, then $\mathrm{Sym}^n(X)$ will be smooth. Moreover the effective divisors of degree d can be identified with points on $\mathrm{Sym}^d(X)$.

1.6 Abelian varieties

An *abelian variety* is a complete group variety. An abelian variety of dimension one is called an *elliptic curve* and an abelian variety of dimension two is called an *abelian surface*. The group law on an abelian variety is always commutative (see Milne [27, Corollary 2.4]) and every abelian variety is projective (see Milne [27, Theorem 7.1]). A *morphism* of abelian varieties $\varphi : \mathcal{A} \to \mathcal{B}$ is a morphism of varieties that is also a group homomorphism with respect to the group laws of $\mathcal{A}$ and $\mathcal{B}$. If φ is finite and surjective it is called an *isogeny*, and two abelian varieties are said to be *isogenous* if there exists an isogeny between them.

Let $\mathscr{L}$ be an invertible sheaf on an abelian variety $\mathcal{A}$. To $\mathscr{L}$ we associate a map $\varphi_{\mathscr{L}} : \mathcal{A} \to \mathrm{Pic}(\mathcal{A})$ defined by $x \mapsto \tau_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$, where $\tau_x^* : \mathcal{A} \to \mathcal{A}$ is the translation-by-x map on $\mathcal{A}$. We define $K_{\mathscr{L}}$ to be

$$K_{\mathscr{L}} = \{x \in \mathcal{A} \mid \tau_x^*\mathscr{L} \cong \mathscr{L}^{-1}\};$$

it is a reduced closed subscheme of $\mathcal{A}$ (see Milne [27, Section 9]). If $\mathscr{L} = \mathscr{O}_A(D)$ for a divisor D on $\mathcal{A}$, we write φ_D for $\varphi_{\mathscr{L}}$ and K_D for $K_{\mathscr{L}}$.

Theorem 1.6.1. *Let $\mathcal{A}$ be an abelian variety of dimension g, and let $\mathscr{L}$ be an invertible sheaf on $\mathcal{A}$. Then*

(i) The degree of $\varphi_{\mathscr{L}}$ is $\chi(\mathscr{L})^2$.

(ii) If $\dim K_{\mathscr{L}} = 0$, then there exists a unique integer $r = r(\mathscr{L})$, $0 \leqslant r \leqslant g$, such that $H^i(\mathcal{A}, \mathscr{L}) = 0$ for $i \neq r$ and $H^r(\mathcal{A}, \mathscr{L}) \neq 0$.

Proof. See Milne [27, Theorem 13.3]. □

There is a canonical way to attach an abelian variety to a curve, as described in the following theorem.

Theorem 1.6.2. *Let X be a smooth projective curve of genus $g \geqslant 1$ over a field k. Then there exists an abelian variety J_X over k and an injection*

$$j : X \to J_X$$

(not necessarily defined over k) with the following properties:

(i) If j is extended linearly to divisors on X, then the induced group homomorphism

$$\mathrm{Pic}^0(X) \to J_X$$

is an isomorphism.

(ii) Let W_0 be the subvariety $\{0\}$ of J_X and for each $r \geqslant 1$, define W_r to be the image in J_X of the map

$$\mathrm{Sym}^r(X) \to J_X$$

defined by

$$(P_1, \ldots, P_r) \mapsto \sum_{i=1}^{r} j(P_i).$$

Then $\dim(W_r) = \min\{r, g\}$ and W_g is birationally equivalent to J_X. In particular, $\dim(J_X) = g$.

Proof. See Hindry and Silverman [18, Theorem A.8.1.1] for a sketch of the above result. A more intrinsic account can be found in the survey of Milne [28], who describes the variety J_X as representing the functor Pic^0. □

The variety J_X appearing in Theorem 1.6.2 is called the *Jacobian* of the curve X and the map j is called the *Abel-Jacobi map*. The *theta divisor* on J_X is the divisor W^{g-1}; it is effective and moreover ample (see Milne [28, Section 6]).

Remark 1.6.3. Note that, if X is defined over k, then J_X will be defined over k, however it may not be possible to define Abel-Jacobi map over k. The injection j is defined by choosing a divisor D on X of degree one and sending a point P on X to the class

$$j(P) = [(P) - D]$$

where (P) denotes the divisor corresponding to P. As D has degree one, $j(P)$ has degree zero and hence gives a valid element of $\mathrm{Pic}^0(X) \cong J_X$. If X has a known k-rational point P_0, then taking $D = (P_0)$ allows one to define j over k.

1.7 Hyperelliptic curves

Let k be a field and let X be a smooth, geometrically connected curve of genus $g \geqslant 2$ over k. Then X is called a *hyperelliptic curve* if there exists a finite separable morphism

$$\kappa_X : X \to \mathbb{P}^1_k$$

of degree 2. A hyperelliptic curve X always comes endowed with a Cartier divisor D_0 such that $\dim \Gamma(X, \mathscr{O}_X(D_0)) = \deg(D_0) = 2$ (Liu [26, Lemma 7.4.8]), though D_0 is not guaranteed to be defined over k, nor is D_0 unique (indeed, any divisor $\kappa_X^{-1}(u)$ for some rational point $u \in \mathbb{P}^1_k$ will produce a divisor of degree 2). All smooth geometrically connected curves of genus 2 are hyperelliptic (Liu [26, Proposition 7.4.9]), however when the genus is greater than 2, being hyperelliptic becomes a rather special property.

Proposition 1.7.1. *Let X be a hyperelliptic curve of genus g over a field k. Let D_0 be the divisor $\kappa_X^{-1}(\infty)$ on X of degree 2. Then $\mathscr{O}_X((g+1)D_0)$ is normally generated. In particular, it is very ample and hence generated by global sections. There exists a basis for $\Gamma(X, \mathscr{O}_X((g+1)D_0))$ of the form*

$$\{1, x, x^2, \ldots, x^g, y, x^{g+1}\}$$

such that $k(X) = k(x)[y]$ is the function field of X.

Proof. That $\mathscr{O}_X((g+1)D_0)$ is normally generated follows from Corollary 1.3.9 since $\deg(\mathscr{O}_X((g+1)D_0)) = 2(g+1) > 2g+1$. That $\mathscr{O}_X((g+1)D_0)$ is very ample follows from Proposition 1.3.6(ii) and so it is generated by global sections.

Since $\dim \Gamma(X, \mathscr{O}_X(D_0)) = 2$, it has a basis $\{1, x\}$. The set of functions $\{1, x, \ldots, x^i\}$ is linearly independent in $\Gamma(X, \mathscr{O}_X(iD_0))$, hence

$$\dim \Gamma(X, \mathscr{O}_X(iD_0)) \geqslant i + 1.$$

Since $\deg((g+1)D_0) > 2g-2$, Corollary 1.2.8 implies that

$$\dim \Gamma\Big(X, \mathscr{O}_X((g+1)D_0)\Big) = \deg\Big((g+1)D_0\Big) + 1 - g = g+3.$$

Thus there exists a function y in $\Gamma(X, \mathscr{O}_X((g+1)D_0))$ which is linearly independent of the $g+2$ elements $\{1, x, x^2, \ldots, x^{g+1}\}$, and the result follows. □

The following proposition shows that the defining equations of a hyperelliptic curve have a rather rigid form.

Proposition 1.7.2. *Let k be a field and let X/k be a hyperelliptic curve of genus g.*

(i) The function field of X is given by $k(X) = k(x)[y]$ with the defining relation

$$y^2 + h(x)y = f(x) \tag{1.3}$$

where h and f are polynomials in $k[x]$ whose degrees are at most $g+1$ and $2g+2$ respectively. If, moreover, $\operatorname{char}(k) \neq 2$, then we can assume that $h = 0$.

(ii) The curve X is covered by the open affine schemes

$$U = \operatorname{Spec} k[x,y]/\Big(y^2 + h(x)y - f(x)\Big)$$
$$V = \operatorname{Spec} k[u,v]/\Big(v^2 + h'(u)v - f'(u)\Big)$$

where $h'(u) = h(1/u)u^{g+1}$ and $f'(u) = f(1/u)u^{2g+2}$ and the two patches glue along the open sets $D(u) \simeq D(x)$ with relations $u = 1/x$ and $v = y/x^{g+1}$ (where $D(u)$ is the basic open set $\operatorname{Spec}(\mathscr{O}_U(U)[1/u])$ and similarly for $D(x)$).

Proof. See Liu [26, Proposition 7.4.24]. □

An equation of the form (1.3) is called an *affine model* for a hyperelliptic curve. If

$$y^2 + h(x)y = f(x) \qquad \text{and} \qquad v^2 + h'(u)v = f'(u)$$

are two affine models for a hyperelliptic curve X of genus $g \geqslant 2$, then there exists a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{GL}_2(k)$, an element $e \in k^*$, and a polynomial $H \in k[x]$ of degree at most $g+1$ such that

$$u = \frac{ax+b}{cx+d} \qquad \text{and} \qquad v = \frac{H(x) + ey}{(cx+d)^{g+1}} \tag{1.4}$$

(see Liu [26, Corollary 7.4.33(a)]).

Let X be a hyperelliptic curve over k. The generator η of $\mathrm{Gal}(k(X)/k(x))$ induces an automorphism of order 2 of X, also denoted by η, called the *hyperelliptic involution* of X. The hyperelliptic involution of X is unique if the genus of X is at least 2 (Liu [26, Proposition 7.4.29]). The non-uniqueness of the rational subfield of degree 2 and the corresponding involution in the case of elliptic curves is the reason why elliptic curves are not generally subsumed in the definition of hyperelliptic curves.

Part I

Relative curves and their Jacobians

Chapter 2

Divisors on relative curves

In this chapter we prove that natural generalisations of Khuri-Makdisi [22, Lemmas 2.2 and 2.3] continue to hold in the case of relative effective Cartier divisors on projective schemes which are smooth of relative dimension one over an arbitrary affine Noetherian base scheme.

Throughout this chapter we fix a scheme $S = \operatorname{Spec}(R)$ where R is a Noetherian ring. We use the following notation: let X be an S-scheme, let s be a closed point of S and let $\mathscr{L}$ be sheaf on X. Denote the the maximal ideal of the local ring $\mathscr{O}_{S,s}$ by $\mathfrak{m}_s$ and its residue field by $k(s) = \mathscr{O}_{S,s}/\mathfrak{m}_s$. Denote the fibre of X above s by $X_s = X \times_S \operatorname{Spec} k(s)$, the projection map from X_s to X by $\rho_s : X_s \to X$, and set $\mathscr{L}_s = \rho_s^* \mathscr{L}$.

2.1 Relative effective Cartier divisors

We begin by recalling some facts about relative effective Cartier divisors. This material can be found in Katz and Mazur [20, Chapter 1]. Let $f : X \to S$ be an S-scheme. Recall (see Section 1.1) that an effective Cartier divisor is a closed subscheme $\iota : D \to X$ of X whose ideal sheaf is invertible. We call D a *relative effective Cartier divisor* if $f \circ \iota : D \to S$ is flat.

The set of relative effective Cartier divisors on X is closed under the usual sum of Cartier divisors. If $T \to S$ is another S-scheme, then for any relative effective Cartier divisor D on X, the fibre $D_T = D \times_S T$ is a relative effective Cartier divisor on $X_T = X \times_S T$. If $f : Y \to X$ is a flat morphism of S-schemes, then $f^*(D)$ is a relative effective Cartier divisor on Y. The usual correspondence between isomorphism classes of invertible sheaves and effective Cartier divisors carries over to a correspondence between isomorphism classes of invertible sheaves flat over S and relative effective Cartier divisors.

Proposition 2.1.1. *Let X be a flat S-scheme of finite type and let D be an effective divisor on X. Then D is a relative effective Cartier divisor on X if and only if, for all geometric points $\mathrm{Spec}(\overline{k}) \to S$, the closed subscheme $D_{\overline{k}}$ is a relative effective Cartier divisor on $X_{\overline{k}}$.*

Proof. See Katz and Mazur [20, Corollary 1.1.5.2]. □

We now look more closely at the case where the fibres of X/S form a flat family of smooth curves. We will call X/S a *relative curve* if X is a smooth projective S-scheme of relative dimension one whose geometric fibres are connected. Therefore X corresponds to a family of geometrically connected, smooth, projective algebraic curves parametrised by S. A relative effective Cartier divisor on a relative curve X/S is automatically proper over S.

Proposition 2.1.2. *Let X/S be a relative curve and let $\mathscr{L}$ be an invertible sheaf on X. Then the mapping*

$$\chi(\mathscr{L}) : S \to \mathbb{Z} \qquad \textit{defined by} \qquad s \mapsto \chi(\mathscr{L}_s)$$

is locally constant on S.

Proof. See Grothendieck [15, Théorème 7.4.3]. □

Proposition 2.1.2 shows that the genus map $g_X : S \to \mathbb{Z}$ sending $s \mapsto g_{X_s}$ of a relative curve is locally constant where g_{X_s} denotes the genus of the algebraic curve X_s. Hence by Riemann-Roch, the degree function $\deg(\mathscr{L}) : S \to \mathbb{Z}$ defined by $s \mapsto \deg(\mathscr{L}_s)$ is locally constant on S. If D is a relative effective Cartier divisor on X, then $\deg(D)$ is given by $\deg(\mathscr{O}_X(D))$.

Proposition 2.1.3. *Let X/S be a relative curve and let D_1 and D_2 be relative effective Cartier divisors on X. Then*

$$\deg(D_1 + D_2) = \deg(D_1) + \deg(D_2).$$

Proof. See Katz and Mazur [20, Lemma 1.2.6]. □

Proposition 2.1.4. *Let X/S be a relative curve and let D be a relative effective Cartier divisor on X. Then for any S-scheme T, we have*

$$\deg(D_T) = \deg(D).$$

Proof. See Katz and Mazur [20, Lemma 1.2.9]. □

Proposition 2.1.5. *Let X/S be a relative curve and let D and D' relative effective Cartier divisors on X satisfying $D' \subset D$. Then there exists a relative effective Cartier divisor D'' such that $D = D' + D''$ and the degree of D'' satisfies*

$$\deg(D'') = \deg(D) - \deg(D').$$

Proof. See Katz and Mazur [20, Section 1.3]. □

Proposition 2.1.6. *Let X/S be a relative curve and let D and D' be relative effective Cartier divisors on X satisfying $D' \subset D$. Then the cokernel of the injection $\mathscr{O}_X(D') \to \mathscr{O}_X(D)$ is flat over S.*

Proof. By Proposition 2.1.5 we have a relative effective Cartier divisor $D'' = D - D'$; let $\iota : D'' \to X$ be the embedding. Tensoring the exact sequence

$$0 \to \mathscr{I}_{D''} \to \mathscr{O}_X \to \iota_* \mathscr{O}_{D''} \to 0$$

with $\mathscr{O}_X(D)$ yields the exact sequence

$$0 \to \mathscr{O}_X(D') \to \mathscr{O}_X(D) \to \mathscr{O}_X(D) \otimes \iota_* \mathscr{O}_{D''} \to 0$$

because

$$\mathscr{I}_{D''} \otimes \mathscr{O}_X(D) \cong \mathscr{O}_X(-D'') \otimes \mathscr{O}(D) \cong \mathscr{O}_X(D - D'') \cong \mathscr{O}_X(D').$$

Hence the cokernel of $\mathscr{O}_X(D') \to \mathscr{O}_X(D)$ is given by $\mathscr{O}_X(D) \otimes \iota_* \mathscr{O}_{D''}$, which is flat because it is the tensor product of flat sheaves. □

Proposition 2.1.7. *Let R be a Noetherian ring, let $S = \operatorname{Spec}(R)$, let X/S be a relative curve and let $\mathscr{F}$ be an $\mathscr{O}_X$-module which is flat over S. If $H^1(X, \mathscr{F})$ is a projective R-module, then so is $H^0(X, \mathscr{F})$.*

Proof. Let $\mathfrak{U} = \{U_i\}_{i \in I}$ be an open affine covering of X which is closed under intersection. Since X is Noetherian we may assume that I is finite, say $I = \{1, \ldots, n\}$. Write $U_{ij} = U_i \cap U_j$. Consider the map of Čech modules

$$d_0 : \prod_{i=1}^{n} H^0(U_i, \mathscr{F}) \to \prod_{1 \leqslant i < j \leqslant n} H^0(U_{ij}, \mathscr{F})$$

where d_0 is the boundary map, defined by sending $(f_i)_{i \in I}$ to the element $(f_i|_{U_{ij}} - f_j|_{U_{ij}})_{1 \leqslant i < j \leqslant n}$. Then $H^0(X, \mathscr{F}) = \operatorname{Ker}(d_0)$ by definition and we have $H^1(X, \mathscr{F}) = \operatorname{Coker}(d_0)$ since the higher cohomology groups vanish by Theorem 1.2.4(i). Note that, since $\mathscr{F}$ is flat, the modules $\prod_{i=1}^{n} H^0(U_i, \mathscr{F})$ and $\prod_{1 \leqslant i < j \leqslant n} H^0(U_{ij}, \mathscr{F})$ are finite direct products of flat R-modules and so are flat over R.

Now, since $H^1(X, \mathscr{F})$ is projective, we obtain an exact sequence

$$0 \to \mathrm{Im}(d_0) \to \prod_{1 \leqslant i < j \leqslant n} H^0(U_{ij}, \mathscr{F}) \to H^1(X, \mathscr{F}) \to 0.$$

Hence $\mathrm{Im}(d_0)$ is flat since both $\prod H^0(U_{ij}, \mathscr{F})$ and $H^1(X, \mathscr{F})$ are flat. Thus, from the induced short exact sequence

$$0 \to H^0(X, \mathscr{F}) \to \prod_{i=1}^{n} H^0(U_i, \mathscr{F}) \to \mathrm{Im}(d_0) \to 0,$$

we see that $H^0(X, \mathscr{F})$ is flat since both $\prod H^0(U_i, \mathscr{F})$ and $\mathrm{Im}(d_0)$ are flat. Therefore $H^0(X, \mathscr{F})$ is a finitely generated R-module (by Theorem 1.2.3) and flat which implies it is projective (see Weibel [39, Theorem 3.2.7]). □

Corollary 2.1.8. *Let X/S be a relative curve and let D and D' be relative effective Cartier divisors on X satisfying $D' \subset D$. If $H^1(X, \mathscr{O}_X(D)) = 0$ and $H^1(X, \mathscr{O}_X(D')$ is projective, then the cokernel of the injection*

$$\varphi : H^0(X, \mathscr{O}_X(D')) \to H^0(X, \mathscr{O}_X(D))$$

is projective.

Proof. Let $\mathscr{F} = \mathscr{O}_X(D)/\mathscr{O}_X(D')$. From the short exact sequence of $\mathscr{O}_X$-modules

$$0 \to \mathscr{O}_X(D') \to \mathscr{O}_X(D) \to \mathscr{F} \to 0$$

we obtain the long exact sequence

$$\begin{aligned} 0 \to H^0(X, \mathscr{O}_X(D')) &\xrightarrow{\varphi} H^0(X, \mathscr{O}_X(D)) \to H^0(X, \mathscr{F}) \\ &\to H^1(X, \mathscr{O}_X(D')) \to H^1(X, \mathscr{O}_X(D)) \to H^1(X, \mathscr{F}) \to 0. \end{aligned}$$

Then $H^1(X, \mathscr{F}) = 0$ since $H^1(X, \mathscr{O}_X(D)) = 0$. Proposition 2.1.6 implies that $\mathscr{F}$ is flat and so $H^0(X, \mathscr{F})$ is projective by Proposition 2.1.7. Thus

$$H^0(X, \mathscr{F}) \cong \mathrm{Coker}(\varphi) \oplus H^1(X, \mathscr{O}_X(D'))$$

since $H^1(X, \mathscr{O}_X(D'))$ is projective. Therefore $\mathrm{Coker}(\varphi)$ is projective. □

All the modules with which we will be dealing in the remainder of this chapter are either global sections of a relative effective Cartier divisor, or the cokernel of a homomorphism between such modules. Together, Proposition 2.1.7 and Corollary 2.1.8 show that all such modules are projective.

2.2 Criteria for very ampleness

Let $f: X \to Y$ be a morphism of schemes and let $\mathscr{F}$ be a coherent sheaf on X. Then the *ith higher direct image* of $\mathscr{F}$ is the sheaf $R^i f_*(\mathscr{F})$ associated to the presheaf

$$V \mapsto H^i(f^{-1}(V), \mathscr{F}|_{f^{-1}(V)})$$

on Y. The most important property of $R^i f_*(\mathscr{F})$ for our purposes is given by the following proposition.

Proposition 2.2.1. *Let X be a Noetherian scheme, let $Y = \mathrm{Spec}(A)$ be an affine scheme, and let $f: X \to Y$ be a morphism. Then for any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ on X, we have*

$$R^i f_*(\mathscr{F}) \cong H^i(X, \mathscr{F})^{\sim}$$

where $H^i(X, \mathscr{F})^{\sim}$ denotes the sheaf on Y associated to the A-module $H^i(X, \mathscr{F})$.

Proof. See Hartshorne [17, Chapter III, Proposition 8.5]. □

Theorem 2.2.2. *Let $f: X \to S$ be a projective morphism of Noetherian schemes and let $\mathscr{F}$ be a coherent sheaf on X which is flat over S. Let s be a point in S.*

(i) If the natural map

$$\varphi(s)^i: R^i f_*(\mathscr{F}) \otimes k(s) \to H^i(X_s, \mathscr{F}_s)$$

is surjective, then it is an isomorphism in a neighbourhood of s.

(ii) If $\varphi(s)^i$ is surjective, then the following conditions are equivalent.

(a) $\varphi(s)^{i-1}$ is surjective;

(b) $R^i f_*(\mathscr{F})$ is locally free in a neighbourhood of s.

Proof. See Hartshorne [17, Chapter III, Theorem 12.11]. □

Proposition 2.2.3. *For $0 < i < n$ and all $d \in \mathbb{Z}$ we have*

$$H^i(\mathbb{P}^n_S, \mathscr{O}_{\mathbb{P}^n_S}(d)) = 0.$$

Proof. See Hartshorne [17, Chapter III, Theorem 5.1(b)]. □

The following two lemmas give convenient reformulations of Nakayama's Lemma (see Atiyah and Macdonald [1, Proposition 2.6]).

Lemma 2.2.4. *Let A be a ring and let M be a finitely generated A-module. If $M/\mathfrak{m}M = 0$ for all maximal ideals $\mathfrak{m}$ of A, then $M = 0$.*

Proof. We have $M = 0$ if and only if $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$ of A, so we reduce to the case where A is local. Then $\mathfrak{m}$ coincides with the Jacobson radical of A and so the result follows by Nakayama's Lemma. □

Lemma 2.2.5. *Let A be a ring, let $u : M \to N$ be a homomorphism of A-modules, and assume that N is finitely generated. If the induced homomorphisms $u_{\mathfrak{m}} : M/\mathfrak{m}M \to N/\mathfrak{m}N$ are surjective for all maximal ideals $\mathfrak{m}$ of A, then u is surjective.*

Proof. By assumption $N/u(M) \otimes A/\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m} \subset A$, hence $u(M) = N$ by Lemma 2.2.4. □

Lemma 2.2.6. *For all $d \geqslant 1$ we have*

$$H^1(\mathbb{P}^1_S, \mathscr{O}_{\mathbb{P}^1_S}(d)) = 0.$$

Proof. Let s be a closed point of S and let $k = k(s)$. Then by Theorem 1.2.4(ii), we have

$$H^1(\mathbb{P}^1_k, \mathscr{O}_{\mathbb{P}^1_k}(d)) = H^0(\mathbb{P}^1_k, \omega_{\mathbb{P}^1_k} \otimes \mathscr{O}_{\mathbb{P}^1_k}(-d)) = 0$$

where $\omega_{\mathbb{P}^1_k}$ is the canonical sheaf on $\mathbb{P}^1_k$, and so the natural map

$$\pi\colon H^1(\mathbb{P}^1_S, \mathscr{O}_{\mathbb{P}^1_S}(d)) \to H^1(\mathbb{P}^1_k, \mathscr{O}_{\mathbb{P}^1_k}(d))$$

is (trivially) surjective. Then Theorem 2.2.2(i) implies that π is an isomorphism and so $H^1(\mathbb{P}^1_S, \mathscr{O}_{\mathbb{P}^1_S}(1)) \otimes k(s) = 0$ for all closed s. The result then follows from Lemma 2.2.4. □

Proposition 2.2.7. *Let X/S be a relative curve and let $\mathscr{L}$ be a very ample invertible sheaf on X/S. Then $H^1(X, \mathscr{L}) = 0$.*

Proof. As $\mathscr{L}$ is very ample we have $\mathscr{L} \cong \iota^* \mathscr{O}_{\mathbb{P}^n}(1)$ for some $n \geqslant 1$. Then

$$H^1(X, \mathscr{L}) \cong H^1(\mathbb{P}^n, \iota_* \iota^* \mathscr{O}_{\mathbb{P}^n}(1)) \cong H^1(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(1)) = 0$$

where the last equality follows from Proposition 2.2.3 when $n \geqslant 2$ from and Lemma 2.2.6 when $n = 1$. □

Proposition 2.2.8. *Let $f : X \to S$ be a relative curve over $S = \operatorname{Spec}(R)$ and let $\mathscr{L}$ be a very ample invertible sheaf on X. Then for all closed points $s \in S$, we have*

$$H^0(X, \mathscr{L}) \otimes_R k(s) \cong H^0(X_s, \mathscr{L}_s).$$

Proof. Let s be a closed point in S. We have $H^1(X, \mathscr{L}) = 0$ by Proposition 2.2.7 so $R^1 f_*(\mathscr{L})$ and $H^1(X_s, \mathscr{L}_s)$ are zero. Hence $\varphi(s)^1$ is (trivially) surjective and $R^1 f_*(\mathscr{L})$ is (trivially) locally free at s. Thus $\varphi(s)^0 : R^0 f_*(\mathscr{L}) \otimes k(s) \to H^0(X_s, \mathscr{L}_s)$ is surjective by Theorem 2.2.2(ii) and therefore an isomorphism by Theorem 2.2.2(i). Taking global sections we see that $H^0(X, \mathscr{L}) \otimes k(s) \cong H^0(X_s, \mathscr{L}_s)$ as required. □

Let $\mathscr{L}$ be a locally free coherent sheaf on a Noetherian scheme X. Let $\mathrm{Sym}^d(\mathscr{L})$ denote the dth symmetric tensor product of $\mathscr{L}$ and let $\mathscr{S} = \bigoplus_{d \geqslant 0} \mathrm{Sym}^d(\mathscr{L})$ be the symmetric algebra of $\mathscr{L}$. It is a sheaf of $\mathscr{O}_X$-algebras. The *projective space bundle* of $\mathscr{L}$ is defined to be the global Proj of $\mathscr{S}$, and is denoted by $\mathbb{P}(\mathscr{L})$.

Proposition 2.2.9. *Let $f : X \to S$ be a quasi-compact morphism and let $\mathscr{L}$ be an invertible sheaf on X. Then $\mathscr{L}$ is very ample if and only if*

(i) the canonical map $f^* f_* \mathscr{L} \to \mathscr{L}$ is surjective, and

(ii) the induced map $X \to \mathbb{P}(f_* \mathscr{L})$ is an immersion.

Proof. See Grothendieck [14, Proposition 4.4.4] □

Corollary 2.2.10. *Let $f : X \to S$ be a quasi-compact morphism of schemes and let $\mathscr{L}$ be an invertible sheaf on X. Then $\mathscr{L}$ is very ample if and only if there exists an open covering $\{U_\alpha\}$ of S such that $\mathscr{L}|_{f^{-1}(U_\alpha)}$ is very ample relative to U_α for all α.*

Proof. See Grothendieck [14, Corollaire 4.4.5]. □

Proposition 2.2.11. *Let X/S be a scheme and let $\mathscr{L}$ and $\mathscr{L}'$ be very ample $\mathscr{O}_X$-modules. Then $\mathscr{L} \otimes \mathscr{L}'$ is very ample.*

Proof. See Grothendieck [14, Corollaire 4.4.9(ii)]. □

Proposition 2.2.12. *Let $f : X \to S$ be a relative curve, let $\mathscr{L}$ be an invertible sheaf on X. Then $\mathscr{L}$ is very ample if and only if $\mathscr{L}_s$ is very ample for all closed points $s \in S$.*

Proof. Suppose $\mathscr{L}$ is very ample and let $s \in S$ be a closed point. By definition $\mathscr{L}$ induces a closed immersion $\iota : X \to \mathbb{P}^n_S$ such that $\mathscr{L} \cong \iota^* \mathscr{O}_{\mathbb{P}^n_S}(1)$. Very ampleness is local on S by Corollary 2.2.10, so $\mathscr{L}_s \cong (\iota \times \mathrm{id}_{k(s)})^* \mathscr{O}_{\mathbb{P}^n_{k(s)}}(1)$ gives a closed immersion and hence $\mathscr{L}_s$ is very ample.

To see the converse, we check the conditions of Proposition 2.2.9, noting that they hold on each closed fibre. Since $f_s^*(f_s)_* \mathscr{L}_s \to \mathscr{L}_s$ is surjective, it is surjective on stalks. Hence $f^* f_* \mathscr{L} \to \mathscr{L}$ is surjective on stalks by

Nakayama's Lemma and is thus surjective. Secondly, $i_{\mathscr{L}_s} : X_s \to \mathbb{P}((f_s)_*\mathscr{L}_s)$ is a closed immersion for each closed $s \in S$ and $H^0(X, \mathscr{L}) \otimes k(s) \cong H^0(X_s, \mathscr{L}_s)$ follows from Proposition 2.2.8. Hence $\mathbb{P}((f_s)_*\mathscr{L}_s) \cong \mathbb{P}(f_*\mathscr{L}) \times \mathrm{Spec}(k(s))$ for all closed s and so $i_{\mathscr{L}} : X \to \mathbb{P}(f_*\mathscr{L})$ is a closed immersion. □

Corollary 2.2.13. *Let X/S be a relative curve of genus g and let $\mathscr{L}$ be an invertible sheaf on X. If $\deg(\mathscr{L}) \geqslant 2g+1$, then $\mathscr{L}$ is very ample.*

Proof. The lower bound on the degree implies that $\mathscr{L}_s$ is very ample for all closed points $s \in S$ by Riemann-Roch. Hence $\mathscr{L}$ is very ample by Proposition 2.2.12. □

2.3 Tensor products and sheaf quotients

In this section we prove Propositions 2.3.5 and 2.3.7, which form the basis of all the algorithms for performing divisor arithmetic described in the next chapter. These two propositions are generalisations of Khuri-Makdisi [22, Lemmas 2.2 and 2.3] to the case of relative curves. Given a very ample sheaf $\mathscr{L}$ on a relative curve X over $\mathrm{Spec}(R)$, these two propositions amount to a description of the R-algebra structure of the homogeneous coordinate ring $\bigoplus_{i \geqslant 1} H^0(X, \mathscr{L}^i)$ of X with respect to the embedding by $\mathscr{L}$. Propositions 2.3.5 will be realised explicitly in Algorithm 3.4.1 and Proposition 2.3.7 in Algorithm 3.4.2.

Recall that an ample invertible sheaf $\mathscr{L}$ on a relative curve X/S is *normally generated* if the maps

$$H^0(X, \mathscr{L})^{\otimes d} \to H^0(X, \mathscr{L}^d)$$

are surjective for all $d \geqslant 1$.

The following proposition is a direct generalisation of a proof of Mumford [31, pp38–39].

Proposition 2.3.1. *Let X/S be a relative curve and let $\mathscr{L}$ be an invertible sheaf on X. If $\mathscr{L}$ is normally generated, then it is very ample.*

Proof. Let $\mathscr{L}$ be normally generated. As $\mathscr{L}$ is ample we obtain morphisms

$$\varphi_{\mathscr{L}} : X \to \mathbb{P}^m \quad \text{and} \quad \varphi_{\mathscr{L}^d} : X \to \mathbb{P}^n$$

for all $d \geqslant 1$. The d-uple embedding of $\mathbb{P}^m$ is a morphism $v_d : \mathbb{P}^m \to \mathbb{P}^{m'}$ where $m' = \binom{m+d}{m} - 1$. We can identify $\mathbb{P}^n$ with a subspace of $\mathbb{P}^{m'}$ via the surjections

$$H^0(X, \mathscr{L})^{\otimes d} \to H^0(X, \mathscr{L}^d).$$

We thus obtain the following commutative diagram:

$$\begin{array}{ccc} X & \xrightarrow{\varphi_{\mathscr{L}^d}} & \mathbb{P}^n \\ {\scriptstyle \varphi_{\mathscr{L}}}\downarrow & & \downarrow \\ \mathbb{P}^m & \xrightarrow[v_d]{} & \mathbb{P}^{m'} \end{array}$$

As $\mathscr{L}$ is ample, $\mathscr{L}^d$ is very ample for all sufficiently large d and hence $\varphi_{\mathscr{L}^d}$ is a closed immersion for all sufficiently large d. Hence, from the diagram we see that $\mathscr{L}$ is also a closed immersion and is thus very ample. □

Proposition 2.3.2. *Let X/S be a relative curve and let $\mathscr{L}$ be an invertible sheaf on X. Then $\mathscr{L}$ is normally generated if and only if $\mathscr{L}$ is very ample and the natural maps*

$$H^0(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(d)) \to H^0(X, \mathscr{L}^d)$$

are surjective for all $d \geqslant 1$.

Proof. If $\mathscr{L}$ is normally generated, then it is very ample by Proposition 2.3.1. For all $d \geqslant 1$, we have canonical isomorphisms

$$H^0(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(d)) \cong H^0(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(1))^{\otimes d} \cong H^0(X, \mathscr{L})^{\otimes d}.$$

Hence, for all $d \geqslant 1$, we see that $H^0(X, \mathscr{L})^{\otimes d} \to H^0(X, \mathscr{L}^{\otimes d})$ is surjective if and only if $H^0(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(d)) \to H^0(X, \mathscr{L}^{\otimes d})$ is surjective. □

Proposition 2.3.3. *Let X/S be a relative curve of genus g and let $\mathscr{L}$ be an invertible sheaf on X. If $\deg(\mathscr{L}) \geqslant 2g+1$, then $\mathscr{L}$ is normally generated.*

Proof. The lower bound on the degree implies $\mathscr{L}$ is very ample by Proposition 2.2.13. Then by Proposition 2.3.2 it remains to prove that

$$\varphi^*_{\mathscr{L}} : H^0(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(d)) \to H^0(X, \mathscr{L}^d)$$

is surjective for all $d \geqslant 1$. For any closed point s of S we have a commutative diagram

$$\begin{array}{ccc} H^0(\mathbb{P}^n, \mathscr{O}(d)) & \xrightarrow{\varphi^*_{\mathscr{L}}} & H^0(X, \mathscr{L}^d) \\ \downarrow & & \downarrow \\ H^0(\mathbb{P}^n_{k(s)}, \mathscr{O}(d)_s) & \xrightarrow[\varphi^*_{\mathscr{L}_s}]{} & H^0(X_s, \mathscr{L}_s^d) \end{array}$$

where the map $\varphi^*_{\mathscr{L}_s}$ is surjective by Proposition 2.3.2 because $\mathscr{L}_s$ is normally generated by Corollary 1.3.9, and the vertical maps arise from taking tensor products with $k(s)$. As this holds for all closed points, we see that $\varphi^*_{\mathscr{L}}$ is surjective by Lemma 2.2.5. □

Lemma 2.3.4. *The natural map*

$$H^0(\mathbb{P}^m_S, \mathscr{O}_{\mathbb{P}^m_S}(1)) \otimes H^0(\mathbb{P}^n_S, \mathscr{O}_{\mathbb{P}^n_S}(1)) \to H^0(\mathbb{P}^m_S \times \mathbb{P}^n_S, \mathscr{O}_{\mathbb{P}^m_S \times \mathbb{P}^n_S}(1))$$

is surjective.

Proof. Let $p_1 : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^m$ and $p_2 : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^n$ be the projection maps. We have

$$p_1^* \mathscr{O}_{\mathbb{P}^m_S}(1) \otimes p_2^* \mathscr{O}_{\mathbb{P}^n_S}(1) \cong \mathscr{O}_{\mathbb{P}^m_S \times \mathbb{P}^n_S}(1)$$

(see Hartshorne [17, Chapter II, Exercise 5.2]), so it suffices to prove that

$$H^0(\mathbb{P}^m_S, \mathscr{O}_{\mathbb{P}^m_S}(1)) \otimes H^0(\mathbb{P}^n_S, \mathscr{O}_{\mathbb{P}^n_S}(1)) \to H^0(\mathbb{P}^m_S \times \mathbb{P}^n_S, p_1^* \mathscr{O}_{\mathbb{P}^m_S}(1) \otimes p_2^* \mathscr{O}_{\mathbb{P}^n_S}(1)) \tag{2.1}$$

is surjective. Let s be a closed point of S and let $k = k(s)$. Then Theorem 1.2.5 implies that the map

$$H^0(\mathbb{P}^m_k, \mathscr{O}_{\mathbb{P}^m_k}(1)) \otimes H^0(\mathbb{P}^n_k, \mathscr{O}_{\mathbb{P}^n_k}(1)) \to H^0(\mathbb{P}^m_k \times \mathbb{P}^n_k, p_1^* \mathscr{O}_{\mathbb{P}^m_k}(1) \otimes p_2^* \mathscr{O}_{\mathbb{P}^n_k}(1)),$$

obtained by tensoring (2.1) with k, is an isomorphism. Hence (2.1) is surjective by Lemma 2.2.5. □

Proposition 2.3.5. *Let X/S be a relative curve and let $\mathscr{M}$ and $\mathscr{N}$ be normally generated sheaves on X/S. Then*

$$\mu_{\mathscr{M}\mathscr{N}} : H^0(X, \mathscr{M}) \otimes H^0(X, \mathscr{N}) \to H^0(X, \mathscr{M} \otimes \mathscr{N}) \tag{2.2}$$

is surjective.

Proof. By Proposition 2.3.2 there exist integers m and n such that the maps

$$H^0(\mathbb{P}^m, \mathscr{O}_{\mathbb{P}^m}(1)) \to H^0(X, \mathscr{M}) \quad \text{and} \quad H^0(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(1)) \to H^0(X, \mathscr{N})$$

are surjective. Now $\mathscr{M} \otimes \mathscr{N}$ is very ample by Proposition 2.2.11 and the embedding it defines factors through the Segre embedding, hence the map

$$H^0(\mathbb{P}^m \times \mathbb{P}^n, \mathscr{O}_{\mathbb{P}^m \times \mathbb{P}^n}(1)) \to H^0(X, \mathscr{M} \otimes \mathscr{N})$$

is surjective. But

$$H^0(\mathbb{P}^m, \mathscr{O}_{\mathbb{P}^m}(1)) \otimes H^0(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(1)) \to H^0(\mathbb{P}^m \times \mathbb{P}^n, \mathscr{O}_{\mathbb{P}^m \times \mathbb{P}^n}(1))$$

is surjective by Lemma 2.3.4, and so we obtain a commutative diagram

$$\begin{array}{ccccc} H^0(\mathbb{P}^m, \mathscr{O}_{\mathbb{P}^m}(1)) \otimes H^0(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(1)) & \longrightarrow & H^0(X, \mathscr{M}) \otimes H^0(X, \mathscr{N}) & \longrightarrow & 0 \\ \downarrow & & \downarrow \mu & & \\ H^0(\mathbb{P}^m \times \mathbb{P}^n, \mathscr{O}_{\mathbb{P}^m \times \mathbb{P}^n}(1)) & \longrightarrow & H^0(X, \mathscr{M} \otimes \mathscr{N}) & \longrightarrow & 0 \end{array}$$

where all maps except μ are known to be surjective. Thus μ is surjective. □

Combining Propositions 2.3.3 and 2.3.5 we see that, if $\mathscr{M}$ and $\mathscr{L}$ have sufficiently large degrees, then $H^0(X, \mathscr{M})$ and $H^0(X, \mathscr{N})$ contain all the information needed to describe $H^0(X, \mathscr{M} \otimes \mathscr{N})$, which in turn completely describes $\mathscr{M} \otimes \mathscr{N}$.

For any submodules $N' \subseteq N$ and $P' \subseteq P$, define the *module quotient* of P' by N' with respect to a homomorphism $\mu : M \otimes N \to P$ to be the submodule

$$(P' : N')_\mu = \{m \in M \mid \mu(m \otimes N') \subseteq P'\}$$

of M. (Similarly, one can define $(P' : M')_\mu \subseteq N$ for a submodule M' of M, but we will not need this.) We will often drop μ from the notation when it clear from the context. By definition the module quotient satisfies the following property: for any submodule $M' \subseteq M$, if $\mu(M' \otimes N) \subseteq P'$, then $M' \subseteq (P' : N')$.

Proposition 2.3.6. *Let X/S be a relative curve of genus g and let s be a closed point of S. Let $\mathscr{M}_s$ and $\mathscr{N}_s$ be invertible sheaves on X_s and assume $\mathscr{N}_s$ is generated by global sections. Then for any divisor D on X_s, we have*

$$H^0(X_s, \mathscr{M}_s(-D)) = \Big(H^0(X_s, \mathscr{M}_s \otimes \mathscr{N}_s(-D)) : H^0(X_s, \mathscr{N}_s)\Big)_{\mu_{\mathscr{M}_s \mathscr{N}_s}}$$

with respect to the canonical map

$$\mu_{\mathscr{M}_s \mathscr{N}_s} : H^0(X_s, \mathscr{M}_s) \otimes H^0(X_s, \mathscr{N}_s) \to H^0(X_s, \mathscr{M}_s \otimes \mathscr{N}_s).$$

Proof. See Khuri-Makdisi [22, Lemma 2.3]. □

Proposition 2.3.7. *Let X/S be a relative curve of genus g and let $\mathscr{M}$ and $\mathscr{N}$ be invertible sheaves on X, each of degree at least $2g+1$. Then for any relative effective Cartier divisor D on X of degree at most $\deg(\mathscr{M}) - (2g+1)$, we have*

$$H^0(X, \mathscr{M}(-D)) = \Big(H^0(X, \mathscr{M} \otimes_{\mathscr{O}_X} \mathscr{N}(-D)) : H^0(X, \mathscr{N})\Big)_{\mu_{\mathscr{M}\mathscr{N}}}$$

with respect to the canonical homomorphism $\mu_{\mathscr{M}\mathscr{N}}$ of (2.2).

Proof. Let s be a closed point of S. Let

$$M = H^0(X, \mathscr{M}), \qquad N = H^0(X, \mathscr{N}), \qquad P = H^0(X, \mathscr{M} \otimes \mathscr{N})$$
$$M' = H^0(X, \mathscr{M}(-D)), \quad \text{and} \quad P' = H^0(X, \mathscr{M} \otimes \mathscr{N}(-D)).$$

Note that $P' \cong H^0(X, \mathscr{M}(-D) \otimes \mathscr{N})$. Denote the corresponding modules on the fibre of X over s by a subscript s; for example $M'_s = H^0(X_s, \mathscr{M}(-D)_s)$.

We have a homomorphism $\mu : M' \otimes N \to P'$ obtained from $\mu : M \otimes N \to P$ by restriction. This induces a homomorphism which, after applying Proposition 2.2.8, is given by $\mu : M'_s \otimes N_s \to P'_s$. Then Proposition 2.3.6 gives the equality

$$M'_s = (P'_s : N_s). \tag{2.3}$$

Now, by the definition of the module quotient we have

$$M' \subseteq (P' : N). \tag{2.4}$$

Applying Proposition 2.2.8, we obtain an induced homomorphism

$$\Big((P' : N) \otimes k(s)\Big) \otimes N_s \to P'_s,$$

and so by (2.3) we have

$$(P' : N) \otimes k(s) \subseteq (P'_s : N_s) = M'_s. \tag{2.5}$$

Hence, combining (2.4) with (2.5), we obtain $(P' : N)/M' \otimes k(s) = 0$ for all closed points $s \in S$ and so $(P' : N) = M'$ by Lemma 2.2.4. □

Chapter 3

Divisor arithmetic on relative Jacobians

In this chapter we describe how to perform arithmetic of relative effective Cartier divisors on a relative curve. The choice of base ring is limited only by the presence of effective linear algebra functions; we formalise this notion in Section 3.2. In Section 3.3 to describe how to calculate homomorphic images of modules and module quotients with respect to a given bilinear map. This leads to the algorithmic realisation of Propositions 2.3.5 and 2.3.7 in Section 3.4. Finally, these algorithms are used to describe arithmetic of divisors on relative curves in Section 3.5, and on relative Jacobians of relative curves in Section 3.6, in a manner directly analogous to the algorithms of Khuri-Makdisi [22].

3.1 Complexity analysis

Let $A = \mathbb{R}[x_1, \ldots, x_s]$ be a multivariate polynomial ring with real coefficients and let f be an element of A. The *big O* class of f, denoted by $O(f)$, is defined to be the set consisting of the polynomials $g \in A$ which satisfy the following condition: there exist $M_g, C_g \in \mathbb{R}$ such that $|g(m_1, \ldots, m_s)| \leqslant C_g|f(m_1, \ldots, m_s)|$ for all $(m_1, \ldots, m_s) \in \mathbb{R}^s$ satisfying $m_i \geqslant M_g$ for all $i = 1, \ldots, s$.

Let M be a projective R-module. Then M is locally free and so there is a map $\mathrm{rank}_M : \mathrm{Spec}(R) \to \mathbb{N}$ defined by $\mathrm{rank}_M(\mathfrak{p}) = \mathrm{rank}(M_\mathfrak{p})$ where $\mathrm{rank}(M_\mathfrak{p})$ is the rank of the free $R_\mathfrak{p}$-module $M_\mathfrak{p}$. The map rank_M is locally constant on $\mathrm{Spec}(R)$, and, since R is Noetherian, takes on finitely many values on X. We define the *size* of M to be $\max\{\mathrm{rank}_M(\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Spec}(R)\}$. The example to keep in mind is of a free module R^m where the size is simply m.

The *space complexity* of an R-module is an estimation of the amount of storage space required to represent it. In the following sections, the space complexity will be estimated relative to the sizes of certain fixed projective modules.

By the *time complexity* of a procedure, we mean the asymptotic number of arithmetic operations in the base ring R required by the procedure to execute, where an operation in the base ring R is an addition, subtraction, multiplication, division by a unit and assignment of elements of R. We will always assume that multiplications and divisions by units are asymptotically more expensive than additions, subtractions and assignments. The performance of the algorithms we discuss will be expressed in terms of the time complexity of the steps that constitute them as a function of the space complexity of the input.

Let M be a projective R-module of size m. We will assume that the space complexity of M is in $O(m)$. If N is a second projective R-module of size n, we will assume that the space complexity of a homomorphism $\varphi\colon M \to N$ is in $O(mn)$. This is analogous to the case of a homomorphism $\varphi\colon R^n \to R^m$ between free modules being represented by an $m \times n$ matrix.

A finitely generated submodule N of a projective module M of size m will always be given as a homomorphic image; that is $\mathrm{Im}(\varphi) = N$ for some homomorphism $\varphi : R^n \to M$. We will often write simply $N \subseteq M$ leaving the homomorphism defining N implicit. By rights, the space complexity of the submodule N is the space complexity of its defining homomorphism, which is in $O(mn)$. However, we will make a further assumption that the space complexity of N is in $O(m^2)$. This assumption will always hold in the applications in Sections 3.4, 3.5 and 3.6 and serves to considerably simplify the expressions describing the time complexities of the algorithms.

3.2 Amenable rings

There are several operations that we need to perform projective R-modules, their finitely generated submodules, and homomorphisms between them. Here we give a name to those rings for which the module operations can be computed. We will say that a ring R is *amenable* if we can perform exact arithmetic on elements of R, and the following functions are effectively computable on projective R-modules and homomorphisms between them:

Dual: Given a homomorphism $\varphi\colon M \to N$, return the dual homomorphism between the dual modules $\varphi^\vee\colon N^\vee \to M^\vee$ where $M^\vee = \mathrm{Hom}(M, R)$. If the space complexities of M and N are in $O(m)$ and $O(n)$ respectively, then we assume that the space complexities of $M^\vee$, $N^\vee$ and $\varphi^\vee$ are in

$O(m)$, $O(n)$ and $O(mn)$ respectively, and that the computation of $\varphi^\vee$ has time complexity in $O(mn)$.

Composite: Given homomorphisms $\varphi : M \to N$ and $\psi : N \to P$, return the homomorphism $\psi \circ \varphi : M \to P$. If the space complexities of M, N and P are in $O(m)$, $O(n)$, and $O(p)$ respectively, then we assume that the space complexity of $\psi \circ \varphi$ is in $O(mp)$ and that the computation of $\psi \circ \varphi$ has time complexity in $O(mnp)$.

Kernel: Given a homomorphism $\varphi : M \to N$, return a homomorphism $\kappa : K \to M$ for some K such that $\mathrm{Im}(\kappa) = \mathrm{Ker}(\varphi)$. If the space complexities of M and N are in $O(m)$ and $O(n)$ respectively, then we assume that K has space complexity in $O(m)$, so κ has space complexity in $O(m^2)$. We denote the time complexity to compute $\mathrm{Ker}(\varphi)$ by $\mathsf{K}(m, n)$.

Common kernel: Given homomorphisms $\varphi_i : M \to N$ for $i = 1, \ldots, r$, return the common kernel $\bigcap_{i=1}^{r} \mathrm{Ker}(\varphi_i)$ of the φ_i. If the space complexities of M and N are in $O(m)$ and $O(n)$ respectively, then we assume that the space complexity of the common kernel is in $O(m^2)$. We denote the cost of computing the common kernel by $\mathsf{CK}(r, m, n)$.

Sum: Given submodules $M_1 \subseteq M$ and $M_2 \subseteq M$, return the sum $M_1 + M_2 \subseteq M$. If the space complexity of M is in $O(m)$, then the space complexities of M_1 and M_2 will be in $O(m^2)$ and we assume that the space complexity of $M_1 + M_2$ is in $O(m^2)$. We denote the time complexity of computing $M_1 + M_2$ by $\mathsf{S}(m)$.

Note that the assumptions for the number operations of each of the functions above are inspired by the analogous case of homomorphisms between free modules given by matrices. Of course the correctness of the following algorithms is not effected in case these assumptions fail to hold for a given amenable ring.

As the primary application is to finite rings, we have made no attempt to analyse the size of intermediate expressions of the algorithms, although this can certainly play a significant role for calculations over infinite rings. Where applicable, working in a quotient ring or employing appropriate variants of the LLL algorithm are common techniques for controlling intermediate expression swell. See Cohen [9, Chapter 2] for some examples over the integers.

For the remainder of this section we provide a brief survey of some rings which are known to be amenable. Cohen [9] discusses the two "classical" amenable rings, namely fields with exact arithmetic and the ring of integers

(or indeed any domain with exact arithmetic and an effectively computable Euclidean function).

Recall that a principal ideal ring is ring in which every ideal is principal; such a ring need not be a domain in general. The work of Storjohann [37], Mulders and Storjohann [29] and Buchmann and Neis [5] shows that a large class of principal ideal rings and their quotients are amenable. This class includes all finite semi-local rings, and in particular, quotients of discrete valuation rings.

The work of Bosma and Pohst [3], Cohen [10] and Neis [33] shows that Dedekind domains are amenable. Caruso and Lubicz [6] have announced algorithms that make certain quotients of the ring $\mathbb{Z}_p[\![u]\!]$ amenable.

3.3 Arithmetic of modules

In this section we describe the algorithms that allow us to evaluate a given homomorphism $\mu : M \otimes N \to P$ between projective modules M, N and P, and to compute the module quotient (also known as the colon module; not to be confused with a quotient module) with respect to μ.

The following operations are described for vector spaces by Khuri-Makdisi [23, Definition 2.5] and algorithms are given by [23, Proposition 2.6]. (Note that Khuri-Makdisi provides several different representations of μ in [23, Section 2]; we follow what he calls "Representation A".) We will describe the analogous operations and algorithms for finitely generated submodules of fixed projective R-modules.

Throughout the remainder of this section we suppose given fixed projective R-modules M, N and P, and a homomorphism

$$\mu : M \otimes_R N \to P.$$

Any element x in M induces a homomorphism

$$\mu_x : N \to P \quad \text{defined by} \quad \mu_x(y) = \mu(x \otimes y).$$

Similarly, we obtain a homomorphism $\mu_y : M \to P$ for any element y in N.

If $\{x_i \mid i = 1, \ldots, m\}$, $\{y_j \mid j = 1, \ldots, n\}$ and $\{z_k \mid k = 1, \ldots, p\}$ are fixed generating sets for M, N and P respectively, then μ can be given as follows: For all $i = 1, \ldots, m$ and $j = 1, \ldots, n$, there exist elements $a_{ijk} \in R$ such that

$$\mu(x_i \otimes y_j) = \sum_k a_{ijk} z_k.$$

The (j, k) entry of the underlying matrix of μ_{x_i} will then be a_{ikj}. Similarly the (i, k) entry of the underlying matrix of μ_{y_j} will be a_{kji}.

Throughout we assume that M, N, and P have sizes m, n and p respectively. Then μ has space complexity in $O(mnp)$ and μ_x has space complexity in $O(np)$ for all $x \in M$. We assume that the time complexity to derive μ_x from μ is $O(mnp)$.

Let $M' \subseteq M$ and $N' \subseteq N$ be submodules of M and N. Since μ is linear, the image of $M' \otimes N'$ under μ is generated by the set $\{\mu(s_i \otimes t_j)\}$ were $M' = \langle s_1, \ldots, s_{m'} \rangle$ and $N' = \langle t_1, \ldots, t_{n'} \rangle$. The following algorithms show how to compute this image $\mu(M' \otimes N')$.

The following algorithm is analogous to Khuri-Makdisi [23, Algorithms 2.6(1) and 2.6(2)].

Algorithm 3.3.1 (Simple product)**.** Given a submodule $N' \subseteq N$ and an element x of M, the following algorithm calculates the submodule $\mu(x \otimes N')$ of P. If the space complexity of N' is in $O(n^2)$, then the time complexity of the algorithm is in $O(np(m+n))$ and the space complexity of $\mu(x \otimes N')$ is in $O(p^2)$.

1. Compute the multiplication-by-x homomorphism $\mu_x : N \to P$.
2. Return $\mu_x(N')$.

Proof. Clearly $\mu_x(N') = \mu(x \otimes N')$, which is the result of step 2.

The time complexity of the computation of μ_x in step 1 is in $O(mnp)$ by assumption. The computation of $\mu_x(N')$ in step 2 is the composite of μ_x and N' having space complexities in $O(np)$ and $O(n^2)$ respectively. Hence step 2 has a time complexity in $O(n^2p)$. Thus the time complexity of the algorithm is in $O(np(m+n))$. The space complexity of $\mu_x(N') \subseteq P$ is in $O(p^2)$ by assumption. □

The following algorithm is analogous to that of Khuri-Makdisi [23, Algorithm 2.6(3)].

Algorithm 3.3.2 (General product)**.** Given submodules $M' \subseteq M$ and $N' \subseteq N$, the following algorithm calculates the submodule $\mu(M' \otimes N')$ of P. If the space complexities of M' and N' are in $O(m^2)$ and $O(n^2)$ respectively, then the time complexity of the algorithm is in $O(mnp(m+n) + m\mathsf{S}(p))$ and the space complexity of $\mu(M' \otimes N')$ is in $O(p^2)$.

1. Let $\{g_1, \ldots, g_{m'}\}$ be a generating set for M' where $m' \in O(m)$.
2. For each $i = 1, \ldots, m'$, compute the image $\mu(g_i \otimes N')$ of N' under multiplication-by-g_i using Algorithm 3.3.1.
3. Return the sum $\sum_{i=1}^{m'} \mu(g_i \otimes N')$.

Proof. In step 2, we compute $\mu(g_i \otimes N') \subseteq P$ for each $i = 1, \ldots, m'$. Then step 3 calculates

$$\sum_{i=1}^{m'} \mu(g_i \otimes N') = \mu(M' \otimes N').$$

There are $m' \in O(m)$ calls to Algorithm 3.3.1 in step 2; hence the time complexity of step 2 is in $O(mnp(m+n))$. The space complexity of each submodule $\mu(g_i \otimes N')$ is in $O(p^2)$, as is the sum of two such modules, so the time complexity to calculate the sum in step 3 is in $O(m\mathsf{S}(p))$ and the space complexity of the result is in $O(p^2)$. The time complexity of the whole algorithm is thus in $O(mnp(m+n) + m\mathsf{S}(p))$. □

The following algorithm computes the module quotient $(P' : N')_\mu$ of submodules $P' \subseteq P$ and $N' \subseteq N$. It is analogous to that of Khuri-Makdisi [23, Algorithm 2.6(4)].

Algorithm 3.3.3 (Module quotient)**.** Given finitely generated projective submodules $N' \subseteq N$ and $P' \subseteq P$ where P' is a direct summand of P, the following algorithm calculates the submodule $(P' : N')$ of M. If the space complexities of N' and P' are in $O(n^2)$ and $O(p^2)$ respectively, then the time complexity of the algorithm is in $O(mnp(n+p) + \mathsf{K}(p,p) + \mathsf{CK}(n,m,p))$ and the space complexity of $(P' : N')$ is in $O(m^2)$.

1. Let $\chi : R^{p'} \to P$ be such that $\mathrm{Im}(\chi) = P'$ and $p' \in O(p)$.
2. Form the dual $\chi^\vee : P^\vee \to R^{p'}$ of χ.
3. Compute the kernel $\kappa : R^k \to P^\vee$ of $\chi^\vee$.
4. Take the dual of κ to obtain $\kappa^\vee : P \to R^k$.
5. Let $\{g_1, \ldots, g_{n'}\}$ be a generating set for N' where $n' \in O(n)$.
6. For each $i = 1, \ldots, n'$, compute the multiplication-by-g_i homomorphism $\mu_{g_i} : M \to P$.
7. For each $i = 1, \ldots, n'$, compute the composite $\kappa^\vee \circ \mu_{g_i} : M \to R^k$.
8. Return the intersection of the kernels $\bigcap_{i=1}^{n'} \mathrm{Ker}(\kappa^\vee \circ \mu_{g_i})$.

Proof. Let $\theta : K \to M$ be the intersection calculated in step 8, that is

$$\theta(K) = \bigcap_{i=1}^{n'} \mathrm{Ker}(\kappa^\vee \circ \mu_{g_i}).$$

We need to show that $\theta(K) = (P' : N')_\mu$. First, steps 2 and 3 construct a sequence

$$R^k \xrightarrow{\kappa} P^\vee \xrightarrow{\chi^\vee} R^{p'} \tag{3.1}$$

which is exact at $P^\vee$. We first show that $\mathrm{Ker}(\kappa^\vee) = P'$. Since P' is a direct summand of P, we have $P \cong P' \oplus P''$ for $P'' \cong P/P'$ projective. Then exactness of (3.1) implies $\mathrm{Im}(\kappa) = \mathrm{Ker}(\chi^\vee) = (P/P')^\vee$. Equating P and $P^{\vee\vee}$, we see that

$$\mathrm{Ker}(\kappa^\vee) = \{x \in P \mid \varphi(x) = 0 \text{ for all } \varphi \in (P/P')^\vee\}.$$

But $(P/P')^\vee$ is a direct summand of $P^\vee$ because direct sums commute with duals, hence if $x = x' + x''$ for $x' \in P'$ and $x'' \in P''$, then $\varphi(x' + x'') = \varphi(x'' + P')$ and since $x'' + P'$ is nonzero there exists a function in $(P/P')^\vee$ which is nonzero at $x'' + P'$. Hence $\mathrm{Ker}(\kappa^\vee) = P'$. The homomorphism $\kappa^\vee$ is calculated in step 4.

Now let $v \in \theta(K)$. Then $v \in \bigcap_{i=1}^{n'} \mathrm{Ker}(\kappa^\vee \circ \mu_{g_i})$ if and only if $v \in \mathrm{Ker}(\kappa^\vee \circ \mu_{g_i})$ for all i if and only if $\mu(v \otimes g_i) \in \mathrm{Ker}(\kappa^\vee) = P'$ for all i if and only if $\mu(v \otimes N') \subseteq P'$. Hence $\theta(K) = (P' : N')$ as required.

The time complexity to compute the dual of $\chi^\vee$ in step 2 is in $O(p^2)$, to compute the kernel in step 3 is in $O(\mathsf{K}(p,p))$ since $k \in O(p)$ by assumption, and to compute the dual in step 4 is in $O(p^2)$. The total time complexity for steps 2 to 4 is thus in $O(p^2 + \mathsf{K}(p,p))$, and the space complexity of $\kappa^\vee$ is in $O(p^2)$.

The time complexity to calculate each μ_{g_i} in step 6 is in $O(mnp)$ and each has space complexity in $O(mp)$. Since there are $n' \in O(n)$ homomorphisms μ_{g_i}, the time complexity of step 6 is in $O(mn^2p)$.

For each $i = 1, \ldots, n'$, the time complexity to calculate each composite $\kappa^\vee \circ \mu_{g_i}$ in step 7 is in $O(mp^2)$ since the space complexities of $\mu_{g_i} : M \to P$ and $\kappa^\vee : P \to R^k$ are in $O(mp)$ and $O(p^2)$ respectively. There are $n' \in O(n)$ such composites, so the time complexity of step 7 is in $O(mnp^2)$.

In step 8 the time complexity to compute the common kernel is $\mathsf{CK}(n,m,p)$ since $n' \in O(n)$ and the space complexity of each $\kappa^\vee \circ \mu_{g_i}$ is in $O(mp)$. Hence the total time complexity of the algorithm is in $O(mnp(n+p) + \mathsf{K}(p,p) + \mathsf{CK}(n,m,p))$. The space complexity of $(P' : N') \subseteq M$ is in $O(m^2)$ by assumption. □

3.4 Tensor products and sheaf quotients

Recall from Theorem 1.2.3 that, for any invertible sheaf $\mathscr{L}$ on X, the set $H^0(X, \mathscr{L})$ of global sections of $\mathscr{L}$ is a finitely generated R-module. We will

represent relative effective Cartier divisors on a relative curve X by first fixing a very ample invertible sheaf $\mathscr{L}$ with large degree whose module $H^0(X, \mathscr{L})$ of global sections is projective. Then a relative effective Cartier divisor D on X will be given by a set of generators for the finitely generated R-submodule $H^0(X, \mathscr{L}(-D))$. By choosing $\mathscr{L}$ such that $\mathscr{L}(-D)$ is very ample, D can always be recovered from $H^0(X, \mathscr{L}(-D))$, at least in principle.

The algorithms in Section 3.3 allow us to explicitly compute the results of Propositions 2.3.5 and 2.3.7. Let R be an amenable ring, let $S = \mathrm{Spec}(R)$ and let X/S be a relative curve. Let $\mathscr{L}$ be a normally generated invertible sheaf on X. Then Propositions 2.1.7 and 2.3.5 imply that

$$\mu_{ij} : H^0(X, \mathscr{L}^i) \otimes H^0(X, \mathscr{L}^j) \to H^0(X, \mathscr{L}^{i+j})$$

is a surjective homomorphism of projective R-modules.

We assume that the size of $H^0(X, \mathscr{L}^i)$ is in $O(ig)$ for all $i \geqslant 1$. In practice, the maximum i required is determined by the maximum degree relative effective Cartier divisor one wishes to represent. Thus in the case of arithmetic on $\mathrm{Pic}^0_X(S)$, as we consider in Section 3.6, i is bounded above by a small constant (in Algorithms 3.6.3 and 3.6.4 we have $i \leqslant 5$).

Algorithm 3.4.1 (Product of global sections)**.** Let i and j be positive integers, let $\mathscr{M}$ be a subsheaf of $\mathscr{L}^i$ and let $\mathscr{N}$ be a subsheaf of $\mathscr{L}^j$, each of degree at least $2g + 1$. Given the submodules $H^0(X, \mathscr{M}) \subseteq H^0(X, \mathscr{L}^i)$ and $H^0(X, \mathscr{N}) \subseteq H^0(X, \mathscr{L}^j)$, the following procedure calculates the submodule $H^0(X, \mathscr{M} \otimes \mathscr{N})$ of $H^0(X, \mathscr{L}^{i+j})$. If the space complexities of $H^0(X, \mathscr{M})$ and $H^0(X, \mathscr{N})$ are in $O(i^2g^2)$ and $O(j^2g^2)$ respectively, then the time complexity of the algorithm is in $O(ij(i+j)^2g^4 + ig\mathsf{S}((i+j)g))$ and the space complexity of the result is in $O((i+j)^2g^2)$.

1. Return $H^0(X, \mathscr{M} \otimes \mathscr{N})$ obtained by applying Algorithm 3.3.2 to the modules $H^0(X, \mathscr{M})$ and $H^0(X, \mathscr{N})$.

Proof. By the hypothesis on the lower bounds of the degrees of $\mathscr{M}$ and $\mathscr{N}$, Proposition 2.3.5 implies that $H^0(X, \mathscr{M}) \otimes H^0(X, \mathscr{N})$ surjects via μ_{ij} onto $H^0(X, \mathscr{M} \otimes \mathscr{N})$. The call to Algorithm 3.3.2 calculates this image of $H^0(X, \mathscr{M}) \otimes H^0(X, \mathscr{N})$. The time complexity of the call to Algorithm 3.3.2 is in $O(ij(i+j)^2g^4 + ig\mathsf{S}((i+j)g))$ and the space complexity of $H^0(X, \mathscr{M} \otimes \mathscr{N})$ is in $O((i+j)^2g^2)$ since it is a submodule of $H^0(X, \mathscr{L}^{i+j})$ which has space complexity in $O((i+j)g)$ by assumption. □

The following algorithm is a generalisation of the descriptions provided by Khuri-Makdisi in [22, Remark 3.8] and [23, Proposition 2.6(4)].

Algorithm 3.4.2 (Sheaf quotient)**.** Let i and j be positive integers, let $\mathscr{M}$ be a subsheaf of $\mathscr{L}^i$ and let $\mathscr{N}$ be a subsheaf of $\mathscr{L}^j$, each of degree at least $2g+1$. Let E be a relative effective Cartier divisor on X whose degree satisfies

$$\deg(E) \leqslant \min\{\deg(\mathscr{M}), \deg(\mathscr{N})\} - (2g+1).$$

Given the submodules $H^0(X,\mathscr{M}) \subseteq H^0(X,\mathscr{L}^i)$, $H^0(X,\mathscr{N}) \subseteq H^0(X,\mathscr{L}^j)$ and $H^0(X,\mathscr{N}(-E)) \subseteq H^0(X,\mathscr{L}^j)$, the following procedure calculates the submodule $H^0(X,\mathscr{M}(-E))$ of $H^0(X,\mathscr{L}^i)$. If the space complexities of the submodules $H^0(X,\mathscr{M})$, $H^0(X,\mathscr{N})$ and $H^0(X,\mathscr{N}(-E))$ are in $O(i^2g^2)$, $O(j^2g^2)$ and $O(j^2g^2)$ respectively, then the time complexity of the algorithm is in $O(ij(i+j)^2g^4 + ig\mathsf{S}((i+j)g) + \mathsf{K}((i+j)g,(i+j)g) + \mathsf{CK}(jg,ig,(i+j)g))$ and the result has space complexity in $O(i^2g^2)$.

1. Apply Algorithm 3.4.1 to $H^0(X,\mathscr{M})$ and $H^0(X,\mathscr{N}(-E))$ to obtain the module $H^0(X,\mathscr{M}\otimes\mathscr{N}(-E))$.

2. Return the module $H^0(X,\mathscr{M}(-E))$ obtained by applying Algorithm 3.3.3 to $H^0(X,\mathscr{M}\otimes\mathscr{N}(-E))$ and $H^0(X,\mathscr{N})$.

Proof. By Proposition 2.3.5, the result of step 1 is $H^0(X,\mathscr{M}\otimes\mathscr{N}(-E))$ which is isomorphic to $H^0(X,\mathscr{M}(-E)\otimes\mathscr{N})$. The bounds on the degrees imply that all the sheaves under consideration are normally generated by Proposition 2.3.3 thus have zero higher cohomology by Proposition 2.2.7 and are hence projective by Proposition 2.1.7. Then $H^0(X,\mathscr{M}\otimes\mathscr{N})/H^0(X,\mathscr{M}\otimes\mathscr{N}(-E))$ is projective by Corollary 2.1.8 and so $H^0(X,\mathscr{M}\otimes\mathscr{N}(-E))$ is a direct summand of $H^0(X,\mathscr{M}\otimes\mathscr{N})$. This proves that the arguments satisfy the conditions for the application of Algorithm 3.3.3 in step 2. Then Proposition 2.3.7 implies that the module quotient calculation in step 2 gives

$$\Big(H^0(X,\mathscr{M}\otimes\mathscr{N}(-E)) : H^0(X,\mathscr{N})\Big) \cong H^0(X,\mathscr{M}(-E))$$

as required. Step 1 has time complexity in $O(ij(i+j)^2g^4 + ig\mathsf{S}((i+j)g))$ and step 2 has time complexity in $O(ij(i+j)^2g^4 + \mathsf{K}((i+j)g,(i+j)g) + \mathsf{CK}(jg,ig,(i+j)g))$. Hence the time complexity of the algorithm is in $O(ij(i+j)^2g^4 + ig\mathsf{S}((i+j)g) + \mathsf{K}((i+j)g,(i+j)g) + \mathsf{CK}(jg,ig,(i+j)g))$. The result $H^0(X,\mathscr{M}(-E))$ is a submodule of $H^0(X,\mathscr{L}^i)$ hence has space complexity in $O(i^2g^2)$ by assumption. □

3.5 Arithmetic of divisors

In this section we give descriptions of the arithmetic operations on divisors given as modules of global sections as described in the previous section.

To this end we employ the theory developed in Section 3.3 to demonstrate that the main algorithms of Khuri-Makdisi [22] continue to hold for relative effective Cartier divisors on relative curves over $S = \mathrm{Spec}(R)$ for an amenable ring R.

Throughout this section and the next we fix the following notation. Let R be an amenable ring, let $S = \mathrm{Spec}(R)$ and let X/S be a relative curve of genus g. Let $\mathscr{L}$ be an invertible sheaf on X of degree $\Delta \geqslant 2g+1$, so $\mathscr{L}$ is normally generated by Proposition 2.3.3. We will assume the size of $H^0(X, \mathscr{L}^i)$ is in $O(ig)$ for all $i \geqslant 1$ and that the space complexity of a submodule of $H^0(X, \mathscr{L}^i)$ is in $O(i^2g^2)$.

The first algorithm is analogous to Khuri-Makdisi [22, Algorithm 3.6].

Algorithm 3.5.1 (Divisor addition)**.** Let D_1 and D_2 be relative effective Cartier divisors on X satisfying $\deg(D_1 + D_2) \leqslant \Delta - (2g+1)$. Given the submodules $H^0(X, \mathscr{L}(-D_1))$ and $H^0(X, \mathscr{L}(-D_2))$ of $H^0(X, \mathscr{L})$, the following procedure calculates $H^0(X, \mathscr{L}(-D_1 - D_2))$. If the space complexities of $H^0(X, \mathscr{L}(-D_1))$ and $H^0(X, \mathscr{L}(-D_2))$ are in $O(g^2)$, then the time complexity of the algorithm is in $O(g^4 + g\mathsf{S}(g) + \mathsf{K}(g,g) + \mathsf{CK}(g,g,g))$ and the result has space complexity $O(g^2)$.

1. Apply Algorithm 3.4.1 to $H^0(X, \mathscr{L}(-D_1))$ and $H^0(X, \mathscr{L}(-D_2))$ to obtain the submodule $H^0(X, \mathscr{L}^2(-D_1 - D_2))$ in $H^0(X, \mathscr{L}^2)$.

2. Return $H^0(X, \mathscr{L}(-D_1 - D_2))$ obtained by applying Algorithm 3.4.2 to the modules $H^0(X, \mathscr{L})$, $H^0(X, \mathscr{L}^2)$ and $H^0(X, \mathscr{L}^2(-D_1 - D_2))$.

Proof. Step 1 produces $H^0(X, \mathscr{L}^2(-D_1 - D_2))$ since $\deg(D_1 + D_2) \leqslant \Delta - (2g+1)$ implies $\deg(\mathscr{L}(-D_i)) \geqslant 2g+1$ for $i = 1, 2$. Now $\deg(\mathscr{L}) \geqslant 2g+1$ and $\deg(\mathscr{L}^2(-D_1 - D_2)) \geqslant 2g+1$, so the application of Algorithm 3.4.2 in step 2 returns $H^0(X, \mathscr{L}(-D_1 - D_2))$.

The time complexity of step 1 is in $O(g^4 + g\mathsf{S}(g))$ and the time complexity of step 2 is in $O(g^4 + g\mathsf{S}(g) + \mathsf{K}(g,g) + \mathsf{CK}(g,g,g))$, hence the time complexity of the algorithm is in $O(g^4 + g\mathsf{S}(g) + \mathsf{K}(g,g) + \mathsf{CK}(g,g,g))$ operations. □

The following algorithm is analogous to Khuri-Makdisi [22, Algorithm 3.10].

Algorithm 3.5.2 (Divisor 'flip')**.** Let D be a relative effective Cartier divisor on X of degree at most $\Delta - (2g+1)$ and let s be a non-zero element of $H^0(X, \mathscr{L}(-D))$. Considering s as a section of $H^0(X, \mathscr{L})$, write

$$\mathrm{div}(s) = E = D + D'$$

where $H^0(X, \mathscr{O}_X(D')) \cong H^0(X, \mathscr{L}(-D))$. Given the submodule $H^0(X, \mathscr{L}(-D))$ of $H^0(X, \mathscr{L})$ and the element s of $H^0(X, \mathscr{L}(-D))$, the following procedure

computes $H^0(X, \mathscr{L}(-D'))$. If the space complexity of $H^0(X, \mathscr{L}(-D))$ is in $O(g^2)$, then the time complexity of the algorithm is in $O(g^4 + g\mathsf{S}(g) + \mathsf{K}(g,g) + \mathsf{CK}(g,g,g))$ and the space complexity of the result is in $O(g^2)$.

1. Compute $H^0(X, \mathscr{L}^2(-D-D'))$ by applying Algorithm 3.4.1 to s and $H^0(X, \mathscr{L})$.

2. Return $H^0(X, \mathscr{L}(-D'))$ obtained by applying Algorithm 3.4.2 to the modules $H^0(X, \mathscr{L})$, $H^0(X, \mathscr{L}(-D))$ and $H^0(X, \mathscr{L}^2(-D-D'))$.

Proof. Since s generates $H^0(X, \mathscr{L}(-D-D'))$ and since $\deg(\mathscr{L}(-D-D')) = \deg(\mathscr{L}) \geqslant 2g+1$, Algorithm 3.4.1 returns $H^0(X, \mathscr{L}^2(-D-D'))$ in step 1. As $\deg(\mathscr{L}(-D)) \geqslant 2g+1$, the call to Algorithm 3.4.2 in step 2 produces $H^0(X, \mathscr{L}(-D'))$ as claimed.

The time complexity of the call to Algorithm 3.4.1 in step 1 is in $O(g^4 + g\mathsf{S}(g))$ operations. The time complexity of step 2 is in $O(g^4 + g\mathsf{S}(g) + \mathsf{K}(g,g) + \mathsf{CK}(g,g,g))$. Hence the time complexity for the algorithm is in $O(g^4 + g\mathsf{S}(g) + \mathsf{K}(g,g) + \mathsf{CK}(g,g,g))$. The result is a submodule of $H^0(X, \mathscr{L})$ and hence has space complexity in $O(g^2)$. □

3.6 Arithmetic on a relative Jacobian

Khuri-Makdisi [22] describes three models for divisor class arithmetic in the Picard group of a curve: the large, medium and small models. Though the complexity of the algorithms for each of the three models is the same, the medium and small models reduce the size of the vector spaces used by a constant factor at the expense of more complicated algorithms. We will describe the algorithms in terms of the medium model. We keep the notation as described at the beginning of the previous section.

Recall that, for a scheme X, the *Picard group*, $\mathrm{Pic}(X)$, is the group $H^1(X, \mathscr{O}_X^*)$ of isomorphism classes of invertible sheaves on Y and that the map $X \mapsto \mathrm{Pic}(X)$ is a functor. Let $f : X \to S$ be a relative curve and let $T \to S$ be an S-scheme. For the purposes of this section, we define

$$\mathrm{Pic}^0_X(T) = \{\mathscr{L} \in \mathrm{Pic}(X_T) \mid \deg(\mathscr{L}_t) = 0 \text{ for all } t \in T\}/f_T^* \mathrm{Pic}(T).$$

When X/S is a relative curve, the group $\mathrm{Pic}^0_X(S)$ can be given the structure of a scheme; it thus becomes an abelian S-scheme whose fibres are isomorphic to the Jacobians of the fibres of X. For more details, see Bosch et al. [2, Chapter 9, Section 4].

Let $\mathscr{M}$ be an invertible sheaf of degree 0. Then the isomorphism class of $\mathscr{M}$ is represented by any relative effective Cartier divisor D of degree

$\deg(\mathscr{L})$ such that $\mathscr{M} \cong \mathscr{L}(-D)$. Since $\deg(\mathscr{L}) \geqslant 2g+1$, for such D we have $\deg(\mathscr{L}^2(-D)) = \deg(\mathscr{L}) \geqslant 2g+1$ and so Proposition 2.3.3 implies that $\mathscr{L}^2(-D)$ is normally generated. Elements of $\mathrm{Pic}^0_X(S)$ will be represented in this way, as the submodule $H^0(X, \mathscr{L}^2(-D))$ of $H^0(X, \mathscr{L}^2)$ for some relative effective Cartier divisor D of degree $\deg(\mathscr{L})$.

Algorithm 3.6.1 (Zero element)**.** The following procedure computes the zero element of $\mathrm{Pic}^0_X(S)$. The time complexity of the algorithm is in $O(g^4 + g\mathsf{S}(g))$ and the space complexity of the result is in $O(g^2)$.

1. Choose any non-zero element s of $H^0(X, \mathscr{L})$.
2. Apply Algorithm 3.4.1 to s and $H^0(X, \mathscr{L})$ and return the result.

Proof. This algorithm constructs a submodule corresponding to the relative effective Cartier divisor $D = \mathrm{div}(s)$, which is in the zero class in $\mathrm{Pic}^0_X(S)$. In step 2, the result of Algorithm 3.4.1 is $\mu(s \otimes H^0(X, \mathscr{L})) = H^0(X, \mathscr{L}^2(-D))$. The time complexity is determined by the call to Algorithm 3.4.1, hence is in $O(g^4 + g\mathsf{S}(g))$. The result is a submodule of $H^0(X, \mathscr{L}^2)$ and hence its space complexity is in $O(g^2)$. □

The following algorithm is analogous to that of Bruin [4, Algorithm 2.10].

Algorithm 3.6.2 (Zero test)**.** Let x be a point in $\mathrm{Pic}^0_X(S)$ given by a submodule $H^0(X, \mathscr{L}^2(-D))$ of $H^0(X, \mathscr{L}^2)$. The following procedure determines whether $x = 0$. If the space complexity of $H^0(X, \mathscr{L}^2(-D))$ is in $O(g^2)$, then the time complexity of the algorithm is in $O(g^4 + g\mathsf{S}(g) + \mathsf{K}(g,g) + \mathsf{CK}(g,g,g))$.

1. Apply Algorithm 3.4.2 to $H^0(X, \mathscr{L})$, $H^0(X, \mathscr{L}^2)$ and $H^0(X, \mathscr{L}^2(-D))$ to obtain $H^0(X, \mathscr{L}(-D))$.
2. Return *false* if $H^0(X, \mathscr{L}(-D)) = 0$ and *true* otherwise.

Proof. Correctness follows from the fact that $\mathscr{L}^2(-D)$ is trivial if and only if there exists an element $s \in H^0(X, \mathscr{L}(-D))$ such that $D = \mathrm{div}(s)$. This is the test performed in step 2. The calculation is dominated by Algorithm 3.4.2 and so the time complexity is in $O(g^4 + g\mathsf{S}(g) + \mathsf{K}(g,g) + \mathsf{CK}(g,g,g))$. □

The following algorithm is analogous to that of Khuri-Makdisi [22, Algorithm 5.1]; see also Bruin [4, Algorithm 2.11].

Algorithm 3.6.3 (Addflip)**.** Let x and y be elements of $\mathrm{Pic}^0_X(S)$ given by submodules $H^0(X, \mathscr{L}^2(-D_1))$ and $H^0(X, \mathscr{L}^2(-D_2))$ of $H^0(X, \mathscr{L}^2)$. The

following procedure computes the submodule $H^0(X, \mathscr{L}^2(-E))$ and a global section s of $H^0(X, \mathscr{L}^3)$, where s and E satisfy

$$\operatorname{div}(s) = D_1 + D_2 + E.$$

If the space complexities of $H^0(X, \mathscr{L}^2(-D_1))$ and $H^0(X, \mathscr{L}^2(-D_2))$ are in $O(g^2)$, then the time complexity of the algorithm is in $O(g^4 + g\mathsf{S}(g) + \mathsf{K}(g,g) + \mathsf{CK}(g,g,g))$ and the space complexity of the result is in $O(g^2)$.

1. Apply Algorithm 3.4.1 to $H^0(X, \mathscr{L}^2(-D_1))$ and $H^0(X, \mathscr{L}^2(-D_2))$ to obtain $H^0(X, \mathscr{L}^4(-D_1 - D_2))$.

2. Apply Algorithm 3.4.2 to the modules $H^0(X, \mathscr{L}^3)$, $H^0(X, \mathscr{L})$ and $H^0(X, \mathscr{L}^4(-D_1 - D_2))$ to obtain $H^0(X, \mathscr{L}^3(-D_1 - D_2))$.

3. Choose a non-zero element s of $H^0(X, \mathscr{L}^3(-D_1 - D_2))$.

4. Apply Algorithm 3.4.1 to s and $H^0(X, \mathscr{L}^2)$ to obtain the module $H^0(X, \mathscr{L}^5(-D_1 - D_2 - E))$.

5. Apply Algorithm 3.4.2 to the modules $H^0(X, \mathscr{L}^2)$, $H^0(X, \mathscr{L}^3(-D_1 - D_2))$ and $H^0(X, \mathscr{L}^5(-D_1 - D_2 - E))$ to obtain

   $$H^0(X, \mathscr{L}^2(-E)) = (H^0(X, \mathscr{L}^5(-D_1 - D_2 - E)) : H^0(X, \mathscr{L}^3(-D_1 - D_2))).$$

6. Return $H^0(X, \mathscr{L}^2(-E))$ and the section s.

Proof. As $\deg(\mathscr{L}^2(-D_i)) \geqslant 2g+1$ for $i = 1, 2$, Algorithm 3.4.1 can be applied in step 1 to obtain $H^0(X, \mathscr{L}^4(-D_1 - D_2))$. As $\deg(\mathscr{L}^3(-D_1 - D_2)) \geqslant 2g+1$, Algorithm 3.4.2 in step 2 calculates $H^0(X, \mathscr{L}^3(-D_1 - D_2))$. The element s chosen in step 3 corresponds to $H^0(X, \mathscr{L}^3(-D_1 - D_2 - E))$, which has degree $3(2g+1)$, and so Algorithm 3.4.1 gives $H^0(X, \mathscr{L}^5(-D_1 - D_2 - E))$ in step 4. Now $\deg(\mathscr{L}^5(-D_1 - D_2 - E)) = 5(2g+1)$ and so Algorithm 3.4.2 in step 5 produces $H^0(X, \mathscr{L}^2(-E))$.

The space complexity of each submodule appearing in the algorithm is $O(g^2)$. Since each step of the algorithm makes at most one call to either Algorithm 3.4.1 or 3.4.2, the time complexity is in $O(g^4 + g\mathsf{S}(g) + \mathsf{K}(g,g) + \mathsf{CK}(g,g,g))$. As $H^0(X, \mathscr{L}^2(-E))$ is a submodule of $H^0(X, \mathscr{L}^2)$, its space complexity is $O(g^2)$. □

All of the familiar arithmetic operations on $\operatorname{Pic}^0_X(S)$ can be described in terms of the 'Addflip' operation given by Algorithm 3.6.3; we show this in the following algorithm.

Algorithm 3.6.4 (Negation, addition, subtraction, and equality)**.** Let x and y be elements of $\mathrm{Pic}^0(X)$ given as submodules of $H^0(X, \mathscr{L}^2)$. Then we can calculate the negation of x, the sum of x and y, the difference of x and y, and whether x and y are equal. If the inputs have space complexities in $O(g^2)$, then each operation has time complexity in $O(g^4 + g\mathsf{S}(g) + \mathsf{K}(g,g) + \mathsf{CK}(g,g,g))$ and the results have space complexities in $O(g^2)$ (except the equality test which is simply true or false).

(i) *Negation*: Apply Algorithm 3.6.3 to x and the result of Algorithm 3.6.1 to produce $-x - 0 = -x$.

(ii) *Addition*: Apply Algorithm 3.6.3 to x and y and then negate the result, giving $x + y = -(-x - y)$.

(iii) *Subtraction*: Negate x and apply Algorithm 3.6.3 to $-x$ and y, giving $x - y = -(-x) - y$.

(iv) *Equality*: Subtract y from x, then apply Algorithm 3.6.2 to test whether the result is zero.

Proof. That the calculations are correct is clear. The dominant calculation in each case is Algorithm 3.6.3, whose time complexity is in $O(g^4 + g\mathsf{S}(g) + \mathsf{K}(g,g) + \mathsf{CK}(g,g,g))$ and whose results have space complexity in $O(g^2)$. □

We can define scalar multiplication by an arbitrary integer using the addition and negation defined in Algorithm 3.6.4. Implemented as the well-known double-and-add algorithm based on Horner's rule for scalar multiplication in an additive group, its time complexity is in $O(\log(n)(g^4 + g\mathsf{S}(g) + \mathsf{K}(g,g) + \mathsf{CK}(g,g,g)))$ operations in R.

Part II

Spaces of sections on algebraic surfaces

Chapter 4

Cohomology of surfaces

In this chapter we analyse the structure of the cohomology groups of divisors on several classes of surfaces, namely $C \times C$ and $\mathrm{Sym}^2(C)$ for a hyperelliptic curve C of genus at least two. We prove decompositions of the spaces of global sections of divisors on these surfaces and deduce formulæ for their dimensions.

Throughout this chapter and the next, by *surface* we will mean a nonsingular projective algebraic surface over an algebraically closed field.

4.1 Intersection theory on surfaces

In this section we recall the basic facts of intersection theory on surfaces. The primary reference is Hartshorne [17, Chapter V].

Let C and D be two prime divisors on a surface X and let x be a point in $C \cap D$. Let f and g be respectively local equations for C and D at x. We say that C and D intersect *transversally* at x if f and g generate the maximal ideal $\mathfrak{m}_x$ of $\mathscr{O}_{X,x}$; this implies, in particular, that C and D are nonsingular at x.

Theorem 4.1.1. *Let X be a surface and let C and D be divisors on X. There exists a unique bilinear symmetric pairing*

$$\mathrm{Div}(X) \times \mathrm{Div}(X) \to \mathbb{Z},$$

denoted by $(C, D) \mapsto C \cdot D$, such that the following conditions are satisfied:

(i) If C and D meet transversally, then $C \cdot D = \#(C \cap D)$, the number of points of intersection of C and D.

(ii) For all C_1 and C_2 in $\mathrm{Div}(X)$, if $C_1 \sim_{\mathrm{rat}} C_2$, then $C_1 \cdot D = C_2 \cdot D$. In particular, the pairing induces a well-defined bilinear symmetric pairing

$$\mathrm{Pic}(X) \times \mathrm{Pic}(X) \to \mathbb{Z}$$

which we also denote by $([C],[D]) \mapsto C \cdot D$.

Proof. Hartshorne [17, Theorem V.1.1]. □

We call $C \cdot D$ the *intersection number* of the divisors C and D. The *self-intersection number* of C is $C \cdot C$ which we will often write as C^2 when there is no chance for confusion with the scheme product of curves. More generally we write $C^n = C \cdot C \cdot \cdots \cdot C$ (n times).

Proposition 4.1.2 (Adjunction formula)**.** *Let X be a surface and let K_X be a canonical divisor on X. Then for any nonsingular curve C of genus g on X,*

$$2g - 2 = C \cdot (C + K_X).$$

Proof. See Hartshorne [17, Proposition V.1.5]. □

Proposition 4.1.3. *Let $f : X \to Y$ be a surjective, projective morphism of Noetherian integral schemes and suppose $n = [K(X) : f^*K(Y)]$ is finite. Then for any Cartier divisor D on Y,*

$$f_* f^* D = nD.$$

Proof. See Liu [26, Proposition 9.2.11]. □

Proposition 4.1.4. *Let $f : X \to Y$ be a dominant map of smooth projective surfaces. Then $n = [K(X) : f^*K(Y)]$ is finite and for any divisors C and D on Y,*

$$f^*C \cdot f^*D = nC \cdot D.$$

Proof. See Liu [26, Proposition 9.2.12(c)]. □

Proposition 4.1.5 (Riemann-Roch for surfaces)**.** *Let X be a surface, let D be a divisor on X, and let K_X be a canonical divisor on X. Then*

$$\chi(D) = \frac{1}{2} D \cdot (D - K_X) + \chi(\mathscr{O}_X).$$

Proof. See Hartshorne [17, Theorem V.1.6]. □

4.2 Equivalence classes of divisors

In this section we introduce the notions of algebraic and numerical equivalence, and the corresponding quotient groups: the Néron-Severi group and the numerical equivalence group of a variety. We will analyse the structure of these groups in the case of squares and symmetric squares of hyperelliptic curves. Many of the results in the first part of this section are true in much greater generality; see Kleiman [24, Sections 4–6] for details.

Let X be a nonsingular projectively variety. Recall from Section 1.4 that the Picard group of X is defined to be the group of isomorphism classes of invertible sheaves on X. By Theorem 1.4.3, $\mathrm{Pic}(X)$ is isomorphic to $\mathrm{CaCl}(X)$, the group of equivalence classes of divisors on X modulo rational equivalence. In the interests of brevity, we will (re)define $\mathrm{Pic}(X)$ to be $\mathrm{Pic}(X) = \mathrm{CaCl}(X)$, and if D is a divisor on X, we will write $[D]$ for the class in $\mathrm{Pic}(X)$.

Let X be a surface and let D be a divisor on X. Then D is said to be *pre-algebraically equivalent to zero* if there exists a nonsingular curve T, an effective divisor E on $X \times T$ which is flat over T, and two closed points s and t on T, such that

$$D = E \cap (X \times \{s\}) - E \cap (X \times \{t\}).$$

Two divisors are said to be *pre-algebraically equivalent* if their difference is pre-algebraically equivalent to zero. Two divisors D and D' on X are said to be *algebraically equivalent* if there exists a finite sequence $D_0 = D, D_1, \ldots, D_n = D'$ of divisors with D_i pre-algebraically equivalent to D_{i+1} for each $i = 0, \ldots, n-1$. If D and D' are algebraically equivalent we write $D \sim_{\mathrm{alg}} D'$.

Lemma 4.2.1. *Let D_1 and D_2 be divisors on a surface X. If $D_1 \sim_{\mathrm{rat}} D_2$, then $D_1 \sim_{\mathrm{alg}} D_2$.*

Proof. Let $D = \mathrm{div}(f)$ be a principal divisor on X and let $D' = \mathrm{div}(uf - v)$ be a divisor on $X \times \mathbb{P}^1$ were u and v are the coordinates on $\mathbb{P}^1$. Then D' is flat over $\mathbb{P}^1$ and

$$D' \cap (X \times \{(1:0)\}) - D' \cap (X \times \{(0:1)\}) = \mathrm{div}(f) - \mathrm{div}(1) = D$$

as required. □

Proposition 4.2.2. *Let X be a surface. The set of divisor classes algebraically equivalent to zero forms a subgroup of* $\mathrm{Pic}(X)$ *isomorphic to* $\mathrm{Pic}^0(X)$.

Proof. Fulton [13, Proposition 10.3] shows that the set of divisors algebraically equivalent to zero is a subgroup of $\mathrm{Div}(X)$. Applying Lemma 4.2.1, we obtain the same result for divisor classes in $\mathrm{Pic}(X)$. Kleiman [24, Proposition 5.10] shows that this subgroup is isomorphic to $\mathrm{Pic}^0(X)$. □

Proposition 4.2.2 allows us to make the following definition. Let X be a surface. Then the quotient

$$\mathrm{NS}(X) = \mathrm{Pic}(X)/\mathrm{Pic}^0(X)$$

is called the *Néron-Severi group* of X.

We now discuss a coarser notion of equivalence, that of numerical equivalence. For any integer $n > 0$, we have a multiplication-by-n map

$$n\colon \mathrm{Div}(X) \to \mathrm{Div}(X)$$

defined by sending a divisor D to nD. There are induced maps

$$n\colon \mathrm{Pic}(X) \to \mathrm{Pic}(X) \quad \text{and} \quad n\colon \mathrm{Pic}^0(X) \to \mathrm{Pic}^0(X)$$

on divisor classes. Define the set $\mathrm{Pic}^\tau(X)$ by the formula

$$\mathrm{Pic}^\tau(X) = \bigcup_{n>0} n^{-1}\,\mathrm{Pic}^0(X).$$

Thus $[D] \in \mathrm{Pic}^\tau(X)$ if and only if there exists a positive integer n such that $n[D] = [nD] \in \mathrm{Pic}^0(X)$.

Let X be a surface and let D be a divisor on X. Then D is said to be *numerically equivalent to zero* if $D \cdot E = 0$ for every divisor E on X. Two divisors are said to be *numerically equivalent* if their difference is numerically equivalent to zero. We write $D_1 \sim_{\mathrm{num}} D_2$ when D_1 and D_2 are numerically equivalent.

Proposition 4.2.3. *Let X be a surface. The set of divisor classes numerically equivalent to zero forms a subgroup of* $\mathrm{Pic}(X)$ *isomorphic to* $\mathrm{Pic}^\tau(X)$.

Proof. See Kleiman [24, Theorem 6.3 and Exercise 6.11]. □

Proposition 4.2.3 allows us to make the following definition. Let X be a surface. Then

$$\mathrm{Num}(X) = \mathrm{Pic}(X)/\mathrm{Pic}^\tau(X)$$

is called the *numerical divisor class group* of X.

Remark 4.2.4. Let X be a surface. An element $[D] \in \mathrm{Pic}^0(X)$ is algebraically equivalent to zero by Proposition 4.2.2 and $\mathrm{Pic}^0(X) \subseteq \mathrm{Pic}^\tau(X)$ by definition. Hence $[D]$ is numerically equivalent to zero. Combining this with Lemma 4.2.1, we see that rational equivalence implies algebraic equivalence implies numerical equivalence.

Proposition 4.2.5. *Let D_1 and D_2 be numerically equivalent divisors on a surface X. Then $\chi(D_1) = \chi(D_2)$.*

Proof. From the definition of numerical equivalence we have $D_1^2 = D_1 \cdot D_2 = D_2^2$ and $D_1 \cdot K_X = D_2 \cdot K_X$ for any canonical divisor K_X on X. Hence by Proposition 4.1.5

$$\chi(D_1) = \frac{1}{2}(D_1^2 - D_1 \cdot K_X) + \chi(\mathscr{O}_X) = \frac{1}{2}(D_2^2 - D_2 \cdot K_X) + \chi(\mathscr{O}_X) = \chi(D_2)$$

as required. □

Remark 4.2.6. In Theorem 4.1.1 we saw that the intersection pairing on a surface X is a bilinear pairing

$$\mathrm{Div}(X) \times \mathrm{Div}(X) \to \mathbb{Z}$$

which induces a pairing

$$\mathrm{Pic}(X) \times \mathrm{Pic}(X) \to \mathbb{Z}.$$

Remark 4.2.4 shows that we have induced pairings

$$\mathrm{NS}(X) \times \mathrm{NS}(X) \to \mathbb{Z} \qquad \text{and} \qquad \mathrm{Num}(X) \times \mathrm{Num}(X) \to \mathbb{Z}$$

on $\mathrm{NS}(X)$ and $\mathrm{Num}(X)$ as well.

Theorem 4.2.7 (Néron-Severi Theorem)**.** *Let X be a surface. Then $\mathrm{NS}(X)$ is a finitely generated abelian group.*

Proof. See Lang and Néron [25]. □

Theorem 4.2.8 (Matsusaka's Theorem)**.** *Let X be a surface. Then the group*

$$\mathrm{NS}(X)_{\mathrm{tors}} = \mathrm{Pic}^\tau(X)/\mathrm{Pic}^0(X)$$

is finite.

Proof. See Kleiman [24, Corollary 6.17]. □

The following corollary is immediate.

Corollary 4.2.9. *Let X be a surface. Then*

$$\mathrm{Num}(X) = \mathrm{NS}(X)/\mathrm{NS}(X)_{\mathrm{tors}}.$$

In particular, $\mathrm{Num}(X)$ *is free.*

We will now look more closely at the structure of the Picard group, the Néron-Severi group, and the numerical divisor class group in the case of a product of curves.

Lemma 4.2.10. *For any curve C, the degree map on divisors induces an isomorphism* $\mathrm{NS}(C) \cong \mathbb{Z}$.

Proof. See Hartshorne [17, Corollary II.6.10]. □

Proposition 4.2.11. *Let C_1 and C_2 be curves and let J_{C_1} and J_{C_2} be their respective Jacobians. Then*

$$\mathrm{Pic}(C_1 \times C_2) \cong \mathrm{Pic}(C_1) \times \mathrm{Pic}(C_2) \times \mathrm{Hom}(J_{C_1}, J_{C_2}).$$

Proof. See Smith [36, Theorem 3.3.12 and Example 3.3.16]. □

The remainder of this section is dedicated to the proof of Proposition 4.2.19, which is a direct analogue of Proposition 4.2.11 for the Néron-Severi group. The proof of Proposition 4.2.19 relies on the fact that

$$\mathrm{Pic}^0(X) \times \mathrm{Pic}^0(Y) \cong \mathrm{Pic}^0(X \times Y).$$

when X and Y are nonsingular projective varieties and either $\operatorname{char} k = 0$ or $\operatorname{char} k > 0$ and X and Y are each isomorphic to the reductions of nonsingular projective varieties over a field of characteristic zero. We now explain what this means in detail.

Let k be a field of positive characteristic and let X be a nonsingular projective variety over k. A *nonsingular projective lifting* of X is a separated scheme $\mathcal{X}$ over a discrete valuation ring $(R, \mathfrak{p})$ such that (i) $\operatorname{char} \mathrm{Frac}(R) = 0$ and $R/\mathfrak{p} = k$, (ii) $\mathcal{X} \times_R k \cong X$, and (iii) $\mathcal{X}$ is nonsingular and projective over R.

Lemma 4.2.12. *Let X and Y be smooth projective varieties over an algebraically closed field k of positive characteristic. If X and Y have nonsingular projective liftings, then so does $X \times Y$.*

Proof. See Diem [11, Proof of Proposition A.4]. □

Proposition 4.2.13. *Let X be a nonsingular projective variety over a field of positive characteristic. If X has a nonsingular projective lifting, then $\mathrm{Pic}^0(X)$ is reduced.*

Proof. See Diem [11, Lemma A.3]. □

Theorem 4.2.14. *Let X be a nonsingular projective variety over a field of positive characteristic. If*

$$H^2(X, \Omega_X^\vee) = H^2(X, \mathscr{O}_X) = 0,$$

then X has a nonsingular projective lifting and so $\mathrm{Pic}^0(X)$ is reduced.

Proof. Grothendieck [16, Exposé III, Théorème 7.3] proves that the lifting exists in this case; then $\mathrm{Pic}^0(X)$ is reduced by Proposition 4.2.13. □

Corollary 4.2.15. *Let X be a nonsingular projective curve. Then $\mathrm{Pic}^0(X)$ is reduced.*

Proof. For a curve, $H^2(X, \Omega_X^\vee) = H^2(X, \mathscr{O}_X) = 0$ by Theorem 1.2.4(i), so the result follows from Theorem 4.2.14. □

Theorem 4.2.16 (Cartier)**.** *Let k be a field of characteristic 0 and let G be a group scheme over k. Then G is nonsingular and hence reduced.*

Proof. See Mumford [30, Lecture 25]. □

Proposition 4.2.17. *Let X and Y be smooth projective varieties over an algebraically closed field k. Then the map*

$$\varphi : \mathrm{Pic}^0(X) \times \mathrm{Pic}^0(Y) \to \mathrm{Pic}^0(X \times Y)$$

given by

$$\varphi(\mathscr{L}, \mathscr{L}') = \pi_1^* \mathscr{L} \otimes \pi_2^* \mathscr{L}'$$

induces an isomorphism of abelian varieties

$$\varphi_{\mathrm{red}} : \mathrm{Pic}^0(X)_{\mathrm{red}} \times \mathrm{Pic}^0(Y)_{\mathrm{red}} \to \mathrm{Pic}^0(X \times Y)_{\mathrm{red}}$$

where $\cdot_{\mathrm{red}}$ denotes the associated unique reduced subscheme.

Proof. See Diem [11, Proposition A.4]. □

Corollary 4.2.18. *Let X and Y be smooth projective varieties over an algebraically closed field k. If $\operatorname{char} k = 0$ or if $\operatorname{char} k > 0$ and X and Y have nonsingular projective liftings, then*

$$\varphi : \mathrm{Pic}^0(X) \times \mathrm{Pic}^0(Y) \to \mathrm{Pic}^0(X \times Y)$$

is an isomorphism of abelian varieties.

Proof. This follows upon combining Theorem 4.2.16, Proposition 4.2.13 and Lemma 4.2.12 with Proposition 4.2.17. □

Proposition 4.2.19. *Let C_1 and C_2 be curves over a field k and let J_{C_1} and J_{C_2} be their respective Jacobians. Then the Néron-Severi group of $C_1 \times C_2$ is given by*

$$\mathrm{NS}(C_1 \times C_2) \cong \mathrm{NS}(C_1) \times \mathrm{NS}(C_2) \times \mathrm{Hom}(J_{C_1}, J_{C_2}).$$

Proof. Consider the following diagram:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \mathrm{Pic}^0(C_1) \times \mathrm{Pic}^0(C_2) & \longrightarrow & \mathrm{Pic}^0(C_1 \times C_2) & \longrightarrow & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Pic}(C_1) \times \mathrm{Pic}(C_2) & \longrightarrow & \mathrm{Pic}(C_1 \times C_2) & \longrightarrow & \mathrm{Hom}(J_{C_1}, J_{C_2}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{NS}(C_1) \times \mathrm{NS}(C_2) & \longrightarrow & \mathrm{NS}(C_1 \times C_2) & \longrightarrow & \mathrm{Hom}(J_{C_1}, J_{C_2}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

The diagram is commutative by construction and the columns are exact by definition (the last column being simply the identity map). The first row is exact by Corollary 4.2.18 and the second row is exact by Proposition 4.2.11. Hence, by the 9-Lemma, the bottom row is exact, giving

$$\mathrm{NS}(C_1 \times C_2) \cong \mathrm{NS}(C_1) \times \mathrm{NS}(C_2) \times \mathrm{Hom}(J_{C_1}, J_{C_2})$$

as required. □

Milne [27, Theorem 12.5] shows that for abelian varieties $\mathcal{A}$ and $\mathcal{B}$, $\mathrm{Hom}(\mathcal{A}, \mathcal{B})$ is a finitely generated free $\mathbb{Z}$-module of rank at most $4 \dim(\mathcal{A}) \dim(\mathcal{B})$. In particular $\mathrm{Hom}(J_{C_1}, J_{C_2}) \cong \mathbb{Z}^r$ for some $r \leqslant 4g_1g_2$, where g_1 and g_2 are the genera of C_1 and C_2 respectively. Further analysis of $\mathrm{Hom}(J_{C_1}, J_{C_2})$ usually takes place by means of the theory of correspondences, for which the reader is invited to consult Smith [36], in particular Chapter 3.

4.3 Notation

The purpose of this section is to collect together the notation used in the remaining sections of this chapter in one place, thus providing an easy reference.

Let $f : X \to Y$ be a morphism of varieties. We denote by Γ_f the divisor on $X \times Y$ corresponding to the graph of f; that is

$$\Gamma_f = (\mathrm{id}_C \times f)(X) = \{(P, f(P)) \in X \times Y \mid \text{for all } P \in X\},$$

where $\mathrm{id}_C : C \to C$ is the identity map.

We fix the following notation for the remainder of this chapter. Let k be a field of characteristic different from two with fixed algebraic closure $\overline{k}$ and let C be a hyperelliptic curve of genus $g \geqslant 2$ over k. For convenience we set $\gamma = g - 1$. Let J_C denote the Jacobian of C. Let η denote the hyperelliptic involution on C, and let $p_i : C \times C \to C$, $i = 1, 2$, be the projection maps. We define the divisor $D_\infty = \kappa^*(\infty)$ in $\mathrm{Div}(C)$ where $\kappa : C \to \mathbb{P}^1$ is the hyperelliptic covering of $\mathbb{P}^1$.

Fix a Weierstrass point $\infty \in C(\overline{k})$. Define the following divisors on $C \times C$:

$$\begin{gathered} V_\infty := p_1^*(\infty) = \{\infty\} \times C; \quad H_\infty := p_2^*(\infty) = C \times \{\infty\}; \\ V := p_1^*(D_\infty); \quad H := p_2^*(D_\infty); \\ F := V + H \\ \Delta = \Gamma_{\mathrm{id}_C}; \quad \nabla = \Gamma_\eta \\ D_\nabla = (\Gamma_\eta)_*(D_\infty) \in \nabla. \end{gathered}$$

Note that $V \times \overline{k} \sim_{\mathrm{rat}} 2V_\infty$ and $H \times \overline{k} \sim_{\mathrm{rat}} 2H_\infty$, so V and H are rational.

Let $\sigma : C \times C \to C \times C$ be defined by $\sigma(P, Q) = (Q, P)$ and set $G = \langle \sigma \rangle$. Let $S = \mathrm{Sym}^2(C) = (C \times C)/G$ and let $\pi : C \times C \to S$ denote the quotient map (see Section 1.5). Define the following divisors on S:

$$\begin{gathered} \Theta_S = \pi(V_\infty) = \pi(H_\infty); \\ \Delta_S = \pi(\Delta); \quad \nabla_S = \pi(\nabla) \end{gathered}$$

(these are the scheme-theoretic images of V_∞, H_∞, Δ and ∇). Note that $2\Theta_S$ is a k-rational divisor since $2\Theta_S \sim_{\mathrm{rat}} \pi_*(V)$, even though Θ_S is not k-rational in general.

4.4 Cohomology of divisors on a hyperelliptic Jacobian

In this section we give formulæ for the dimensions of the cohomology groups of a divisor on an abelian variety. We are primarily interested in the case of surfaces, which, for an abelian variety, often arise as the Jacobian of a curve of genus two. This section is included for completeness to cover the case of abelian surfaces.

Proposition 4.4.1. *The canonical divisor on an abelian variety is trivial.*

Proof. See Shafarevich [35, Example II.6.3]. □

Proposition 4.4.2. *Let $\mathcal{A}$ be an abelian variety and let $\mathscr{L}$ be an invertible sheaf on $\mathcal{A}$ such that $H^0(\mathcal{A}, \mathscr{L}) \neq 0$. Then $\mathscr{L}$ is ample if and only if $\dim K_{\mathscr{L}} = 0$ (where $K_{\mathscr{L}}$ is the closed subscheme of $\mathcal{A}$ defined in Section 1.6).*

Proof. See Milne [27, Proposition 9.1]. □

Proposition 4.4.3. *Let $\mathcal{A}$ be an abelian variety of dimension g. Then for $i = 0, \ldots, g$, we have*

$$h^i(\mathcal{A}, \mathscr{O}_{\mathcal{A}}) = \binom{g}{i}.$$

In particular, $\chi(\mathscr{O}_{\mathcal{A}}) = 0$.

Proof. See Mumford [32, Section 13, Corollary 2] for the dimension formula. The last part follows from the well known identity: $\sum_{i=0}^{g}(-1)^i\binom{g}{i} = 0$ for any $g > 0$. □

Theorem 4.4.4 (Riemann-Roch for abelian varieties)**.** *Let $\mathcal{A}$ be an abelian variety of dimension g, and let D be a divisor on $\mathcal{A}$. Then*

$$\chi(D) = \frac{D^g}{g!}\cdot$$

Proof. See Milne [27, Theorem 13.3]. □

Remark 4.4.5. Let $\mathcal{A}$ be an abelian surface and let D be a divisor on $\mathcal{A}$. Then Theorem 4.4.4 and Proposition 4.1.5 give two different formulæ for $\chi(D)$. To see that they agree, note that $K_{\mathcal{A}} \sim_{\text{rat}} 0$ for any canonical divisor $K_{\mathcal{A}}$ on $\mathcal{A}$ by Proposition 4.4.1 and $\chi(\mathscr{O}_{\mathcal{A}}) = 0$ by Proposition 4.4.3. Hence

$$\frac{1}{2}D \cdot (D - K_{\mathcal{A}}) + \chi(\mathscr{O}_{\mathcal{A}}) = \frac{1}{2}D^2$$

which shows that Theorem 4.4.4 and Proposition 4.1.5 agree when $g = 2$.

Lemma 4.4.6. *Let J be a Jacobian variety of dimension g and let Θ be the theta divisor of J. Then $h^0(J, m\Theta) \neq 0$ and $h^i(J, m\Theta) = 0$ for all $i > 0$ and $m > 0$. In particular, $\chi(m\Theta) = h^0(J, m\Theta) > 0$ for all $m > 0$.*

Proof. We have $h^0(\mathcal{A}, m\Theta) \neq 0$ because Θ is effective and hence $m\Theta$ is effective. Further, $m\Theta$ is ample since Θ is ample, and so Proposition 4.4.2 implies that $\dim K_{m\Theta} = 0$. Thus $h^i(\mathcal{A}, m\Theta) = 0$ for $i > 0$ by Theorem 1.6.1(ii). □

Proposition 4.4.7. *Let J be a Jacobian variety of dimension g and let Θ be the theta divisor of J. Then $\Theta^g = g!$ and $\chi(m\Theta) = h^0(J, m\Theta) = m^g$ for $m > 0$.*

Proof. The map $\varphi_\Theta : J \to \mathrm{Pic}(J)$ is an isomorphism (see Milne [28, Theorem 6.6]) and hence has degree 1. Thus $\chi(\Theta)^2 = 1$ by Theorem 1.6.1(i) and hence $\chi(\Theta) = \pm 1$. But $\chi(\Theta) > 0$ by Lemma 4.4.6, hence $\chi(\Theta) = h^0(\mathcal{A}, \Theta) = 1$.

Now Theorem 4.4.4 implies that $1 = \chi(\Theta) = \Theta^g/g!$, hence $\Theta^g = g!$. Applying Theorem 4.4.4 to $m\Theta$ for $m > 0$ gives $\chi(m\Theta_J) = h^0(J, m\Theta) = m^g$ by the linearity of the intersection pairing and Lemma 4.4.6. □

Proposition 4.4.8. *Let $\mathcal{A}$ be an abelian variety. Then $\mathrm{NS}(\mathcal{A}) \cong \mathbb{Z}^\rho$ for some ρ satisfying $1 \leqslant \rho \leqslant 4\dim(\mathcal{A})^2$.*

Proof. As Θ_{J_C} is ample, $\operatorname{rank} \mathrm{NS}(\mathcal{A}) \geqslant 1$. Mumford [32, Section 19, Corollaries 1 and 2] shows that the map $\varphi_{\mathscr{L}} : \mathcal{A} \to \mathrm{Pic}(\mathcal{A})$ defined by $x \mapsto \tau_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$ induces an injection of $\mathrm{NS}(\mathcal{A})$ into $\mathrm{End}(\mathcal{A})$ and that $\mathrm{End}(\mathcal{A})$ has rank at most $4\dim(\mathcal{A})^2$. □

Proposition 4.4.9. *Let J be the Jacobian of a curve of genus g. Then*

(i) $h^i(J, \mathscr{O}_J) = \binom{g}{i}$ *for* $i = 0, \ldots, g$.

(ii) If $m \neq 0$, *then* $h^i(J, \mathscr{O}_J(m\Theta_J)) = 0$ *for* $0 < i < g$.

(iii) If $m > 0$, *then* $h^0(J, \mathscr{O}_J(m\Theta_J)) = m^g$ *and* $h^g(J, \mathscr{O}_J(m\Theta_J)) = 0$.

(iv) If $m < 0$, *then* $h^g(J, \mathscr{O}_J(m\Theta_J)) = m^g$ *and* $h^0(J, \mathscr{O}_J(m\Theta_J)) = 0$.

Proof. The case $m = 0$ is proved in Proposition 4.4.3, and the case $m > 0$ in Proposition 4.4.7.

Let $m < 0$. Then $H^i(J, m\Theta) \cong H^{g-i}(J, -m\Theta)$ by Theorem 1.2.4(ii), since the canonical divisor of J is trivial by Proposition 4.4.1. Since $-m > 0$, Proposition 4.4.7 gives $h^i(J, m\Theta) = h^{g-i}(J, -m\Theta) = 0$ for $i = 0, \ldots, g-1$ and $h^g(J, m\Theta) = h^0(J, -m\Theta) = m^g$. □

4.5 Cohomology of divisors on the square of a hyperelliptic curve

This section forms the core of this chapter. We prove a decomposition result for the space of sections of a divisor on the square of a hyperelliptic curve in Theorem 4.5.11, from which we derive explicit formulæ for the dimension of such a space.

Lemma 4.5.1. *A canonical divisor on $C \times C$ is given by*

$$K_{C\times C} = \gamma F$$

and we have $\chi(\mathscr{O}_{C\times C}) = \gamma^2$.

Proof. Let $K_C = \gamma D_\infty$ be a canonical divisor on C. Hartshorne [17, Exercise II.8.3(b)] states that $p_1^* K_C + p_2^* K_C$ is in the canonical class of $C \times C$ hence $K_{C\times C} = p_1^* K_C + p_2^* K_C = \gamma(V+H)$ is a canonical divisor. We have $\chi(\mathscr{O}_{C\times C}) = g^2 - 2g + 1 = (g-1)^2$ by Hartshorne [17, Exercise I.7.2(e)]. □

Lemma 4.5.2. *On $C \times C$ we have*

$$\Delta + \nabla \sim_{\text{rat}} 2V_\infty + 2H_\infty.$$

Proof. Let $\{1, x\}$ is a basis for $\Gamma(C, D_\infty)$ and write $x_1 = x \otimes 1$ and $x_2 = 1 \otimes x$ in $k(C \times C)$. Then

$$\operatorname{div}(x_1 - x_2) = \Delta + \nabla - 2V_\infty - 2H_\infty.$$ □

Proposition 4.5.3. *The intersection pairing on* $\operatorname{Div}(C \times C) \times \operatorname{Div}(C \times C)$ *is given by the following table:*

$\cdot$	V_∞	H_∞	Δ	∇
V_∞	*0*	*1*	*1*	*1*
H_∞	*1*	*0*	*1*	*1*
Δ	*1*	*1*	$2-2g$	$2+2g$
∇	*1*	*1*	$2+2g$	$2-2g$

Let $D = mV_\infty + nH_\infty + r\nabla$ be a divisor on $C \times C$. Then

$$\chi(D) = (m-\gamma)(n-\gamma) + r(m+n) - \gamma r(r+2).$$

In particular, when $m = n$ and $g = 2$,

$$\chi(D) = (m-1)^2 + 2mr - r(r+2).$$

Proof. First note that $2V_\infty \sim_{\mathrm{rat}} \{P\} \times C + \{\eta(P)\} \times C$ for any point $P \in C$. Pick $P \neq \infty \in C(\overline{k})$. Then $2V_\infty^2 \sim_{\mathrm{rat}} V_\infty \cdot (\{P\} \times C + \{\eta(P)\} \times C) = 0$ since $V_\infty \cap \{P\} \times C = V_\infty \cap \{\eta(P)\} \times C = \emptyset$. Hence $V_\infty^2 = 0$. The same proof, *mutatis mutandis*, shows that $H_\infty^2 = 0$.

Next, we have

$$V_\infty \cdot H_\infty = V_\infty \cdot \Delta = V_\infty \cdot \nabla = H_\infty \cdot \Delta = H_\infty \cdot \nabla = 1$$

because each pair intersect transversally at a unique point.

We have $\Delta \cdot \nabla = \#(\Delta \cap \nabla) = 2g + 2$ since each point of intersection corresponds to a Weierstrass point on C and the intersections are non-singular hence transversal. Then

$$\Delta^2 = \Delta \cdot (2V_\infty + 2H_\infty - \nabla) = 2 + 2 - (2g + 2) = 2 - 2g.$$

A similar calculation yields $\nabla^2 = 2 - 2g$.

Now let $D = mV_\infty + nH_\infty + r\nabla$. By Lemma 4.5.1, a canonical divisor on $C \times C$ is given by $K_{C\times C} = 2\gamma(V_\infty + H_\infty)$, so Proposition 4.1.5 gives

$$\begin{aligned}
\chi(D) &= \frac{1}{2} D \cdot (D - K_{C\times C}) + \chi(\mathscr{O}_{C\times C}) \\
&= \frac{1}{2}(mV_\infty + nH_\infty + r\nabla) \cdot ((m - 2\gamma)V_\infty + (n - 2\gamma)H_\infty + r\nabla) + \gamma^2 \\
&= \frac{1}{2}((r + m)(n - 2\gamma) + r(m + n) + (r + n)(m - 2\gamma) - 2\gamma r^2) + \gamma^2 \\
&= (m - \gamma)(n - \gamma) + r(m + n) - \gamma r(r + 2)
\end{aligned}$$

as required. In particular, when $g = 2$ and $m = n$, we obtain

$$\chi(D) = (m - 1)^2 + 2mr - r(r + 2),$$

which completes the proof. □

Lemma 4.5.4. *The divisor classes* $[V_\infty]$, $[H_\infty]$ *and* $[\Delta]$ *are linearly independent in* $\mathrm{Num}(C \times C)$. *In particular,* $\operatorname{rank} \mathrm{Num}(C \times C) \geqslant 3$.

Proof. Let $D_{m,n,r} = m[V_\infty] + n[H_\infty] + r[\Delta]$ be numerically equivalent to zero. Then by Proposition 4.5.3 we obtain the simultaneous equations

$$\begin{aligned}
0 &= D_{m,n,r} \cdot [V_\infty] = n + r \\
0 &= D_{m,n,r} \cdot [H_\infty] = m + r \\
0 &= D_{m,n,r} \cdot [\Delta] = m + n - 2\gamma r.
\end{aligned}$$

Since $\gamma \geqslant 1$, it immediately follows that $m = n = r = 0$; hence $[V_\infty]$, $[H_\infty]$ and $[\Delta]$ are linearly independent in $\mathrm{Num}(C \times C)$. □

Proposition 4.5.5. *The Néron-Severi group of $C \times C$ is given by*

$$\mathrm{NS}(C \times C) \cong \mathbb{Z}^{2+\rho}$$

for some ρ satisfying $1 \leqslant \rho \leqslant 4g^2$. In particular, $\mathrm{NS}(C \times C) \cong \mathrm{Num}(C \times C)$.

Proof. That $\mathrm{NS}(C \times C) \cong \mathbb{Z}^{2+\rho}$ follows immediately from Lemma 4.2.10 and Proposition 4.2.19. So $\mathrm{NS}(C \times C)$ is free, hence $\mathrm{Num}(C \times C) \cong \mathrm{NS}(C \times C)$ by Corollary 4.2.9. □

Proposition 4.5.5 shows that, up to algebraic equivalence, all divisors on $C \times C$ are of the form $mV_\infty + nH_\infty + r\Delta$ or come from additional structure of $\mathrm{End}(J)$.

Lemma 4.5.6. *Let m and r be non-negative integers. Then*

$$0 \to \mathscr{O}_{C\times C}(mF + (r-1)\nabla) \to \mathscr{O}_{C\times C}(mF + r\nabla) \to \iota_*\mathscr{O}_\nabla((2m - \gamma r)D_\nabla) \to 0$$

is an exact sequence where $\iota : \nabla \to C \times C$ is the embedding. We thus obtain a long exact sequence of cohomology

$$\begin{aligned} 0 &\to H^0(C \times C, mF + (r-1)\nabla) \to H^0(C \times C, mF + r\nabla) \\ &\to H^0(\nabla, (2m - \gamma r)D_\nabla) \to H^1(C \times C, mF + (r-1)\nabla) \\ &\to H^1(C \times C, mF + r\nabla) \to H^1(\nabla, (2m - \gamma r)D_\nabla) \to \cdots \end{aligned} \tag{4.1}$$

Proof. By definition we have a short exact sequence

$$0 \to \mathscr{O}_{C\times C}(-\nabla) \to \mathscr{O}_{C\times C} \to \iota_*\mathscr{O}_\nabla \to 0. \tag{4.2}$$

Tensoring (4.2) with $\mathscr{O}_{C\times C}(mF + r\nabla)$ (which is invertible, hence flat) preserves exact sequences, so we obtain

$$0 \to \mathscr{O}_{C\times C}(mF+(r-1)\nabla) \to \mathscr{O}_{C\times C}(mF+r\nabla) \to \mathscr{O}_{C\times C}(mF+r\nabla)\otimes\iota_*\mathscr{O}_\nabla \to 0.$$

Thus it remains to show that $\mathscr{O}_{C\times C}(mF + r\nabla) \otimes \mathscr{O}_\nabla \cong \iota_*\mathscr{O}_\nabla((2m - \gamma r)D_\nabla)$.

First note that $\mathscr{O}_{C\times C}(mF+r\nabla) \cong \mathscr{O}_{C\times C}((m+r)F-r\Delta)$ by Lemma 4.5.2. Then, using the fact that ∇ is effective, we have

$$\begin{aligned} \mathscr{O}_{C\times C}(mF + r\nabla) \otimes \mathscr{O}_\nabla &\cong \mathscr{O}_{C\times C}((m+r)F - r\Delta) \otimes \iota_*\mathscr{O}_\nabla \\ &\cong \mathscr{O}_{C\times C}((m+r)F - r\Delta)|_\nabla \\ &\cong \iota_*\mathscr{O}_\nabla((m+r)F|_\nabla - r\Delta|_\nabla). \end{aligned}$$

Since $F|_\nabla \sim_{\mathrm{rat}} 2D_\nabla$ and $\Delta|_\nabla \sim_{\mathrm{rat}} (g+1)D_\nabla$, we have

$$(m+r)F|_\nabla - r\Delta|_\nabla \sim_{\mathrm{rat}} (2m + r - gr)D_\nabla = (2m - \gamma r)D_\nabla$$

as required. Finally, the long exact sequence follows from Proposition 1.2.2. □

Lemma 4.5.7. *Let $m > \gamma$ be an integer. Then*

$$H^1(C \times C, mF) = H^2(C \times C, mF) = 0.$$

Proof. Note that $mF = p_1^*(mD_\infty) + p_2^*(mD_\infty)$, so by Theorem 1.2.5,

$$H^1(C \times C, mF) \cong (H_C^0 \otimes H_C^1) \oplus (H_C^1 \otimes H_C^0) \tag{4.3}$$

and

$$H^2(C \times C, mF) \cong (H_C^0 \otimes H_C^2) \oplus (H_C^1 \otimes H_C^1) \oplus (H_C^2 \otimes H_C^0) \tag{4.4}$$

where we have denoted $H^i(C, mD_\infty)$ by H_C^i for $i = 0, 1, 2$. Theorem 1.2.4(i) implies that $H_C^2 = 0$, so it suffices to prove that $H_C^1 = 0$, for then (4.3) and (4.4) will be sums of zero spaces and hence zero.

By Theorem 1.2.4(ii), $H^1(C, mD_\infty) \cong H^0(C, K_C - mD_\infty)$ where $K_C = \gamma D_\infty$ is a canonical divisor on C. But $\deg(K_C - mD_\infty) = \deg((\gamma - m)D_\infty) < 0$ since $m > \gamma$, and so $H^0(C, K_C - mD_\infty) = 0$ by Proposition 1.1.3. □

Proposition 4.5.8. *Let m be an integer satisfying $m > \gamma$ and let r be a positive integer satisfying $2m - \gamma r > 0$. Then*

$$H^1(C \times C, mF + (r-1)\nabla) = 0.$$

Proof. We proceed by induction on r. The case $r = 1$ follows from Lemma 4.5.7.

Now assume $H^1(C \times C, mF + (r-2)\nabla) = 0$ for $r \geqslant 2$ and $2m - \gamma r > 0$. Considering the long exact sequence of cohomology (4.1) of Lemma 4.5.6 (with $r - 1$ in place of r there) it suffices to prove that

$$H^1(\nabla, (2m - \gamma(r-1))D_\nabla) = 0,$$

for then, applying the induction hypothesis, $H^1(C \times C, mF + (r-1)\nabla)$ will be surrounded by zeros in (4.1) and hence must be zero. But

$$H^1(\nabla, (2m - \gamma(r-1))D_\nabla) \cong H^0(\nabla, K_\nabla - (2m - \gamma(r-1))D_\nabla)$$

by Theorem 1.2.4(ii), where $K_\nabla = \gamma D_\nabla$ is a canonical divisor on ∇. Then $\deg_\nabla(K_\nabla - (2m - \gamma(r-1))D_\nabla) = \deg_\nabla(-(2m - \gamma r)D_\nabla) < 0$ since $2m - \gamma r > 0$ and so by Proposition 1.1.3 we obtain $H^1(\nabla, (2m - \gamma(r-1))D_\nabla) = 0$. □

Proposition 4.5.9. *Let m be an integer satisfying $m > \gamma$. Then for all positive integers r satisfying $2m - \gamma r \neq 0$, we have a short exact sequence*

$$\begin{aligned} 0 \to H^0(C \times C, mF + (r-1)\nabla) \\ \to H^0(C \times C, mF + r\nabla) \\ \to H^0(\nabla, (2m - \gamma r)D_\nabla) \to 0. \end{aligned} \tag{4.5}$$

Proof. If $2m-\gamma r < 0$, then Proposition 1.1.3 implies $H^0(\nabla, (2m-\gamma r)D_\nabla) = 0$. From the long exact sequence (4.1) of Lemma 4.5.6 we thus obtain

$$H^0(C \times C, mF + (r-1)\nabla) \cong H^0(C \times C, mF + r\nabla) \tag{4.6}$$

and so (4.5) follows.

If $2m - \gamma r > 0$, we obtain

$$\begin{aligned} 0 \to H^0(C \times C, mF + (r-1)\nabla) &\to H^0(C \times C, mF + r\nabla) \\ \to H^0(\nabla, (2m - \gamma r)D_\nabla) &\to H^1(C \times C, mF + (r-1)\nabla) \to \cdots \end{aligned}$$

from the long exact sequence (4.1) of Lemma 4.5.6. Proposition 4.5.8 implies $H^1(C \times C, mF + (r-1)\nabla) = 0$ from which (4.5) follows. □

Unfortunately we have been unable to prove Proposition 4.5.9 in the case where $2m - \gamma r = 0$, nor have we been able to find a counterexample. In Chapter 5 we present an algorithm which produces an explicit basis for the space $H^0(C \times C, mF + r\nabla)$ for all integers $m > \gamma$ and $r \geqslant 0$. Using this algorithm we are able to compute the codimension of the space $H^0(C \times C, mF + (r-1)\nabla)$ in $H^0(C \times C, mF + r\nabla)$. In each of the many tests we performed, the codimension has always been equal to one, in which case we can deduce that the injection

$$\frac{H^0(C \times C, mF + r\nabla)}{H^0(C \times C, mF + (r-1)\nabla)} \to H^0(\nabla, \mathscr{O}_\nabla)$$

must be surjective since $h^0(\nabla, \mathscr{O}_\nabla) = 1$ and hence that (4.5) is exact. So we see that the numerical evidence thus supports the claim that the sequence (4.5) is exact, though a proof has not been forthcoming. In lieu of a proof, we present the exactness of (4.5) in the case $2m - \gamma r = 0$ as the following conjecture, and we therefore treat the case $2m - \gamma r = 0$ separately in the results which follow.

Conjecture 4.5.10. *Let m and r be integers satisfying $2m = \gamma r$. Then the sequence*

$$0 \to H^0(C \times C, mF + (r-1)\nabla) \to H^0(C \times C, mF + r\nabla) \to H^0(\nabla, \mathscr{O}_\nabla) \to 0.$$

is exact.

Theorem 4.5.11. *Let m and r be integers satisfying $m > \gamma$ and $r \geqslant 0$. Suppose $2m - \gamma i \neq 0$ for $i = 1, \ldots, r$. We have*

$$H^0(C \times C, mF + r\nabla) \cong H^0(C \times C, mF) \oplus \bigoplus_{i=1}^{r} H^0(\nabla, (2m - \gamma i)D_\nabla). \tag{4.7}$$

and

$$h^0(C \times C, mF + r\nabla) = \begin{cases} (2m-\gamma)^2 + 4mr - \gamma r(r+2) & \text{if } \gamma < 2m - \gamma r, \\ (2m-\gamma)^2 + 4mr - \gamma r(r+1) - 2m + g & \text{if } 0 < 2m - \gamma r \leqslant \gamma, \\ h^0(C \times C, mF + \left\lfloor \frac{2m}{\gamma} \right\rfloor \nabla) & \text{if } 2m - \gamma r < 0. \end{cases}$$

If $2m - \gamma i = 0$ for some i satisfying $1 \leqslant i \leqslant r$ and if Conjecture 4.5.10 is true, then (4.7) holds and

$$h^0(C \times C, mF + r\nabla) = (2m-\gamma)^2 + 2m(i-2) + g + 1.$$

Proof. We first consider the case where $2m - \gamma i \neq 0$ for all $i = 1, \ldots, r$.

The isomorphism (4.7) is trivial for $r = 0$, so assume $r > 0$. Since the sequence (4.5) is exact, $H^0(C \times C, mF + r\nabla)$ splits as

$$\begin{aligned} &H^0(C \times C, mF + r\nabla) \\ &\quad \cong H^0(C \times C, mF + (r-1)\nabla) \oplus H^0(\nabla, (2m - \gamma r)D_\nabla). \end{aligned} \tag{4.8}$$

and we obtain (4.7) by applying (4.8) recursively. It follows that

$$h^0(C \times C, mF + r\nabla) = h^0(C \times C, mF) + \sum_{i=1}^{r} h^0(\nabla, (2m - \gamma i)D_\nabla).$$

As $m > \gamma$, $\deg(mD_\infty) = 2m > 2\gamma$ so Riemann-Roch for curves implies $h^0(C, mD_\infty) = 2m - g + 1 = 2m - \gamma$. Then by Theorem 1.2.5,

$$h^0(C \times C, mF) = h^0(C, mD_\infty)^2 = (2m-\gamma)^2.$$

For an integer i satisfying $\gamma < 2m - \gamma i$, we have

$$h^0(\nabla, (2m - \gamma i)D_\nabla) = 2(2m - \gamma i) - \gamma$$

by Riemann-Roch for curves. When $\gamma < 2m - \gamma r$ we thus obtain

$$\sum_{i=1}^{r} h^0(\nabla, (2m - \gamma i)D_\nabla) = 4mr - \gamma r(r+2) \tag{4.9}$$

and hence

$$h^0(C \times C, mF + r\nabla) = (2m-\gamma)^2 + 4mr - \gamma r(r+2). \tag{4.10}$$

Now suppose $0 < 2m - \gamma r \leqslant \gamma$. In this case $\gamma < 2m - \gamma(r-1)$ so we can apply (4.10) to obtain

$$h^0(C \times C, mF + (r-1)\nabla) = (2m-\gamma)^2 + 4m(r-1) - \gamma(r-1)(r+1).$$

Note that, since $\nabla \cong C$, we have $h^0(\nabla, nD_\nabla) = h^0(C, nD_\infty) = h^0(C, 2n(\infty))$. Hence the Weierstrass Gap Theorem (see, for example, Hirschfeld et al. [19, Theorem 6.89]) implies that $h^0(\nabla, (2m - \gamma r)D_\nabla) = 2m - \gamma r + 1$. We thus obtain

$$\begin{aligned} &h^0(C \times C, mF + r\nabla) \\ &\quad = h^0(C \times C, mF + (r-1)\nabla) + h^0(\nabla, (2m - \gamma r)D_\nabla) \\ &\quad = (2m - \gamma)^2 + 4mr - \gamma r(r+1) - 2m + g. \end{aligned} \tag{4.11}$$

Next, when $2m - \gamma r < 0$, we have $h^0(\nabla, (2m - \gamma r)D_\nabla) = 0$ and so

$$\begin{aligned} h^0(C \times C, mF + r\nabla) &= h^0(C \times C, mF) + \sum_{i=1}^{\lfloor 2m/\gamma \rfloor} h^0(\nabla, (2m - \gamma i)D_\nabla) \\ &= h^0(C \times C, mF + \left\lfloor \tfrac{2m}{\gamma} \right\rfloor \nabla). \end{aligned} \tag{4.12}$$

Finally, suppose $2m - \gamma i = 0$ for some i such that $1 \leqslant i \leqslant r$ and that Conjecture 4.5.10 is true. Then the arguments used to show (4.8) and (4.12) carry over *mutatis mutandis*. Since $2m - \gamma r \leqslant 0$, from (4.12) we obtain

$$h^0(C \times C, mF + r\nabla) = h^0(C \times C, mF + \left\lfloor \tfrac{2m}{\gamma} \right\rfloor \nabla) = h^0(C \times C, mF + i\nabla).$$

Now $2m - \gamma(i-1) = \gamma$, so we can apply (4.11) to obtain

$$h^0(C \times C, mF + (i-1)\nabla) = (2m - \gamma)^2 + 2m(i-2) + g. \tag{4.13}$$

Since $h^0(\nabla, (2m - \gamma i)D_\nabla) = h^0(\nabla, \mathscr{O}_\nabla) = 1$, we have

$$\begin{aligned} &h^0(C \times C, mF + i\nabla) \\ &\quad = h^0(C \times C, mF + (i-1)\nabla) + h^0(\nabla, \mathscr{O}_\nabla) \\ &\quad = (2m - \gamma)^2 + 2m(i-2) + g + 1. \end{aligned}$$

This completes the proof. □

In Theorem 4.5.11, we see that

$$h^0(C \times C, mF + r\nabla) = h^0(C \times C, mF + \left\lfloor \tfrac{2m}{\gamma} \right\rfloor \nabla)$$

when r satisfies $2m - \gamma r < 0$ which is essentially a consequence of (4.6). In this case, $0 \leqslant \left\lfloor \frac{2m}{\gamma} \right\rfloor < \gamma$ and so $h^0(C \times C, mF + r\nabla)$ is indeed described by the other cases of the theorem.

Corollary 4.5.12. *Let $m > \gamma$ and $r \geqslant 0$ be integers. Then*

$$h^2(C \times C, mF + r\nabla) = 0. \tag{4.14}$$

If $2m - \gamma i \neq 0$ for all $i = 1, \ldots, r$, then

$$h^1(C\times C, mF+r\nabla) = \begin{cases} 0 & \text{if } \gamma < 2m - \gamma r, \\ g - (2m - \gamma r) & \text{if } 0 < 2m - \gamma r \leqslant \gamma, \text{ and} \\ h^1(C \times C, mF + \left\lfloor \frac{2m}{\gamma} \right\rfloor \nabla) & \text{if } 2m - \gamma r < 0. \end{cases}$$

If $2m - \gamma i = 0$ for some i satisfying $1 \leqslant i \leqslant r$ and if Conjecture 4.5.10 is true, then

$$h^1(C \times C, mF + r\nabla) = g + 1.$$

Proof. By Lemma 4.5.1, $K_{C\times C} = \gamma F$ is a canonical divisor on $C \times C$. Then using Theorem 1.2.4(ii) we obtain

$$\begin{aligned} H^2(C \times C, mF + r\nabla) &\cong H^0(C \times C, (\gamma - m)F - r\nabla) \\ &\subseteq H^0(C \times C, (\gamma - m)F) \end{aligned}$$

and since $\gamma - m < 0$, we must have $H^0(C \times C, (\gamma - m)F) = 0$; this proves (4.14). Consequently

$$h^1(C \times C, mF + r\nabla) = h^0(C \times C, mF + r\nabla) - \chi(mF + r\nabla)$$

and the formulæ for $h^1(C \times C, mF + r\nabla)$ follow immediately by combining the formulæ for $\chi(mF+r\nabla)$ in Proposition 4.5.3 and for $h^0(C\times C, mF+r\nabla)$ in Theorem 4.5.11. □

4.6 Cohomology of divisors on the symmetric square of a hyperelliptic curve

This section follows the form of the previous section. We prove a decomposition result for the space of sections of a divisor on the symmetric square of a hyperelliptic curve in Theorem 4.6.12, from which we derive explicit formulæ for the dimension of such a space.

Proposition 4.6.1. *A canonical divisor on S is given by*

$$K_S = 2(g - 2)\Theta_S + \nabla_S.$$

The following proof of Proposition 4.6.1 was communicated to the author by Qing Liu.

Proof of Proposition 4.6.1. Since the quotient morphism π is étale outside of Δ on $C \times C$, the canonical map of differentials

$$\pi^*\Omega^1_{S/k} \to \Omega^1_{C\times C/k}$$

is then an isomorphism outside of Δ, and induces an injective homomorphism $\pi^*\omega_{S/k} \to \omega_{C\times C/k}$ of canonical sheaves. So $\pi^*\omega_{S/k} = \omega_{C\times C/k}(-D)$ for some effective divisor D on $C \times C$, with support in Δ, hence $D = r\Delta$ for some integer $r \geqslant 0$. It remains to show that $r = 1$, for then

$$\pi^*\omega_{S/k} = \omega_{C\times C/k}(-\Delta)$$

and the result will follow from the fact that

$$2K_S = \pi_*(\omega_{C\times C/k}(-\Delta)) = \pi_*(\gamma F - \Delta) \sim_{\mathrm{rat}} \pi_*((\gamma - 1)F + \nabla) = 4(g-2)\Theta_S + 2\nabla_S$$

where the first equality follows from Proposition 4.1.3.

Let ξ be the generic point of Δ. Then

$$\omega_{S/k,\pi(\xi)} \otimes \mathscr{O}_{C\times C,\xi} = (\pi^*\omega_{S/k})_\xi = \omega_{C\times C/k}(-r\Delta)_\xi = \omega_{C\times C/k,\xi}(-r\Delta)$$

and thus r may be computed Zariski locally. Let U be a dense open subset of C. Then one can compute r on $U^2 \to \mathrm{Sym}^2(U)$. If we can write U as an étale cover $U \to V \subseteq \mathbb{A}^1_k$, then the map

$$\pi^*\Omega^1_{\mathrm{Sym}^2(U)/k} \to \Omega^1_{U\times U/k}$$

is just the pull-back of the map

$$\pi^*\Omega^1_{\mathrm{Sym}^2(V)/k} \to \Omega^1_{V\times V/k}.$$

Let $\{dx_2, dx_2\}$ be a local basis for $\Omega^1_{V\times V/k}$. Then $\{d(x_1+x_2), d(x_1x_2)\}$ is a local basis for $\Omega^1_{\mathrm{Sym}^2(V)/k}$, and their pull-backs to $U \times U$ (respectively $\mathrm{Sym}^2(U)$) are local bases, and r can be computed with respect to these local bases. Now $\omega_{V\times V/k}$ is generated by $dx_1 \wedge dx_2$, and $\omega_{\mathrm{Sym}^2(V)/k}$ is generated by $d(x_1+x_2) \wedge d(x_1x_2)$ whose image in $\omega_{V\times V/k}$ is $(x_1 - x_2)(dx_1 \wedge dx_2)$. As $x_1 - x_2$ generates locally the ideal of Δ, we see that $r = 1$ as required. □

Corollary 4.6.2. *The self-intersection of K_S is $K_S^2 = (g-1)(4g-9)$.*

Proof. In the proof of Proposition 4.6.1 we saw that $\pi^*(K_S) = K_{C\times C} - \Delta$. Since $[K(C \times C) : K(S)] = 2$, Proposition 4.1.4 implies

$$2K_S^2 = (K_{C\times C} - \Delta)^2.$$

Now calculating the self-intersection with Proposition 4.5.3 we obtain

$$\begin{aligned} 2K_S^2 &= (K_{C\times C} - \Delta)^2 \\ &= 4\gamma^2(V_\infty + H_\infty)^2 - 4\gamma\Delta\cdot(V_\infty + H_\infty) + \Delta^2 \\ &= 8\gamma^2 - 8\gamma - 2\gamma \\ &= 2(g-1)(4g-9) \end{aligned}$$

and so $K_S^2 = (g-1)(4g-9)$ as required. □

Lemma 4.6.3. *For $m > \gamma$,*

$$h^0(S, 2m\Theta_S) = \binom{2m-\gamma+1}{2}.$$

Proof. By Proposition 1.5.2 we have

$$H^0(S, 2m\Theta_S) \cong H^0(C\times C, \pi^*(2m\Theta_S))^G = H^0(C\times C, mF)^G,$$

by Theorem 1.2.5 we have

$$H^0(C\times C, mF)^G \cong \Big(H^0(C, mD_\infty)\otimes H^0(C, mD_\infty)\Big)^G,$$

and by Riemann-Roch for curves we have

$$h^0(C, mD_\infty) = 2m - \gamma$$

for $m > \gamma$. So let $X_1, \ldots, X_{2m-\gamma}$ be a basis of $H^0(C, mD_\infty)$. Then $\{X_i \otimes X_j \mid 1 \leqslant i, j \leqslant 2m-\gamma\}$ is a basis for $H^0(C, mD_\infty)^{\otimes 2}$. An element

$$\sum_{i,j} \alpha_{ij} X_i \otimes X_j \in H^0(C, mD_\infty)^{\otimes 2}$$

is fixed by G if and only if $\alpha_{ij} = \alpha_{ji}$ for all i and j. A basis for such elements is given by

$$B = \{X_i \otimes X_j + X_j \otimes X_i \mid 1 \leqslant i, j \leqslant 2m-\gamma\}$$

of which there are

$$\#B = \binom{2m-\gamma+1}{2} = \frac{(2m-\gamma)(2m-\gamma+1)}{2}.$$

This completes the proof. □

Proposition 4.6.4. *The Euler characteristic of S is*

$$\chi(\mathscr{O}_S) = \frac{(g-1)(g-2)}{2}.$$

Proof. Let $m > \gamma$ and note that and $\pi_*(mF) = 4m\Theta_S$. By Proposition 1.2.6,

$$H^i(S, 4m\Theta_S) \cong H^i(C \times C, mF)$$

for any $i \geqslant 0$, but our choice of m implies

$$H^1(C \times C, mF) = H^2(C \times C, mF) = 0$$

by Proposition 4.5.7. Hence $H^1(S, 4m\Theta_S) = H^2(S, 4m\Theta_S) = 0$ and so $\chi(4m\Theta_S) = h^0(S, 4m\Theta_S)$ for $m > \gamma$. Then using Lemma 4.6.3, we see that

$$\begin{aligned}\chi(4m\Theta_S) &= h^0(S, 4m\Theta_S) \\ &= \binom{4m - \gamma + 1}{2} \\ &= \frac{4m(4m - 2\gamma + 1)}{2} + \binom{\gamma}{2}.\end{aligned}$$

But $\chi(4m\Theta_S)$ is a polynomial for *all* m (see Hartshorne [17, Exercise III.5.2]), so the result follows upon setting $m = 0$. □

Lemma 4.6.5. *On S we have*

$$4\Theta_S \sim_{\mathrm{rat}} \Delta_S + 2\nabla_S.$$

Proof. The result follows from the facts that

$$\pi^*(4\Theta_S - 2\nabla_S - \Delta_S) = 2F - 2\nabla - 2\Delta = \mathrm{div}((x_1 - x_2)^2)$$

and $\mathrm{div}((x_1 - x_2)^2)$ is symmetric, hence corresponds to a function on $\mathrm{Sym}^2(C)$. □

Proposition 4.6.6. *The intersection pairing on* $\mathrm{Div}(S) \times \mathrm{Div}(S)$ *is given by the following table:*

$\cdot$	Θ_S	Δ_S	∇_S
Θ_S	*1*	*2*	*1*
Δ_S	*2*	*4 - 4g*	*2 + 2g*
∇_S	*1*	*2 + 2g*	*1 - g*

Proof. The entries in the table follow immediately from Propositions 4.1.4 and 4.5.3:

$$\begin{aligned}
\Theta_S^2 &= \tfrac{1}{2}(\pi^*\Theta_S)^2 = \tfrac{1}{2}(V_\infty + H_\infty)^2 = 1;\\
\Delta_S^2 &= \tfrac{1}{2}(\pi^*\Delta_S)^2 = 2\Delta^2 = 4-4g;\\
\nabla_S^2 &= \tfrac{1}{2}(\pi^*\nabla_S)^2 = \tfrac{1}{2}\nabla^2 = 1-g;\\
\Theta_S\cdot\Delta_S &= \tfrac{1}{2}\pi^*(\Theta_S)\cdot\pi^*(\Delta_S) = (V_\infty+H_\infty)\cdot\Delta = 2;\\
\Theta_S\cdot\nabla_S &= \tfrac{1}{2}\pi^*(\Theta_S)\cdot\pi^*(\nabla_S) = \tfrac{1}{2}(V_\infty+H_\infty)\cdot\nabla = 1;\\
\Delta\cdot\nabla &= \tfrac{1}{2}\pi^*(\Delta)\cdot\pi^*(\nabla) = \Delta\cdot\nabla = 2+2g.
\end{aligned}$$

The remaining entries in the table then follow by the symmetry of the intersection pairing (see Theorem 4.1.1). □

Proposition 4.6.7. *If $D = m\Theta_S + r\nabla_S$ is an element of* $\mathrm{Div}(S)$*, then*

$$\chi(D) = \frac{(m-\gamma)(m-\gamma+1)}{2} + r(m+1) - \gamma\frac{r(r+1)}{2}$$

where $\gamma = g-1$.

Proof. This follows Propositions 4.1.5, 4.6.1 and 4.6.4 and the table of intersection pairings from Proposition 4.6.6: we have

$$\begin{aligned}
\chi(D) &= \frac{1}{2}D\cdot(D-K_S) + \chi(\mathscr{O}_S)\\
&= \frac{1}{2}(m\Theta_S + r\nabla_S)\cdot((m-2(g-2))\Theta_S + (r-1)\nabla_S) + \frac{(g-1)(g-2)}{2}\\
&= \frac{1}{2}\Big(m^2 - (2\gamma-1)m + \gamma(\gamma-1) + 2r(m-(g-2)) - \gamma r(r-1)\Big)\\
&= \frac{(m-\gamma)(m-\gamma+1)}{2} + r(m+1) - \gamma\frac{r(r+1)}{2}
\end{aligned}$$

as required. □

Remark 4.6.8. Let $D = m\Theta_S + n\Delta_S + r\nabla_S$ be an element of $\mathrm{Div}(S)$. Then by Lemma 4.6.5,

$$D \sim_{\mathrm{num}} m\Theta_S + n(4\Theta_S - 2\nabla_S) + r\nabla_S = (m+4n)\Theta_S + (r-2n)\nabla_S.$$

Since χ is constant on numerical equivalence classes by Proposition 4.2.5, we can apply Proposition 4.6.7 to obtain

$$\begin{aligned}
\chi(D) &= \chi((m+4n)\Theta_S + (r-2n)\nabla_S)\\
&= \frac{(m-\gamma)(m-\gamma+1)}{2} + 2mn + (m+1)r + 2\varepsilon nr\\
&\qquad - \gamma n(2n+3) - \gamma\frac{r(r+1)}{2}
\end{aligned}$$

where $\gamma = g-1$ and $\varepsilon = g+1$.

Proposition 4.6.9. *The torsion subgroup of* $\mathrm{NS}(S)$ *is given by*

$$\mathrm{NS}(S)_{\mathrm{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^{\tau}$$

for some τ *satisfying* $0 \leqslant \tau < \infty$.

Proof. Let D be a class in $\mathrm{NS}(S)$ and suppose that $mD = 0$ for some m. Then taking the pullback we get $m\pi^*(D) = 0$ on $\mathrm{NS}(C \times C)$, which implies $\pi^*(D) = 0$ since $\mathrm{NS}(C \times C)$ is torsion free by Proposition 4.5.5. Since $\pi_*\pi^*$ is multiplication-by-2 on $\mathrm{Div}(S)$ by Proposition 4.1.3, we have $2D = \pi_*\pi^*(D) = 0$, so D is 2-torsion. Hence $\mathrm{NS}(S)_{\mathrm{tors}} = (\mathbb{Z}/2\mathbb{Z})^{\tau}$. That τ is finite follows from Theorem 4.2.7. □

Proposition 4.6.10. *The rank of* $\mathrm{Num}(S)$ *satisfies*

$$2 \leqslant \operatorname{rank} \mathrm{Num}(S) \leqslant \operatorname{rank} \mathrm{Num}(C \times C).$$

The divisor classes $[\Theta_S]$ *and* $[\Delta_S]$ *are linearly independent in* $\mathrm{Num}(S)$.

Proof. Let $D_1, \ldots, D_\rho$ in $\mathrm{Num}(S)$ be a set of linearly independent divisor classes, where $\rho > \operatorname{rank} \mathrm{Num}(C \times C)$. Then $\sum_{i=1}^{\rho} n_i \pi^*(D_i) = 0$ for some integers n_i not all zero, and so by linearity we have $\pi^*(\sum_{i=1}^{\rho} n_i D_i) = 0$. Since $\pi_*\pi^*$ is multiplication-by-2 on $\mathrm{Div}(S)$ by Proposition 4.1.3, we obtain

$$2\sum_{i=1}^{\rho} n_i D_i = \pi_*\pi^*(\sum_{i=1}^{\rho} n_i D_i) = 0$$

which shows that $\sum_{i=1}^{\rho} n_i D_i$ is 2-torsion, contradicting the linear independence of the D_i. Hence $\rho \leqslant \operatorname{rank} \mathrm{Num}(C \times C)$.

Let $D_{m,r} = m[\Theta_S] + r[\Delta_S]$ be numerically equivalent to zero. Then by Proposition 4.6.6 we obtain the simultaneous equations

$$\begin{aligned} 0 &= D_{m,r} \cdot [\Theta_S] = m + 2r \\ 0 &= D_{m,r} \cdot [\Delta_S] = 2m - 4\gamma r \end{aligned}$$

and it immediately follows that $m = r = 0$; hence $[\Theta_S]$ and $[\Delta_S]$ are linearly independent in $\mathrm{Num}(S)$ and so $\operatorname{rank} \mathrm{Num}(S) \geqslant 2$. □

Corollary 4.6.11. *The Néron-Severi group of* S *is given by*

$$\mathrm{NS}(S) \cong \mathbb{Z}^{1+\rho} \times (\mathbb{Z}/2\mathbb{Z})^{\tau}$$

for ρ *satisfying* $1 \leqslant \rho \leqslant 4g^2$ *and* τ *satisfying* $0 \leqslant \tau < \infty$.

Proof. By Corollary 4.2.9, this is immediate from Proposition 4.6.10 and Proposition 4.6.9. □

Theorem 4.6.12. *Let m and r be integers satisfying $m > \gamma$ and $r \geqslant 0$. Assume that Conjecture 4.5.10 is true. Then*

$$H^0(S, 2m\Theta_S + r\nabla_S) \cong H^0(S, 2m\Theta_S) \oplus \bigoplus_{i=1}^{r} H^0(\mathbb{P}^1, (2m - \gamma i)(\infty)).$$

If $2m - \gamma r \geqslant 0$, then

$$h^0(S, 2m\Theta_S + r\nabla_S) = \binom{2m - \gamma + 1}{2} + r(2m + 1) - \gamma\binom{r + 1}{2}.$$

Otherwise

$$h^0(S, 2m\Theta_s + r\nabla) = h^0(S, 2m\Theta_S + \left\lfloor \tfrac{2m}{\gamma} \right\rfloor \nabla).$$

If Conjecture 4.5.10 is false, then the theorem holds for r such that $2m - \gamma i \neq 0$ for all $i = 1, \ldots, r$.

Proof. First assume that Conjecture 4.5.10 is true. By Proposition 1.5.2 and Theorem 4.5.11 we have

$$\begin{aligned} H^0(S, 2m\Theta_S + r\nabla_S) &\cong H^0(C \times C, \pi^*(2m\Theta_S + r\nabla_S))^G \\ &\cong H^0(C \times C, mF + r\nabla)^G \\ &\cong H^0(C \times C, mF)^G \oplus \bigoplus_{i=1}^{r} H^0(\nabla, (2m - \gamma i)D_\nabla)^G \\ &\cong H^0(S, 2m\Theta_S) \oplus \bigoplus_{i=1}^{r} H^0(\nabla, (2m - \gamma i)D_\nabla)^G \end{aligned}$$

where the second last isomorphism follows from the fact that the isomorphism of Theorem 4.5.11 is an isomorphism of G-modules. Since

$$\nabla/\langle\sigma\rangle \cong \mathbb{P}^1 \cong C/\langle\eta\rangle,$$

we have

$$H^0(\nabla, (2m - \gamma i)D_\nabla)^G \cong H^0(\mathbb{P}^1, (2m - \gamma i)(\infty)).$$

It follows that

$$h^0(S, 2m\Theta_S + r\nabla_S) = h^0(S, 2m\Theta_S) + \sum_{i=1}^{r} h^0(\mathbb{P}^1, (2m - \gamma i)(\infty)).$$

First, Lemma 4.6.3 shows that

$$h^0(S, 2m\Theta_S) = \binom{2m - \gamma + 1}{2} = \frac{(2m - \gamma)(2m - \gamma + 1)}{2}. \tag{4.15}$$

We have $h^0(\mathbb{P}^1,(2m-\gamma i)(\infty))\neq 0$ if and only if $2m-\gamma i\geqslant 0$, and a basis of $H^0(\mathbb{P}^1,(2m-\gamma i)(\infty))$ is given by all monomials in two variables of degree $2m-\gamma i$. Hence, when $0\leqslant 2m-\gamma r\leqslant 2m-\gamma i$, we obtain $h^0(\mathbb{P}^1,(2m-\gamma i)(\infty))=2m-\gamma i+1$ and so

$$\sum_{i=1}^{r} h^0(\mathbb{P}^1,(2m-\gamma i)(\infty)) = r(2m+1)-\gamma\frac{r(r+1)}{2} \tag{4.16}$$

If $2m-\gamma r<0$, then we obtain

$$\sum_{i=1}^{r} h^0(\mathbb{P}^1,(2m-\gamma i)(\infty)) = \sum_{i=1}^{\lfloor 2m/\gamma\rfloor} h^0(\mathbb{P}^1,(2m-\gamma i)(\infty)). \tag{4.17}$$

Combining (4.16) and (4.17) with (4.15) completes the proof in the case when Conjecture 4.5.10 is true. If the conjecture is false, it is clear that the proof remains the same except that we must omit the cases where $2m-\gamma i=0$ for some i satisfying $1\leqslant i\leqslant r$. □

Corollary 4.6.13. *Let $m>\gamma$ and $r\geqslant 0$ be integers. Then*

$$h^2(S,2m\Theta_S+r\nabla_S)=0. \tag{4.18}$$

Assume Conjecture 4.5.10 is true. Then

$$h^1(S,2m\Theta_S+r\nabla_S)=(r-r')\Big(\frac{\gamma}{2}(r+r'+1)-(2m+1)\Big)$$

where $r'=\min\{r,\left\lfloor\frac{2m}{\gamma}\right\rfloor\}$. In particular, $h^1(S,2m\Theta_S+r\nabla_S)=0$ if $0\leqslant 2m-\gamma r$. If Conjecture 4.5.10 is false, then the corollary remains true for $r\geqslant 0$ such that $2m-\gamma i\neq 0$ for all $i=1,\dots,r$.

Proof. By Proposition 4.6.1, a canonical divisor on S is given by $K_S=2(g-2)\Theta_S+\nabla_S$ and $\pi^*K_S=\gamma F-\Delta$. Hence by Theorem 1.2.4(ii) and Proposition 1.5.2,

$$\begin{aligned} H^2(S,2m\Theta_S+r\nabla_S) &\cong H^0(S,K_S-2m\Theta_S-r\nabla_S)\\ &= H^0(C\times C,\gamma F-\Delta-mF-r\nabla)^G\\ &\subseteq H^0(C\times C,(\gamma-m)F)^G. \end{aligned}$$

But $H^0(C\times C,(\gamma-m)F)=0$ since $m>\gamma$. This proves (4.18).

Assume Conjecture 4.5.10 is true. Combining the formula for $\chi(2m\Theta_S+r\nabla_S)$ in Proposition 4.6.7 with the formula for $h^0(S,2m\Theta_S+r\nabla_S)$ in Theorem 4.6.12, we obtain

$$\begin{aligned} &h^1(S,2m\Theta_S+r\nabla_S)\\ &\quad= h^0(S,2m\Theta_S+r\nabla_S)-\chi(2m\Theta_S+r\nabla_S)\\ &\quad= (r-r')\Big(\frac{\gamma}{2}(r+r'+1)-(2m+1)\Big) \end{aligned}$$

where $r' = \min\{r, \left\lfloor \frac{2m}{\gamma} \right\rfloor\}$. If $0 \leqslant 2m - \gamma r$, then $r = r'$ and so

$$h^1(S, 2m\Theta_S + r\nabla_S) = 0.$$

This completes the proof of the case where Conjecture 4.5.10 is true. If the conjecture is false, the same proof holds for r such that $2m - \gamma i \neq 0$ for $i = 1, \ldots, r$. □

Chapter 5

Explicit bases of sections and applications

The goal of this chapter is to describe an algorithm which produces an explicit basis for spaces of global sections of divisors on the square and the symmetric square of a hyperelliptic curve that we studied in Chapter 4.

Let C be a curve of genus 2 and let J_C be its Jacobian. With this algorithm in hand, we show how to re-derive the rational map $\mathrm{Sym}^2(C) \to J_C$ described by Cassels [7], Flynn [12] and Cassels and Flynn [8, Chapter 2]. We will subsequently consider several other applications, including various embeddings of $C \times C$ and $\mathrm{Sym}^2(C)$ and applications to coding theory on these surfaces.

Throughout this chapter we continue to assume the setup and notation described in Section 4.3. Let x_1, y_1, x_2, y_2 be the coordinate functions in $k(C \times C) = k(x_1, y_1, x_2, y_2)$.

5.1 Eigenspace decompositions

Let $\varepsilon = \pm 1$ and define W_m^ε to be the subspace of $H^0(C \times C, mF)$ on which σ has the eigenvalue ε. Set $W_{m,r}^\varepsilon = W_m^\varepsilon \cap H^0(C \times C, mF - r\Delta)$.

Lemma 5.1.1. *Let m and r be non-negative integers. Then there is a decomposition*

$$H^0(C \times C, mF - r\Delta) \cong W_{m,r}^1 \oplus W_{m,r}^{-1}.$$

Proof. Since σ is idempotent, the group ring $k[\langle\sigma\rangle]$ decomposes as $k[\langle\sigma\rangle] \cong k \times k$ which induces the stated decomposition of $H^0(C \times C, mF - r\Delta)$. □

Lemma 5.1.1 is true more generally for any divisor D on $C \times C$ which satisfies $D^\sigma = D$.

The following proposition shows that the σ-invariant sections of the space $H^0(C \times C, mF + r\nabla)$ are the sections of $H^0(C \times C, (m+r)F - r\Delta)$ on which σ acts by $(-1)^r$, thus reducing the task of computing $H^0(S, 2m\Theta_S + r\nabla_S)$ to computing a basis of $W^{(-1)^r}_{m+r,r}$.

Proposition 5.1.2. *Let m and r be non-negative integers. Then there is an isomorphism*

$$\varphi : H^0(C \times C, mF + r\nabla)^{\langle\sigma\rangle} \to W^{(-1)^r}_{m+r,r}$$

where φ is defined by $\varphi(w) = (x_1 - x_2)^r w$.

Proof. There is an isomorphism

$$\varphi : H^0(C \times C, mF + r\nabla) \to H^0(C \times C, (m+r)F - r\Delta)$$

defined by $\varphi(w) = (x_1 - x_2)^r w$, since $\operatorname{div}((x_1 - x_2)^r) = rF - r\Delta - r\nabla$ by Lemma 4.5.2. For all w in $H^0(C \times C, mF + r\nabla)$ we have $w^\sigma = w$ if and only if $\varphi(w)^\sigma = (-1)^r (x_1 - x_2)^r w$. Hence σ-invariant sections in $H^0(C \times C, mF + r\nabla)$ correspond to sections in $H^0(C \times C, (m+r)F - r\Delta)$ on which σ acts by $(-1)^r$. Since

$$H^0(C \times C, (m+r)F - r\Delta) \cong W^1_{m+r,r} \oplus W^{-1}_{m+r,r}$$

by Lemma 5.1.1, the subspace of sections of $H^0(C \times C, (m+r)F - r\Delta)$ on which σ acts by $(-1)^r$ is $W^{(-1)^r}_{m+r,r}$ as required. □

Lemma 5.1.3. *A basis of $H^0(C \times C, mF)$ is given by the submodule of polynomials in $k[x_1, y_1, x_2, y_2]$ of the form*

$$w = a + by_1 + cy_2 + dy_1y_2 \tag{5.1}$$

where a, b, c and d are polynomials in $k[x_1, x_2]$ satisfying the following bounds on the degrees:

$$\begin{aligned} &\deg_{x_1}(a), \deg_{x_2}(a), \deg_{x_1}(c), \deg_{x_2}(b) \leqslant m \\ &\deg_{x_1}(b), \deg_{x_2}(c), \deg_{x_1}(d), \deg_{x_2}(d) \leqslant m - (g+1). \end{aligned}$$

Proof. By Theorem 1.2.5, $H^0(C \times C, mF) \cong H^0(C, mD_\infty)^{\otimes 2}$, so every element can be written as a product of an element in $\{1, x_1, \ldots, x_1^r, y_1, x_1^{r+t}, \ldots\}$ with an element from $\{1, x_2, \ldots, x_2^r, y_2, x_2^{r+t}, \ldots\}$ for some non-negative integers r and t. Any occurrence of y_i^2 can be replaced by $f(x_i)$ which shows that $\deg_{y_i}(w) \leqslant 1$ for $i = 1, 2$ and hence gives the form of w in (5.1). The degree bounds on a, b, c and d are then imposed by mF. □

Lemma 5.1.4. *Let*

$$w = a + by_1 + cy_2 + dy_1y_2 \tag{5.2}$$

be an element of $H^0(C \times C, mF)$ with a, b, c and d as in Lemma 5.1.3. Then w belongs to W_m^1 if and only if $a = a^\sigma$, $d = d^\sigma$ and $c = b^\sigma$.

Proof. Let w have the stated form. Then

$$w^\sigma = a^\sigma + c^\sigma y_1 + b^\sigma y_2 + d^\sigma y_1 y_2. \tag{5.3}$$

By definition $w \in W_m^1$ if and only if $w = w^\sigma$, so the result follows upon equating the coefficients of 1, y_1, y_2 and y_1y_2 in (5.2) and (5.3). □

Lemma 5.1.5. *Let w be in $H^0(C \times C, mF)$. Then w is in W_m^{-1} if and only if there exists $w' \in W_{m-1}^1$ such that $w = (x_1 - x_2)w'$.*

Proof. By definition, w belongs to W_m^{-1} if and only if $w^\sigma = -w$, in which case $x_1 - x_2$ divides w. Hence $w = (x_1 - x_2)w'$ where w' is symmetric, so w' belongs to W_{m-1}^1. The converse is immediate. □

5.2 Hasse-Schmidt derivations

In this section, we describe the Hasse partial derivative of a multivariate polynomial. This derivative is a generalisation of the usual formal derivative of a polynomial, and it has the advantage that it allows us to calculate Taylor series expansions in arbitrary characteristic. The primary references for this section are Vojta [38, §1] and Hirschfeld et al. [19, Section 5.10].

Let A be a ring, let $\alpha : A \to B$ and $A \to R$ be A-algebras and let m be a positive integer. A *higher derivation of order m from B to R over A* is a sequence $(D_0, \ldots, D_m)$ where $D_0 : B \to R$ is an A-algebra homomorphism and $D_i : B \to R$ are homomorphisms of additive abelian groups for $i = 1, \ldots, m$ satisfying

(i) $D_i(\alpha(a)) = 0$ for all $a \in A$ and all $i = 1, \ldots, m$, and

(ii) (Leibniz rule) for all x and y in B and all $h = 0, \ldots, m$,

$$D_i(xy) = \sum_{j=0}^{i} D_j(x) D_{i-j}(y).$$

It follows immediately that the maps $D_i : B \to R$ are in fact A-module homomorphisms for all $i = 0, \ldots, m$.

Let A be a ring and let $j \geqslant 0$ be an integer. The *jth Hasse derivative* of a polynomial $w = \sum_{i=0}^{n} a_i t^i$ in $A[t]$ is defined to be

$$D_t^{(j)} w = \sum_{i=j}^{n} \binom{i}{j} a_i t^{i-j}.$$

When $\mathrm{char}(A)$ is coprime to $j!$ we have $D_t^{(j)} w = \frac{1}{j!} \frac{d^j}{dt^j} w$, where $\frac{d}{dt} w$ is the usual formal derivative of a polynomial. In particular, $D_t^{(0)} w = w$ and $D_t^{(1)} w = \frac{d}{dt} w$ for all w in $A[t]$, however $D_t^{(i)} D_t^{(j)} w \neq D_t^{(i+j)} w$ in general.

Proposition 5.2.1. *Let A be a ring. Then the sequence $(D_t^{(0)}, \ldots, D_t^{(m)})$ of Hasse derivatives is a higher derivation of order m from $A[t]$ to $A[t]$ over A.*

Proof. See Hirschfeld et al. [19, Lemma 5.72]. □

Proposition 5.2.2. *Let A be a ring, let a be in A, and let w be an element of $A[t]$. Then*

$$w = \sum_{i=0}^{\deg(w)} (D_t^{(i)} w)(a)(t-a)^i.$$

Proof. By linearity it suffices to consider the case $w = t^n$. Then

$$\sum_{i=0}^{\deg(w)} (D_t^{(i)} w)(a)(t-a)^i = \sum_{i=0}^{\deg(w)} \binom{n}{i} a^{n-i} (t-a)^i = t^n$$

as required. □

5.3 Formal neighbourhoods of Δ

Define $s = (x_1 + x_2)/2$ and $t = (x_1 - x_2)/2$ (recall that we assume $\mathrm{char}(k)$ is not two). Then t is a uniformising parameter at Δ in $C \times C$; that is, t generates the maximal ideal $\mathfrak{m}_\Delta$ of the local ring $\mathscr{O}_{C \times C, \Delta}$. The formal expansion of an element $w \in \mathscr{O}_{C \times C, \Delta}$ in the neighbourhood of Δ is given by its image in the completion $\widehat{\mathscr{O}}_{C \times C, \Delta} \cong k(\Delta)[\![t]\!]$ of $\mathscr{O}_{C \times C, \Delta}$ with respect to $\mathfrak{m}_\Delta$ (here we are abusing notation by writing t for the variable in power series $k(\Delta)[\![t]\!]$ which is the image of the element $t = (x_1 - x_2)/2$ in $\mathscr{O}_{C \times C, \Delta}$). By Proposition 5.2.2, this image is given by

$$w = \sum_{j=0}^{\infty} D_t^{(j)} w \Big|_\Delta \, t^j$$

where $D_t^{(j)}w\big|_\Delta$ denotes the image of $D_t^{(j)}w$ under the quotient

$$\mathscr{O}_{C\times C,\Delta} \to \mathscr{O}_{C\times C,\Delta}/\mathfrak{m}_\Delta \cong k(\Delta),$$

which, for $i = 1, 2$, sends x_i to x and y_i to y in $k(\Delta) = k(x, y)$.

Proposition 5.3.1. *For $i = 1, 2$ and for all $j > 0$ we have*

$$\begin{aligned} D_t^{(j)}x_1^m &= \tbinom{m}{j}x_1^{m-j} \\ D_t^{(j)}x_2^m &= (-1)^j\tbinom{m}{j}x_2^{m-j} \\ D_t^{(j)}y_i &= \frac{1}{2f(x_i)}\Big(D_t^{(j)}f(x_i) - \sum_{\ell=1}^{j-1} D_t^{(\ell)}y_i D_t^{(j-\ell)}y_i\Big)y_i \end{aligned}$$

Proof. Let $b \in k(\Delta)$. From the Leibniz rule, we obtain

$$D_t^{(j)}(b-t)^m = \sum_{\substack{0\leqslant r_1,\dots,r_m\leqslant 1 \\ \sum r_\ell = j}} D_t^{(r_1)}(b-t)\cdots D_t^{(r_m)}(b-t)$$

by induction on m, from which it follows that

$$D_t^{(j)}x_2^m = (-1)^j\tbinom{m}{j}x_2^{m-j}$$

since $x_2 = s - t$ and $s \in k(\Delta)$. A similar argument shows that

$$D_t^{(j)}x_1^m = \tbinom{m}{j}x_1^{m-j}.$$

Since $y_i^2 - f(x_i) = 0$ for $i = 1, 2$, linearity and the Leibniz rule imply that

$$0 = D_t^{(j)}y_i^2 - D_t^{(j)}f(x_i) = 2y_iD_t^{(j)}y_i + \sum_{\ell=1}^{j-1} D_t^{(\ell)}y_iD_t^{(j-\ell)}y_i - D_t^{(j)}f(x_i)$$

and so

$$D_t^{(j)}y_i = \frac{1}{2y_i}\Big(D_t^{(j)}f(x_i) - \sum_{\ell=1}^{j-1} D_t^{(\ell)}y_iD_t^{(j-\ell)}y_i\Big).$$

The result follows upon noting that $1/y_i = y_i/f(x_i)$. □

Proposition 5.3.2. *For $i = 1, 2$ and all $j \geqslant 1$, there exists a polynomial G_j in $k[x_i]$ of degree at most $j(\deg(f) - 1)$ such that*

$$D_t^{(j)}y_i = \frac{G_j(x_i)}{(2f(x_i))^j}y_i.$$

Proof. For $j = 1$, we have

$$D_t^{(1)} y_i = \frac{D^{(1)} f(x_i)}{2f(x_i)} y_i$$

by Proposition 5.3.1. Now suppose the result holds for $\ell < j$. We obtain

$$\begin{aligned} D_t^{(j)} y_i &= \frac{1}{2f(x_i)} \Big(D_t^{(j)} f(x_i) - \sum_{\ell=1}^{j-1} D_t^{(\ell)} y_i D_t^{(j-\ell)} y_i \Big) y_i \\ &= \frac{1}{2f(x_i)} \Big(D_t^{(j)} f(x_i) - \sum_{\ell=1}^{j-1} \frac{G_\ell(x_i) G_{j-\ell}(x_i)}{2^j f(x_i)^{j-1}} \Big) y_i \\ &= \frac{1}{2^j f(x_i)^j} \Big(2^{j-1} f(x_i)^{j-1} D_t^{(j)} f(x_i) - \frac{1}{2} \sum_{\ell=1}^{j-1} G_\ell(x_i) G_{j-\ell}(x_i) \Big) y_i \end{aligned}$$

where the first equality follows from Proposition 5.3.1 and the second the induction hypothesis. Hence by induction

$$G_j(x_i) = 2^{j-1} f(x_i)^{j-1} D_t^{(j)} f(x_i) - \frac{1}{2} \sum_{\ell=1}^{j-1} G_\ell(x_i) G_{j-\ell}(x_i)$$

is the required polynomial. Clearly $\deg(f(x_i)^{j-1} D_t^{(j)} f(x_i)) \leqslant j(\deg(f) - 1)$ and, by induction, $\deg(G_\ell(x_i) G_{j-\ell}(x_i)) \leqslant j(\deg(f) - 1)$, so it follows that $\deg(G_j) \leqslant j(\deg(f) - 1)$. □

Let m and j be non-negative. Define the map

$$\varphi_m^{(j)} : H^0(C \times C, mF) \to k(\Delta)$$

by $\varphi_m^{(j)}(w) = D_t^{(j)} w|_\Delta$. Define $M_m^{(j)}$ to be the sub-vector space of $k[x, y, f^{-1}] \subset k(\Delta)$ consisting of those polynomials g such that

$$\deg_x(g) \leqslant 2m + j(\deg(f) - 1), \quad \deg_y(g) \leqslant 1, \quad \text{and} \quad \deg_{f^{-1}}(g) \leqslant 2j,$$

where we write $f = f(x)$.

Corollary 5.3.3. *The image of $\varphi_m^{(j)}$ lies in $M_m^{(j)}$*

Proof. Let m and r be integers and assume m is non-negative. By Lemma 5.1.3, an element w of $H^0(C \times C, mF)$ has the form $w = a + by_1 + cy_2 + dy_1y_2$ where a, b, c, d are in $k[x_1, x_2]$ and have degrees satisfying

$$\begin{aligned} &\deg_{x_1}(a), \deg_{x_2}(a), \deg_{x_2}(b), \deg_{x_1}(c) \leqslant m, \\ &\deg_{x_1}(b), \deg_{x_2}(c), \deg_{x_1}(d), \deg_{x_2}(d) \leqslant m - (g + 1). \end{aligned}$$

From the Leibniz rule and Proposition 5.3.1 we see that

$$D_t^{(j)} w = a' + b' y_1 + c' y_2 + d' y_1 y_2,$$

whose image in $k(\Delta)$ is given by

$$D_t^{(j)} w \Big|_\Delta = a'(\Delta) + d'(\Delta) f(x) + (b'(\Delta) + c'(\Delta)) y.$$

Let a_n, b_n, c_n and d_n be the numerators of $a'(\Delta)$, $b'(\Delta)$, $c'(\Delta)$ and $d'(\Delta)$ respectively. Then by Propositions 5.3.1 and 5.3.2,

$$\begin{aligned} \deg_x(a_n) &\leqslant 2m - j \\ \deg_x(b_n) + \deg_x(c_n) &\leqslant 2m - (g+1) + j(\deg(f) - 1) \\ \deg_x(d_n) &\leqslant 2(m - (g+1)) + j(\deg(f) - 1). \end{aligned}$$

Let a_d, b_d, c_d and d_d be the denominators of $a'(\Delta)$, $b'(\Delta)$, $c'(\Delta)$ and $d'(\Delta)$ respectively. Then by Proposition 5.3.2,

$$\begin{aligned} \deg_{f^{-1}}(a_d) = \deg_{f^{-1}}(b_d) = \deg_{f^{-1}}(c_d) &= 0 \\ \deg_{f^{-1}}(b_d), \deg_{f^{-1}}(c_d) &= j \\ \deg_{f^{-1}}(d_d) &= 2j \end{aligned}$$

where we write $f = f(x)$. This completes the proof. □

5.4 Explicit bases of sections

In this section we describe an algorithm for generating explicit bases for $H^0(C \times C, mF + r\nabla)$ and $H^0(S, 2m\Theta_S + r\nabla_S)$.

Algorithm 5.4.1. Let m and r be non-negative integers and let V be a subspace of $H^0(C^2, (m+r)F)$ given as a basis B of monomials. The following procedure computes a basis for $V \cap H^0(C^2, (m+r)F - r\Delta)$.

1. Fix a basis for the vector space $M_{m+r}^{(r-1)}$.
2. Set $K \leftarrow V$.
3. For $j \leftarrow 0, \ldots, r-1$,
   (a) Calculate the map $\varphi_{m+r}^{(j)} : V \to M_{m+r}^{(j)} \subseteq M_{m+r}^{(r-1)}$ by applying the Leibniz rule and the formulæ of Proposition 5.3.1 to the elements of B.

(b) Set $K \leftarrow K \cap \mathrm{Ker}(\varphi^{(j)}_{m+r})$.

4. Return K.

Proof. Let w be an element of V. If $r = 0$, then the loop in step 3 is not executed and so $K = V$ from step 2. If $r > 0$, then it is clear from step 3(b) that $K = \bigcap_{j=0}^{r-1} \mathrm{Ker}(\varphi^{(j)}_{m+r})$ at step 4. Hence we have $w \in K$ if and only if $\varphi^{(j)}_{m+r}(w) = D^{(j)}_t w|_\Delta = 0$ for $j = 0, \ldots, r-1$ if and only if $w \in V \cap H^0(C^2, (m+r)F - r\Delta)$. □

Applying Algorithm 5.4.1 to the basis of $H^0(C^2, (m+r)F)$ given by Lemma 5.1.3 produces a basis for

$$H^0(C^2, (m+r)F - r\Delta) = (x_1 - x_2)^r H^0(C^2, mF + r\nabla),$$

and applying Algorithm 5.4.1 to the basis of $W^{(-1)^r}_{m+r}$ described by Lemmas 5.1.4 and 5.1.5 produces a basis for

$$W^{(-1)^r}_{m+r,r} = (x_1 - x_2)^r H^0(S, 2m\Theta_S + r\nabla_S).$$

The following proposition shows that a certain constant improvement to the time complexity of Algorithm 5.4.1 is possible.

Proposition 5.4.2. *Let m and r be integers with m non-negative. Let w be an element of $W^{(-1)^r}_m$ and let i be a non-negative integer. If $i \not\equiv r \pmod 2$, then $D^{(i)}_t w|_\Delta = 0$.*

Proof. Consider the power series expansion of w at Δ:

$$w(t) = \sum_{i \geqslant 0} w_i t^i \quad \text{where} \quad w_i = D^{(i)}_t w\Big|_\Delta .$$

As $w \in W^{(-1)^r}_m$, we have $w(t)^\sigma = (-1)^r w(t)$. But

$$w(t)^\sigma = \sum_{i \geqslant 0} (-1)^i w_i t^i$$

since $t^\sigma = -t$ and $w_i^\sigma = w_i$ for all i; hence $(-1)^r w_i = (-1)^i w_i$ for all i. If $i \not\equiv r \pmod 2$, then $-w_i = w_i$ and so $w_i = 0$ since $\mathrm{char}(k) \neq 2$. □

Proposition 5.4.2 shows that when the input to Algorithm 5.4.1 is $W^{(-1)^r}_{m+r}$, then the kernel intersection on step 3(b) need only be executed $r/2$ times since $D^{(i)}_t w|_\Delta = 0$ when $i \not\equiv r \pmod 2$. The map $\varphi^{(j)}_{m+r}$ in step 3(a) of Algorithm 5.4.1 should nevertheless be calculated as this permits iterative calculation of the Hasse derivatives of the monomial basis of V using the formulæ of Proposition 5.3.1.

5.5 Applications

In this final section we look at several applications of Algorithm 5.4.1.

5.5.1 Projective embeddings

Let X be a smooth projective variety of dimension n, let K_X be a canonical divisor on X, and let H be an ample divisor on X. The Fujita Conjecture states that $K_X + \lambda H$ is generated by global sections if $\lambda \geqslant n+1$ and it is very ample if $\lambda \geqslant n+2$. The Fujita conjecture was proved for surfaces by Reider [34]. As Lemma 4.5.1 and Proposition 4.6.1 give the forms of canonical divisors on $C \times C$ and $\mathrm{Sym}^2(C)$ respectively, we can use Algorithm 5.4.1 to explicitly find many projective embeddings of these surfaces.

Let C be a curve of genus 2 and let J_C be its Jacobian. In this case $S = \mathrm{Sym}^2(C)$ is the blowup of J_C at the identity and ∇_S is the exceptional divisor on S. Then ∇_S is a canonical divisor on S (see Hartshorne [17, Chapter V, Proposition 3.3]). The pullback of $4\Theta_J$ from J_C to S is given by $4\Theta_S + 4\nabla_S$ and this is very ample by the result of Reider. In the work of Cassels [7], Flynn [12] and Cassels and Flynn [8, Chapter 2] they describe a basis for $H^0(S, 4\Theta_S + 4\nabla_S)$ which we can verify (up to projective linear transformation) with Algorithm 5.4.1.

5.5.2 Conjecture 4.5.10

First note that the conjecture is true in the case $g = 2$ on account of the explicit basis for $H^0(S, 4\Theta_S + 4\nabla_S)$ described in the work of Cassels and Flynn cited at the end of the previous section. It therefore suffices to consider $g \geqslant 3$.

Let $m > \gamma$ and r satisfy $2m - \gamma r = 0$. We can deduce from Theorems 4.5.11 and 4.6.12 that Conjecture 4.5.10 holds if and only if

$$h^0(C \times C, mF + r\nabla) = (2m-\gamma)^2 + 2m(r-2) + g + 1$$

and

$$h^0(\mathrm{Sym}^2(C), 2m\Theta_S + r\nabla_S) = \binom{2m-\gamma+1}{2} + r(2m+1) - \gamma\binom{r+1}{2}. \quad (5.4)$$

Algorithm 5.4.1 allows us to confirm these formulæ in any given special case. For each g with $3 \leqslant g \leqslant 6$ we randomly selected ten hyperelliptic curves C over $\mathbb{Q}$ of genus g, and calculated bases of the spaces $H^0(C \times C, mF + r\nabla)$ and $H^0(\mathrm{Sym}^2(C), 2m\Theta_S + r\nabla_S)$ for m and r such that $2m - \gamma r = 0$ and $\gcd(m, r) = 1$. In each case we confirmed that the number of basis elements calculated agreed with the dimension predicted by the conjecture.

5.5.3 Codes on surfaces

Let C be a hyperelliptic curve of genus $g \geqslant 2$ over a field $\mathbb{F}_q$ of characteristic different from two and let S denote either $C \times C$ or $\mathrm{Sym}^2(C)$. We finish by showing how to construct linear codes on $C \times C$ and $\mathrm{Sym}^2(C)$.

Let $T \subseteq S(\mathbb{F}_q)$ be a subset of cardinality n and let D be a very ample divisor on S giving an embedding $\varphi\colon S \to \mathbb{P}^{k-1}$. Note that the result of Reider [34] described in Section 5.5.1 gives one means of producing very ample divisors D. The set $\varphi(T) \subset \mathbb{P}^{k-1}(\mathbb{F}_q)$ defines a *linear* $[n, k, d]$*-code*. The parameters n and k are called the *block length* and *dimension* of the code respectively. The dimension of the code is given by Theorem 4.5.11 or 4.6.12 depending on where $S = C \times C$ or $S = \mathrm{Sym}^2(C)$. Algorithm 5.4.1 can be used to compute a basis of $H^0(S, D)$ which determines the map into $\mathbb{P}^{k-1}$; this provides a means of calculating the image of T. The parameter d is called the *minimal distance* and is given by

$$d = n - \max_H \{\varphi(T) \cap H\}$$

where H runs over all hyperplanes in $\mathbb{P}^{k-1}$. The minimal distance is difficult to compute in general.

Bibliography

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[3] W. Bosma and M. Pohst. Computations with finitely generated modules over dedekind rings. In *Proceedings of the 1991 international symposium on Symbolic and algebraic computation*, ISSAC '91, pages 151–156, New York, NY, USA, 1991. ACM.

[4] P. Bruin. Computing in Picard groups of projective curves over finite fields. arXiv:1003.2563v1 [math.AG], March 2010.

[5] J. Buchmann and S. Neis. Algorithms for linear algebra problems over principal ideal rings. Technical Report TI-7/96, Technische Hochschule Darmstadt, 1996.

[6] X. Caruso and D. Lubicz. Linear algebra over $\mathbb{Z}_p[\![u]\!]$. Article in preparation. Results presented at GeoCrypt 2011, Bastia, France, the slides for which are available at `http://iml.univ-mrs.fr/ati/GeoCrypt2011/slides/caruso.pdf`., 2011.

[7] J. W. S. Cassels. Arithmetic of curves of genus 2. In *Number theory and applications (Banff, AB, 1988)*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 27–35. Kluwer Acad. Publ., Dordrecht, 1989.

[8] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[9] H. Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics **138**. Springer-Verlag, Berlin, 1993.

[10] H. Cohen. Hermite and Smith normal form algorithms over Dedekind domains. *Math. Comp.*, 65(216):1681–1699, 1996.

[11] C. Diem. *A Study on Theoretical and Practical Aspects of Weil-Restriction of Varieties*. PhD thesis, Universität Gesamthochschule Essen, 2001.

[12] E. V. Flynn. The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field. *Math. Proc. Cambridge Philos. Soc.*, 107(3): 425–441, 1990.

[13] W. Fulton. *Intersection theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 1998.

[14] A. Grothendieck. Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphismes. *Inst. Hautes Études Sci. Publ. Math.*, 8, 1961.

[15] A. Grothendieck. Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. II. *Inst. Hautes Études Sci. Publ. Math.*, 17, 1963.

[16] A. Grothendieck. *Revêtements étales et groupe fondamental*. Springer-Verlag, Berlin, 1971. Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1), Dirigé par Alexandre Grothendieck. Augmenté de deux exposés de M. Raynaud, Lecture Notes in Mathematics, Vol. 224.

[17] R. Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics **52**. Springer-Verlag, New York, 1977.

[18] M. Hindry and J. H. Silverman. *Diophantine Geometry: An Introduction*. Graduate Texts in Mathematics **201**. Springer-Verlag, New York, 2000.

[19] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic Curves over a Finite Field*. Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008.

[20] N. M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[21] G. R. Kempf. *Algebraic varieties*, volume 172 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1993.

[22] K. Khuri-Makdisi. Linear algebra algorithms for divisors on an algebraic curve. *Math. Comp.*, 73(245):333–357, 2004.

[23] K. Khuri-Makdisi. Asymptotically fast group operations on Jacobians of general curves. *Math. Comp.*, 76(260):2213–2239, 2007.

[24] S. L. Kleiman. The Picard scheme. In *Fundamental algebraic geometry*, volume 123 of *Math. Surveys Monogr.*, pages 235–321. Amer. Math. Soc., Providence, RI, 2005.

[25] S. Lang and A. Néron. Rational points of abelian varieties over function fields. *Amer. J. Math.*, 81:95–118, 1959.

[26] Q. Liu. *Algebraic geometry and arithmetic curves*. Oxford Graduate Texts in Mathematics **6**. Oxford University Press, Oxford, 2002.

[27] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.

[28] J. S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.

[29] T. Mulders and A. Storjohann. Fast algorithms for linear algebra modulo N. In *Algorithms—ESA '98 (Venice)*, volume 1461 of *Lecture Notes in Comput. Sci.*, pages 139–150. Springer, Berlin, 1998.

[30] D. Mumford. *Lectures on curves on an algebraic surface*, volume 59 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, N.J., 1966.

[31] D. Mumford. Varieties defined by quadratic equations. In *Questions on Algebraic Varieties (C.I.M.E., III Ciclo, Varenna, 1969)*, pages 29–100. Edizioni Cremonese, Rome, 1970.

[32] D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[33] S. Neis. Reducing ideal arithmetic to linear algebra problems. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 299–310. Springer, Berlin, 1998.

[34] I. Reider. Vector bundles of rank 2 and linear systems on algebraic surfaces. *Ann. of Math. (2)*, 127(2):309–316, 1988.

[35] I. R. Shafarevich. *Basic Algebraic Geometry I: Varieties in Projective Space*. Springer-Verlag, Berlin, second edition, 1994. Translated from the 1988 Russian edition and with notes by Miles Reid.

[36] B. Smith. *Explicit Endomorphisms and Correspondences*. PhD thesis, University of Sydney, 2006.

[37] A. Storjohann. *Algorithms for Matrix Canonical Forms*. PhD thesis, Swiss Federal Institute of Technology, Zürich, 2000.

[38] P. Vojta. Jets via Hasse-Schmidt derivations. arXiv:math/0407113v2 [math.AG], February 2008.

[39] C. A. Weibel. *An Introduction to Homological Algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.