10
Hyperelliptic curves

Hyperelliptic curves are a natural generalisation of elliptic curves, and it was suggested by Koblitz [298] that they might be useful for public key cryptography. Note that there is not a group law on the points of a hyperelliptic curve; instead, we use the divisor class group of the curve. The main goals of this chapter are to explain the geometry of hyperelliptic curves, to describe Cantor's algorithm [105] (and variants) to compute in the divisor class group of hyperelliptic curves and then to state some basic properties of the divisor class group.

Definition 10.0.1 Let $\mathbb{k}$ be a perfect field. Let $H(x), F(x) \in \mathbb{k}[x]$ (we stress that $H(x)$ and $F(x)$ are not assumed to be monic). An affine algebraic set of the form $C : y^2 + H(x)y = F(x)$ is called a **hyperelliptic equation**. The **hyperelliptic involution** $\iota : C \to C$ is defined by $\iota(x, y) = (x, -y - H(x))$.

Exercise 10.0.2 Let C be a hyperelliptic equation over $\mathbb{k}$. Show that if $P \in C(\mathbb{k})$ then $\iota(P) \in C(\mathbb{k})$.

When the projective closure of the algebraic set C in Definition 10.0.1 is irreducible, dimension 1, non-singular and of genus $g \geq 2$, then we will call it a hyperelliptic curve. By definition, a curve is projective and non-singular. We will give conditions for when a hyperelliptic equation is non-singular. Exercise 10.1.15 will give a projective non-singular model, but, in practice, one can work with the affine hyperelliptic equation. To "see" the points at infinity we will move them to points on a related affine equation, namely, the curve $C^\dagger$ of equation (10.2).

The genus has already been defined (see Definition 8.4.7) as a measure of the complexity of a curve. The treatment of the genus in this chapter is very "explicit". We will give precise conditions (Lemmas 10.1.6 and 10.1.8) that explain when the degree of a hyperelliptic equation is minimal. From this minimal degree we define the genus. In contrast, the approach of most other authors is to use the Riemann–Roch theorem.

We remark that one can also consider the algebraic group quotient $\mathrm{Pic}^0_{\mathbb{F}_q}(C)/[-1]$ of equivalence classes $\{D, -D\}$ where D is a reduced divisor. For genus 2 curves this object can be described as a variety, called the **Kummer surface**. It is beyond the scope of this book to give the details of this case. We refer to Chapter 3 of Cassels and Flynn [115] for

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

background. Gaudry [224] and Gaudry and Lubicz [227] have given fast algorithms for computing with this algebraic group quotient.

10.1 Non-singular models for hyperelliptic curves

Consider the singular points on the affine curve $C(x, y) = y^2 + H(x)y - F(x) = 0$. The partial derivatives are $\partial C(x, y)/\partial y = 2y + H(x)$ and $\partial C(x, y)/\partial x = H'(x)y - F'(x)$, so a singular point in particular satisfies $2F'(x) + H(x)H'(x) = 0$. If $H(x) = 0$ and if the characteristic of $\mathbb{k}$ is not 2 then C is non-singular over $\overline{\mathbb{k}}$ if and only if $F(x)$ has no repeated root in $\overline{\mathbb{k}}$.

Exercise 10.1.1 Show that the curve $y^2 + H(x)y = F(x)$ over $\mathbb{k}$ has no affine singular points if and only if one of the following conditions hold.

1. $\mathrm{char}(\mathbb{k}) = 2$ and $H(x)$ is a non-zero constant.
2. $\mathrm{char}(\mathbb{k}) = 2$, $H(x)$ is a non-zero polynomial and $\gcd(H(x), F'(x)^2 - F(x)H'(x)^2) = 1$.
3. $\mathrm{char}(\mathbb{k}) \neq 2$, $H(x) = 0$ and $\gcd(F(x), F'(x)) = 1$.
4. $\mathrm{char}(\mathbb{k}) \neq 2$, $H(x) \neq 0$ and $\gcd(H(x)^2 + 4F(x), 2F'(x) + H(x)H'(x)) = 1$ (this applies even when $H(x) = 0$ or $H'(x) = 0$).

We will now give a simple condition for when a hyperelliptic equation is geometrically irreducible and of dimension 1. The proof also applies in many other cases. For the remaining cases, one has to test irreducibility directly.

Lemma 10.1.2 *Let $C(x, y) = y^2 + H(x)y - F(x)$ over $\mathbb{k}$ be a hyperelliptic equation. Suppose that* $\deg(F(x))$ *is odd. Suppose also that there is no point $P = (x_P, y_P) \in C(\overline{\mathbb{k}})$ such that $(\partial C(x, y)/\partial x)(P) = (\partial C(x, y)/\partial y)(P) = 0$. Then the affine algebraic set $V(C(x, y))$ is geometrically irreducible. The dimension of $V(C(x, y))$ is* 1.

Proof From Theorem 5.3.8, $C(x, y) = 0$ is $\overline{\mathbb{k}}$-reducible if and only if $C(x, y)$ factors over $\overline{\mathbb{k}}[x, y]$. By considering $C(x, y)$ as an element of $\overline{\mathbb{k}}(x)[y]$ it follows that such a factorisation must be of the form $C(x, y) = (y - a(x))(y - b(x))$ with $a(x), b(x) \in \overline{\mathbb{k}}[x]$. Since $\deg(F)$ is odd it follows that $\deg(a(x)) \neq \deg(b(x))$ and that at least one of $a(x)$ and $b(x)$ is non-constant. Hence, $a(x) - b(x)$ is a non-constant polynomial, so let $x_P \in \overline{\mathbb{k}}$ be a root of $a(x) - b(x)$ and set $y_P = a(x_P) = b(x_P)$ so that $(x_P, y_P) \in C(\overline{\mathbb{k}})$. It is then easy to check that both partial derivatives vanish at P. Hence, under the conditions of the Lemma, $V(C(x, y))$ is $\overline{\mathbb{k}}$-irreducible and so is an affine variety.

Now that $V(C(x, y))$ is known to be a variety we can consider the dimension. The function field of the affine variety is $\mathbb{k}(x)(y)$, which is a quadratic algebraic extension of $\mathbb{k}(x)$ and so has transcendence degree 1. Hence, the dimension of is 1. □

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

Let $H(x), F(x) \in \mathbb{k}[x]$ be such that $y^2 + H(x)y = F(x)$ is a non-singular affine curve. Define $D = \max\{\deg(F(x)), \deg(H(x)) + 1\}$. The projective closure of C in $\mathbb{P}^2$ is given by

$$y^2 z^{D-2} + z^{D-1} H(x/z) y = z^D F(x/z). \tag{10.1}$$

Exercise 10.1.3 Show that if $D > 2$ then there are at most two points at infinity on the curve of equation (10.1). Show further that if $D > 3$ and $\deg(F) > \deg(H) + 1$ then there is a unique point $(0 : 1 : 0)$ at infinity, which is a singular point.

In Definition 10.1.10 we will define the genus of a hyperelliptic curve in terms of the degree of the hyperelliptic equation. To do this, it will be necessary to have conditions that ensure that this degree is minimal. Example 10.1.4 and Exercise 10.1.5 show how a hyperelliptic equation that is a variety can be isomorphic to an equation of significantly lower degree (remember that isomorphism is only defined for varieties).

Example 10.1.4 The curve $y^2 + xy = x^{200} + x^{101} + x^3 + 1$ over $\mathbb{F}_2$ is isomorphic over $\mathbb{F}_2$ to the curve $Y^2 + xY = x^3 + 1$ via the map $(x, y) \mapsto (x, Y + x^{100})$.

Exercise 10.1.5 Let $\mathbb{k}$ be any field. Show that the affine algebraic variety $y^2 + (1 - 2x^3)y = -x^6 + x^3 + x + 1$ is isomorphic to a variety having an equation of total degree 2. Show that the resulting curve has genus 0.

Lemma 10.1.6 *Let $\mathbb{k}$ be a perfect field of characteristic 2 and $h(x), f(x) \in \mathbb{k}[x]$. Suppose the hyperelliptic equation $C : y^2 + h(x)y = f(x)$ is a variety. Then it is isomorphic over $\mathbb{k}$ to $Y^2 + H(x)Y = F(x)$ where one of the following conditions hold:*

1. $\deg(F(x)) > 2\deg(H(x))$ *and* $\deg(F(x))$ *is odd;*
2. $\deg(F(x)) = 2\deg(H(x)) = 2d$ *and the equation* $u^2 + H_d u + F_{2d}$ *has no solution in* $\mathbb{k}$ *(where* $H(x) = H_d x^d + H_{d-1}x^{d-1} + \cdots + H_0$ *and* $F(x) = F_{2d}x^{2d} + \cdots + F_0$*);*
3. $\deg(F(x)) < \deg(H(x))$.

Proof Let $d_H = \deg(H(x))$ and $d_F = \deg(F(x))$. The change of variables $y = Y + cx^i$ transforms $y^2 + H(x)y = F(x)$ to $Y^2 + H(x)Y = F(x) + c^2x^{2i} + H(x)cx^i$. Hence, if $\deg(F(x)) > 2\deg(H(x))$ and $\deg(F(x))$ is even then one can remove the leading coefficient by choosing $i = \deg(F(x))/2$ and $c = \sqrt{F_{2i}}$ (remember that $\mathrm{char}(\mathbb{k}) = 2$ and $\mathbb{k}$ is perfect so $c \in \mathbb{k}$). Similarly, if $\deg(H(x)) \leq j = \deg(F(x)) < 2\deg(H(x))$ then one can remove the leading coefficient $F_j x^i$ from F by taking $i = j - \deg(H(x))$ and $c = F_j/H_{d_H}$. Repeating these processes yields the first and third claims. The second case follows easily. □

Note that in the second case in Lemma 10.1.6 one can lower the degree using a $\overline{\mathbb{k}}$-isomorphism. Hence, geometrically (i.e., over $\overline{\mathbb{k}}$) one can assume that a hyperelliptic equation is of the form of case 1 or 3.

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

Example 10.1.7 The affine curve $y^2 + x^3 y = x^6 + x + 1$ is isomorphic over $\mathbb{F}_{2^2}$ to $Y^2 + x^3 Y = x + 1$ via $Y = y + ux^3$ where $u \in \mathbb{F}_{2^2}$ satisfies $u^2 + u = 1$. (Indeed, these curves are quadratic twists; see Definition 10.2.2.)

Lemma 10.1.8 *Let $\Bbbk$ be a field such that* $\mathrm{char}(\Bbbk) \neq 2$. *Every hyperelliptic curve over $\Bbbk$ is isomorphic over $\Bbbk$ to an equation of the form $y^2 + (H_d x^d + \cdots + H_0)y = F_{2d}x^{2d} + F_{2d-1}x^{2d-1} + \cdots + F_0$ where either:*

1. *$H_d = 0$ and ($F_{2d} \neq 0$ or $F_{2d-1} \neq 0$);*
2. *$H_d \neq 0$ and ($F_{2d} \neq -(H_d/2)^2$ or $F_{2d-1} \neq -H_d H_{d-1}/2$).*

Proof If $H_d = F_{2d} = F_{2d-1} = 0$ then just replace d by $d-1$. If $H_d \neq 0$ and both $F_{2d} = -(H_d/2)^2$ and $F_{2d-1} = -H_d H_{d-1}/2$ then the morphism $(x, y) \mapsto (x, Y = y + \frac{H_d}{2}x^d)$ maps the hyperelliptic equation to

$$(Y - \tfrac{H_d}{2}x^d)^2 + (H_d x^d + \cdots + H_0)(Y - \tfrac{H_d}{2}x^d) - (F_{2d}x^{2d} + F_{2d-1}x^{2d-1} + \cdots + F_0).$$

This can be shown to have the form

$$Y^2 + h(x)Y = f(x)$$

with $\deg(h(x)) \leq d-1$ and $\deg(f(x)) \leq 2d-2$. (This is what happened in Exercise 10.1.5.) □

Exercise 10.1.9 Show that the hyperelliptic curve $y^2 + (2x^3 + 1)y = -x^6 + x^5 + x + 1$ is isomorphic to $Y^2 + Y = x^5 + x^3 + x + 1$.

10.1.1 Projective models for hyperelliptic curves

For the rest of the chapter we will assume that our hyperelliptic equations are $\overline{\Bbbk}$-irreducible and non-singular as affine algebraic sets. We also assume that when $\mathrm{char}(\Bbbk) = 2$ one of the conditions of Lemma 10.1.6 holds and when $\mathrm{char}(\Bbbk) \neq 2$ one of the conditions of Lemma 10.1.8 holds. The interpretation of $\deg(H(x))$ and $\deg(F(x))$ in terms of the genus of the curve will be discussed in Section 10.1.3.

Suppose $y^2 + H(x)y = F(x)$ is a non-singular affine hyperelliptic equation for a projective non-singular curve C. Write H_j for the coefficients of $H(x)$ and F_j for the coefficients of $F(x)$. Define $d_H = \deg(H(x))$ and $d_F = \deg(F(x))$. Let $d = \max\{d_H, \lceil d_F/2 \rceil\}$ and suppose $d > 0$. Set $H_d = \cdots = H_{d_H+1} = 0$ and $F_{2d} = \cdots = F_{d_F+1} = 0$ if necessary.

The rational map $(Z, Y) = \rho(x, y) = (1/x, y/x^d)$ maps C to the affine algebraic set

$$C^\dagger : Y^2 + (H_d + H_{d-1}Z + \cdots H_0 Z^d)Y = F_{2d} + F_{2d-1}Z + \cdots F_0 Z^{2d}. \tag{10.2}$$

It is easy to check that $C^\dagger$ is geometrically irreducible, since C is. Now, all affine points (z, y) on $C^\dagger$ with $z \neq 0$ correspond to affine points on C and so are non-singular (since non-singularity is a local property; see Remark 7.1.3). To show that $C^\dagger$ is non-singular it is sufficient to consider the points $(z, y) = (0, \alpha)$ where $\alpha^2 + H_d\alpha - F_{2d} = 0$.

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

The partial derivatives evaluated at $(0, \alpha)$ are $2\alpha + H_d$ and $H_{d-1}\alpha - F_{2d-1}$. When $\mathrm{char}(\mathbb{k}) \neq 2$ the point being singular would imply $H_d = -2\alpha$ in which case $F_{2d} = \alpha^2 + H_d\alpha = -\alpha^2 = -(H_d/2)^2$ and $F_{2d-1} = H_{d-1}\alpha = -H_d H_{d-1}/2$. One easily sees that these equations contradict the conditions of Lemma 10.1.8.

Hence, $C^\dagger$ is a hyperelliptic curve and $\rho : C \to C^\dagger$ is a birational map. It follows that ρ induces a morphism between the corresponding projective curves. The point(s) $(0, \alpha)$ are the images of the point(s) at infinity on C. Hence, we can use $C^\dagger$ to visualise the points at infinity on C.

Up to now the phrase "hyperelliptic curve" has meant a projective non-singular curve of genus $g \geq 2$ that has an affine model as a hyperelliptic equation. Definition 10.1.10 gives an equivalent formulation that will be used throughout the book. Technically, this is an abuse of notation since C is not projective.

Definition 10.1.10 Let $\mathbb{k}$ be a perfect field. Let $H(x), F(x) \in \mathbb{k}[x]$ be such that:

- $\deg(H(x)) \geq 3$ or $\deg(F(x)) \geq 5$;
- the affine hyperelliptic equation $C : y^2 + H(x)y = F(x)$ is $\overline{\mathbb{k}}$-irreducible and non-singular;
- the conditions of Lemma 10.1.6 and Lemma 10.1.8 hold.

Then C is called a **hyperelliptic curve**. The **genus** of the hyperelliptic curve is $g = \max\{\deg(H(x)) - 1, \lfloor \deg(F(x)) - 1)/2 \rfloor\}$ (see Section 10.1.3 for justification of this).

It looks like Definition 10.1.10 excludes some potentially interesting equations (such as $y^2 + H(x)y = F(x)$ where $\deg(F(x)) = 4$ and $\deg(H(x)) = 2$). In fact, it can be shown that all the algebraic sets excluded by the definition are either $\overline{\mathbb{k}}$-reducible, singular over $\overline{\mathbb{k}}$ or birational over $\overline{\mathbb{k}}$ to a curve of genus 0 or 1 over $\overline{\mathbb{k}}$.

The equation $\alpha^2 + H_d\alpha - F_{2d} = 0$ can have a $\mathbb{k}$-rational repeated root, two roots in $\mathbb{k}$, or two conjugate roots in $\overline{\mathbb{k}}$. It follows that there are three possible behaviours at infinity: a single $\mathbb{k}$-rational point, two distinct $\mathbb{k}$-rational points and a pair of distinct points defined over a quadratic extension of $\mathbb{k}$ (which are Galois conjugates). These three cases correspond to the fact that the place at infinity in $\mathbb{k}[x]$ is ramified, split or inert respectively in the field extension $\mathbb{k}(C)/\mathbb{k}(x)$. A natural terminology for the three types of behaviour at infinity is therefore to call them ramified, split and inert.

Definition 10.1.11 Let C be a hyperelliptic curve and let $C^\dagger$ be as in equation (10.2). Let $\rho : C \to C^\dagger$ be as above. Let α^+, α^- be the roots in $\overline{\mathbb{k}}$ of the polynomial $\alpha^2 + H_d\alpha - F_{2d}$. We write ∞^+ for the **point at infinity** on C such that $\rho(\infty^+) = (0, \alpha^+)$ and ∞^- for the point such that $\rho(\infty^-) = (0, \alpha^-)$.

If $\alpha^+ = \alpha^-$ then C is called a **ramified model of a hyperelliptic curve**. If there are two distinct points at infinity with $\alpha^+, \alpha^- \in \mathbb{k}$ then C is called a **split model of a hyperelliptic curve** and if $\alpha^+, \alpha^- \notin \mathbb{k}$ then C is an **inert model of a hyperelliptic curve**.

One finds in the literature the names **imaginary hyperelliptic curve** (respectively, **real hyperelliptic curve**) for ramified model and split model respectively. Exercise 10.1.13

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

classifies ramified hyperelliptic models. Exercise 10.1.14 shows that if $C(\Bbbk) \neq \varnothing$ then one may transform C into a ramified or split model. Hence, when working over finite fields, it is not usually necessary to deal with curves having an inert model.

Exercise 10.1.12 With notation as in Definition 10.1.11 show that $\iota(\infty^+) = \infty^-$.

Exercise 10.1.13 Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve over $\Bbbk$ satisfying all the conditions above. Let $d = \max\{\deg(H(x)), \lceil \deg(F(x))/2 \rceil\}$. Show that this is a ramified model if and only if ($\deg(H(x)) < d$ and $\deg(F(x)) = 2d - 1$) or ($\mathrm{char}(\Bbbk) \neq 2$, $\deg(F(x)) = 2d$, $\deg(H(x)) = d$ and $F_{2d} = -(H_d/2)^2$).

Exercise 10.1.14 Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve over $\Bbbk$ and let $P \in C(\Bbbk)$. Define the rational map

$$\rho_P(x, y) = (1/(x - x_P), y/(x - x_P)^d).$$

Then $\rho_P : C \to C'$ where C' is also a hyperelliptic curve. Show that ρ_P is just the translation map $P \mapsto (0, y_P)$ followed by the map ρ and so is an isomorphism from C to C'.

Show that if $P = \iota(P)$ then C is birational over $\Bbbk$ (using ρ_P) to a hyperelliptic curve with ramified model. Show that if $P \neq \iota(P)$ then C is birational over $\Bbbk$ to a hyperelliptic curve with split model.

We now indicate a different projective model for hyperelliptic curves.

Exercise 10.1.15 Let the notation and conditions be as above. Assume $C : y^2 + H(x)y = F(x)$ is irreducible and non-singular as an affine curve. Let $Y, X_d, X_{d-1}, \ldots, X_1, X_0$ be coordinates for $\mathbb{P}^{d+1}$ (one interprets $X_i = x^i$). The **projective hyperelliptic equation** is the projective algebraic set in $\mathbb{P}^{d+1}$ given by

$$\begin{aligned} Y^2 + (H_d X_d + H_{d-1} X_{d-1} + \cdots + H_0 X_0)Y &= F_{2d} X_d^2 + F_{2d-1} X_d X_{d-1} + \cdots \\ &\quad + F_1 X_1 X_0 + F_0 X_0^2, \\ X_i^2 &= X_{i-1} X_{i+1}, && \text{for } 1 \leq i \leq d-1, \\ X_d X_i &= X_{\lceil (d+i)/2 \rceil} X_{\lfloor (d+i)/2 \rfloor}, && \text{for } 0 \leq i \leq d-2. \end{aligned} \tag{10.3}$$

1. Give a birational map (assuming for the moment that the above model is a variety) between the affine algebraic set C and the model of equation (10.3).
2. Show that the hyperelliptic involution ι extends to equation (10.3) as

$$\iota(Y : X_d : \cdots : X_0) = (-Y - H_d X_d - H_{d-1} X_{d-1} - \cdots - H_0 X_0 : X_d : \cdots : X_0).$$

3. Show that the points at infinity on equation (10.3) satisfy $X_0 = X_1 = X_2 = \cdots = X_{d-1} = 0$ and $Y^2 + H_d X_d Y - F_{2d} X_d^2 = 0$. Show that if $F_{2d} = H_d = 0$ then there is a single point at infinity.
4. Show that if the conditions of Lemma 10.1.6 or Lemma 10.1.8 hold then equation (10.3) is non-singular at infinity.
5. Show that equation (10.3) is a variety.

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

10.1.2 Uniformisers on hyperelliptic curves

The aim of this section is to determine uniformisers for all points on hyperelliptic curves. We begin in Lemma 10.1.16 by determining uniformisers for the affine points of a hyperelliptic curve.

Lemma 10.1.16 *Let $P = (x_P, y_P) \in C(\Bbbk)$ be a point on a hyperelliptic curve. If $P = \iota(P)$ then $(y - y_P)$ is a uniformiser at P (and $v_P(x - x_P) = 2$). If $P \neq \iota(P)$ then $(x - x_P)$ is a uniformiser at P.*

Proof We have

$$\begin{aligned}(y - y_P)(y + y_P + H(x_P)) &= y^2 + H(x_P)y - (y_P^2 + H(x_P)y_P)\\ &= F(x) + y(H(x_P) - H(x)) - F(x_P).\end{aligned}$$

Now, use the general fact for any polynomial that $F(x) = F(x_P) + (x - x_P)F'(x_P)$ (mod $(x - x_P)^2$). Hence, the above expression is congruent modulo $(x - x_P)^2$ to

$$(x - x_P)(F'(x_P) - yH'(x_P)) \pmod{(x - x_P)^2}.$$

When $P = \iota(P)$ then $(y - y_P)(y + (y_P + H(x_P))) = (y - y_P)^2$. Note also that $F'(x_P) - y_P H'(x_P)$ is not zero since $2y_P + H(x_P) = 0$ and yet C is not singular. Writing $G(x, y) = (y - y_P)^2/(x - x_P) \in \Bbbk[x, y]$ we have $G(x_P, y_P) \neq 0$ and

$$x - x_P = (y - y_P)^2 \frac{1}{G(x, y)}.$$

Hence, a uniformiser at P is $(y - y_P)$ and $v_P(x - x_P) = 2$.

For the case $P \neq \iota(P)$ note that $v_P(y - y_P) > 0$ and $v_P(y + y_P + H(x_P)) = 0$. It follows that $v_P(y - y_P) \geq v_P(x - x_P)$. □

We now consider uniformisers at infinity on a hyperelliptic curve C over $\Bbbk$. The easiest way to proceed is to use the curve $C^\dagger$ of equation (10.2).

Lemma 10.1.17 *Let C be a hyperelliptic curve and let $\rho : C \to C^\dagger$ be as in equation (10.2). Let $P = \rho(\infty^+) = (0, \alpha^+) \in C^\dagger(\Bbbk)$. If $\iota(\infty^+) = \infty^+$ (i.e., if there is one point at infinity) then $Y - \alpha^+$ is a uniformiser at P on $C^\dagger$ and so $(y/x^d) - \alpha^+$ is a uniformiser at ∞^+ on C. If $\iota(\infty^+) \neq \infty^+$ then Z is a uniformiser at P on $C^\dagger$ (i.e., $1/x$ is a uniformiser at ∞^+ on C).*

Proof Note that if $\iota(\infty^+) = \infty^+$ then $\iota(P) = P$ and if $\iota(\infty^+) \neq \infty^+$ then $\iota(P) \neq P$. It immediately follows from Lemma 10.1.16 that $Y - \alpha^+$ or Z is a uniformiser at P on $C^\dagger$. Lemma 8.1.13, Exercise 8.2.8 and Lemma 8.2.6 show that for any $f \in \Bbbk(C^\dagger)$ and $P \in C(\Bbbk)$, $v_P(f \circ \rho) = v_{\rho(P)}(f)$. Hence, uniformisers at infinity on C are $(Y - \alpha^+) \circ \rho = (y/x^d) - \alpha^+$ or $Z \circ \rho = 1/x$. □

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

Exercise 10.1.18 Let C be a hyperelliptic curve in ramified model. Show that $v_\infty(x) = -2$. Show that if the curve has equation $y^2 = F(x)$ where $\deg(F(x)) = 2g + 1$ then x^g/y is an alternative uniformiser at infinity.

Now suppose C is given as a split or inert model. Show that $v_{\infty^+}(x) = v_{\infty^-}(x) = -1$.

Exercise 10.1.19 Let C be a hyperelliptic curve (ramified, split or inert). If $u(x) = (x - x_0)$ is a function on C and $P_0 = (x_0, y_0) \in C(\overline{\Bbbk})$ then $\operatorname{div}(u(x)) = (P_0) + (\iota(P_0)) - (\infty^+) - (\infty^-)$.

Exercise 10.1.20 Let C be a hyperelliptic curve of genus g. Show that if C is in ramified model then $v_\infty(y) = -(2g + 1)$ and if C is in split model then $v_{\infty^+}(y) = v_{\infty^-}(y) = -(g + 1)$.

Exercise 10.1.21 Let C be a hyperelliptic curve. Let $A(x), B(x) \in \Bbbk[x]$ and let $P = (x_P, y_P) \in C(\overline{\Bbbk})$ be a point on the affine curve. Show that $v_P(A(x) - yB(x))$ is equal to e where $(x - x_P)^e \| (A(x)^2 + H(x)A(x)B(x) - F(x)B(x)^2)$.

We now describe a polynomial that will be crucial for arithmetic on hyperelliptic curves with a split model. Essentially, $G^+(x)$ is a function that cancels the pole of y at ∞^+. This leads to another choice of uniformiser at ∞^+ for these models.

Exercise 10.1.22 Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve with split model over $\Bbbk$ of genus g. Let $\alpha^+, \alpha^- \in \Bbbk$ be the roots of $Y^2 + H_d Y - F_{2d}$. Show that there exists a polynomial $G^+(x) = \alpha^+ x^d + \cdots \in \Bbbk[x]$ of degree $d = g + 1$ such that $\deg(G^+(x)^2 + H(x)G^+(x) - F(x)) \leq d - 1 = g$. Similarly, show that there is a polynomial $G^-(x) = \alpha^- x^d + \cdots$ such that $\deg(G^-(x)^2 + H(x)G^-(x) - F(x)) \leq d - 1 = g$. Indeed, show that $G^-(x) = -G^+(x) - H(x)$.

Exercise 10.1.23 Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve with split model over $\Bbbk$ of genus g and let $G^+(x)$ be as in Exercise 10.1.22. Show that $v_{\infty^+}(y - G^+(x)) \geq 1$.

10.1.3 The genus of a hyperelliptic curve

In Lemma 10.1.6 and Lemma 10.1.8 we showed that some hyperelliptic equations $y^2 + h(x)y = f(x)$ are birational to hyperelliptic equations $y^2 + H(x)y = F(x)$ with $\deg(F(x)) < \deg(f(x))$ or $\deg(H(x)) < \deg(h(x))$. Hence, it is natural to suppose that the geometry of the curve C imposes a lower bound on the degrees of the polynomials $H(x)$ and $F(x)$ in its curve equation. The right measure of the complexity of the geometry is the genus.

Indeed, the Riemann–Roch theorem implies that if C is a hyperelliptic curve over $\Bbbk$ of genus g and there is a function $x \in \Bbbk(C)$ of degree 2 then C is birational over $\Bbbk$ to an equation of the form $y^2 + H(x)y = F(x)$ with $\deg(H(x)) \leq g + 1$ and $\deg(F(x)) \leq 2g + 2$. Furthermore, the Hurwitz genus formula shows that if $y^2 + H(x)y = F(x)$ is

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

non-singular and with degrees reduced as in Lemma 10.1.6 and Lemma 10.1.8 then the genus is $\max\{\deg(H(x)) - 1, \lceil \deg(F(x))/2 - 1 \rceil\}$. (Theorem 8.7.3, as it is stated, cannot be applied for hyperelliptic curves in characteristic 2, but a more general version of the Hurwitz genus formula proves the above statement about the genus.) Hence, writing $d = g + 1$, the conditions of Lemma 10.1.6 and Lemma 10.1.8 together with

$$\deg(H(x)) = d \quad \text{or} \quad 2d - 1 \leq \deg(F(x)) \leq 2d \tag{10.4}$$

are equivalent to the curve $y^2 + H(x)y = F(x)$ having genus g.

It is not necessary for us to prove the Riemann–Roch theorem or the Hurwitz genus formula. Our discussion of Cantor reduction (see Lemma 10.3.20 and Lemma 10.4.6) will directly prove a special case of the Riemann–Roch theorem for hyperelliptic curves, namely that every divisor class contains a representative corresponding to an effective divisor of degree at most $g = d - 1$.

The reader should interpret the phrase "hyperelliptic curve of genus g" as meaning the conditions of Lemma 10.1.6 and Lemma 10.1.8 together with equation (10.4) on the degrees of $H(x)$ and $F(x)$ hold.

10.2 Isomorphisms, automorphisms and twists

We consider maps between hyperelliptic curves in this section. We are generally interested in isomorphisms over $\overline{\mathbb{k}}$ rather than just $\mathbb{k}$.

In the elliptic curve case (see Section 9.3) there was no loss of generality by assuming that isomorphisms fix infinity (since any isomorphism can be composed with a translation map). Since the points on a hyperelliptic curve do not, in general, form a group, one can no longer make this assumption. Nevertheless, many researchers have restricted attention to the special case of maps between curves that map points at infinity (with respect to an affine model of the domain curve) to points at infinity on the image curve. Theorem 10.2.1 classifies this special case.

In this chapter, and in the literature as a whole, isomorphisms are usually not assumed to fix infinity. For example, the isomorphism ρ_P defined earlier in Exercise 10.1.14 does not fix infinity. Isomorphisms that map points at infinity to points at infinity map ramified models to ramified models and unramified models to unramified models.

Theorem 10.2.1 *Let $C_1 : y_1^2 + H_1(x_1)y_1 = F_1(x_1)$ and $C_2 : y_2^2 + H_2(x_2)y_2 = F_2(x_2)$ be hyperelliptic curves over $\mathbb{k}$ of genus g. Then every isomorphism $\phi : C_1 \to C_2$ over $\mathbb{k}$ that maps points at infinity of C_1 to points at infinity of C_2 is of the form*

$$\phi(x_1, y_1) = (ux_1 + r, wy_1 + t(x_1))$$

where $u, w, r \in \mathbb{k}$ and $t \in \mathbb{k}[x_1]$. If C_1 and C_2 have ramified models then $\deg(t) \leq g$. If C_1 and C_2 have split or inert models then $\deg(t) \leq g + 1$, and the leading coefficient of $t(x_1)$ is not equal to the leading coefficient of $-wG^+(x_1)$ or $-wG^-(x_1)$ (where G^+ and G^- are as in Exercise 10.1.22).

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

Proof (Sketch) The proof is essentially the same as the proof of Proposition 3.1(b) of Silverman [505]; one can also find the ramified case in Proposition 1.2 of Lockhart [353]. One notes that the valuations at infinity of x_1 and x_2 have to agree, and similarly for y_1 and y_2. It follows that x_2 lies in the same Riemann–Roch spaces as x_1 and similarly for y_2 and y_1. The result follows (the final conditions are simply that the valuations at infinity of y_1 and y_2 must agree, so we are prohibited from setting $y_2 = w(y_1 + t(x))$ such that it lowers the valuation of y_2). □

We now introduce quadratic twists in the special case of finite fields. As mentioned in Example 9.5.2, when working in characteristic zero there are infinitely many quadratic twists.

Definition 10.2.2 Let $C : y^2 = F(x)$ be a hyperelliptic curve over a finite field $\mathbb{k}$ where $\mathrm{char}(\mathbb{k}) \neq 2$. Let $u \in \mathbb{k}^*$ be a non-square (i.e., there is no $v \in \mathbb{k}^*$ such that $u = v^2$) and define $C^{(u)} : y^2 = uF(x)$.

Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve over a finite field $\mathbb{k}$ where $\mathrm{char}(\mathbb{k}) = 2$. Let $u \in \mathbb{k}$ be such that $\mathrm{Tr}_{\mathbb{k}/\mathbb{F}_2}(u) = 1$. Define $C^{(u)} : y^2 + H(x)y = F(x) + uH(x)^2$.

In both cases, the $\mathbb{k}$-isomorphism class of the curve $C^{(u)}$ is called the non-trivial **quadratic twist** of C.

Exercise 10.2.3 Show that the quadratic twist is well-defined when $\mathbb{k}$ is a finite field. In other words, show that in the case $\mathrm{char}(\mathbb{k}) \neq 2$ if u and u' are two different non-squares in $\mathbb{k}^*$ then the corresponding curves $C^{(u)}$ and $C^{(u')}$ as in Definition 10.2.2 are isomorphic over $\mathbb{k}$. Similarly, if $\mathrm{char}(\mathbb{k}) = 2$ and for two different choices of trace one elements $u, u' \in \mathbb{k}$ show that the corresponding curves $C^{(u)}$ and $C^{(u')}$ are isomorphic over $\mathbb{k}$.

Exercise 10.2.4 Let C be a hyperelliptic curve over a finite field $\mathbb{k}$ and let $C^{(u)}$ be a non-trivial quadratic twist. Show that $\#C(\mathbb{F}_q) + \#C^{(u)}(\mathbb{F}_q) = 2(q + 1)$.

We now consider automorphisms. Define $\mathrm{Aut}(C)$ to be the set of all isomorphisms $\phi : C \to C$ over $\overline{\mathbb{k}}$. As usual, $\mathrm{Aut}(C)$ is a group under composition.

Example 10.2.5 Let $p > 2$ be a prime and $C : y^2 = x^p - x$ over $\mathbb{F}_p$. For $a \in \mathbb{F}_p^*$, $b \in \mathbb{F}_p$ one has isomorphisms

$$\phi_a(x, y) = (ax, \pm\sqrt{a}y) \qquad \text{and} \qquad \psi_{b,\pm}(x, y) = (x + b, \pm y)$$

from C to itself (in both cases they fix the point at infinity). Hence, the subgroup of $\mathrm{Aut}(C)$ consisting of maps that fix infinity is a group of at least $2p(p - 1)$ elements.

There is also the birational map $\rho(x, y) = (-1/x, y/x^{(p+1)/2})$ that corresponds to an isomorphism $\rho : C \to C$ on the projective curve. This morphism does not fix infinity. Since all the compositions $\psi_{b',\pm} \circ \rho \circ \psi_{b,\pm} \circ \phi_a$ are distinct one has $2p^2(p - 1)$ isomorphisms of this form. Hence, $\mathrm{Aut}(C)$ has size at least $2p(p - 1) + 2p^2(p - 1) = 2p(p + 1)(p - 1)$.

Exercise 10.2.6 Let $p > 2$ be a prime and $C : y^2 = x^p - x + 1$ over $\mathbb{F}_p$. Show that the subgroup of $\mathrm{Aut}(C)$ consisting of automorphisms that fix infinity has order $2p$.

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

Exercise 10.2.7 Let $p > 2$ be a prime and $C : y^2 = x^n + 1$ over $\mathbb{F}_p$ with $n \neq p$ (when $n = p$ the equation is singular). Show that the subgroup of $\mathrm{Aut}(C)$ consisting of automorphisms that fix infinity has order $2n$.

Exercise 10.2.8 Let $p \equiv 1 \pmod 8$ and let $C : y^2 = x^5 + Ax$ over $\mathbb{F}_p$. Write $\zeta_8 \in \overline{\mathbb{F}}_p$ for a primitive 8th root of unity. Show that $\zeta_8 \in \mathbb{F}_{p^4}$. Show that $\psi(x, y) = (\zeta_8^2 x, \zeta_8 y)$ is an automorphism of C. Show that $\psi^4 = \iota$.

10.3 Effective affine divisors on hyperelliptic curves

This section is about how to represent effective divisors on affine hyperelliptic curves, and algorithms to compute with them. A convenient way to represent divisors is using Mumford representation, and this is only possible if the divisor is semi-reduced.

Definition 10.3.1 Let C be a hyperelliptic curve over $\mathbb{k}$ and denote by $C \cap \mathbb{A}^2$ the affine curve. An **effective affine divisor** on C is

$$D = \sum_{P \in (C \cap \mathbb{A}^2)(\overline{\mathbb{k}})} n_P(P)$$

where $n_P \geq 0$ (and, as always, $n_P \neq 0$ for only finitely many P). A divisor on C is **semi-reduced** if it is an effective affine divisor and for all $P \in (C \cap \mathbb{A}^2)(\overline{\mathbb{k}})$ we have:

1. If $P = \iota(P)$ then $n_P = 1$.
2. If $P \neq \iota(P)$ then $n_P > 0$ implies $n_{\iota(P)} = 0$.

We slightly adjust the notion of equivalence for divisors on $C \cap \mathbb{A}^2$.

Definition 10.3.2 Let C be a hyperelliptic curve over a field $\mathbb{k}$ and let $f \in \mathbb{k}(C)$. We define

$$\mathrm{div}(f) \cap \mathbb{A}^2 = \sum_{P \in (C \cap \mathbb{A}^2)(\overline{\mathbb{k}})} v_P(f)(P).$$

Two divisors D, D' on $C \cap \mathbb{A}^2$ are **equivalent**, written $D \equiv D'$, if there is some function $f \in \overline{\mathbb{k}}(C)$ such that $D = D' + \mathrm{div}(f) \cap \mathbb{A}^2$.

Lemma 10.3.3 *Let C be a hyperelliptic curve. Every divisor on $C \cap \mathbb{A}^2$ is equivalent to a semi-reduced divisor.*

Proof Let $D = \sum_{P \in C \cap \mathbb{A}^2} n_P(P)$. By Exercise 10.1.19 the function $x - x_P$ has divisor $(P) + (\iota(P))$ on $C \cap \mathbb{A}^2$. If $n_P < 0$ for some $P \in (C \cap \mathbb{A}^2)(\overline{\mathbb{k}})$ then, by adding an appropriate multiple of $\mathrm{div}(x - x_P)$, one can arrange that $n_P = 0$ (this will increase $n_{\iota(P)}$). Similarly, if $n_P > 0$ and $n_{\iota(P)} > 0$ (or if $P = \iota(P)$ and $n_P \geq 2$) then subtracting a multiple of $\mathrm{div}(x - x_P)$ lowers the values of n_P and $n_{\iota(P)}$. Repeating this process yields a semi-reduced divisor. □

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

Example 10.3.4 Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on a hyperelliptic curve C such that $x_1 \neq x_2$. Let $D = -(P_1) + 2(P_2) + (\iota(P_2))$. Then D is not semi-reduced. One has

$$D + \mathrm{div}(x - x_1) = D + (P_1) + (\iota(P_1)) = (\iota(P_1)) + 2(P_2) + (\iota(P_2)),$$

which is still not semi-reduced. Subtracting $\mathrm{div}(x - x_2)$ from the above gives

$$D + \mathrm{div}((x - x_1)/(x - x_2)) = (\iota(P_1)) + (P_2),$$

which is semi-reduced.

10.3.1 Mumford representation of semi-reduced divisors

Mumford [399] introduced[1] a representation for semi-reduced divisors. The condition that the divisor is semi-reduced is crucial: if points $P = (x_P, y_P)$ and (x_P, y'_P) with $y_P \neq y'_P$ both appear in the support of the divisor then no polynomial $v(x)$ can satisfy both $v(x_P) = y_P$ and $v(x_P) = y'_P$.

Lemma 10.3.5 *Let $D = \sum_{i=1}^{l} e_i(x_i, y_i)$ be a non-zero semi-reduced divisor on a hyperelliptic curve $C : y^2 + H(x)y = F(x)$ (hence, D is affine and effective). Define*

$$u(x) = \prod_{i=1}^{l} (x - x_i)^{e_i} \in \overline{\Bbbk}[x].$$

Then there is a unique polynomial $v(x) \in \overline{\Bbbk}[x]$ such that $\deg(v(x)) < \deg(u(x))$, $v(x_i) = y_i$ for all $1 \leq i \leq l$, and

$$v(x)^2 + H(x)v(x) - F(x) \equiv 0 \pmod{u(x)}. \tag{10.5}$$

In particular, $v(x) = 0$ if and only if $u(x) \mid F(x)$.

Proof Since D is semi-reduced there is no conflict in satisfying the condition $v(x_i) = y_i$. If all $e_i = 1$ then the result is trivial. For each i such that $e_i > 1$ write $v(x) = y_i + (x - x_i)W(x)$ for some polynomial $W(x)$. We compute $v(x) \pmod{(x - x_i)^{e_i}}$ so it satisfies $v(x)^2 + H(x)v(x) - F(x) \equiv 0 \pmod{(x - x_i)^{e_i}}$ by Hensel lifting (see Section 2.13) as follows: if $v(x)^2 + H(x)v(x) - F(x) = (x - x_i)^j G_j(x)$ then set $v^\dagger(x) = v(x) + w(x - x_i)^j$ where w is an indeterminate and note that

$$v^\dagger(x)^2 + H(x)v^\dagger(x) - F(x) \equiv (x - x_i)^j (G_j(x) + 2v(x)w + H(x)w) \pmod{(x - x_i)^{j+1}}.$$

It suffices to find w such that this is zero, in other words, solve $G_j(x_i) + w(2y_i + H(x_i)) = 0$. Since D is semi-reduced, we know $2y_i + H(x_i) \neq 0$ (since $P = \iota(P)$ implies $n_P = 1$). The result follows by the Chinese remainder theorem. □

[1] Mumford remarks on pages 3–17 of [399] that a special case of these polynomials arises in the work of Jacobi. However, Jacobi only gives a representation for semi-reduced divisors with g points in their support, rather than arbitrary semi-reduced divisors.

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

Definition 10.3.6 Let D be a non-zero semi-reduced divisor. The polynomials $(u(x), v(x))$ of Lemma 10.3.5 are the **Mumford representation** of D. If $D = 0$ then take $u(x) = 1$ and $v(x) = 0$. A pair of polynomials $u(x), v(x) \in \bar{\mathbb{k}}[x]$ is called a **Mumford representation** if $u(x)$ is monic, $\deg(v(x)) < \deg(u(x))$ and if equation (10.5) holds.

We have shown that every semi-reduced divisor D has a Mumford representation and that the polynomials satisfying the conditions in Definition 10.3.6 are unique. We now show that one can easily recover an affine divisor D from the pair $(u(x), v(x))$: write $u(x) = \prod_{i=1}^{l}(x - x_i)^{e_i}$ and let $D = \sum_{i=1}^{l} e_i(x_i, v(x_i))$.

Exercise 10.3.7 Show that the processes of associating a Mumford representation to a divisor and associating a divisor to a Mumford representation are inverse to each other. More precisely, let D be a semi-reduced divisor on a hyperelliptic curve. Show that if one represents D in Mumford representation, and then obtains a corresponding divisor D' as explained above, then $D' = D$.

Exercise 10.3.8 Let $u(x), v(x) \in \mathbb{k}[x]$ be such that equation (10.5) holds. Let D be the corresponding semi-reduced divisor. Show that

$$D = \sum_{P \in (C \cap \mathbb{A}^2)(\bar{\mathbb{k}})} \min\{v_P(u(x)), v_P(y - v(x))\}(P).$$

This is called the **greatest common divisor** of $\operatorname{div}(u(x))$ and $\operatorname{div}(y - v(x))$ and is denoted $\operatorname{div}(u(x), y - v(x))$.

Exercise 10.3.9 Let $(u_1(x), v_1(x))$ and $(u_2(x), v_2(x))$ be the Mumford representations of two semi-reduced divisors D_1 and D_2. Show that if $\gcd(u_1(x), u_2(x)) = 1$ then $\operatorname{Supp}(D_1) \cap \operatorname{Supp}(D_2) = \varnothing$.

Lemma 10.3.10 *Let C be a hyperelliptic curve over $\mathbb{k}$ and let D be a semi-reduced divisor on C with Mumford representation $(u(x), v(x))$. Let $\sigma \in \operatorname{Gal}(\bar{\mathbb{k}}/\mathbb{k})$.*

1. *$\sigma(D)$ is semi-reduced.*
2. *The Mumford representation of $\sigma(D)$ is $(\sigma(u(x)), \sigma(v(x)))$.*
3. *D is defined over $\mathbb{k}$ if and only if $u(x), v(x) \in \mathbb{k}[x]$.*

Exercise 10.3.11 Prove Lemma 10.3.10.

Exercise 10.3.8 shows that the Mumford representation of a semi-reduced divisor D is natural from the point of view of principal divisors. This explains why condition (10.5) is the natural definition for the Mumford representation. There are two other ways to understand condition (10.5). First, the divisor D corresponds to an ideal in the ideal class group of the affine coordinate ring $\mathbb{k}[x, y]$, and condition (10.5) shows this ideal is equal to the $\mathbb{k}[x, y]$-ideal $(u(x), y - v(x))$. Second, from a purely algorithmic point of view, condition (10.5) is needed to make the Cantor reduction algorithm work (see Section 10.3.3).

A divisor class contains infinitely many divisors whose affine part is semi-reduced. Later we will define a reduced divisor to be one whose degree is sufficiently small. One can then

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

consider whether there is a unique such representative of the divisor class. This issue will be considered in Lemma 10.3.24 below.

Exercise 10.3.12 is relevant for the index calculus algorithms on hyperelliptic curves and it is convenient to place it here.

Exercise 10.3.12 A semi-reduced divisor D defined over $\mathbb{k}$ with Mumford representation $(u(x), v(x))$ is said to be a **prime divisor** if the polynomial $u(x)$ is irreducible over $\mathbb{k}$. Show that if D is not a prime divisor, then D can be efficiently expressed as a sum of prime divisors by factoring $u(x)$. More precisely, show that if $u(x) = \prod u_i(x)^{c_i}$ is the complete factorisation of $u(x)$ over $\mathbb{k}$, then $D = \sum c_i \mathrm{div}(u_i(x), y - v_i(x))$ where $v_i(x) = v(x) \bmod u_i(x)$.

10.3.2 Addition and semi-reduction of divisors in Mumford representation

We now present Cantor's algorithm [111][2] for addition of semi-reduced divisors on a hyperelliptic curve C. As above, we take a purely geometric point of view. An alternative, and perhaps more natural, interpretation of Cantor's algorithm is multiplication of ideals in $\mathbb{k}[x, y] \subset \mathbb{k}(C)$.

Given two semi-reduced divisors D_1 and D_2 with Mumford representation $(u_1(x), v_1(x))$ and $(u_2(x), v_2(x))$ we want to compute the Mumford representation $(u_3(x), v_3(x))$ of the sum $D_1 + D_2$. Note that we are not yet considering reduction of divisors in the divisor class group. There are two issues that make addition not completely trivial. First, if P is in the support of D_1 and $\iota(P)$ is in the support of D_2 then we remove a suitable multiple of $(P) + (\iota(P))$ from $D_1 + D_2$. Second, we must ensure that the Mumford representation takes multiplicities into account (i.e., so that equation (10.5) holds for $(u_3(x), v_3(x))$).

Example 10.3.13 Let $P = (x_P, y_P)$ on $y^2 + H(x)y = F(x)$ be such that $P \neq \iota(P)$. Let $D_1 = D_2 = (P)$ so that $u_1(x) = u_2(x) = (x - x_P)$ and $v_1(x) = v_2(x) = y_P$. Then $D_1 + D_2 = 2(P)$. The Mumford representation for this divisor has $u_3(x) = (x - x_P)^2$ and $v(x) = y_P + w(x - x_P)$ for some $w \in \overline{\mathbb{k}}$. To satisfy equation (10.5) one finds that

$$y_P^2 + 2y_P w(x - x_P) + H(x)y_P + wH(x)(x - x_P) - F(x) \equiv 0 \pmod{(x - x_P)^2}.$$

Writing $F(x) \equiv F(x_P) + F'(x_P)(x - x_P) \pmod{(x - x_P)^2}$ and $H(x) \equiv H(x_P) + H'(x_P)(x - x_P) \pmod{(x - x_P)^2}$ gives

$$w = \frac{F'(x_P) - y_P H'(x_P)}{2y_P + H(x_P)},$$

which is defined since $P \neq \iota(P)$.

To help motivate the formula for $v_3(x)$ in Theorem 10.3.14 we now make some observations. First, note that the equation

$$1 = s_1(x)(x - x_P) + s_3(x)(2y_P + H(x))$$

[2] The generalisation of Cantor's algorithm to all hyperelliptic curves was given by Koblitz [311].

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

has the solution

$$s_3(x) = \frac{1}{2y_P + H(x_P)} \quad \text{and} \quad s_1(x) = -s_3(x)(H'(x_P) + (x - x_P)G(x))$$

where $G(x) = (H(x) - H(x_P) - H'(x_P)(x - x_P))/(x - x_P)^2$. Furthermore, note that

$$v(x) \equiv s_1(x)(x - x_P)y_P + s_3(x)(y_P^2 + F(x)) \pmod{(x - x_P)^2}.$$

The core of Cantor's addition and semi-reduction algorithm is to decide which functions $(x - x_P)$ are needed (and to which powers) to obtain a semi-reduced divisor equivalent to $D_1 + D_2$. The **crucial observation** is that if P is in the support of D_1 and $\iota(P)$ is in the support of D_2 then $(x - x_P) \mid u_1(x)$, $(x - x_P) \mid u_2(x)$ and $v_1(x_P) = -v_2(x_P) - H(x_P)$ and so $(x - x_P) \mid (v_1(x) + v_2(x) + H(x))$. The exact formulae are given in Theorem 10.3.14. The process is called **Cantor's addition algorithm** or **Cantor's composition algorithm**.

Theorem 10.3.14 *Let $(u_1(x), v_1(x))$ and $(u_2(x), v_2(x))$ be Mumford representations of two semi-reduced divisors D_1 and D_2. Let $s(x) = \gcd(u_1(x), u_2(x), v_1(x) + v_2(x) + H(x))$ and let $s_1(x), s_2(x), s_3(x) \in \Bbbk[x]$ be such that*

$$s(x) = s_1(x)u_1(x) + s_2(x)u_2(x) + s_3(x)(v_1(x) + v_2(x) + H(x)).$$

Define $u_3(x) = u_1(x)u_2(x)/s(x)^2$ and

$$v_3(x) = (s_1(x)u_1(x)v_2(x) + s_2(x)u_2(x)v_1(x) + s_3(x)(v_1(x)v_2(x) + F(x)))/s(x). \quad (10.6)$$

Then $u_3(x), v_3(x) \in \Bbbk[x]$ and the Mumford representation of the semi-reduced divisor D equivalent to $D_1 + D_2$ is $(u_3(x), v_3(x))$.

Proof Let $D = D_1 + D_2 - \operatorname{div}(s(x)) \cap \mathbb{A}^2$ so that D is equivalent to $D_1 + D_2$. By the "crucial observation" above, $s(x)$ has a root x_P for some point $P = (x_P, y_P)$ on the curve if and only if P and $\iota(P)$ lie in the supports of D_1 and D_2. Taking multiplicities into account, it follows that D is semi-reduced.

It is immediate that $s(x)^2 \mid u_1(x)u_2(x)$ and so $u_3(x) \in \Bbbk[x]$. It is also immediate that $u_3(x)$ is the correct first component of the Mumford representation of D.

To show $v_3(x) \in \Bbbk[x]$ re-write $v_3(x)$ as

$$v_3 = \frac{v_2(s - s_2u_2 - s_3(v_1 + v_2 + H)) + s_2u_2v_1 + s_3(v_1v_2 + F)}{s} \quad (10.7)$$

$$= v_2 + s_2(v_1 - v_2)(u_2/s) + s_3(F - v_2H - v_2^2)/s. \quad (10.8)$$

Since $s(x) \mid u_2(x)$ and $u_2(x) \mid (F - v_2H - v_2^2)$ the result follows.

We now need the equation

$$(v_1 + v_2 + H)(v_3 - y) \equiv (y - v_1)(y - v_2) \pmod{u_3}. \quad (10.9)$$

This is proved by inserting the definition of v_3 from equation (10.6) to get

$$(v_1 + v_2 + H)(v_3 - y) \equiv -(v_1 + v_2 + H)y + (s_1u_1(v_2^2 + Hv_2 - F) + s_2u_2(v_1^2 + Hv_1 - F) + (v_1v_2 + F)(s_1u_1 + s_2u_2 + s_3(v_1 + v_2 + H))/s \pmod{u_3(x)}.$$

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

Then using $(y - v_1)(y - v_2) = F - (v_1 + v_2 + H)y + v_1 v_2$ and $u_i \mid (v_i^2 + Hv_i - F)$ for $i = 1, 2$ proves equation (10.9).

Finally, it remains to prove that equation (10.5) holds. We do this by showing that

$$v_P(v(x)^2 + H(x)v(x) - F(x)) \geq v_P(u(x))$$

for all $P = (x_P, y_P) \in \mathrm{Supp}(D)$. Suppose first that $P \neq \iota(P)$ and that $(x - x_P)^e \| u_3(x)$. Then it is sufficient to show that $v_P(y - v_3(x)) \geq e$. This will follow from equation (10.9). First note that $v_P(y - v_3) = v_P((v_1 + v_2 + H)(v_3 - y))$ and that this is at least $\min\{v_P(u_3), v_P((y - v_1)(y - v_2))\}$. Then $v_P(y - v_1) + v_P(y - v_2) \geq v_P(u_1(x)) + v_P(u_2(x)) \geq e$.

Now for the case $P = \iota(P) \in \mathrm{Supp}(D)$. Recall that such points only occur in semi-reduced divisors with multiplicity 1. Since $u_3(x)$ is of minimal degree we know $(x - x_P) \| u_3(x)$. It suffices to show that $v_3(x_P) = y_P$, but this follows from equation (10.8). Without loss of generality, $P \in \mathrm{Supp}(D_2)$ and $P \notin \mathrm{Supp}(D_1)$ (if $P \in \mathrm{Supp}(D_i)$ for both $i = 1, 2$ then $P \notin \mathrm{Supp}(D)$) so $(x - x_P) \nmid s(x)$, $v_2(x_P) = y_P$ and $(u_2/s)(x_P) = 0$. Hence, $v_3(x_P) = v_2(x_P) + 0 = y_P$. □

Exercise 10.3.15 Let $C : y^2 + (x^2 + 2x + 10)y = x^5 + x + 1$ over $\mathbb{F}_{11}$. Let $D_1 = (0, 4) + (6, 4)$ and $D_2 = (0, 4) + (1, 1)$. Determine the Mumford representation of $D_1, D_2, 2D_1, D_1 + D_2$.

We remark that, in practical implementation, one almost always has $\gcd(u_1(x), u_2(x)) = 1$ and so $s(x) = 1$ and the addition algorithm can be simplified. Indeed, it is possible to give explicit formulae for the general cases in the addition algorithm for curves of small genus, we refer to Sections 14.4, 14.5 and 14.6 of [16].

Exercise 10.3.16 Show that the Cantor addition algorithm for semi-reduced divisors of degree $\leq m$ has complexity $O(m^2 M(\log(q))$ bit operations.

10.3.3 Reduction of divisors in Mumford representation

Suppose we have an affine effective divisor D with Mumford representation $(u(x), v(x))$. We wish to obtain an equivalent divisor (affine and effective) whose Mumford representation has $\deg(u(x))$ of low degree. We will show in Theorem 10.3.21 and Lemma 10.4.6 that one can ensure $\deg(u(x)) \leq g$, where g is the genus; we will call such divisors reduced. The idea is to consider

$$u^\dagger(x) = \mathrm{monic}((v(x)^2 + H(x)v(x) - F(x))/u(x)), \; v^\dagger(x) = -v(x) - H(x) \pmod{u^\dagger(x)} \tag{10.10}$$

where $\mathrm{monic}\left(u_0 + u_1 x + \cdots + u_k x^k\right)$ for $u_k \neq 0$ is defined to be $(u_0/u_k) + (u_1/u_k)x + \cdots + x^k$. Obtaining $(u^\dagger(x), v^\dagger(x))$ from $(u(x), v(x))$ is a **Cantor reduction step**. This operation appears in the classical reduction theory of binary quadratic forms.

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

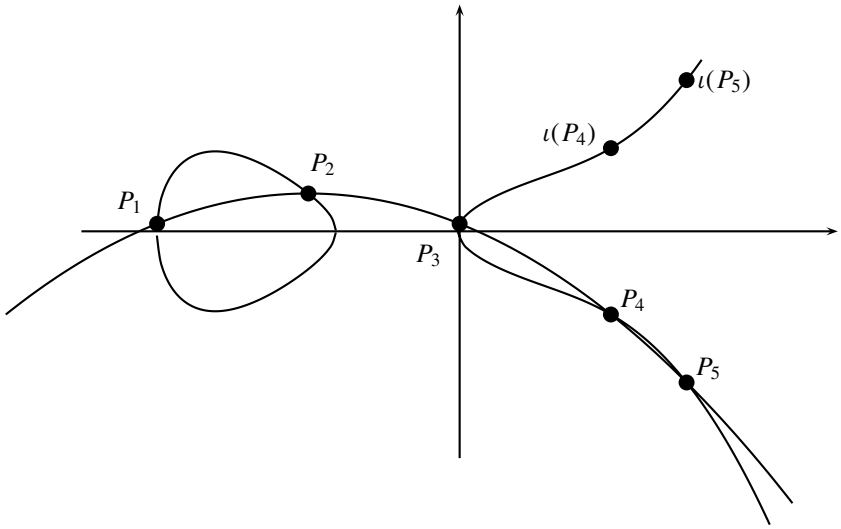

Figure 10.1 Cantor reduction on a hyperelliptic curve.

Lemma 10.3.17 *Let D be an affine effective divisor on a hyperelliptic curve C with Mumford representation $(u(x), v(x))$. Define $(u^\dagger(x), v^\dagger(x))$ as in equation (10.10). Then $(u^\dagger(x), v^\dagger(x))$ is the Mumford representation of a semi-reduced divisor $D^\dagger$ and $D^\dagger \equiv D$ on $C \cap \mathbb{A}^2$.*

Proof One checks that $(u^\dagger(x), v^\dagger(x))$ satisfies condition (10.5) and so there is an associated semi-reduced divisor $D^\dagger$.

Write $D = (P_1) + \cdots + (P_n)$ (where the same point can appear more than once). Then $\operatorname{div}(y - v(x)) \cap \mathbb{A}^2 = (P_1) + \cdots + (P_n) + (P_{n+1}) + \cdots + (P_{n+m})$ for some points $P_{n+1}, \ldots, P_{n+m}$ (not necessarily distinct from the earlier n points, or from each other) and $\operatorname{div}(v(x)^2 + H(x)v(x) - F(x)) \cap \mathbb{A}^2 = \operatorname{div}((y - v(x))(-y - H(x) - v(x))) \cap \mathbb{A}^2 = (P_1) + (\iota(P_1)) + \cdots + (P_{n+m}) + (\iota(P_{n+m}))$. Now, $\operatorname{div}(u^\dagger(x)) = (P_{n+1}) + (\iota(P_{n+1})) + \cdots + (P_{n+m}) + (\iota(P_{n+m}))$. It follows that $D^\dagger = (\iota(P_{n+1})) + \cdots + (\iota(P_{n+m}))$ and that $D = D^\dagger + \operatorname{div}(y - v(x)) \cap \mathbb{A}^2 - \operatorname{div}(u^\dagger(x)) \cap \mathbb{A}^2$. □

Example 10.3.18 Consider

$$C : y^2 = F(x) = x^5 + 2x^4 - 8x^3 + 10x^2 + 40x + 1$$

over $\mathbb{Q}$. Let $P_1 = (-4, 1)$, $P_2 = (-2, 5)$, $P_3 = (0, 1)$ and $D = (P_1) + (P_2) + (P_3)$. The Mumford representation of D is $(u(x), v(x)) = (x(x + 2)(x + 4), -x^2 - 4x + 1)$, which is easily checked by noting that $v(x_{P_i}) = y_{P_i}$ for $1 \le i \le 3$.

To reduce D one sets $u^\dagger(x) = \operatorname{monic}\big((v(x)^2 - F(x))/u(x)\big) = \operatorname{monic}(-x^2 + 5x - 6) = (x - 3)(x - 2)$ and $v^\dagger(x) = -v(x) \pmod{u^\dagger(x)} = 9x - 7$.

One can check that $\operatorname{div}(y - v(x)) = (P_1) + (P_2) + (P_3) + (P_4) + (P_5)$ where $P_4 = (2, -11)$ and $P_5 = (3, -20)$, that $\operatorname{div}(u^\dagger(x)) = (P_4) + (\iota(P_4)) + (P_5) + (\iota(P_5))$ and that $D \equiv \operatorname{div}(u^\dagger(x), y - v^\dagger(x)) \cap \mathbb{A}^2 = (\iota(P_4)) + (\iota(P_5))$. See Figure 10.1 for an illustration.

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

Exercise 10.3.19 Show that the straight lines $l(x, y)$ and $v(x)$ in the elliptic curve addition law (Definition 7.9.1) correspond to the polynomials $y - v(x)$ and $u^\dagger(x)$ (beware of the double meaning of $v(x)$ here) in a Cantor reduction step.

Lemma 10.3.20 *Let $C : y^2 + H(x)y = F(x)$ and let $(u(x), v(x))$ be the Mumford representation of a semi-reduced divisor D. Write $d_H = \deg(H(x))$, $d_F = \deg(F(x))$, $d_u = \deg(u(x))$ and $d_v = \deg(v(x))$. Let $d = \max\{d_H, \lceil d_F/2 \rceil\}$. Let $(u^\dagger(x), v^\dagger(x))$ be the polynomials arising from a Cantor reduction step.*

1. *If $d_v \geq d$ then $\deg(u^\dagger(x)) \leq d_u - 2$.*
2. *If $d_F \leq 2d - 1$ and $d_u \geq d > d_v$ then $\deg(u^\dagger(x)) \leq d - 1$ (this holds even if $d_H = d$).*
3. *If $d_F = 2d$ and $d_u > d > d_v$ then $\deg(u^\dagger(x)) \leq d - 1$.*

Proof Note that $d_u > d_v$. If $d_v \geq d$ then

$$\begin{aligned}\deg(v(x)^2 + H(x)v(x) - F(x)) &\leq \max\{2d_v, d_H + d_v, d_F\} \\ &\leq \max\{2(d_u - 1), d + (d_u - 1), 2d\}.\end{aligned}$$

Hence, $\deg(u^\dagger(x)) = \deg(v^2 + Hv - F) - d_u \leq \max\{d_u - 2, d - 1, 2d - d_u\} = d_u - 2$.

If $d_F \leq 2d - 1$ and $d_u \geq d > d_v$ then, by a similar argument, $\deg(u^\dagger(x)) \leq 2d - 1 - d_u \leq d - 1$. Finally, if $d_F = 2d$ and $d_u > d > d_v$ then $\deg(v^2 + Hv + F) = 2d$ and $\deg(u^\dagger) = 2d - d_u < d$. □

Theorem 10.3.21 *Suppose $C : y^2 + H(x)y = F(x)$ is a hyperelliptic curve of genus g with $\deg(F(x)) \leq 2g + 1$. Then every semi-reduced divisor is equivalent to a semi-reduced divisor of degree at most g.*

Proof Perform Cantor reduction steps repeatedly. By Lemma 10.3.20 the desired condition will eventually hold. □

Theorem 10.3.21 is an "explicit Riemann–Roch theorem" for hyperelliptic curves with a single point at infinity (also for hyperelliptic curves $y^2 + H(x)y = F(x)$ with two points at infinity but $\deg(F(x)) \leq 2g + 1$) as it shows that every divisor class contains a representative as an affine effective divisor of degree at most g. The general result is completed in Lemma 10.4.6 below.

Definition 10.3.22 Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve of genus g. A semi-reduced divisor on C is **reduced** if its degree is at most g.

Exercise 10.3.23 Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve with $d = \max\{\deg(H), \lceil \deg(F)/2 \rceil\}$. Let $(u(x), v(x))$ be the Mumford representation of a divisor with $\deg(v(x)) < \deg(u(x)) < d$. Show that if $\deg(F(x)) \geq 2d - 1$ and one performs a Cantor reduction step on $(u(x), v(x))$ then the resulting polynomials $(u^\dagger(x), v^\dagger(x))$ are such that $\deg(u^\dagger(x)) \geq d$.

When $\deg(F) = 2d$ then Lemma 10.3.20 is not sufficient to prove an analogue of Theorem 10.3.21. However, one can at least reduce to a divisor of degree $d = g + 1$. It

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

is notable that performing a Cantor reduction step on a divisor of degree d in this case usually yields another divisor of degree d. This phenomena will be discussed in detail in Section 10.4.2.

We now consider the uniqueness of the reduced divisor of Theorem 10.3.21. Lemma 10.3.24 below shows that non-uniqueness can only arise with split or inert models. It follows that there is a unique reduced divisor in every divisor class for hyperelliptic curves with ramified model. For hyperelliptic curves with split or inert model there is not necessarily a unique reduced divisor.

Lemma 10.3.24 *Let $y^2 + H(x)y = F(x)$ be a hyperelliptic curve over $\mathbb{k}$ of genus g. Let $d_H = \deg(H(x))$ and $d_F = \deg(F(x))$. Let D_1 and D_2 be semi-reduced divisors of degree at most g. Assume that $D_1 \neq D_2$ but $D_1 \equiv D_2$. Then $d_F = 2g + 2$ or $d_H = g + 1$.*

Proof First note that $d_H \leq g + 1$ and $d_F \leq 2g + 2$. Let $D_3' = D_1 + \iota_*(D_2)$ so that $D_3' \equiv D_1 - D_2 \equiv 0$ as an affine divisor. Let D_3 be the semi-reduced divisor equivalent to D_3' (i.e., by removing all occurences $(P) + (\iota(P))$). Note that the degree of D_3 is at most $2g$ and that $D_3 \neq 0$. Since $D_3 \equiv 0$ and D_3 is an effective affine divisor we have $D_3 = \operatorname{div}(G(x, y))$ on $C \cap \mathbb{A}^2$ for some non-zero polynomial $G(x, y)$. Without loss of generality, $G(x, y) = a(x) - b(x)y$. Furthermore, $b(x) \neq 0$ (since $\operatorname{div}(a(x))$ is not semi-reduced for any non-constant polynomial $a(x)$).

Exercise 10.1.21 shows that the degree of $\operatorname{div}(a(x) - b(x)y)$ on $C \cap \mathbb{A}^2$ is the degree of $a(x)^2 + H(x)a(x)b(x) - F(x)b(x)^2$. We need this degree to be at most $2g$. This is easily achieved if $d_F \leq 2g$ (in which case $d_H = g + 1$ for the curve to have genus g). However, if $2g + 1 \leq d_F \leq 2g + 2$ then we need either $\deg(a(x)^2) = \deg(F(x)b(x)^2)$ or $\deg(H(x)a(x)b(x)) = \deg(F(x)b(x)^2)$. The former case is only possible if d_F is even (i.e., $d_F = 2g + 2$). If $d_F = 2g + 1$ and $d_H \leq g$ then the latter case implies $\deg(a(x)) \geq g + 1 + \deg(b(x))$ and so $\deg(a(x)^2) > \deg(F(x)b(x)^2)$ and $\deg(G(x, y)) > 2g$. □

For hyperelliptic curves of fixed (small) genus it is possible to give explicit formulae for the general cases of the composition and reduction algorithms. For genus 2 curves this was done by Harley [251] (the basic idea is to formally solve for $u^\dagger(x)$ such that $u^\dagger(x)u(x) = \operatorname{monic}(v(x)^2 + H(x)v(x) - F(x))$ as in equation (10.10)). For extensive discussion and details (and also for non-affine coordinate systems for efficient hyperelliptic arithmetic) we refer to Sections 14.4, 14.5 and 14.6 of [16].

10.4 Addition in the divisor class group

We now show how Cantor's addition and reduction algorithms for divisors on the affine curve can be used to perform arithmetic in the divisor class group of the projective curve. A first remark is that Lemma 10.3.3 implies that every degree zero divisor class on a hyperelliptic curve has a representative of the form $D + n^+(\infty^+) + n^-(\infty^-)$ where D is a semi-reduced (hence, affine and effective) divisor and $n^+, n^- \in \mathbb{Z}$ (necessarily, $\deg(D) + n^+ + n^- = 0$).

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

10.4.1 Addition of divisor classes on ramified models

On a hyperelliptic curve with ramified model there is only a single point at infinity. We will show in this section that, for such curves, one can compute in the divisor class group using only affine divisors.

We use the Cantor algorithms for addition, semi-reduction and reduction. In general, if one has a semi-reduced divisor D then, by case 1 of Lemma 10.3.20, a reduction step reduces the degree of D by 2. Hence, at most $\deg(D)/2$ reduction steps are possible.

Theorem 10.4.1 *Let C be a hyperelliptic curve with ramified model. Then every degree zero divisor class on C has a unique representative of the form $D - n(\infty)$ where D is semi-reduced and where $0 \leq n \leq g$.*

Proof Theorem 10.3.21 showed that every affine divisor is equivalent to a semi-reduced divisor D such that $0 \leq \deg(D) \leq g$. This corresponds to the degree zero divisor $D - n(\infty)$ where $n = \deg(D)$. Uniqueness was proved in Lemma 10.3.24. □

A degree zero divisor of the form $D - n(\infty)$ where D is a semi-reduced divisor of degree n and $0 \leq n \leq g$ is called **reduced**. We represent D using Mumford representation as $(u(x), v(x))$ and we know that the polynomials $u(x)$ and $v(x)$ are unique. The divisor class is defined over $\Bbbk$ if and only if the corresponding polynomials $u(x), v(x) \in \Bbbk[x]$. Addition of divisors is performed using Cantor's composition and reduction algorithms as above.

Exercise 10.4.2 Let $C : y^2 + H(x)y = F(x)$ be a ramified model of a hyperelliptic curve over $\mathbb{F}_q$. Show that the inverse (also called the negative) of a divisor class on C represented as $(u(x), v(x))$ is $(u(x), -v(x) - (H(x) \pmod{u(x)}))$.

Exercise 10.4.3 Let C be a hyperelliptic curve over $\Bbbk$ of genus g with ramified model. Let D_1 and D_2 be reduced divisors on C. Show that one can compute a reduced divisor representing $D_1 + D_2$ in $O(g^3)$ operations in $\Bbbk$. Show that one can compute $[n]D_1$ in $O(\log(n)g^3)$ operations in $\Bbbk$ (here $[n]D_1$ means the n-fold addition $D_1 + D_1 + \cdots + D_1$).

When the genus is 2 (i.e., $d = 3$) and one adds two reduced divisors (i.e., effective divisors of degree ≤ 2) then the sum is an effective divisor of degree at most 4 and so only one reduction operation is needed to compute the reduced divisor. Similarly, for curves of any genus, at most one reduction operation is needed to compute a reduced divisor equivalent to $D + (P)$ where D is a reduced divisor (such ideas were used by Katagi, Akishita, Kitamura and Takagi [299, 298] to speed up cryptosystems using hyperelliptic curves).

For larger genus there are several variants of the divisor reduction algorithm. In Section 4 of [111], Cantor gives a method that uses higher degree polynomials than $y - v(x)$ and requires fewer reduction steps. In Section VII.2.1 of [61], Gaudry presents a reduction algorithm, essentially due to Lagrange, that is useful when $g \geq 3$. The NUCOMP algorithm (originally proposed by Shanks in the number field setting) is another useful alternative.

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

We refer to Jacobson and van der Poorten [289] and Section VII.2.2 of [61] for details. It seems that NUCOMP should be used once the genus of the curve exceeds 10 (and possibly even for $g \geq 7$).

Exercise 10.4.4 Let C be a hyperelliptic curve of genus 2 over a field $\mathbb{k}$ with a ramified model. Show that every $\mathbb{k}$-rational divisor class has a unique representative of one of the following four forms:

1. $(P) - (\infty)$ where $P \in C(\mathbb{k})$, including $P = \infty$. Here $u(x) = (x - x_P)$ or $u(x) = 1$.
2. $2(P) - 2(\infty)$ where $P \in C(\mathbb{k})$, excluding points P such that $P = \iota(P)$. Here $u(x) = (x - x_P)^2$.
3. $(P) + (Q) - 2(\infty)$ where $P, Q \in C(\mathbb{k})$ are such that $P, Q \neq \infty$, $P \neq Q$, $P \neq \iota(Q)$. Here $u(x) = (x - x_P)(x - x_Q)$.
4. $(P) + (\sigma(P)) - 2(\infty)$ where $P \in C(\mathbb{K}) - C(\mathbb{k})$ for any quadratic field extension $\mathbb{K}/\mathbb{k}$, $\mathrm{Gal}(\mathbb{K}/\mathbb{k}) = \langle \sigma \rangle$ and $\sigma(P) \notin \{P, \iota(P)\}$. Here $u(x)$ is an irreducible quadratic in $\mathbb{k}[x]$.

Exercise 10.4.5 can come in handy when computing pairings on hyperelliptic curves.

Exercise 10.4.5 Let $D_1 = \mathrm{div}(u_1(x), y - v_1(x)) \cap \mathbb{A}^2$ and $D_2 = \mathrm{div}(u_2(x), y - v_2(x)) \cap \mathbb{A}^2$ be semi-reduced divisors on a hyperelliptic curve with ramified model over $\mathbb{k}$. Write $d_1 = \deg(u_1(x))$ and $d_2 = \deg(u_2(x))$. Let $D_3 = \mathrm{div}(u_3(x), y - v_3(x)) \cap \mathbb{A}^2$ be a semi-reduced divisor of degree d_3 such that $D_3 - d_3(\infty) \equiv D_1 - d_1(\infty) + D_2 - d_2(\infty)$. Show that if $d_2 = d_3$ then $D_1 - d_1(\infty) \equiv D_3 - D_2$.

10.4.2 Addition of divisor classes on split models

This section is rather detailed and can safely be ignored by most readers. It presents results of Paulus and Rück [429] and Galbraith, Harrison and Mireles [202].

Let C be a hyperelliptic curve of genus g over $\mathbb{k}$ with a split model. We have already observed that every degree zero divisor class has a representative of the form $D + n^+(\infty^+) + n^-(\infty^-)$ where D is semi-reduced and $n^+, n^- \in \mathbb{Z}$. Lemma 10.3.20 has shown that we may assume $0 \leq \deg(D) \leq g + 1$. One could consider the divisor to be reduced if this is the case, but this would not be optimal.

The Riemann–Roch theorem implies we should be able to take $\deg(D) \leq g$ but Cantor reduction becomes "stuck" if the input divisor has degree $g + 1$. The following simple trick allows us to reduce to semi-reduced divisors of degree g (and this essentially completes the proof of the "Riemann–Roch theorem" for these curves). Recall the polynomial $G^+(x)$ of degree $d = g + 1$ from Exercise 10.1.22.

Lemma 10.4.6 *Let $y^2 + H(x)y = F(x)$ be a hyperelliptic curve of genus g over $\mathbb{k}$ with split model. Let $u(x), v(x)$ be a Mumford representation such that* $\deg(u(x)) = g + 1$. *Define*

$$v^{\ddagger}(x) = G^+(x) + (v(x) - G^+(x) \pmod{u(x)}) \in \mathbb{k}[x]$$

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

where we mean that $v(x) - G^+(x)$ *is reduced to a polynomial of degree at most* $\deg(u(x)) - 1 = g$. *Define*

$$u^\dagger(x) = \text{monic}\left(\frac{v^\ddagger(x)^2 + H(x)v^\ddagger(x) - F(x)}{u(x)}\right) \quad \textit{and}$$
$$v^\dagger(x) = -v^\ddagger(x) - H(x) \pmod{u^\dagger(x)}. \tag{10.11}$$

Then $\deg(u^\dagger(x)) \leq g$ *and*

$$\begin{aligned}\text{div}(u(x), y - v(x)) \cap \mathbb{A}^2 &= \text{div}(u^\dagger(x), y - v^\dagger(x)) \cap \mathbb{A}^2 - \text{div}(u^\dagger(x)) \cap \mathbb{A}^2 \\ &\quad + \text{div}(y - v^\ddagger(x)) \cap \mathbb{A}^2. \end{aligned} \tag{10.12}$$

Proof Note that $v^\ddagger(x) \equiv v(x) \pmod{u(x)}$ and so $v^\ddagger(x)^2 + H(x)v^\ddagger(x) - F(x) \equiv 0 \pmod{u(x)}$; hence, $u^\dagger(x)$ is a polynomial. The crucial observation is that $\deg(v^\ddagger(x)) = \deg(G^+(x)) = d = g + 1$ and so the leading coefficient of $v^\ddagger(x)$ agrees with that of $G^+(x)$. Hence, $\deg(v^\ddagger(x)^2 + H(x)v^\ddagger(x) - F(x)) \leq 2d - 1 = 2g + 1$ and so $\deg(u^\dagger(x)) \leq 2d - 1 - d = d - 1 = g$ as claimed. To show equation (10.12) it is sufficient to write $u(x)u^\dagger(x) = \prod_{i=1}^{l}(x - x_i)^{e_i}$ and to note that

$$\begin{aligned}\text{div}(y - v^\ddagger(x)) \cap \mathbb{A}^2 &= \sum_{i=1}^{l} e_i(x_i, v^\ddagger(y_i)) \\ &= \text{div}(u(x), y - v(x)) \cap \mathbb{A}^2 + \text{div}(u^\dagger(x), y + H(x) + v^\dagger(x)) \cap \mathbb{A}^2\end{aligned}$$

and that $\text{div}(u^\dagger(x)) = \text{div}(u^\dagger(x), y - v^\dagger(x)) + \text{div}(u^\dagger(x), y + v^\dagger(x) + H(x))$. □

Example 10.4.7 Let $C : y^2 = F(x) = x^6 + 6 = (x - 1)(x + 1)(x - 2)(x + 2)(x - 3)(x + 3)$ over $\mathbb{F}_7$. Then $G^+(x) = x^3$. Consider the divisor $D = (1, 0) + (-1, 0) + (2, 0)$ with Mumford representation $(u(x), v(x)) = ((x - 1)(x + 1)(x - 2), 0)$. Performing standard Cantor reduction gives $u^\dagger(x) = F(x)/u(x) = (x + 2)(x - 3)(x + 3)$, which corresponds to the trivial divisor equivalence $D \equiv (-2, 0) + (3, 0) + (-3, 0)$. Instead, we take $v^\ddagger = G^+(x) + (-G^+(x) \pmod{u(x)}) = x^3 + (-x^3 + u(x)) = u(x)$. Then $u^\dagger(x) = \text{monic}\left((v^\ddagger(x)^2 - F(x))/u(x)\right) = x^2 + 5x + 2$ and $v^\dagger(x) = 3x + 5$. The divisor $\text{div}(u^\dagger(x), y - v^\dagger(x)) \cap \mathbb{A}^2$ is a sum $(P) + (\sigma(P))$ where $P \in C(\mathbb{F}_{7^2}) - C(\mathbb{F}_7)$ and σ is the non-trivial element of $\text{Gal}(\mathbb{F}_{7^2}/\mathbb{F}_7)$.

The operation $(u(x), v(x)) \mapsto (u^\dagger(x), v^\dagger(x))$ of equation (10.11) is called **composition and reduction at infinity**; the motivation for this is given in equation (10.17) below. Some authors call it a **baby step**. This operation can be performed even when $\deg(u(x)) < d$, and we analyse it in the general case in Lemma 10.4.14.

Exercise 10.4.8 Let the notation be as in Lemma 10.4.6. Let $d_u = \deg(u(x))$ so that $v^\ddagger(x)$ agrees with $G^+(x)$ for the leading $d - d_u + 1$ coefficients and so $m = \deg(v^\ddagger(x)^2 +$

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

$H(x)v^{\ddagger}(x) - F(x)) \leq d + d_u - 1$. Let $d_{u^\dagger} = \deg(u^\dagger(x))$ so that $m = d_u + d_{u^\dagger}$. Show that $v_{\infty^-}(y - v^{\ddagger}(x)) = -d$, $\operatorname{div}(y - v^{\ddagger}(x)) =$

$$\begin{aligned}&\operatorname{div}(u(x), y - v(x)) \cap \mathbb{A}^2 + \operatorname{div}(u^\dagger(x), y + H(x) + v^\dagger(x)) \cap \mathbb{A}^2 \\ &\quad - (d_u + d_{u^\dagger} - d)(\infty^+) - d(\infty^-) \end{aligned} \tag{10.13}$$

and $v_{\infty^+}(y - v^{\ddagger}(x)) = -(d_u + d_{u^\dagger} - d)$.

We now discuss how to represent divisor classes. An obvious choice is to represent classes as $D - d(\infty^+)$ where D is an affine effective divisor of degree d (see Paulus and Rück [429] for a full discussion of this case). A more natural representation, as pointed out by Galbraith, Harrison and Mireles [202], is to use balanced representations at infinity: in other words, when g is even, to represent divisor classes as $D - (g/2)((\infty^+) + (\infty^-))$ where D is an effective divisor of degree g.

Definition 10.4.9 Let C be a hyperelliptic curve of genus g over $\mathbb{k}$ with split model. If g is even then define $D_\infty = \frac{g}{2}((\infty^+) + (\infty^-))$. If g is odd then define $D_\infty = \frac{(g+1)}{2}(\infty^+) + \frac{(g-1)}{2}(\infty^-)$.

Let $u(x), v(x) \in \mathbb{k}[x]$ be the Mumford representation of a semi-reduced divisor $D = \operatorname{div}(u(x), y - v(x)) \cap \mathbb{A}^2$ and $n \in \mathbb{Z}$. Then $\operatorname{div}(u(x), v(x), n)$ denotes the degree zero divisor

$$D + n(\infty^+) + (g - \deg(u(x)) - n)(\infty^-) - D_\infty.$$

If $0 \leq \deg(u(x)) \leq g$ and $0 \leq n \leq g - \deg(u(x))$ then such a divisor is called **reduced**.

Uniqueness of this representation is shown in Theorem 10.4.19. When g is odd then one could also represent divisor classes using $D_\infty = (g+1)/2((\infty^+) + (\infty^-))$. This is applicable in the inert case too. A problem is that this would lead to polynomials of higher degree than necessary in the Mumford representation, and divisor class representatives would no longer necessarily be unique.

It is important to realise that $u(x)$ and $v(x)$ are only used to specify the affine divisor. The values of $v_{\infty^+}(y - v(x))$ and $v_{\infty^-}(y - v(x))$ have no direct influence over the degree zero divisor under consideration. Note also that we allow $n \in \mathbb{Z}$ in Definition 10.4.9 in general, but reduced divisors must have $n \in \mathbb{Z}_{\geq 0}$.

For hyperelliptic curves with split model, $\infty^+, \infty^- \in \mathbb{k}$ and so a divisor $(u(x), v(x), n)$ is defined over $\mathbb{k}$ if and only if $u(x), v(x) \in \mathbb{k}[x]$. Note that when the genus is even then D_∞ is $\mathbb{k}$-rational even when the model is inert, though in this case a divisor $(u(x), v(x), n)$ with $n \neq 0$ is not defined over $\mathbb{k}$ if $u(x), v(x) \in \mathbb{k}[x]$.

We may now consider Cantor's addition algorithm in this setting.

Lemma 10.4.10 *Let C be a hyperelliptic curve over $\mathbb{k}$ of genus g with split model. Let* $\operatorname{div}(u_1(x), v_1(x), n_1)$ *and* $\operatorname{div}(u_2(x), v_2(x), n_2)$ *be degree zero divisors as above. Write* $D_i = \operatorname{div}(u_i(x), y - v_i(x)) \cap \mathbb{A}^2$ *for $i = 1, 2$ and let* $D_3 = \operatorname{div}(u_3(x), y - v_3(x)) \cap \mathbb{A}^2$ *be the semi-reduced divisor equivalent to $D_1 + D_2$, and $s(x)$ such that $D_1 + D_2 = D_3 +$*

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

$\mathrm{div}(s(x)) \cap \mathbb{A}^2$. *Let* $m = g/2$ *when* g *is even and* $m = (g+1)/2$ *otherwise. Then*

$$\mathrm{div}(u_1, v_1, n_1) + \mathrm{div}(u_2, v_2, n_2) \equiv \mathrm{div}(u_3, v_3, n_1 + n_2 + \deg(s) - m). \tag{10.14}$$

Proof We will show that

$$\mathrm{div}(u_1, v_1, n_1) + \mathrm{div}(u_2, v_2, n_2) = \mathrm{div}(u_3, v_3, n_1 + n_2 + \deg(s) - m) \ + \ \mathrm{div}(s(x)).$$

The left-hand side is

$$\begin{aligned} &D_1 + D_2 + (n_1 + n_2 - m)(\infty^+) + (3m - \deg(u_1) - \deg(u_2) \\ &\quad - n_1 - n_2)(\infty^-) \ - \ D_\infty. \end{aligned} \tag{10.15}$$

Replacing $D_1 + D_2$ by $D_3 + \mathrm{div}(s(x)) \cap \mathbb{A}^2$ has no effect on the coefficients of ∞^+ or ∞^-, but since we actually need $\mathrm{div}(s(x))$ on the whole of C we have $D_1 + D_2 = D_3 + \mathrm{div}(s(x)) + \deg(s(x))((\infty^+) + (\infty^-))$. Writing $\mathrm{div}(u_3, v_3, n_3) = \mathrm{div}(u_3, y - v_3) \cap \mathbb{A}^2 + n_3(\infty^+) + (g - \deg(u_3) - n_3)(\infty^-) - D_\infty$ gives $n_3 = n_1 + n_2 + \deg(s(x)) - m$ as required.

Note that $\deg(u_3) + \deg(s) = \deg(u_1) + \deg(u_2)$, so the coefficient of ∞^- in equation (10.15) is also correct (as it must be). □

We now discuss reduction of divisors on a hyperelliptic curve with a split model. We first consider the basic Cantor reduction step. There are two relevant cases for split models (namely, the first and third cases in Lemma 10.3.20) that we handle as Lemma 10.4.11 and Exercise 10.4.12.

Lemma 10.4.11 *Let* $C : y^2 + H(x)y = F(x)$ *where* $\deg(F(x)) = 2d = 2g + 2$ *be a hyperelliptic curve over* $\mathbb{k}$ *of genus* g *with split model. Let* $\mathrm{div}(u(x), v(x), n)$ *be a degree zero divisor as in Definition 10.4.9. Let* $(u^\dagger(x), v^\dagger(x))$ *be the polynomials arising from a Cantor reduction step (i.e.,* $u^\dagger(x)$ *and* $v^\dagger(x)$ *are given by equation (10.10)). If* $\deg(v(x)) \geq d = g + 1$ *then set* $n^\dagger = n + \deg(v(x)) - \deg(u^\dagger(x)) = n + (\deg(u(x)) - \deg(u^\dagger(x)))/2$ *and if* $\deg(v(x)) < g + 1 < \deg(u(x))$ *then set* $n^\dagger = n + g + 1 - \deg(u^\dagger(x))$. *Then*

$$\mathrm{div}(u, v, n) = \mathrm{div}(u^\dagger, v^\dagger, n^\dagger) + \mathrm{div}(y - v(x)) - \mathrm{div}(u^\dagger(x)) \tag{10.16}$$

and $\mathrm{div}(u, v, n) \equiv \mathrm{div}(u^\dagger, v^\dagger, n^\dagger)$.

Proof If $\deg(v(x)) \geq d$ then $\deg(u(x)) + \deg(u^\dagger(x)) = 2\deg(v(x))$ and $v_{\infty^+}(y - v(x)) = v_{\infty^-}(y - v(x)) = -\deg(v(x))$. For equation (10.16) to be satisfied we require

$$n = n^\dagger + v_{\infty^+}(y - v(x)) - v_{\infty^+}(u^\dagger(x))$$

and the formula for $n^\dagger$ follows (the coefficients of ∞^- must also be correct, as the divisors all have degree zero).

In the second case of reduction, we have $\deg(v(x)) < d < \deg(u(x))$ and hence $\deg(u(x)) + \deg(u^\dagger(x)) = 2d$ and $v_{\infty^+}(y - v(x)) = v_{\infty^-}(y - v(x)) = -d$. The formula for $n^\dagger$ follows as in the first case. □

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

Exercise 10.4.12 Let $C : y^2 + H(x)y = F(x)$ where $\deg(F(x)) < 2d = 2g + 2$ be a hyperelliptic curve over $\mathbb{k}$ of genus g with split model. Let $\mathrm{div}(u(x), v(x), n)$ be a degree zero divisor as in Definition 10.4.9 such that $d \leq \deg(u(x))$. Let $(u^\dagger(x), v^\dagger(x))$ be the polynomials arising from a Cantor reduction step. Show that $\mathrm{div}(u, v, n) \equiv \mathrm{div}(u^\dagger, v^\dagger, n^\dagger)$ where if $\deg(v(x)) < d$ then $n^\dagger = n + g + 1 - \deg(u^\dagger(x))$ and if $\deg(v(x)) \geq d$ then $n^\dagger = n + \deg(v(x)) - \deg(u^\dagger(x))$.

Example 10.4.13 Let $C : y^2 = x^6 + 3$ over $\mathbb{F}_7$. Let $D_1 = \mathrm{div}((x-1)(x-2), 2, 0) = (1, 2) + (2, 2) - D_\infty$ and $D_2 = \mathrm{div}((x-3)(x-4), 2, 0) = (3, 2) + (4, 2) - D_\infty$. Cantor addition gives $D_1 + D_2 = D_3 = \mathrm{div}((x-1)(x-2)(x-3)(x-4), 2, -1)$, which is not a reduced divisor. Applying Cantor reduction to D_3 results in $u^\dagger(x) = (x-5)(x-6)$ and $v^\dagger(x) = -2$ and $n^\dagger = n_3 + (g+1) - \deg(u^\dagger(x)) = -1 + 3 - 2 = 0$. Hence, we have $D_3 \equiv \mathrm{div}((x-5)(x-6), -2, 0)$, which is a reduced divisor.

We now explain the behaviour of a composition at infinity and reduction step.

Lemma 10.4.14 *Let $C : y^2 + H(x)y = F(x)$ where $\deg(F(x)) = 2d = 2g + 2$ be a hyperelliptic curve over $\mathbb{k}$ of genus g with split model. Let $\mathrm{div}(u(x), v(x), n)$ be a degree zero divisor as in Definition 10.4.9 such that $1 \leq \deg(u(x)) \leq g + 1$. Let $v^\ddagger(x)$, $u^\dagger(x)$ and $v^\dagger(x)$ be as in Lemma 10.4.6. Let $n^\dagger = n + \deg(u(x)) - (g+1)$ and $D^\dagger = \mathrm{div}(u^\dagger(x), v^\dagger(x), n^\dagger)$. Then*

$$D = D^\dagger + \mathrm{div}(y - v^\ddagger(x)) - \mathrm{div}(u^\dagger(x)).$$

If one uses $G^-(x)$ in Lemma 10.4.6 then $n^\dagger = n + g + 1 - \deg(u^\dagger(x))$.

It follows that if $\deg(u(x)) = g + 1$ then $\mathrm{div}(u, y - v) \cap \mathbb{A}^2 \equiv \mathrm{div}(u^\dagger, y - v^\dagger) \cap \mathbb{A}^2$ and there is no adjustment at infinity (the point of the operation in this case is to lower the degree from $\deg(u(x)) = g + 1$ to $\deg(u^\dagger(x)) \leq g$). But if, for example, $\deg(u(x)) = \deg(u^\dagger(x)) = g$ then we have

$$\mathrm{div}(u, y - v) \cap \mathbb{A}^2 - D_\infty \equiv \mathrm{div}(u^\dagger, y - v^\dagger) \cap \mathbb{A}^2 + (\infty^+) - (\infty^-) - D_\infty \qquad (10.17)$$

and so the operation corresponds to addition of D with the degree zero divisor $(\infty^-) - (\infty^+)$. This justifies the name "composition at infinity". To add $(\infty^+) - (\infty^-)$ one should use $G^-(x)$ instead of $G^+(x)$ in Lemma 10.4.6.

Exercise 10.4.15 Prove Lemma 10.4.14.

We can finally put everything together and obtain the main result about reduced divisors on hyperelliptic curves with split model.

Theorem 10.4.16 *Let C be a hyperelliptic curve over $\mathbb{k}$ of genus g with split model. Then every divisor class contains a reduced divisor as in Definition 10.4.9.*

Proof We have shown the existence of a divisor in the divisor class with semi-reduced affine part, and hence of the form $(u(x), v(x), n)$ with $n \in \mathbb{Z}$. Cantor reduction and composition and reduction at infinity show that we can assume $\deg(u(x)) \leq g$. Finally, to show that one

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

may assume $0 \leq n \leq g - \deg(u(x))$ note that Lemma 10.4.14 maps n to $n^\dagger = n + (g + 1) - \deg(u(x))$. Hence, if $n > g - \deg(u(x))$ then $n > n^\dagger \geq 0$ and continuing the process gives a reduced divisor. On the other hand, if $n < 0$ then using $G^-(x)$ instead one has $n^\dagger = n + g + 1 - \deg(u^\dagger(x)) \leq g - \deg(u^\dagger(x))$. □

Exercise 10.4.17 Let $C : y^2 + H(x)y = F(x)$ be a hyperelliptic curve of genus g over $\mathbb{F}_q$ with split model. If g is even, show that the inverse of $\operatorname{div}(u(x), v(x), n)$ is $\operatorname{div}(u(x), -v(x) - (H(x) \pmod{u(x)}), g - \deg(u(x)) - n)$. If g is odd then show that computing the inverse of a divisor may require performing composition and reduction at infinity.

Example 10.4.18 Let $C : y^2 = x^6 + x + 1$ over $\mathbb{F}_{37}$. Then $d = 3$ and $G^+(x) = x^3$. Let $D = (1, 22) + (2, 17) + (\infty^+) - (\infty^-) - D_\infty$, which is represented as $\operatorname{div}(u(x), v(x), 1)$ where $u(x) = (x - 1)(x - 2) = x^2 + 34x + 2$ and $v(x) = 32x + 27$. This divisor is not reduced. Then $v^\ddagger(x) = x^3 + 25x + 33$ and $\deg(v^\ddagger(x)^2 - F(x)) = 4$. Indeed, $v^\ddagger(x)^2 - F(x) = 13u(x)u^\dagger(x)$ where $u^\dagger(x) = x^2 + 28x + 2$. It follows that $v^\dagger(x) = 7x + 22$ and that

$$\operatorname{div}(u(x), v(x), 1) \equiv \operatorname{div}(u^\dagger(x), v^\dagger(x), 0),$$

which is reduced.

Explicit formulae for all these operations for genus 2 curves of the form $y^2 = x^6 + F_4x^4 + F_3x^3 + F_2x^2 + F_1x + F_0$ have been given by Erickson, Jacobson, Shang, Shen and Stein [184].

Uniqueness of the representation

We have shown that every divisor class for hyperelliptic curves with a split model contains a reduced divisor. We now discuss the uniqueness of this reduced divisor, following Paulus and Rück [429].

Theorem 10.4.19 *Let C be a hyperelliptic curve over $\mathbb{k}$ of genus g with split model. Then every divisor class has a unique representative of the form*

$$D + n(\infty^+) + (g - \deg(D) - n)(\infty^-) - D_\infty$$

where D is a semi-reduced divisor (hence, affine and effective) and $0 \leq n \leq g - \deg(D)$.

Proof Existence has already been proved using the reduction algorithms above, so it suffices to prove uniqueness. Hence, suppose

$$\begin{aligned} &D_1 + n_1(\infty^+) + (g - \deg(D_1) - n_1)(\infty^-) - D_\infty \\ &\quad \equiv D_2 + n_2(\infty^+) + (g - \deg(D_2) - n_2)(\infty^-) - D_\infty \end{aligned}$$

with all terms satisfying the conditions of the theorem. Then, taking the difference and adding $\operatorname{div}(u_2(x)) = D_2 + \iota(D_2) - \deg(D_2)((\infty^+) + (\infty^-))$, there is a function $f(x, y)$

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

such that

$$\operatorname{div}(f(x,y)) = D_1 + \iota(D_2) - (n_2 + \deg(D_2) - n_1)(\infty^+) - (n_1 + \deg(D_1) - n_2)(\infty^-).$$

Since $f(x,y)$ has poles only at infinity it follows that $f(x,y) = a(x) + yb(x)$ where $a(x), b(x) \in \mathbb{k}[x]$. Now, $0 \leq n_i \leq n_i + \deg(D_i) \leq g$ and so $-g \leq v_{\infty^+}(f(x,y)) = -(n_2 + \deg(D_2) - n_1) \leq g$ and $-g \leq v_{\infty^-}(f(x,y)) = -(n_1 + \deg(D_1) - n_2) \leq g$. But $v_{\infty^+}(y) = v_{\infty^-}(y) = -(g+1)$ and so $b(x) = 0$ and $f(x,y) = a(x)$. But $\operatorname{div}(a(x)) = D + \iota(D) - \deg(a(x))((\infty^+) + (\infty^-))$ and so $D_1 = D_2$, $n_1 + \deg(D_1) - n_2 = n_2 + \deg(D_2) - n_1$ and $n_1 = n_2$. □

Exercise 10.4.20 Let C be a hyperelliptic curve over $\mathbb{k}$ of genus $g = d - 1$ with split model. Show that $(\infty^+) - (\infty^-)$ is not a principal divisor and that this divisor is represented as $(1, 0, \lceil g/2 \rceil + 1)$.

10.5 Jacobians, Abelian varieties and isogenies

As mentioned in Section 7.8, we can consider $\operatorname{Pic}^0_{\mathbb{k}}(C)$ as an algebraic group, by considering the **Jacobian variety** J_C of the curve. The fact that the divisor class group is an algebraic group is not immediate from our description of the group operation as an algorithm (rather than a formula).

Indeed, J_C is an Abelian variety (namely, a projective algebraic group). The dimension of the variety J_C is equal to the genus of C. Unfortunately, we do not have space to introduce the theory of Abelian varieties and Jacobians in this book. We remark that the Mumford representation directly gives an affine part of the Jacobian variety of a hyperelliptic curve (see Propositions 1.2 and 1.3 of Mumford [399] for the details).

An explicit description of the Jacobian variety of a curve of genus 2 has been given by Flynn; we refer to Chapter 2 of Cassels and Flynn [115] for details, references and further discussion.

There are several important concepts in the theory of Abelian varieties that are not able to be expressed in terms of divisor class groups.[3] Hence, our treatment of hyperelliptic curves will not be as extensive as the case of elliptic curves. In particular, we do not give a rigorous discussion of isogenies (i.e., morphisms of varieties that are group homomorphisms with finite kernel) for Abelian varieties of dimension $g > 1$. However, we do mention one important result. The Poincaré reducibility theorem (see Theorem 1 of Section 19 (page 173) of Mumford [398]) states that if A is an Abelian variety over $\mathbb{k}$ and B is an Abelian subvariety of A (i.e., B is a subset of A that is an Abelian variety over $\mathbb{k}$) then there is an Abelian subvariety $B' \subseteq A$ over $\mathbb{k}$ such that $B \cap B'$ is finite and $B + B' = A$. It follows that A is isogenous over $\mathbb{k}$ to $B \times B'$. If an Abelian variety A over $\mathbb{k}$ has no Abelian subvarieties over $\mathbb{k}$ then we call it **simple**. An Abelian variety is **absolutely simple** if is has no Abelian subvarieties over $\overline{\mathbb{k}}$.

[3] There are two reasons for this: first, the divisor class group is merely an abstract group and so does not have the geometric structure necessary for some of these concepts; second, not every Abelian variety is a Jacobian variety.

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

Despite not discussing isogenies in full generality, it is possible to discuss isogenies that arise from maps between curves purely in terms of divisor class groups. We now give some examples, but first introduce a natural notation.

Definition 10.5.1 Let C be a curve over a field $\mathbb{k}$ and let $n \in \mathbb{N}$. For $D \in \mathrm{Pic}^0_{\mathbb{k}}(C)$ define

$$[n]D = D + \cdots + D \quad (n \text{ times}).$$

Indeed, we usually assume that $[n]D$ is a reduced divisor representing the divisor class nD. Define

$$\mathrm{Pic}^0_{\mathbb{k}}(C)[n] = \{D \in \mathrm{Pic}^0_{\mathbb{k}}(C) : [n]D = 0\}.$$

Recall from Corollary 8.3.10 that if $\phi : C_1 \to C_2$ is a non-constant rational map (and hence a non-constant morphism) over $\mathbb{k}$ between two curves then there are corresponding group homomorphisms $\phi^* : \mathrm{Pic}^0_{\mathbb{k}}(C_2) \to \mathrm{Pic}^0_{\mathbb{k}}(C_1)$ and $\phi_* : \mathrm{Pic}^0_{\mathbb{k}}(C_1) \to \mathrm{Pic}^0_{\mathbb{k}}(C_2)$. Furthermore, by part 5 of Theorem 8.3.8 we have $\phi_*\phi^*(D) = [\deg(\phi)]D$ on $\mathrm{Pic}^0_{\mathbb{k}}(C_2)$.

In the special case of a non-constant rational map $\phi : C \to E$ over $\mathbb{k}$ where E is an elliptic curve we can compose with the Abel–Jacobi map $E \to \mathrm{Pic}^0_{\mathbb{k}}(E)$ of Theorem 7.9.8 given by $P \mapsto (P) - (\mathcal{O}_E)$ to obtain group homomorphisms that we call $\phi^* : E \to \mathrm{Pic}^0_{\mathbb{k}}(C)$ and $\phi_* : \mathrm{Pic}^0_{\mathbb{k}}(C) \to E$.

Exercise 10.5.2 Let $\phi : C \to E$ be a non-constant rational map over $\mathbb{k}$ where E is an elliptic curve over $\mathbb{k}$. Let $\phi^* : E \to \mathrm{Pic}^0_{\mathbb{k}}(C)$ and $\phi_* : \mathrm{Pic}^0_{\mathbb{k}}(C) \to E$ be the group homomorphisms as above. Show that ϕ_* is surjective as a map from $\mathrm{Pic}^0_{\overline{\mathbb{k}}}(C)$ to $E(\overline{\mathbb{k}})$ and that the kernel of ϕ^* is contained in $E[\deg(\phi)]$.

If C is a curve of genus 2 and there are two non-constant rational maps $\phi_i : C \to E_i$ over $\overline{\mathbb{k}}$ for elliptic curves E_1, E_2 then one naturally has a group homomorphism $\phi_{1,*} \times \phi_{2,*} : \mathrm{Pic}^0_{\overline{\mathbb{k}}}(C) \to E_1(\overline{\mathbb{k}}) \times E_2(\overline{\mathbb{k}})$. If $\ker(\phi_{1,*}) \cap \ker(\phi_{2,*})$ is finite then it follows from the theory of Abelian varieties that the Jacobian variety J_C is isogenous to the product $E_1 \times E_2$ of the elliptic curves and one says that J_C is a **split Jacobian**.

Example 10.5.3 Let $C : y^2 = x^6 + 2x^2 + 1$ be a genus 2 curve over $\mathbb{F}_{11}$. Consider the rational maps

$$\phi_1 : C \to E_1 : Y^2 = X^3 + 2X + 1$$

given by $\phi_1(x, y) = (x^2, y)$ and

$$\phi_2 : C \to E_2 : Y^2 = X^3 + 2X^2 + 1$$

given by $\phi_2(x, y) = (1/x^2, y/x^3)$. The two elliptic curves E_1 and E_2 are neither isomorphic or isogenous. One has $\#E_1(\mathbb{F}_{11}) = 16$, $\#E_2(\mathbb{F}_{11}) = 14$ and $\#\mathrm{Pic}^0_{\mathbb{F}_{11}}(C) = 14 \cdot 16$.

It can be shown (this is not trivial) that $\ker(\phi_{1,*}) \cap \ker(\phi_{2,*})$ is finite. Further, since $\deg(\phi_1) = \deg(\phi_2) = 2$ it can be shown that the kernel of $\phi_{1,*} \times \phi_{2,*}$ is contained in $\mathrm{Pic}^0_{\overline{\mathbb{k}}}(C)[2]$.

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

The Jacobian of a curve satisfies the following universal property. Let $\phi : C \to A$ be a morphism where A is an Abelian variety. Let $P_0 \in C(\overline{\mathbb{k}})$ be such that $\phi(P_0) = 0$ and consider the Abel–Jacobi map $\psi : C \to J_C$ (corresponding to $P \mapsto (P) - (P_0)$). Then there is a homomorphism of Abelian varieties $\phi' : J_C \to A$ such that $\phi = \phi' \circ \psi$. Exercise 10.5.4 gives a special case of this universal property.

Exercise 10.5.4 Let $C : y^2 = x^6 + a_2x^4 + a_4x^2 + a_6$ over $\mathbb{k}$ where $\mathrm{char}(\mathbb{k}) \neq 2$, and let $\phi(x, y) = (x^2, y)$ be non-constant rational map $\phi : C \to E$ over $\mathbb{k}$ where E is an elliptic curve. Let $P_0 \in C(\overline{\mathbb{k}})$ be such that $\phi(P_0) = \mathcal{O}_E$. Show that the composition

$$C(\overline{\mathbb{k}}) \to \mathrm{Pic}^0_{\overline{\mathbb{k}}}(C) \to E(\overline{\mathbb{k}})$$

where the first map is the Abel–Jacobi map $P \mapsto (P) - (P_0)$ and the second map, ϕ_*, is just the original map ϕ.

There is a vast literature on split Jacobians and we are unable to give a full survey. We refer to Sections 4, 5 and 6 of Kuhn [321] or Chapter 14 of Cassels and Flynn [115] for further examples.

10.6 Elements of order n

We now bound the size of the set of elements of order dividing n in the divisor class group of a curve. As with many other results in this chapter, the best approach is via the theory of Abelian varieties. We state Theorem 10.6.1 for general curves, but without proof. The result is immediate for Abelian varieties over $\mathbb{C}$, as they are isomorphic to $\mathbb{C}^g/L$ where L is a rank $2g$ lattice. The elements of order n in $\mathbb{C}^g/L$ are given by the n^{2g} points in $\frac{1}{n}L/L$.

Theorem 10.6.1 *Let C be a curve of genus g over $\mathbb{k}$ and let $n \in \mathbb{N}$. If* $\mathrm{char}(\mathbb{k}) = 0$ *or* $\gcd(n, \mathrm{char}(\mathbb{k})) = 1$ *then* $\#\mathrm{Pic}^0_{\overline{\mathbb{k}}}(C)[n] = n^{2g}$. *If* $\mathrm{char}(\mathbb{k}) = p > 0$ *then* $\#\mathrm{Pic}^0_{\overline{\mathbb{k}}}(C)[p] = p^e$ *where* $0 \leq e \leq g$.

Proof See Theorem 4 of Section 7 of Mumford [398]. □

10.7 Hyperelliptic curves over finite fields

There are a finite number of points on a curve C of genus g over a finite field $\mathbb{F}_q$. There are also finitely many possible values for the Mumford representation of a reduced divisor on a hyperelliptic curve over a finite field. Hence, the divisor class group $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$ of a curve over a finite field is a finite group. Since the affine part of a reduced divisor is a sum of at most g points (possibly defined over a field extension of degree bounded by g) it is not surprising that there is a connection between $\{\#C(\mathbb{F}_{q^i}) : 1 \leq i \leq g\}$ and $\#\mathrm{Pic}^0_{\mathbb{F}_q}(C)$. Indeed, there is also a connection between $\{\#\mathrm{Pic}^0_{\mathbb{F}_{q^i}}(C) : 1 \leq i \leq g\}$ and $\#C(\mathbb{F}_q)$. The aim of this section is to describe these connections. We also give some important bounds on these

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

numbers (analogous to the Hasse bound for elliptic curves). Most results are presented for general curves (i.e., not only hyperelliptic curves).

One of the most important results in the theory of curves over finite fields is the following theorem of Hasse and Weil. The condition that the roots of $L(t)$ have absolute value $\sqrt{q}$ can be interpreted as an analogue of the Riemann hypothesis. This result gives precise bounds on the number of points on curves and divisor class groups over finite fields.

Theorem 10.7.1 *(Hasse–Weil) Let C be a curve of genus g over $\mathbb{F}_q$. There exists a polynomial $L(t) \in \mathbb{Z}[t]$ of degree $2g$ with the following properties:*

1. $L(1) = \#\mathrm{Pic}^0_{\mathbb{F}_q}(C)$.
2. *One can write $L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$ with $\alpha_i \in \mathbb{C}$ such that $\alpha_{g+i} = \overline{\alpha_i}$ (this is complex conjugation) and $|\alpha_i| = \sqrt{q}$ for $1 \leq i \leq g$.*
3. *$L(t) = q^g t^{2g} L(1/(qt))$ and so*
$$L(t) = 1 + a_1 t + \cdots + a_{g-1}t^{g-1} + a_g t^g + q a_{g-1} t^{g+1} + \cdots + q^{g-1} a_1 t^{2g-1} + q^g t^{2g}.$$
4. *For $n \in \mathbb{N}$ define $L_n(t) = \prod_{i=1}^{2g}(1 - \alpha_i^n t)$. Then $\#\mathrm{Pic}^0_{\mathbb{F}_{q^n}}(C) = L_n(1)$.*

Proof The polynomial $L(t)$ is the numerator of the zeta function of C. For details see Section V.1 of Stichtenoth [529], especially Theorem V.1.15. The proof that $|\alpha_i| = \sqrt{q}$ for all $1 \leq i \leq 2g$ is Theorem V.2.1 of Stichtenoth [529].

A proof of some parts of this result in a special case is given in Exercise 10.7.14. □

Exercise 10.7.2 Show that part 3 of Theorem 10.7.1 follows immediately from part 2.

Definition 10.7.3 The polynomial $L(t)$ of Theorem 10.7.1 is called the **L-polynomial** of the curve C over $\mathbb{F}_q$.

Theorem 10.7.4 *(Schmidt) Let C be a curve of genus g over $\mathbb{F}_q$. There there exists a divisor D on C of degree 1 that is defined over $\mathbb{F}_q$.*

We stress that this result does not prove that C has a point defined over $\mathbb{F}_q$ (though when q is large compared with the genus, existence of a point in $C(\mathbb{F}_q)$ will follow by the Weil bounds). The result implies that even a curve with no points defined over $\mathbb{F}_q$ does have a divisor of degree 1 (hence, not an effective divisor) that is defined over $\mathbb{F}_q$.

Proof See Corollary V.1.11 of Stichtenoth [529]. □

We now describe the precise connection between the roots α_i of the polynomial $L(t)$ (corresponding to $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$) and $\#C(\mathbb{F}_{q^n})$ for $n \in \mathbb{N}$.

Theorem 10.7.5 *Let C be a curve of genus g over $\mathbb{F}_q$ and let $\alpha_i \in \mathbb{C}$ for $1 \leq i \leq 2g$ be as in Theorem 10.7.1. Let $n \in \mathbb{N}$. Then*

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n. \tag{10.18}$$

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

Proof See Corollary V.1.16 of Stichtenoth [529]. □

Equation (10.18) can be read in two ways. On the one hand, it shows that given $L(t)$ one can determine $\#C(\mathbb{F}_{q^n})$. On the other hand, it shows that if one knows $\#C(\mathbb{F}_{q^n})$ for $1 \leq n \leq g$ then one has g non-linear equations in the g variables $\alpha_1, \ldots, \alpha_g$ (there are only g variables since $\alpha_{i+g} = q/\alpha_i$ for $1 \leq i \leq g$). The following result shows that one can therefore deduce the coefficients $a_1, \ldots, a_g$ giving the polynomial $L(t)$.

Lemma 10.7.6 *(Newton's identities) Let $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ and define $t_n = \sum_{i=1}^{2g} \alpha_i^n$. Let $a_1, \ldots, a_{2g}$ be such that $\prod_{i=1}^{2g}(x - \alpha_i) = x^{2g} + a_1 x^{2g-1} + \cdots + a_{2g}$. Then, for $1 \leq n \leq 2g$,*

$$na_n = -t_n - \sum_{i=1}^{n-1} a_{n-i} t_i.$$

In particular, $a_1 = -t_1$ and $a_2 = (t_1^2 - t_2)/2$.

Exercise 10.7.7★ Prove Lemma 10.7.6.

Exercise 10.7.8 Suppose C is a genus 3 curve over $\mathbb{F}_7$ such that $\#C(\mathbb{F}_7) = 8$, $\#C(\mathbb{F}_{7^2}) = 92$, $\#C(\mathbb{F}_{7^3}) = 344$. Determine $L(t)$ and hence $\#\mathrm{Pic}^0_{\mathbb{F}_7}(C)$. (One can take $y^2 = x^7 + x + 1$ for C.)

Exercise 10.7.9 (**Weil bounds**) Let C be a curve of genus g over $\mathbb{F}_q$. Use Theorem 10.7.1 and Theorem 10.7.5 to show that

$$|\#C(\mathbb{F}_{q^n}) - (q^n + 1)| \leq 2g\sqrt{q^n}$$

and

$$(\sqrt{q^n} - 1)^{2g} \leq \#\mathrm{Pic}^0_{\mathbb{F}_{q^n}}(C) \leq (\sqrt{q^n} + 1)^{2g}.$$

More precise bounds on $\#C(\mathbb{F}_q)$ are known; we refer to Section V.3 of Stichtenoth [529] for discussion and references.

Consider the q-power Frobenius map $\pi : C \to C$ given by $\pi(x, y) = (x^q, y^q)$. This map induces a morphism $\pi : J_C \to J_C$ (indeed, an isogeny of Abelian varieties) where J_C is the Jacobian variety of C. By considering the action of π on the Tate module (the Tate module of an Abelian variety is defined in the analogous way to elliptic curves, see Section 19 of Mumford [398]) it can be shown that π satisfies a characteristic equation given by a monic polynomial $P(T) \in \mathbb{Z}[T]$ of degree $2g$. It can further be shown that $P(T) = T^{2g} L(1/T)$ (we refer to Section 21 of [398], especially the subsection entitled "Application II: The Riemann Hypothesis").

Definition 10.7.10 Let C be a curve over $\mathbb{F}_q$. The **characteristic polynomial of Frobenius** is the polynomial $P(T) = T^{2g} L(1/T)$.

The Frobenius map $\pi : C \to C$ also induces the map $\pi_* : \mathrm{Pic}^0_{\mathbb{F}_q}(C) \to \mathrm{Pic}^0_{\mathbb{F}_q}(C)$, and we abuse notation by calling it π as well. If D is any divisor representing a divisor class in

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

$\mathrm{Pic}^0_{\overline{\mathbb{F}}_q}(C)$ then $P(\pi)D \equiv 0$. In other words, if $P(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_1 q^{g-1} T + q^g$ then

$$\pi^{2g}(D) + [a_1]\pi^{2g-1}(D) + \cdots + [a_1 q^{g-1}]\pi(D) + [q^g]D \equiv 0 \tag{10.19}$$

where the notation $[n]D$ is from Definition 10.5.1.

Exercise 10.7.11 Let C be a curve over $\mathbb{F}_q$ and D a reduced divisor on C over $\overline{\mathbb{F}}_q$ with Mumford representation $(u(x), v(x))$. Let π be the q-power Frobenius map on C. For a polynomial $u(x) = \sum_{i=0}^d u_i x^i$ define $u^{(q)}(x) = \sum_{i=0}^d u_i^q x^i$. Show that the Mumford representation of $\pi_*(D)$ is $(u^{(q)}(x), v^{(q)}(x))$.

Example 10.7.12 (Koblitz [298]) Let $a \in \{0, 1\}$ and consider the genus 2 curve $C_a : y^2 + xy = x^5 + ax^2 + 1$ over $\mathbb{F}_2$. One can verify that $\#C_0(\mathbb{F}_2) = 4$, $\#C_1(\mathbb{F}_2) = 2$ and $\#C_0(\mathbb{F}_{2^2}) = \#C_1(\mathbb{F}_{2^2}) = 4$. Hence, the characteristic polynomial of Frobenius is $P(T) = T^4 + (-1)^a T^3 + 2(-1)^a T + 4$. One can determine $\#\mathrm{Pic}^0_{\mathbb{F}_{2^n}}(C_a)$ for any $n \in \mathbb{N}$. If n is composite and $m \mid n$ one has $\#\mathrm{Pic}^0_{\mathbb{F}_{2^m}}(C_a) \mid \#\mathrm{Pic}^0_{\mathbb{F}_{2^n}}(C_a)$. For cryptographic applications one would like $\#\mathrm{Pic}^0_{\mathbb{F}_{2^n}}(C_a)/\#\mathrm{Pic}^0_{\mathbb{F}_2}(C_a)$ to be prime, so restrict attention to primes values for n. For example, taking $n = 113$ and $a = 1$ gives group order $2 \cdot r$ where $r = 539 \cdots 381$ is a 225-bit prime.

If $D \in \mathrm{Pic}^0_{\mathbb{F}_{2^n}}(C_1)$ then $\pi^4(D) - \pi^3(D) - [2]\pi(D) + [4]D \equiv 0$ where π is the map induced on $\mathrm{Pic}^0_{\mathbb{F}_{2^n}}(C_1)$ from the 2-power Frobenius map $\pi(x, y) = (x^2, y^2)$ on C.

A major result, whose proof is beyond the scope of this book, is Tate's isogeny theorem.

Theorem 10.7.13 *(Tate) Let A and B be Abelian varieties over a field $\mathbb{F}_q$. Then A is $\mathbb{F}_q$-isogenous to B if and only if $P_A(T) = P_B(T)$. Similarly, A is $\mathbb{F}_q$-isogenous to an Abelian subvariety of B if and only if $P_A(T) \mid P_B(T)$.*

Proof See [540]. □

Exercise 10.7.14 gives a direct proof of Theorems 10.7.1 and 10.7.5 for genus 2 curves with ramified model.

Exercise 10.7.14 ★ Let q be an odd prime power. Let $F(x) \in \mathbb{F}_q[x]$ be square-free and of degree 5. Then $C : y^2 = F(x)$ is a hyperelliptic curve over $\mathbb{F}_q$ of genus 2 with a ramified model. For $n = 1, 2$ let $N_n = \#C(\mathbb{F}_{q^n})$ and define $t_n = q^n + 1 - N_n$ so that $N_n = q^n + 1 - t_n$. Define $a_1 = -t_1$ and $a_2 = (t_1^2 - t_2)/2$. Show, using direct calculation and Exercise 10.4.4, that $\mathrm{Pic}^0_{\overline{\mathbb{F}}_q}(C)$ has order $q^2 + a_1(q + 1) + a_2 + 1$.

10.8 Supersingular curves

Recall from Theorem 10.6.1 that if C is a curve of genus g over a field $\mathbb{k}$ of characteristic p then $\#\mathrm{Pic}^0_{\overline{\mathbb{k}}}(C)[p] \leq p^g$.

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

Definition 10.8.1 Let $\mathbb{k}$ be a field such that $\mathrm{char}(\mathbb{k}) = p > 0$ and let C be a curve of genus g over $\mathbb{k}$. The **p-rank** of C is the integer $0 \leq r \leq g$ such that $\#\mathrm{Pic}^0_{\mathbb{k}}(C)[p] = p^r$.

An Abelian variety of dimension g over $\mathbb{F}_q$ is defined to be **supersingular** if it is isogenous over $\overline{\mathbb{F}}_q$ to E^g where E is a supersingular elliptic curve over $\overline{\mathbb{F}}_q$. A curve C over $\mathbb{F}_q$ is **supersingular** if J_C is a supersingular Abelian variety. It follows that the p-rank of a supersingular Abelian variety over $\mathbb{F}_{p^n}$ is zero. The converse is not true (i.e., p-rank zero does not imply supersingular) when the dimension is 3 or more; see Example 10.8.8). If the p-rank of a dimension g Abelian variety A over $\mathbb{F}_{p^n}$ is g then A is said to be **ordinary**.

Lemma 10.8.2 *Suppose A is a supersingular Abelian variety over $\mathbb{F}_q$ and write $P_A(T)$ for the characteristic polynomial of Frobenius on A. The roots α of $P_A(T)$ are such that $\alpha/\sqrt{q}$ is a root of unity.*

Proof Since the isogeny to E^g is defined over some finite extension $\mathbb{F}_{q^n}$ it follows from part 4 of Theorem 9.11.2 that $\alpha^n/\sqrt{q^n}$ is a root of unity. Hence, $\alpha/\sqrt{q}$ is a root of unity. □

The converse of Lemma 10.8.2 follows from the Tate isogeny theorem.

Example 10.8.3 Let $C : y^2 + y = x^5$ over $\mathbb{F}_2$. One can check that $\#C(\mathbb{F}_2) = 3$ and $\#C(\mathbb{F}_{2^2}) = 5$ and so the characteristic polynomial of the 2-power Frobenius is $P(T) = T^4 + 4 = (T^2 + 2T + 2)(T^2 - 2T + 2)$. It follows from Theorem 10.7.13 (Tate's isogeny theorem) that J_C is isogenous to $E_1 \times E_2$ where E_1 and E_2 are supersingular curves over $\mathbb{F}_2$. The characteristic polynomial of the 2^2-power Frobenius can be shown to be $T^4 + 8T^2 + 16 = (T^2 + 4)^2$ and it follows that J_C is isogenous over $\mathbb{F}_{2^2}$ to the square of a supersingular elliptic curve. Hence, C is a supersingular curve.

Note that the endomorphism ring of J_C is non-commutative since the map $\phi(x, y) = (\zeta_5 x, y)$, where $\zeta_5 \in \mathbb{F}_{2^4}$ is a root of $z^4 + z^3 + z^2 + z + 1 = 0$, does not commute with the 2-power Frobenius map.

Exercise 10.8.4★ Show that if C is a supersingular curve over $\mathbb{F}_q$ of genus 2 then $\#\mathrm{Pic}^0_{\mathbb{F}_q}(C) \mid (q^k - 1)$ for some $1 \leq k \leq 12$.

The following result shows that computing the p-rank and determining supersingularity are easy when $P(T)$ is known.

Theorem 10.8.5 *Let A be an Abelian variety of dimension g over $\mathbb{F}_{p^n}$ with characteristic polynomial of Frobenius $P(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_g T^g + \cdots + p^{ng}$.*

1. *The p-rank of A is the smallest integer $0 \leq r \leq g$ such that $p \mid a_i$ for all $1 \leq i \leq g - r$. (In other words, the p-rank is zero if $p \mid a_i$ for all $1 \leq i \leq g$ and the p-rank is g if $p \nmid a_1$.)*
2. *A is supersingular if and only if*

$$p^{\lceil in/2 \rceil} \mid a_i \qquad \text{for all} \qquad 1 \leq i \leq g.$$

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

Proof Part 1 is Satz 1 of Stichtenoth [528]. Part 2 is Proposition 1 of Stichtenoth and Xing [530]. □

We refer to Yui [572] for a survey of the Cartier–Manin matrix and related criteria for the p-rank.

Exercise 10.8.6 Let A be an Abelian variety of dimension 2 over $\mathbb{F}_p$ that has p-rank zero. Show that A is supersingular.

In fact, the result of Exercise 10.8.6 holds when $\mathbb{F}_p$ is replaced by any finite field; see page 9 of Li and Oort [348].

Exercise 10.8.7 Let $C : y^2 + y = F(x)$ over $\mathbb{F}_{2^n}$ where $\deg(F(x)) = 5$ be a genus 2 hyperelliptic curve. Show that C has 2-rank zero (and hence is supersingular).

Example 10.8.8 shows that, once the genus is at least 3, p-rank zero does not imply supersingularity.

Example 10.8.8 Define $C : y^2 + y = x^7$ over $\mathbb{F}_2$. Then $P(T) = T^6 - 2T^3 + 2^3$ and so by Theorem 10.8.5 the 2-rank of C is zero but C is not supersingular.

Example 10.8.9 (Hasse/Hasse-Davenport/Duursma [171]) Let $p > 2$ be prime and $C : y^2 = x^p - x + 1$ over $\mathbb{F}_p$. One can verify that C is non-singular and the genus of C is $(p-1)/2$. It is shown in [171] that, over $\mathbb{F}_{p^2}$, $L(T) = \Phi_p((\frac{-1}{p})pT)$ where $\Phi_p(T)$ is the p-th cyclotomic polynomial. It follows that the roots of $P(T)$ are roots of unity and so C is supersingular.

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press

https://doi.org/10.1017/CBO9781139012843.011 Published online by Cambridge University Press