Arithmetic of Curves of Higher Genus

Samir Siksek

Samir Siksek, Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom

E-mail address: samirsiksek@yahoo.com

Abstract. These are my (partial) lecture notes for the course “Arithmetic of Curves of Higher Genus”. The course is heavily influenced by a course Bjorn Poonen gave at the *Institut Henri Poincaré* in 2004. I hope these notes will grow as the term progresses, but I do not promise that. Thanks to Owen Jones for many comments and corrections. Please send any misprints or comments to me at `samirsiksek@yahoo.com`.

CHAPTER I

Varieties

You have probably met algebraic geometry before, but over $\mathbb{C}$, or over an algebraically closed field. We would like to develop a little algebraic geometry over non-algebraically closed fields. Our reference for this are Chapters I and II of Silverman's book [**1**]. This is easier if we restrict to perfect fields; a field k is *perfect* if every algebraic extension of k is separable. Note that $\mathbb{Q}$, algebraic numbers fields, finite fields, and p-adic fields are all perfect, thus the restriction to perfect fields is not really severe for people who are interested in arithmetic.

Let k be a perfect field and $\overline{k}$ be a fixed algebraic closure of k.

1. Affine Varieties

$\mathbb{A}^n$ will denote "n-dimensional affine space". For any field $L \supseteq k$, $\mathbb{A}^n(L) := L^n$, that is the points in n-dimensional space with coordinates in L.

A (closed) affine variety over k is a subset V of $\mathbb{A}^n$ (for some n) cut out by a finite system of polynomial equations:

$$f_1(x_1, \dots, x_n) = 0,$$
$$\vdots$$
$$f_m(x_1, \dots, x_n) = 0,$$

with coefficients in k. Thus, for any field $L \supseteq k$,

$$V(L) := \{\mathbf{a} \in L^n \ : \ f_1(\mathbf{a}) = \cdots = f_m(\mathbf{a}) = 0\}.$$

Example I.1. You can think of Affine n-space as given by an empty set of equations in n-variables.

Example I.2. Define $\mathbb{R}$-varieties in $\mathbb{A}^2$:

$$X \ : \ x^2 + y^2 = 1,$$

and

$$Y \ : \ 1 = 0.$$

Note that $X(\mathbb{R}) = \emptyset = Y(\mathbb{R})$, but X is not the same as Y since

$$X(\mathbb{C}) \neq \emptyset = Y(\mathbb{C}).$$

Example I.3. $\mathrm{Gal}(\overline{k}/k)$ acts on $\overline{k}$ and so acts in a natural way on many objects associated with $\overline{k}$ (for example $\overline{k}^2$, $\overline{k}[x]$ and so on. If $\mathrm{Gal}(\overline{k}/k)$ acts on a set S, we write

$$H^0\left(\mathrm{Gal}(\overline{k}/k), S\right) := \left\{s \in S : \sigma(s) = s \text{ for all } \sigma \in \mathrm{Gal}(\overline{k}/k)\right\}.$$

This is merely the set of elements of S fixed by the action of $\mathrm{Gal}(\overline{k}/k)$. The elements fixed by $\mathrm{Gal}(\overline{k}/k)$ are called "k-rational". By Galois Theory,

$$H^0\left(\mathrm{Gal}(\overline{k}/k), \overline{k}\right) = k, \qquad H^0\left(\mathrm{Gal}(\overline{k}/k), \overline{k}^*\right) = k^*.$$

It is easy to see that the set of k-rational elements of $\mathbb{A}^n(\overline{k})$ is

$$H^0\left(\mathrm{Gal}(\overline{k}/k), \mathbb{A}^n(\overline{k})\right) = \mathbb{A}^n(k).$$

In these examples "k-rational" is consistent with what we would expect, though this is not always the case, as we will see later.

Example I.4. The adjective 'closed' in the definition of varieties means we are not throwing anything away. Consider the following two closed varieties defined over $\mathbb{Q}$:

$$X : x^2 + y^2 = 6, \qquad Y : x^2 = 2.$$

Here closed means we are taking **all** solutions of the given equations to get X and Y. An example of a non-closed variety is $X - Y$. Write $Z = X - Y$. The points of Z are the points of X that do not belong to Y. Note that for any $L \supseteq \mathbb{Q}$,

$$Z(L) = \begin{cases} X(L) & \text{if } \sqrt{2} \notin L \\ X(L) \backslash \{(\pm\sqrt{2}, \pm 2)\} & \text{if } \sqrt{2} \in L. \end{cases}$$

A very useful example of a non-closed subvariety of $\mathbb{A}^1$ is $\mathbb{G}_m := \mathbb{A}^1 \backslash \{x = 0\}$, thus $\mathbb{G}_m(k) = k^*$ (and we think of $\mathbb{G}_m$ as a 'group variety'; in other words, it is a variety and has an algebraic group operation on it—in this case multiplication).

The word closed has a topological meaning. For this look up the Zariski topology in any algebraic geometry text (this will take you 10 minutes to learn).

From now on, we will focus on closed varieties.

2. Ideals and Varieties

Given a variety $V \subset \mathbb{A}^n$ over k, we define the ideal

$$I(V) := \{f \in k[x_1, \ldots, x_n] : \ f(P) = 0 \text{ for all } P \in V(\overline{k})\}.$$

Given an ideal I of $k[x_1, \ldots, x_n]$, we can write $I = (f_1, \ldots, f_m)$ (that is, it has a finite set of generators $f_1, \ldots, f_m$). We define the corresponding (closed) variety $V(I)$ to be the k variety given by the system of polynomial equations $f_1 = \cdots = f_m = 0$. It should be easy to see that $V(I)$ depends on the ideal I and not on the generators chosen.

We obtain inclusion-reversing maps [1]:

$$\{\text{ideals of } k[x_1, \ldots, x_n]\} \overset{\twoheadrightarrow}{\hookleftarrow} \{\text{closed } k\text{-subvarieties of } \mathbb{A}^n\}$$

$$I \mapsto V(I)$$

$$V \mapsfrom I(V).$$

Note that $I(V(I)) = \sqrt{I}$ the radical of I, and $V(I(V)) = V$ (for closed varieties V). The above maps restrict to bijections:

$$\{\text{radical ideals of } k[x_1, \ldots, x_n]\} \longleftrightarrow \{\text{closed } k\text{-subvarieties of } \mathbb{A}^n\}$$

[1] $\twoheadrightarrow$ means surjection, and $\hookrightarrow$ means injection.

If V is a closed k-subvariety of $\mathbb{A}^n$ and $I = I(V)$ we define the **affine coordinate ring** of V to be

$$k[V] := k[x_1, \dots, x_n]/I.$$

Note that it makes sense to evaluate elements of $k[V]$ at points $P \in V(\overline{k})$.

Since $I(V)$ is a radical ideal, the affine coordinate ring is *reduced* (meaning that it does not have non-zero nilpotent elements).

3. Projective Varieties

$\mathbb{P}^n$ is n-dimensional projective space. For any field $L \supseteq k$,

$$\mathbb{P}^n(L) = \frac{L^{n+1} - \{(0, \dots, 0)\}}{L^*}.$$

Example I.5. In $\mathbb{P}^2(\mathbb{Q})$,

$$(1 : -2 : 5) = (10 : -20 : 50) = \left(\frac{1}{5} : \frac{-2}{5} : 1\right).$$

Example I.6. Let us think of $\mathbb{P}^n(\mathbb{Q})$ as a subset of $\mathbb{P}^n(\overline{\mathbb{Q}})$. Then $(\sqrt{5} : 2\sqrt{5}) \in \mathbb{P}^1(\mathbb{Q})$ (why?), but $(\sqrt{5} : 2) \notin \mathbb{P}^1(\mathbb{Q})$.

Exercise I.7. Show that

$$H^0\left(\mathrm{Gal}(\overline{k}/k), \mathbb{P}^n(\overline{k})\right) = \mathbb{P}^n(k).$$

Big Hint: In Silverman's book (page 20) it is suggested that you use Hilbert's Theorem 90. This is actually a good way of learning how H90 works. However, you can do this exercise by taking a point in $\mathbb{P}^n(\overline{k})$ fixed by $\mathrm{Gal}(\overline{k}/k)$ and scaling so one of the coordinates is 1.

Definition I.8. A **projective variety** over k is a subset of $\mathbb{P}^n$ cut out by a finite system of *homogeneous* polynomial equations in $k[x_0, \dots, x_n]$.

Let H_i be the hyperplane $x_i = 0$. Let

$$\phi_i : \mathbb{A}^n \xrightarrow{\simeq} \mathbb{P}^n - H_i \subset \mathbb{P}^n,$$
$$(x_0, x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \mapsto (x_0 : x_1 : \dots : x_{i-1} : 1 : x_{i+1}, \dots, x_n).$$

The sets $\{\phi_i(\mathbb{A}^n) : 0 \le i \le n\}$ form the "standard open covering of $\mathbb{P}^n$ by affine spaces ".

Similarly, any projective variety $V \subseteq \mathbb{P}^n$ has an open covering by $n+1$ affine varieties $V \subset \mathbb{A}^n$ (or strictly speaking $\phi_i^{-1}(V)$), which are called the "affine patches" of V.

Now fix $\mathbb{A}^n \subset \mathbb{P}^n$ (by one of the standard embeddings) and let H be the complement. If V_0 is k-variety in $\mathbb{A}^n$, its **projective closure** is defined as the smallest k-variety in $\mathbb{P}^n$ containing V_0. Observe the maps

$$\{k\text{-subvarieties of } \mathbb{A}^n\} \overset{\hookrightarrow}{\twoheadleftarrow} \{\text{projective } k\text{-subvarieties of } \mathbb{P}^n\}$$
$$V_0 \mapsto \text{projective closure of } V_0$$
$$V \cap \mathbb{A}^n \leftarrow\!\shortmid V.$$

Example I.9. Take $\mathbb{P}^2$ with coordinates x, y, z. Let $\mathbb{A}^2 = \{z \neq 0\} \subset \mathbb{P}^2$. Note

$$V_0 : \ y^2 = x^3 + 17 \qquad \underset{\text{dehomogenization: } z=1\ .}{\overset{\text{homogenization}}{\underset{\longleftarrow}{\longrightarrow}}} \qquad V : \ y^2 z = x^3 + 17z^3$$

4. Irreducibility

Definition I.10. A k-variety V is **irreducible** if and only if $V \neq \emptyset$ and it is impossible to write $V = W_1 \cup W_2$ where W_1, $W_2 \subsetneq V$ are closed k-subvarieties.

Theorem I.11. *An affine k-variety V is irreducible if and only if its affine coordinate ring is an integral domain.*

Example I.12. Let $V : \ x^2 - 2y^2 = 0$ in $\mathbb{A}^2_{\mathbb{Q}}$. The affine coordinate ring of V is

$$\mathbb{Q}[x, y]/(x^2 - 2y^2).$$

The polynomial x^2-2y^2 is an irreducible element of the unique factorization domain $\mathbb{Q}[x, y]$; it thus generates a prime ideal, and so the quotient ring is an integral domain. Hence V is irreducible.

We denote by $V_{\overline{\mathbb{Q}}}$ the base extension of V to a variety over $\overline{\mathbb{Q}}$ (all this means is that we take the $\overline{\mathbb{Q}}$-variety defined by the same equation). The affine coordinate ring of $V_{\overline{\mathbb{Q}}}$ is

$$\overline{\mathbb{Q}}[x, y]/(x^2 - 2y^2) = \mathbb{Q}[x, y]/(x^2 - 2y^2) \otimes_{\mathbb{Q}} \overline{\mathbb{Q}},$$

which clearly is not an integral domain. In fact,

$$V_{\overline{\mathbb{Q}}} = \{x - \sqrt{2}y = 0\} \cup \{x + \sqrt{2}y = 0\}$$

is not irreducible.

Definition I.13. A k-variety V is said to be **geometrically irreducible** (or **absolutely irreducible**) if $V_{\overline{k}}$ is irreducible.

Theorem I.14. *Let V be a k-variety. If V is irreducible but not geometrically irreducible then*

$$V_{\overline{k}} = \bigcup_{\sigma \in \mathrm{Gal}(\overline{k}/k)} W^\sigma$$

for some $\overline{k}$-variety W.

Example I.15. In arithmetic geometry we are primarily interested in rational points on varieties. We however normally restrict our attention to geometrically irreducible varieties. This is not really a restriction, since the determination of k-rational points on any k-variety reduces easily to the determination of k-rational points on geometrically irreducible k-varieties. To understand this suppose that V is is irreducible but geometrically reducible. So

$$V_{\overline{k}} = \bigcup_{\sigma \in \mathrm{Gal}(\overline{k}/k)} W^\sigma = W^{\sigma_1} \cup \cdots \cup W^{\sigma_n}.$$

The fact that V is geometrically reducible means that $n > 1$. Since V is not reducible, the action of Galois on the W^{σ_i} must be transitive. Now suppose $Q \in V(k)$. Then Q lies on one of the W^{σ_i}, and so Q lies on all of them. Hence the k-rational points on V lie on the intersection:

$$W^{\sigma_1} \cap W^{\sigma_2} \cap \cdots \cap W^{\sigma_n}.$$

This is in fact a k-variety, but it has smaller dimension than V. So geometric reducibility means that we can reduce the problem of determining the k-rational points to an easier problem [2].

Let us illustrate this with an example. Consider the $\mathbb{Q}$-variety

$$V : 2x^6 - 1 = y^2 + 2y.$$

V is irreducible, but not geometrically irreducible since

$$V_{\overline{\mathbb{Q}}} = \{y + 1 + \sqrt{2}x^3 = 0\} \cup \{y + 1 - \sqrt{2}x^3 = 0\}.$$

The point we want to illustrate is that is easier to obtain the $\mathbb{Q}$-rational points of geometrically reducible varieties. Let us see this in the current example: take any rational point $(x, y) \in V(\mathbb{Q})$. This must have rational x and y coordinates and satisfy either $y + 1 + \sqrt{2}x^3 = 0$ or $y + 1 - \sqrt{2}x^3 = 0$. But, since x, y are rational, if we satisfy one we must satisfy both. Hence

$$y + 1 + \sqrt{2}x^3 = y + 1 - \sqrt{2}x^3 = 0.$$

In other words

$$y = -1, \qquad x = 0.$$

So $V(\mathbb{Q}) = \{(0, -1)\}$.

By contrast, if we consider the $\mathbb{Q}$ variety

$$V' : 2x^6 - 1 = y^2;$$

this is geometrically irreducible (exercise: all you have to show is that $y^2 + 1 - 2x^6$ is irreducible in $\mathbb{Q}[x, y]$), but finding all the rational points is a non-trivial task.

5. Function Field

Theorem I.11 says that the affine coordinate ring of an irreducible affine k-variety is an integral domain. Thus it makes sense to speak about its field of fractions:

Definition I.16. Let V be an irreducible k-variety. The **function field** $k(V)$ of V is defined as follows:

- if V is affine with affine coordinate ring A then $k(V)$ is the field of fractions of A;
- if V is projective, let $k(V) := k(V \cap \mathbb{A}^n)$, for any standard $\mathbb{A}^n \subset \mathbb{P}^n$ that meets V.

It might appear from the definition above that a projective variety has several different function fields, depending on which of the standard $\mathbb{A}^n$ we choose. In fact all these are isomorphic, so we really only have one. Let us illustrate this with an example.

[2] Note that the intersection $W^{\sigma_1} \cap W^{\sigma_2} \cap \cdots \cap W^{\sigma_n}$ does not have to be geometrically irreducible, but in this case we can repeat the process above. Let us see an example that shows this intersection does not have to be geometrically irreducible. Let $V = C \cup D$ where C is a plane curve of degree $m > 1$ defined over a quadratic number field and D is its conjugate. In the above notation $n = 2$, $W^{\sigma_1} = C$ and $W^{\sigma_2} = D$. By Bezout's Theorem, $W^{\sigma_1} \cap W^{\sigma_2}$ consists of m^2 points defined over $\overline{\mathbb{Q}}$, and hence is not geometrically irreducible.

Example I.17. Let $V \subset \mathbb{P}^2_k$ be the variety given by $V : zy^2 = x^3 + z^3$. The standard $\mathbb{A}^2 \subset \mathbb{P}^2$ are respectively given by $z \neq 0$, $x \neq 0$ and $y \neq 0$. Let $V_0 = V \cap \{z \neq 0\}$ and $V_1 = V \cap \{x \neq 0\}$. Thus

$$V_0 : y_0^2 = x_0^3 + 1, \qquad x_0 = x/z, \quad y_0 = y/z,$$

and

$$V_1 : z_1 y_1^2 = 1 + z_1^3, \qquad z_1 = z/x, \quad y_1 = y/x.$$

The function field of V_0 is the field of fractions of $k[x_0, y_0]/(y_0^2 - x_0^3 - 1)$; thus

$$k(V_0) = k(x_0)\left(\sqrt{x_0^3 + 1}\right).$$

The function field of V_1 is

$$k(V_1) = k(z_1)\left(\sqrt{\frac{1 + z_1^3}{z_1}}\right).$$

The claim is that the two function fields are isomorphic. The isomorphism will not be any isomorphism, but an isomorphism that comes from the construction of V_0 and V_1 as affine patches of the same projective variety V. Now on V, $z_1 = z/x = 1/x_0$. Thus it is very reasonable to expect that the isomorphism will be given by

$$k(x_0)\left(\sqrt{x_0^3 + 1}\right) \to k(z_1)\left(\sqrt{\frac{1 + z_1^3}{z_1}}\right), \qquad x_0 \mapsto 1/z_1.$$

We leave it as an easy exercise to the reader to check that this does indeed give an isomorphism of fields. Similarly we can check that the function field of the third affine patch $V_2 = V \cap \{y \neq 0\}$ is naturally isomorphic to the first two.

Definition I.18. Let V be an irreducible k-variety. Elements of $k(V)$ are called rational functions on V. Suppose $f \in k(V)$ and $P \in V(\overline{k})$.

- If V is affine with coordinate ring A, then f is **defined at** P if and only if $f = g/h$ for some g, $h \in A$ with $h(P) \neq 0$.
- If V is projective, f is **defined at** P if and only if $f|_{V \cap \mathbb{A}^n}$ is defined at P for some standard $\mathbb{A}^n \subset \mathbb{P}^n$ containing P.

Theorem I.19. *Suppose V is an irreducible k-variety. Then V is geometrically irreducible if and only if*

$$\{\alpha \in k(V) : \alpha \textit{ is algebraic over } k\} = k.$$

Example I.20. In Example I.12, observe that $x/y \in \mathbb{Q}(V)$ satisfies $(x/y)^2 = 2$ and so Theorem I.19 gives another way of showing that V is geometrically reducible.

6. Dimension

Definition I.21. Let V be an irreducible k-variety. The dimension of V is defined to be the largest d for which there exists a d-step chain

$$V_0 \subsetneqq V_1 \subsetneqq \cdots \subsetneqq V_d$$

of irreducible closed subvarieties of V.

Theorem I.22. *Suppose V is a geometrically irreducible k-variety.*

- $\dim V$ *equals the transcendence degree of $k(V)/k$.*

- $\dim V_L = \dim V$ *for any field extension* $L \supseteq k$.

Varieties of dimension 1 are called **curves**, varieties of dimension 2 are called **surfaces**, varieties of dimension 3 are called **threefolds**, and so on.

Example I.23. Take the variety $V : y^2 = x^3 + 1$. The function field is just $k(x)(\sqrt{x^3+1})$. This is clearly an extension of k of transcendence degree 1. Thus V is a curve.

Exercise I.24. Let $V \subset \mathbb{A}^n$ be given a single non-constant irreducible polynomial

$$V : f(x_1, \ldots, x_n).$$

Show that V has dimension $n-1$.

7. Smooth Varieties

Let $V \subset \mathbb{A}^n$ be an affine variety of dimension d, given by equations

$$V : \begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \qquad\vdots \\ f_m(x_1, \ldots, x_n) = 0. \end{cases}$$

Let $P \in V(\overline{k})$. We say that V is **smooth** (or **non-singular**) at P if and only if

$$\operatorname{rank}\left(\frac{\partial f_i}{\partial x_j}(P)\right)_{1 \le i \le m, 1 \le j \le n} = n - d.$$

For $V \subseteq \mathbb{P}^n$, we say that V is **smooth** at $P \in V(\overline{k})$ if $V \cap \mathbb{A}^n$ is smooth at P for some standard $\mathbb{A}^n$ containing P.

The k-variety V is said to be smooth if it is smooth at all $P \in V(\overline{k})$.

Example I.25. Let V be an affine k-variety given by a single non-constant irreducible polynomial; say $V : f(x_1, \ldots, x_n) = 0$. In Exercise I.24 you showed that $\dim(V) = n - 1$. Thus $P \in V(\overline{k})$ is singular if the $1 \times n$ matrix

$$\left(\frac{\partial f}{\partial x_i}\right)$$

is zero. In other words, **singular locus** (set of non-smooth points) is the set points satisfying the equations

$$\frac{\partial f}{\partial x_1} = \cdots = \frac{\partial f}{\partial x_n} = f = 0.$$

Example I.26. Consider the k-variety in $\mathbb{A}^2$ given by

$$V : y^2 = x^3 - 3x.$$

The singular locus is given by

$$3x^2 - 3 = 2y = y^2 - x^3 - x = 0.$$

If $\operatorname{char}(k) \neq 2$ then we see that V is smooth. If $\operatorname{char}(k) = 2$ then there is exactly one singular point $(1, 0)$.

Now let W be the k-variety in $\mathbb{A}^2$ given by

$$W : y^2 = x^3 + x^2.$$

The singular locus is given by

$$3x^2 + 2x = 2y = y^2 - x^3 - x^2 = 0.$$

In other words, there is exactly one singular point $(0, 0)$.

Exercise I.27. Let V be a projective k-variety given by a single equation; say $V : F(x_0, \dots, x_n) = 0$. Here F must be a homogeneous polynomial.

(i) Show that the singular locus is given by

$$\frac{\partial F}{\partial x_0} = \cdots = \frac{\partial F}{\partial x_n} = F = 0.$$

(ii) if $\operatorname{char}(k)$ does not divide d, show that the singular locus is the set of solutions to

$$\frac{\partial F}{\partial x_0} = \cdots = \frac{\partial F}{\partial x_n} = 0.$$

Hint for (ii): google 'Euler's Homogeneous Function Theorem'.

CHAPTER II

Curves

1. What is a curve?

Recall that we defined a curve over k to be a 1-dimensional k-variety. In fact, by **curve over** k we will usually mean **smooth, projective, geometrically irreducible, 1-dimensional, closed k-variety**. Under the equivalence of categories between irreducible k-varieties and finitely generated field extensions of k, our (smooth, projective, geometrically irreducible, closed) curves correspond to field extensions K/k of transcendence degree 1 such that $K \cap \overline{k} = k$.

2. Valuations

If K is a field, a **discrete valuation** on K is a function $\phi : K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ satisfying the conditions:

- $\phi(a) = \infty$ if and only if $a = 0$;
- $\phi(ab) = \phi(a) + \phi(b)$;
- $\phi(a + b) \geq \min(\phi(a), \phi(b))$.

As we explain in this section, if C is a smooth curve, then corresponding to every point $P \in C(\overline{k})$ is a discrete valuation which measure the order of vanishing of functions $f \in \overline{k}(C)$ at P.

Let C be a curve over k. Let $\overline{C} = C_{\overline{k}}$ be the base extension of C to $\overline{k}$, and let $\overline{k}(C)$ be the function field of $\overline{C}$. Let $P \in C(\overline{k})$; we emphasize the assumption that C is smooth (or at least smooth at P).

Theorem II.1. *There is unique (surjective) function*

$$\mathrm{ord}_P : \overline{k}(C) \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$$

satisfying the following:

(i) $\mathrm{ord}_P(f) = \infty$ *if and only if* $f = 0$*;*
(ii) $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$*;*
(iii) $\mathrm{ord}_P(f + g) \geq \min(\mathrm{ord}_P(f), \mathrm{ord}_P(g))$*;*
(iv) $\mathrm{ord}_P(f) \geq 0$ *if and only if f is defined at P;*
(v) $\mathrm{ord}_P(f) > 0$ *if and only f has a zero at P, and* $\mathrm{ord}_P(f) < 0$ *if and only if $1/f$ has a zero at P.*

Moreover, if $P \in C(k)$ then ord_P *restricts to a surjective* $\mathrm{ord}_P : k(C) \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$.

We call $\mathrm{ord}_P(f)$ the order of f at P. If $\mathrm{ord}_P(f) < 0$ we say that f has a pole at P; this is a simple, double, triple, etc. pole at P according to whether $\mathrm{ord}_P(f) = -1, -2, -3, \ldots$. Likewise, f has a simple, double, triple, etc. zero at P according to whether $\mathrm{ord}_P(f) = 1, 2, 3, \ldots$.

Definition II.2. An element $t \in \overline{k}(C)$ with $\mathrm{ord}_P(t) = 1$ is called a **uniformizer at** P.

Theorem II.1 tells us that $\mathrm{ord}_P : \overline{k}(C) \to \mathbb{Z} \cup \{\infty\}$ is surjective. Thus there is a uniformizer at every (smooth) point. Moreover, if P is k-rational (i.e. $P \in C(k)$) then we can choose the uniformizer t at P to be also k-rational (i.e. $t \in k(C)$). Of course our choice of uniformizer is not unique.

Exercise II.3. Suppose $\mathrm{ord}_P(f) \neq \mathrm{ord}_P(g)$. Show that

$$\mathrm{ord}_P(f + g) = \min\{\mathrm{ord}_P(f), \mathrm{ord}_P(g)\}.$$

Exercise II.4. Suppose $t \in \overline{k}(C)$ is a uniformizer at P. Show that any function of the form

$$s = \frac{a_1 t + a_2 t^2 + \cdots a_m t^m}{b_0 + b_1 t + \cdots b_n t^n}$$

with a_1, $b_0 \neq 0$ is also a uniformizer at P.

Geometrically speaking, t is a uniformizer at P if the graph of $t = 0$ passes through P, but does not touch the curve C at P; that is the C and $t = 0$ have distinct tangents at P.

Example II.5. Knowing how to write down a uniformizer at a given point will be important later on. Here is a fail proof method. Suppose $P = (a, b)$ is a point on an affine patch of the curve C given by $f(x, y) = 0$ in $\mathbb{A}^2$. Let

$$t_1 = x - a, \qquad t_2 = y - b.$$

Note that t_1 and t_2 vanish at P. In fact, $t_1 = 0$ is the vertical line through P and $t_2 = 0$ is the horizontal line through P. Since C is smooth at P,

$$\text{either} \qquad \frac{\partial f}{\partial x}(P) \neq 0, \qquad \text{or} \qquad \frac{\partial f}{\partial y}(P) \neq 0.$$

If $\frac{\partial f}{\partial x}(P) \neq 0$ then the tangent line is not horizontal at P and so t_2 is a uniformizer. If $\frac{\partial f}{\partial y}(P) \neq 0$ then the tangent line is not vertical at P and so t_1 is a uniformizer.

Example II.6. Let C be the projective closure of the affine plane patch

$$C_0 : y^2 = x^3 - x.$$

We want to specify a uniformizer at each point P of C. Start with the points belonging to the affine patch C_0. If $P = (a, b) \in C_0$ then $x - a$ is a uniformizer at all points where it the tangent is not vertical. Thus we can choose as a our uniformizer, $x - a$ unless $b = 0$ in which case take y as the uniformizer. Note of course that these choices are not unique.

The projective closure of C_0 is

$$C : ZY^2 = X^3 - XZ^2.$$

Note that $x = X/Z$, $y = Y/Z$. The only extra point belonging to C that does not belong to the affine patch C_0 is $[0 : 1 : 0]$ which you know is the point at infinity. To construct a uniformizer at this point we should construct an affine patch the contains $[0 : 1 : 0]$. We can do this by dehomogenizing: let $u = Z/Y$ and $v = X/Y$, so that $[0 : 1 : 0]$ becomes the point $(0, 0)$ on the affine patch

$$C_1 : u = v^3 - vu^2.$$

If we write $f = u - v^3 + vu^2$, we see that $\partial f/\partial u$ is non-zero at $(0,0)$, and so v is a uniformizer at $(0,0)$ on C_1. Thus, in terms of coordinate functions on the original affine patch C_0, the uniformizer at ∞ is $x/y = X/Y = v$.

Let us see some examples of how to determine the valuation of a function at a point. Let $Q = (0,0)$ on the affine patch C_0; in other words $Q = [0:0:1]$ on C. Now y is a uniformizer at Q, so $\operatorname{ord}_Q(y) = 1$. We would like to determine $\operatorname{ord}_Q(x)$. From $y^2 = x(x^2-1)$ we see that $x = y^2/(x^2-1)$. But $\operatorname{ord}(x^2-1) = 0$, since x^2-1 neither vanishes nor has a pole at Q. Thus

$$\operatorname{ord}_Q(x) = 2\operatorname{ord}_Q(y) - \operatorname{ord}_Q(x^2-1) = 2.$$

Clearly x does not vanish or have a pole at any other point on C_0. However, x must have a pole at ∞. We would like to determine the order of the pole that x has at ∞. For this we have to switch to the other affine patch C_1; on C_1, $x = v/u$ and ∞ becomes $Q' = (0,0)$. Recall that v is a uniformizer at Q'. We can use a similar trick to the above to obtain $\operatorname{ord}_{Q'}(v/u)$. Another very useful method is to expand u as a power-series in the uniformizer v; we only need the first few terms. Recall $u = v^3 - vu^2$. Substituting this into itself a few times, obtain

$$\begin{aligned} u &= v^3 - v(v^3 - vu^2)^2 = v^3 - v^7 + 2v^5u^2 - v^3u^4 \\ &= v^3 - v^7 + 2v^5(v^3 - vu^2)^2 - v^3(v^3 - vu^2)^4 = \dots \\ &= v^3 - v^7 + 2v^{11} + \cdots . \end{aligned}$$

Thus u has a zero of order 3 at Q' and so v/u has a pole of order 2 at Q'. In fact we can expand

$$\begin{aligned} x &= \frac{v}{u} = \frac{1}{v^2 - v^6 + 2v^{10} + \cdots} \\ &= \frac{v^{-2}}{1 - v^4 + 2v^9 + \cdots} \\ &= v^{-2}\left(1 + (v^4 - 2v^9 + \cdots) + (v^4 - 2v^9 + \cdots)^2 + \cdots\right) \\ &= v^{-2} + v^2 + v^6 - 2v^7 \cdots . \end{aligned}$$

Hence $\operatorname{ord}_\infty(x) = -2$.

Warning/Remark. For now, the trick used here of expanding x in terms of v is purely formal and only tells us about x at $Q' = \infty$ and at no other point. If we are working over fields with a topology (for example $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}_p$) then the powerseries does say something about the behaviour of x at points within the radius of convergence (which we have not determined). Thus if are interested in x at some other point, then we should expand x in terms of the uniformizer at that point and not use the expansion in terms of v.

Exercise II.7. In Example II.6, write down the zeros and poles of y and their multiplicities.

2.1. Local rings.

Definition II.8. The **local ring of $\overline{C}$ at** P is

$$\mathcal{O}_{\overline{C},P} := \{f \in \overline{k}(C) : f \text{ is defined at } P\} = \{f \in \overline{k}(C) : \operatorname{ord}_P(f) \geq 0\}.$$

Theorem II.9. *$\mathcal{O}_{\overline{C},P}$ is a local ring* [1] *with unique maximal ideal*

$$\mathfrak{m}_{\overline{C},P} := \{f \in \mathcal{O}_{\overline{C},P} : f(P) = 0\} = \{f \in \mathcal{O}_{\overline{C},P} : \mathrm{ord}_P(f) > 0\}.$$

Exercise II.10. By considering the 'evaluation homomorphism'

$$\mathcal{O}_{\overline{C},P} \to \overline{k}, \qquad f \mapsto f(P)$$

Show that $\mathfrak{m}_{\overline{C},P}$ is indeed maximal.

3. Divisors

Definition II.11. A **divisor** on C is a formal finite $\mathbb{Z}$-linear combination of points belonging to $C(\overline{k})$. We write $\mathrm{Div}(\overline{C})$ for the group of all divisors. We write

$$\mathrm{Div}(C) := H^0\left(\mathrm{Gal}(\overline{k}/k), \mathrm{Div}(\overline{C})\right),$$

for the k-rational divisors. In other words, the k-rational divisors are the ones fixed by the action of $\mathrm{Gal}(\overline{k}/k)$.

Example II.12. Let $C/\mathbb{Q}$ be the closed curve in $\mathbb{P}^2$:

$$C : x^2 + y^2 = z^2.$$

An example of an element of $\mathrm{Div}(\overline{C})$ are

$$3(1:0:1) - 2(\sqrt{-3}:2:1).$$

An example of an element of $\mathrm{Div}(C)$ is

$$3(1:0:1) - 2(\sqrt{-3}:2:1) - 2(-\sqrt{-3}:2:1).$$

Definition II.13. The **degree** of the divisor $D = \sum n_P P$ is defined by

$$\deg(D) = \sum_{P \in C(\overline{k})} n_P.$$

3.1. Principal Divisors.

Suppose $f \in \overline{k}(C)^*$. Then the **divisor of** f is defined by

$$\mathrm{div}(f) = (f) := \sum_{P \in C(\overline{k})} \mathrm{ord}_P(f) P.$$

A divisor of the form $\mathrm{div}(f)$ is called a **principal divisor**.

Theorem II.14. *Let C/k be a curve. Let $f \in \overline{k}(C)$. Then*

(i) *There are finitely many points $P \in C(\overline{k})$ at which f has a pole or a zero (thus* $\mathrm{div}(f)$ *is truly a divisor).*
(ii) $\deg(\mathrm{div}(f)) = 0$.
(iii) *If f has no zeros (or no poles) then $f \in \overline{k}^*$.*
(iv) *If $f \in k(C)^*$, then* $\mathrm{div}(f) \in \mathrm{Div}(C)$.

Exercise II.15. In the theorem, by curve we mean a smooth, projective, geometrically irreducible, 1-dimensional, closed, k-variety. Pick an **affine** curve of your choice, and show that (ii) and (iii) in Theorem II.14 need not hold.

Exercise II.16. (trivial) Write down a non-constant function on $\mathbb{G}_m$ that has neither poles nor zeros.

[1] A local ring is a ring with a unique maximal ideal

Exercise II.17. Show that $\operatorname{div} : k(C)^* \to \operatorname{Div}(C)$ is a homomorphism.

Example II.18. This exercise is a continuation of Example II.6 and Exercise II.7. From the example/exercise we know that

$$\operatorname{div}(x) = 2(0,0) - 2\infty, \qquad \operatorname{div}(y) = (-1,0) + (0,0) + (1,0) - 3\infty;$$

here we are giving the coordinates of points with respect to the affine patch C_0. Observe that $\deg(\operatorname{div}(x)) = \deg(\operatorname{div}(y)) = 0$, which is consistent with Theorem II.14. In fact had we known this earlier, we could have avoided the long-winded computation of $\operatorname{ord}_\infty(x)$: we showed that x has a zero of order 2 at $(0,0)$ and it has no other zeros or poles on C_0, so the only way we will get $\deg(\operatorname{div}(x)) = 0$ is for x to have a double pole at ∞.

4. The Picard Group

Definition II.19. We shall say that two divisors D_1, D_2 are **linearly equivalent** and write $D_1 \sim D_2$ if $D_1 - D_2$ is a principal divisor.

Let $\operatorname{Princ}(C)$ be the subgroup of $\operatorname{Div}(C)$ consisting of principal divisors. Define the **Picard Group** (or the **divisor class group**) of C to be

$$\operatorname{Pic}(C) := \operatorname{Div}(C)/\operatorname{Princ}(C).$$

In other words, $\operatorname{Pic}(C)$ is divisors modulo linear equivalence. We also let

$$\operatorname{Pic}(\overline{C}) := \operatorname{Div}(\overline{C})/\operatorname{Princ}(\overline{C}).$$

Theorem II.20. *We obtain exact sequences*

$$1 \to k^* \to k(C)^* \to \operatorname{Div}(C) \to \operatorname{Pic}(C) \to 0$$

and

$$1 \to \overline{k}^* \to \overline{k}(C)^* \to \operatorname{Div}(\overline{C}) \to \operatorname{Pic}(\overline{C}) \to 0.$$

Proof. The exactness is obvious except at $k(C)^*$ where it follows from part (iii) of Theorem II.14. □

We have obvious inclusions, $\operatorname{Div}(C) \subseteq \operatorname{Div}(\overline{C})$ and $\operatorname{Princ}(C) \subseteq \operatorname{Princ}(\overline{C})$. Thus we obtain a natural homomorphism

$$\operatorname{Pic}(C) \to \operatorname{Pic}(\overline{C}).$$

There is a natural Galois action on $\operatorname{Pic}(\overline{C})$. If $D \in \operatorname{Div}(\overline{C})$ and $[D]$ denotes its equivalence class in Pic then $[D]^\sigma = [D^\sigma]$.

Theorem II.21. *The natural map* $\operatorname{Pic}(C) \to \operatorname{Pic}(\overline{C})$ *is injective:* $\operatorname{Pic}(C) \hookrightarrow \operatorname{Pic}(\overline{C})$*. Thus we obtain a natural injection*

$$\operatorname{Pic}(C) \hookrightarrow H^0(\operatorname{Gal}(\overline{k}/k), \operatorname{Pic}(\overline{C})).$$

Proof. The first part requires Hilbert's Theorem 90, and we return to it later. The second part is obvious. □

Warnings and Remark. Let us make two warnings:

- In Silverman's book, $\operatorname{Pic}(C)$ is defined as $H^0\left(\operatorname{Gal}(\overline{k}/k), \operatorname{Pic}(\overline{C})\right)$ and not as we have defined.
- The map $\operatorname{Pic}(C) \hookrightarrow H^0\left(\operatorname{Gal}(\overline{k}/k), \operatorname{Pic}(\overline{C})\right)$ need not be surjective, as we shall see in Example II.23 below. Thus our definition is genuinely different from Silverman's.

We will eventually see that the degree 0 part of $H^0\left(\mathrm{Gal}(\overline{k}/k), \mathrm{Pic}(\overline{C})\right)$ can be identified with the Jacobian of C. However, explicit computations are most easily performed in $\mathrm{Pic}(C)$. The discrepancy between the two groups needs some care.

Example II.22. Let $C = \mathbb{P}^1/\mathbb{C}$. Then $\mathbb{P}^1(\mathbb{C}) = \mathbb{A}^1(\mathbb{C}) \cup \{\infty\}$. A divisor on $\mathbb{P}^1_{\mathbb{C}}$ is simply a formal $\mathbb{Z}$-linear combination of points

$$\sum_{\alpha\in\mathbb{C}} m_\alpha(\alpha) + m_\infty(\infty).$$

The affine coordinate ring of $\mathbb{A}^1$ is $\mathbb{C}[t]$ and so the function field $\mathbb{C}(\mathbb{P}^1) = \mathbb{C}(t)$. Any $f \in \mathbb{C}(\mathbb{P}^1)^*$ has the form

$$c\prod_{\alpha\in\mathbb{C}}(t-\alpha)^{n_\alpha}, \qquad n_\alpha \in \mathbb{Z}.$$

Observe that

$$(f) = \sum_{\alpha\in\mathbb{C}} n_\alpha(\alpha) + n_\infty(\infty).$$

Since f must have degree 0, we observe that $n_\infty = -\sum_{\alpha\in\mathbb{C}} n_\alpha$. It is now obvious that divisors of degree 0 on $\mathbb{P}^1$ are principal. Thus

$$C(\mathbb{P}^1)^* \to \mathrm{Div}(\mathbb{P}^1) \overset{\deg}{\twoheadrightarrow} \mathbb{Z} \to 0,$$

is exact. We obtain that an isomorphism

$$\mathrm{Pic}(\mathbb{P}^1_{\mathbb{C}}) \xrightarrow{\overset{\deg}{\cong}} \mathbb{Z}.$$

Note that this means the following: let $P \in \mathbb{P}^1(\mathbb{C})$. Then $[P]$ (the equivalence class of P in $\mathrm{Pic}(\mathbb{P}^1)$) generates $\mathrm{Pic}(\mathbb{P}^1)$. Moreover, if P, $Q \in \mathbb{P}^1(\mathbb{C})$ then their classes have the same degree and so their classes are equal. It follows that any two points are linearly equivalent.

Example II.23. Let $C/\mathbb{R}$ be the curve in $\mathbb{P}^2_{\mathbb{R}}$ given by

$$C : x^2 + y^2 + z^2 = 0.$$

Let $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Since $C(\mathbb{R}) = \emptyset$, every point in $C(\mathbb{C})$ has G-orbit of size 2. Hence every element of $\mathrm{Pic}(C)$ has even degree.

Now fix any point $P \in C(\mathbb{C})$, for example $P = (i : 1 : 0)$. Let $[P]$ denote the equivalence class of P in $\mathrm{Pic}(C_{\mathbb{C}})$. We know that $C_{\mathbb{C}}$ is isomorphic to $\mathbb{P}^1_{\mathbb{C}}$. Hence, by Example II.22, $\mathrm{Pic}(C_{\mathbb{C}}) = \mathbb{Z}\cdot[P]$. Let σ denote complex conjugation. Again, by Example II.22 any two points on $C_{\mathbb{C}}$ are linearly equivalent, so $[P]^\sigma = [P^\sigma] = [P]$, hence

$$H^0(G, \mathrm{Pic}(C_{\mathbb{C}})) = \mathbb{Z}\cdot[P] = \mathrm{Pic}(C_{\mathbb{C}}),$$

where as $\mathrm{Pic}(C)$ has only elements of even degree. It follows that that the injective map $\mathrm{Pic}(C) \hookrightarrow H^0(G, \mathrm{Pic}(C_{\mathbb{C}}))$ is not a surjection.

5. Differentials

Definition II.24. Let C be a curve over a field k. The space of meromorphic differential forms Ω_C on C is defined as as the $k(C)$-vector space of symbols of the form dx with $x \in k(C)$ subject to the usual relations:

(1) $d(x+y) = dx + dy$ for all x, $y \in k(C)$,

(2) $d(xy) = xdy + ydx$ for all $x, y \in k(C)$,
(3) $da = 0$ for all $a \in k$.

In other words, all that the definition is saying, is take the $k(C)$-vector space generated by the symbols dx with $x \in k(C)$, and the quotient out by the subspace generated by $d(x+y) - dx - dy$, $d(xy) - xdy - ydx$ for $x, y \in k(C)$ and da for $a \in k$. That gives us the differentials.

Exercise II.25. Show that

$$d\left(\frac{x}{y}\right) = \frac{ydx - xdy}{y^2}.$$

Theorem II.26. *Ω_C is a 1-dimensional $k(C)$-vector space.*

Definition II.27. (**Order of a differential at a point**) Given $P \in C(\overline{k})$ and $\omega \in \Omega_C$, choose a uniformizer $t \in k(C)$ at P. It turns out that $dt \neq 0$ in Ω_C. Thus, by Theorem II.26, $\omega = fdt$ for some $f \in k(C)$. Define

$$\operatorname{ord}_P(\omega) := \operatorname{ord}_P(f).$$

It is a fact that the order of a differential at a point does not depend on the choice of uniformizer at that point, and so it well-defined.

Definition II.28. If $\omega \in \Omega_C$ is a non-zero differential form, define

$$\operatorname{div}(\omega) := \sum_{P \in C(\overline{k})} \operatorname{ord}_P(\omega) P.$$

This turns out to be fixed under the action of Galois and so $\div(\omega) \in \operatorname{Div}(C)$. Any divisor of this type is called a **canonical divisor**. Note that this depends on the choice of ω and so is non-unique.

Let ω' be another non-zero element of Ω_C. As Ω_C is 1-dimensional as a $k(C)$-vector space, $\omega' = f\omega$ for some rational function $f \in k(C)^*$. Thus

$$\operatorname{div}(\omega') = (f) + \operatorname{div}(\omega).$$

In other words, any two canonical divisors differ by a principal divisor. In particular, $\operatorname{div}(\omega') \equiv \operatorname{div}(\omega)$ in $\operatorname{Pic}(C)$.

Definition II.29. This element of $\operatorname{Pic}(C)$ is called the **canonical class**.

Definition II.30. If a differential ω has no poles the it is called **regular** or (**holomorphic**).

Example II.31. This example is a continuation of Examples II.6, II.18 and exercise II.7. Let

$$C \quad : \quad y^2 = x^3 - x.$$

Compute the divisors of dx and dx/y.
Answer: The curve is given by an affine patch, but in this course we alway consider *complete curves*; in other words, it is implicit in the question that we want the divisors of dx and dx/y on the complete curve one of whose affine patches is given.

We work on the given patch, then for the points at infinity we transfer to the other patch.

Suppose first that $P \in C(\overline{k})$, $P = (a, b)$ and $a \neq 0, \pm 1$. Then $x - a$ is a uniformizer at P. Thus

$$dx = d(x - a) = 1.d(x - a)$$

and hence $\operatorname{ord}_P(dx) = 0$.

Now let $P = (0, 0)$ or $(1, 0)$ or $(-1, 0)$. Then y is a uniformizer at P. Note that $2ydy = (3x^2 - 1)dx$, and so

$$\operatorname{ord}_P(dx) = \operatorname{ord}_P\left(\frac{2y}{3x^2 - 1}\right) = 1,$$

since $3x^2 - 1$ is regular and does not vanish at the three points $(0, 0)$, $(\pm 1, 0)$.

All that remains is to consider the point at infinity. Recall that in Example II.6 we determined that $x = v^{-2} + v^2 + v^6 + 2v^7 + \cdots$ where v is a uniformizer at infinity. Thus

$$dx = (-2v^{-3} + 2v + 6v^5 + \cdots)dv.$$

Hence $\operatorname{ord}_\infty(dx) = \operatorname{ord}_\infty(-2v^{-3} + 2v + 6v^5 + \cdots) = -3$.

Putting everything together we see that

$$\operatorname{div}(dx) = (0, 0) + (1, 0) + (-1, 0) - 3\infty.$$

We recall that

$$\operatorname{div}(y) = (0, 0) + (1, 0) + (-1, 0) - 3\infty,$$

hence

$$\operatorname{div}\left(\frac{dx}{y}\right) = 0.$$

In other words dx/y is a non-vanishing holomorphic differential.

6. Genus

Write

$$\Omega_C^{\text{reg}} := \{\omega \in \Omega_C : \omega \text{ is regular}\}$$

for the set of regular (or holomorphic differentials) on C. Clearly Ω_C^{reg} is a k-vector space.

Theorem II.32. $\dim_k \Omega_C^{\text{reg}} = \dim_{\overline{k}} \Omega_{\overline{C}}^{\text{reg}} < \infty$.

Definition II.33. The **genus** g of the curve C is simply $\dim_k \Omega_C^{\text{reg}}$.

Theorem II.34. *The genus of* $\mathbb{P}^1$ *is* 0.

Proof. By Theorem II.32 we may assume that $k = \overline{k}$. We will prove the theorem by showing that $\Omega_C^{\text{reg}} = \{0\}$. As usual, think of $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$ and let $k[x]$ be the affine coordinate ring of $\mathbb{A}^1$. Now the function field of $\mathbb{P}^1$ is $k(x)$ and every differential has the form fdx where $f \in k(x)$. Suppose that $\omega = fdx$ is regular.

If $a \in \mathbb{A}^1(k)$ then $x - a$ is a uniformizer at a, and so $fdx = fd(x - a)$. Thus f is regular at a. Since this is true for all $a \in \mathbb{A}^1(k)$, $f \in k[x]$. It remains to show that ω is not holomorphic at infinity. Now x has a simple zero at 0 and no poles anywhere on $\mathbb{A}^1$. Hence it must have a simple pole at ∞. Thus $z := 1/x$ is uniformizer at ∞. Hence

$$\omega = \frac{-1}{z^2} f(1/z) dz.$$

Clearly ω is not holomorphic at ∞ unless $f = 0$. This proves the theorem. □

Example II.35. It follows from Example II.31 that the genus of $y^2 = x^3 - x$ is at least 1. In fact it is precisely 1 as we shall see.

CHAPTER III

Riemann–Roch

1. Riemann–Roch Space

As usual, C denotes a curve over k (i.e. a smooth, projective, geometrically irreducible, closed, 1-dimensional variety).

Definition III.1. (Partial Ordering on Divisors) If $D_1 = \sum n_P P$ and $D_2 = \sum m_P P$, then $D_1 \geq D_2$ means that $n_P \geq m_p$ for all P. Divisors satisfying $D \geq 0$ are called **positive** or **effective**.

Observe that if $D_1 \geq D_2$ then $\deg(D_1) \geq \deg(D_2)$. Also, if ω is a differential, then $\operatorname{div}(\omega) \geq 0$ means that ω is holomorphic.

Exercise III.2. (trivial) Which $f \in k(C)$ satisfy $\operatorname{div}(f) \geq 0$?

Definition III.3. Let $D \in \operatorname{Div}(C)$. Define the **Riemann–Roch space** associated to D by

$$L(D) := \{f \in k(C)^* \ : \ \operatorname{div}(f) + D \geq 0\} \cup \{0\}.$$

Clearly $L(D)$ is a k-vector space.

Example III.4. If C is a curve and $P \neq Q$ are distinct k-rational points then $L(3P - 2Q)$ is the space of rational functions on C such that

$$\operatorname{ord}_P(f) \geq -3, \qquad \operatorname{ord}_Q(f) \geq 2, \qquad f \text{ is defined at all other points.}$$

In other words, a non-zero element of $L(3P - 2Q)$ has a pole of order at worst 3 at P, a zero of order at least 2 at Q and is defined at all other points.

Definition III.5. $l(D) := \dim_k L(D)$. We call $l(D)$ the **dimension** of the divisor D.

Example III.6. Consider $\mathbb{P}^1_{\mathbb{C}}$ with homogeneous coordinates $(X_0 : X_1)$ and let $x = X_0/X_1$. Then $k(\mathbb{P}^1) = k(x)$. Let $\infty = (1 : 0)$. Then $L(n\infty)$ consists of functions with no poles anywhere except for a pole of order at most n at ∞. Hence $L(n\infty)$ is the vector space of polynomials of degree at most n. In particular,

$$l(n\infty) = \begin{cases} n+1 & \text{if } n \geq 0 \\ 0 & \text{otherwise.} \end{cases}$$

In general, it is harder to compute the dimension of a divisor, and would probably need the Riemann–Roch Theorem.

Lemma III.7. *Let $D \in \operatorname{Div}(C)$.*

(a) $l(D) < \infty$.
(b) *If* $\deg(D) < 0$ *then* $L(D) = \{0\}$ *and* $l(D) = 0$.

(c) *If $D' \in \mathrm{Div}(C)$ is linearly equivalent to D, say $D' = D + \mathrm{div}(h)$ with $h \in k(C)^*$, then $L(D') = h^{-1}L(D)$. In particular, linearly equivalent divisors have the same dimension.*

Proof. We omit (a) and go straight to (b). Suppose f is non-zero and satisfies $\mathrm{div}(f) \geq -D$. Then

$$0 = \deg(\mathrm{div}(f)) \geq \deg(-D) = -\deg(D) > 0$$

which is impossible. Hence $L(D) = \{0\}$.

Let's prove (c). Suppose $f \in k(C)^*$. Then

$$\begin{aligned} f \in L(D') &\iff \mathrm{div}(f) + D' \geq 0 \\ &\iff \mathrm{div}(f) + \mathrm{div}(h) + D \geq 0 \\ &\iff \mathrm{div}(fh) + D \geq 0 \\ &\iff fh \in L(D) \\ &\iff f \in h^{-1}L(D). \end{aligned}$$

□

2. Genus Revisited

Recall that we defined Ω_C^{reg} to be the vector space of regular (or holomorphic) differentials, and we defined the genus g to be the dimension of this as a k-vector space.

Now let $\omega \in \Omega_C$ be any non-zero differential (regular or otherwise). We shall write $K_\omega = \mathrm{div}(\omega)$ for the corresponding canonical divisor.

Lemma III.8. *$L(K_\omega) \cong \Omega_C^{\mathrm{reg}}$. The isomorphism is simply given by $f \mapsto f\omega$. In particular, the Riemann–Roch spaces of canonical classes are all isomorphic and $l(K_\omega) = g$.*

Proof. Recall that the space of differentials Ω_C is 1-dimensional as a $k(C)$-vector space. Hence every non-zero differential has the form $f\omega$ for some $f \in k(C)^*$. Now

$$\begin{aligned} f\omega \in \Omega_C^{\mathrm{reg}} &\iff \mathrm{div}(f\omega) \geq 0 \\ &\iff \mathrm{div}(f) + K_\omega \geq 0 \\ &\iff f \in L(K_\omega), \end{aligned}$$

showing indeed that $L(K_\omega) \cong \Omega_C^{\mathrm{reg}}$. □

3. Riemann–Roch

Theorem III.9. *(***The Riemann–Roch Theorem***) Let C be a curve (usual restrictions) of genus g, and let K be any canonical divisor on C. For every divisor $D \in \mathrm{Div}(C)$,*

$$l(D) - l(K - D) = \deg(D) - g + 1.$$

We omit the proof of the Riemann–Roch theorem, but concentrate on its consequences.

Corollary III.10. (a) $\deg(K) = 2g - 2$,

(b) *If* $\deg(D) > 2g - 2$, *then* $l(D) = \deg(D) - g + 1$.

Proof. By Lemma III.8, $l(K) = g$. Let $D = K$ in the Riemann–Roch Theorem. Then $\deg(K) = 2g - 1 - l(0)$. However, $f \in L(0)$ if and only if it has no poles, and hence $L(0) = k$, showing that $l(0) = 1$. Part (a) follows.

For part (b), suppose $\deg(D) > 2g - 2$. Hence $\deg(K - D) < 0$ and so by Lemma III.7, $l(K - D) = 0$. Hence $l(D) = \deg(D) - g + 1$. □

Part (a) of the corollary gives a very useful method of determining the genus of a curve. Choose any non-zero differential, write down its canonical divisor and compute the degree to get $2g - 2$.

Part (b) of the corollary is the most useful special case of the Riemann–Roch Theorem.

Example III.11. We continue Example II.31. Recall that

$$C : y^2 = x^3 - x, \qquad \operatorname{div}\left(\frac{dx}{y}\right) = 0.$$

Hence $2g - 2 = \deg(0) = 0$ and so $g = 1$. It follows that dx/y is a k-basis for the space of holomorphic differentials Ω_C^{reg}.

4. A Reinterpretation of the Riemann–Roch Space

We will see how the Riemann–Roch Theorem can be used to construct suitable models for curves. First we explain how it can be used to show the existence of certain divisors of given specification. For this we need the following reinterpretation of the Riemann–Roch space.

Theorem III.12.

$$\frac{(L(D) - \{0\})}{k^*} \cong \{D' \in \operatorname{Div}(C) : D' \geq 0 \text{ and } D' \sim D\}.$$

The bijection is given simply by $f \mapsto D + \operatorname{div}(f)$.

Thus, if $l(D) > 0$, then there is a positive k-rational divisor D' linearly equivalent to D.

Proof. Define

$$(L(D) - \{0\}) \longrightarrow \{D' \in \operatorname{Div}(C) : D' \geq 0 \text{ and } D' \sim D\}, \qquad f \mapsto D + \operatorname{div}(f).$$

The map is a surjection by the definition of $L(D)$. Suppose $D + \operatorname{div}(f) = D + \operatorname{div}(g)$ for non-zero functions f, g. Then $\operatorname{div}(f/g) = 0$ and hence $f/g \in k^*$ as required. □

The following corollary is a typical application of the Riemann–Roch Theorem.

Corollary III.13. *Let C be a curve of genus 1 over a field k. Then C has a k-rational divisor of degree 1 if and only if $C(k) \neq \emptyset$.*

Proof. It is clear that any $P \in C(k)$ is a k-rational divisor of degree 1. Suppose now that D is a k-rational divisor of degree 1. By Corollary III.10, $l(D) = 1$. Hence by Theorem III.12, there is a positive k-rational divisor $D' \sim D$. However, $\deg(D') = 1$ as linearly equivalent divisors have the same degree. It follows that $D' = P$ for some point $P \in C(\overline{k})$ that is fixed under the action of Galois. Hence $P \in C(k)$ as required. □

Exercise III.14. Let k be a field of characteristic $\neq 2$. Suppose a, b, $c \in k^*$ and let $C \subset \mathbb{P}^2$ be the curve

$$C : ax^4 + by^4 + cz^4 = 0.$$

(i) Show that C is non-singular of genus of C is 3.
(ii) Write down a positive k-rational divisor D_0 of degree 4.
(iii) Suppose C has a k-rational divisor D_1 of odd degree. Show that C has a k-rational divisor D of degree 1. (**Hint:** Take D to be a suitable linear combination of D_0 and D_1.)
(iv) Continuing with the assumption of (iii), show that either $C(k) \neq \emptyset$, or that there is a positive k-rational divisor of degree 3. (**Hint:** You need to consider two cases, according to whether $l(K - 3D)$ is positive or zero.)

5. Galois Properties

Theorem III.15. *Let $D \in \mathrm{Div}(C)$ (in other words D is a divisor defined over k) and let*

$$L_{\overline{k}}(D) := \{f \in \overline{k}(C)^* \ : \ \mathrm{div}(f) + D \geq 0\} \cup \{0\}.$$

Write $G = \mathrm{Gal}(\overline{k}/k)$. Then

(i) $H^0(G, L_{\overline{k}}(D)) = L(D)$,
(ii) $L_{\overline{k}}(D) = \overline{k} \otimes_k L(D)$,
(iii) $\dim_{\overline{k}} L_{\overline{k}}(D) = \dim_k L(D) = l(D)$.

The proof uses Hilbert's Theorem 90 for GL_n.

Remark: If you are not sure what (ii) is saying, the following fact about tensor products of vector spaces will help clarify. Let V be a finite-dimensional vector space over the field k. Let K be an extension of k. Choose some basis $v_1, \ldots, v_n$ for V over k. Then $V \otimes_k K$ is the vector space over K with basis $v_1, \ldots, v_n$. Knowing this, we see that part (ii) of the theorem immediately implies (iii).

CHAPTER IV

Morphisms

1. Rational Maps and Morphisms of Varieties

Definition IV.1. Let V_1 be an irreducible k-variety.

(i) A **rational map** $V_1 \dashrightarrow \mathbb{A}^n$ (note the dashed arrow) is a "function" ϕ of the form
$$P \mapsto (f_1(P), \dots, f_n(P))$$
for some $f_1, \dots, f_n \in k(V_1)$. We say that ϕ is **defined** (or **regular**) at a point $P \in V_1(\overline{k})$ if and only if each f_i is defined at P.

(ii) A rational map $V_1 \dashrightarrow \mathbb{P}^n$ is a "function" ϕ of the form
$$P \mapsto (f_0(P) : \dots : f_n(P))$$
for some $f_i \in k(V_1)$ (not all identically zero). We say ϕ is **defined** (or **regular**) at $P \in V_1(\overline{k})$ if and only if there is some $g \in k(V)$ such that
$$(gf_0)(P), \dots, (gf_n)(P)$$
are all defined and not all zero.

(iii) If $V_2 \subseteq \mathbb{A}^n$ or $\mathbb{P}^n$ is any k-variety, a rational map $V_1 \dashrightarrow V_2$ is a rational map
$$V_1 \dashrightarrow \mathbb{A}^n \text{ or } \mathbb{P}^n$$
whose image lies inside V_2.

Definition IV.2. A **morphism** $V_1 \to V_2$ is a rational map that is defined at all points $P \in V_1(\overline{k})$.

Example IV.3. Let us see an example of this taken from Silverman's book [**1**, page 17]. Let $C \subset \mathbb{P}^2_k$ be
$$C : x^2 + y^2 = z^2$$
and let
$$\phi : C \to \mathbb{P}^1, \qquad [x : y : z] \mapsto [x + z : y].$$
It appears at first that ϕ is not defined at $[1 : 0 : -1]$. However, note that in the function field of the curve, $x^2 - z^2 = y^2$ and so
$$\phi([x : y : z]) = [x + z : y] = [x^2 - z^2 : y(x - z)] = [-y^2 : y(x - z)] = [-y : x - z].$$
Hence $\phi([1 : 0 : -1]) = [0 : 2]$. Thus if $\text{char}(k) \neq 2$, then ϕ is a morphism.

What happens if $\text{char}(k) = 2$? In this case $x^2 + y^2 - z^2 = (x + y + z)^2$. Thus we can simplify the equation for C:
$$C : x + y + z = 0.$$
Thus $\phi([x : y : z]) = [x + z : y] = [y : y] = [1 : 1]$ again a morphism, but now a constant morphism.

Exercise IV.4. Show that $\phi : \mathbb{P}^2 \to \mathbb{P}^2$, $\phi([x : y : z]) = [x^2 : xy : z^2]$ is not regular at $[0 : 1 : 0]$. Here it is not enough to simply say that if we substitute $[0 : 1 : 0]$ in $[x^2 : xy : z^2]$ we obtain $[0 : 0 : 0]$.

Note that k-varieties (together with morphisms) form a category, and so we can define **endomorphisms** and **isomorphisms**.

Remark. A rational map $V_1 \dashrightarrow V_2$ can be interpreted as a point belonging to $V_2(k(V_1))$.

Definition IV.5. A rational map $\phi : V \dashrightarrow W$ is **dominant** if its image is not contained in any smaller closed subvariety of W.

We obtain a (contravariant) equivalence of categories:

$$\left\{ \begin{array}{c} \text{irreducible } k\text{-varieties,} \\ \text{dominant rational maps} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{finitely generated field extensions of } k, \\ k\text{-algebra homomorphisms} \end{array} \right\}^{\text{op}}$$

$$\begin{array}{rcl} V & \mapsto & k(V) \\ V \overset{\phi}{\dashrightarrow} W & \mapsto & \underbrace{k(W) \hookrightarrow k(V)}_{f \mapsto f \circ \phi}. \end{array}$$

Definition IV.6. Let V_1, V_2 be two irreducible k-varieties. Then V_1 and V_2 are **birationally equivalent** if and only if there are dominant rational maps

$$V_1 \overset{\phi}{\dashrightarrow} V_2, \qquad V_2 \overset{\psi}{\dashleftarrow} V_1$$

such that

$$\left. \begin{array}{l} \psi \circ \phi = \mathrm{id}_{V_1} \\ \phi \circ \psi = \mathrm{id}_{V_2} \end{array} \right\} \text{where defined.}$$

This is equivalent to the existence of an isomorphism $k(V_1) \simeq k(V_2)$ whose restriction to k is the identity.

Example IV.7. Let $V : y^2 = x^3$.

$$\phi : \mathbb{A}^1 \to V, \qquad t \mapsto (t^2, t^3)$$

and

$$\psi : V \dashrightarrow \mathbb{A}^1, \qquad (x, y) \mapsto y/x.$$

ψ is not a morphism since it is not defined at $(0, 0)$. It is easy to see that $\phi \circ \psi$ and $\psi \circ \psi$ are identity maps (where defined) and so $\mathbb{A}^1$ and V are birational.

Let us show that $\mathbb{A}^1$ and V are not isomorphic. To do this it is enough to show that their affine coordinate rings

$$k[t] \qquad \text{and} \qquad k[x, y]/(y^2 - x^3)$$

are not isomorphic k-algebras. The latter is isomorphic to $k[t^2, t^3] \subset k[t]$. But $k[t^2, t^3]$ is not a unique factorization domain as it is not integrally closed, and hence it is not isomorphic to $k[t]$.

2. Rational Maps and Morphisms of Curves

Theorem IV.8. *Let C_1, C_2 be curves (with the usual restrictions). Then any rational map $C_1 \dashrightarrow C_2$ is in fact a morphism.*

For an illustration of this fact, see Example IV.3. This result does not extend to higher dimensional varieties as you saw in Exercise IV.4.

Exercise IV.9. Let $C_0 : y^2 = x^3 + x$. Define $\phi_0 : C_0 \dashrightarrow \mathbb{A}^1$ by $\phi_0(x, y) = x/y$. Observe that ϕ_0 is not a morphism. Let C be the projective closure of C_0 in $\mathbb{P}^2$. Show that C is non-singular and that ϕ_0 extends to a morphism $\phi : C \to \mathbb{P}^1$.

Definition IV.10. Let $\phi : C_1 \to C_2$ be a k-morphism. We say that ϕ is **surjective** if the map $\phi : C_1(\overline{k}) \to C_2(\overline{k})$ is surjective. We say that ϕ is **constant** if $\phi(C_1(\overline{k}))$ is a single point in $C_2(\overline{k})$.

Theorem IV.11. *Let $\phi : C_1 \to C_2$ be a k-morphism of curves. Then ϕ is either constant or ϕ is surjective. In the latter case, ϕ is dominant and we obtain an a monorphism (i.e. an injective homomorphism)*

$$\phi^* : k(C_2) \hookrightarrow k(C_1), \qquad \phi^*(f) = f \circ \phi.$$

Proof. We omit the proof of the first part of the theorem. The proof of the second part is an easy exercise. □

Definition IV.12. Let $\phi : C_1 \to C_2$ be a morphism of curves. We define the **degree** of ϕ as follows:

$$\deg(\phi) = \begin{cases} 0 & \text{if } \phi \text{ is constant} \\ [k(C_1) : k(C_2)] & \text{if } \phi \text{ is non-constant.} \end{cases}$$

If ϕ is non-constant and the extension $k(C_1)/k(C_2)$ is separable, we say that ϕ is **separable**.

3. Fibres

Definition IV.13. Let $\phi : C_1 \to C_2$ be a k-morphism of curves, and let $Q \in C_2(\overline{k})$. The **fibre** of ϕ above Q is

$$\phi^{-1}(Q) := \{P \in C_1(\overline{k}) : \phi(P) = Q\}.$$

Theorem IV.14. *Let $\phi : C_1 \to C_2$ be a non-constant (and hence surjective) k-morphism of curves. Then for all $Q \in C_2(\overline{k})$, the fibre $\phi^{-1}(Q)$ is finite. Moreover, if ϕ is separable, then for all but finitely many $Q \in C_2(\overline{k})$, $\#\phi^{-1}(Q) = \deg(\phi)$.*

Example IV.15. It is much easier to determine the degree using Theorem IV.14 than it is to use the definition. Here is an example. Suppose $\mathrm{char}(k) \neq 2$.

$$C_1 : x_1^4 + y_1^4 + z_1^4 = 0, \qquad\qquad C_2 : x_2^2 + y_2^2 + z_2^2 = 0,$$

and let $\phi : C_1 \to C_2$ be given by $\phi(x_1 : y_1 : z_1) = (x_1^2 : y_1^2 : z_1^2)$. We see that for any $(x_2 : y_2 : z_2) \in C_2(\overline{k})$ with $x_2 y_2 z_2 \neq 0$, $\#\phi^{-1}(x_2 : y_2 : z_2) = 4$ (yes 4 and not 8). Hence ϕ has degree 4.

4. Ramification

Let $\phi : C_1 \to C_2$ be a non-constant separable k-morphism of curves. Theorem IV.14 tells us that all but finitely many fibres have cardinality equal to $\deg(\phi)$. In fact this is true for all fibres provided that each point is counted with the correct multiplicity. The correct multiplicity is given by the ramification index.

Definition IV.16. Let $\phi : C_1 \to C_2$ be a non-constant k-morphism of curves (separable or otherwise). Suppose $\phi(P) = Q$ for some $P \in C_1(\overline{k})$ and $Q \in C_2(\overline{k})$. Let t_Q be a uniformizer for C_2 at Q. Then $\phi^*(t_Q)(P) = t_Q(\phi(P)) = t_Q(Q) = 0$.

Hence $\mathrm{ord}_P(\phi^*(t_Q)) \geq 1$. We call $\mathrm{ord}_P(\phi^*(t_Q))$ the **ramification index of ϕ at P** and is denoted by

$$e = e_\phi(P) = e_{P/Q}.$$

It is easy to show that the ramification index is well-defined (that is, independent of the choice of uniformizer t_Q).

If $e_\phi(P) = 1$, we say that ϕ is **unramified (or étale) at** P. The morphism ϕ is said to be **unramified (or étale)** if $e_\phi(P) = 1$ for all $P \in C(\overline{k})$.

If $e_\phi(P) > 1$, we call P a **ramification point** and call $Q = \phi(P)$ a **branch point**.

Theorem IV.17. *Let $\phi : C_1 \to C_2$ be a non-constant k-morphism of curves (separable or otherwise). For all $Q \in C_2(\overline{k})$,*

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi).$$

The following corollary is immediate.

Corollary IV.18. *$Q \in C_2(\overline{k})$ is a branch point if and only if $\#\phi^{-1}(Q) < \deg(\phi)$.*

Example IV.19. We shall continue with Example IV.15. We would like to determine the branch points, the ramification points and the ramification indicies. It is clear from the previous calculation that the branch points are $(x_2 : y_2 : z_2) \in C_2(\overline{k})$ with $x_2 y_2 z_2 = 0$. Hence there are six branch points.

Fix $i^2 = -1$ and $\zeta^2 = i$ in $\overline{k}$. The six branch points are

$$(0 : \pm i : 1), \qquad (\pm i : 0 : 1), \qquad (\pm i : 1 : 0).$$

Take one of these $Q = (0 : i : 1)$, and let $P = (0 : \zeta : 1) \in \phi^{-1}(Q)$. We shall determine the ramification index at the point $P = (0 : \zeta : 1)$. As usual, it is more convenient to work with affine patches:

$$C_1 \cap \mathbb{A}^2 : x_1^4 + y_1^4 = 1, \qquad C_2 \cap \mathbb{A}^2 : x_2^2 + y_2^2 = 1, \qquad \phi(x_1, y_1) = (x_1^2, y_1^2).$$

On the chosen affine patches, $P = (0, \zeta)$ and $Q = \phi(P) = (0, i)$. One checks that x_1 is a uniformizer at P and x_2 is a uniformizer at Q. Now $\phi^*(x_2) = x_2 \circ \phi = x_1^2$, and so

$$e_P = \mathrm{ord}_P(x_1^2) = 2.$$

In fact, above each branch point there are precisely two ramification points with ramification index 2. In other words there are 12 ramfication points with ramification index 2.

5. Hurwitz's Theorem

Definition IV.20. Let $\phi : C_1 \to C_2$ be a separable k-morphism of curves. We shall say that the ramification at $P \in C_1(\overline{k})$ is **tame** is $\mathrm{char}(k) \nmid e_\phi(P)$, otherwise the ramification at P is said to be **wild**.

Theorem IV.21. ***(Hurwitz's Theorem)*** *Let $\phi : C_1 \to C_2$ be a separable k-morphism of curves and suppose that all the ramification is tame. Write g_1, g_2 respectively for the genus of C_1 and C_2 and d for the degree of ϕ. Then*

$$2g_1 - 2 = d(2g_2 - 2) + \sum_{P \in C_1(\overline{k})} (e_P - 1).$$

Example IV.22. We continue with Examples IV.15 and IV.19. We determined the degree $d = 4$ and that there are precisely 12 ramification points each with ramification index 2. Applying Hurwitz's Theorem we obtain

$$2g_1 - 2 = 4(2g_2 - 2) + 12.$$

However, C_2 is a conic and so C_2 is isomorphic to $\mathbb{P}^1$ over $\overline{k}$. Hence $g_2 = g(C_2) = g(\mathbb{P}^1) = 0$. It follows that $g(C_1) = g_1 = 3$.

CHAPTER V

Models of Curves

What do curves of a given genus look like? In this chapter we write down models for curves of small genus.

1. An Embedding Theorem

Definition V.1. Let $C \subset \mathbb{P}^n$ be a projective curve. The **degree** of C is defined to be $\#(H \cap C)$ for any hyperplane $H \subset \mathbb{P}^n$ not containing C, where the elements of $\#(H \cap C)$ are counted with appropriate multiplicities.

Theorem V.2. *Let C be a curve over k be a curve of genus g. Let $D \in \mathrm{Div}(X)$ be a k-divisor satisfying* $\deg(D) \geq 2g+1$. *Let $f_0, \dots, f_n$ be a k-basis for the Riemann–Roch space $L(D)$. (By the Riemann–Roch Theorem $n = \deg(D) - g$.) Then*

$$\varphi_D : C \to \mathbb{P}^n, \qquad P \mapsto (f_0(P) : \cdots : f_n(P))$$

*maps C **isomorphically** to its image $C' \subset \mathbb{P}^n$. The curve C' is defined over k $\deg(C') = \deg(D)$.*

2. Curves of Genus 0

Theorem V.3. *Let C be a curve of genus 0 defined over k. Then C is isomorphic (over k) to a smooth plane curve* [1] *of degree 2 (i.e. a conic). Moreover, if $C(k) \neq \emptyset$ then C is isomorphic over k to $\mathbb{P}^1$.*

Proof. We will apply Theorem V.2. For this we need to start with some k-divisor of degree ≥ 1. Since all we know is the genus of C, the only divisors that we know anything about are the canonical divisors. Let $K \in \mathrm{Div}(C)$ be a canonical divisor; then $\deg(K) = 2g - 2 = -2$. So it makes sense to take $D = -K$, which has degree $\deg(D) = 2$. In the notation of Theorem V.2, $n = \deg(D) - g = 2$. Thus we obtain an embedding $\varphi_D : C \hookrightarrow \mathbb{P}^2$ defined over k whose image C' has degree 2. Moreover, since C is smooth and φ_D is an embedding, C' is also smooth. This proves the first part of the theorem.

For the second part, let $P \in C(k)$. Take $D = P$ which has degree $\deg(D) = 1 \geq 2g + 1$. Then $n = \deg(D) - g = 1$, and $\varphi_D : C \hookrightarrow \mathbb{P}^1$ is an embedding defined over k. This must be surjective by Theorem IV.11, and so C is isomorphic to $\mathbb{P}^1$ over k. □

[1] A plane curve is a curve in $\mathbb{P}^2$

3. Curves of Genus 1

Any canonical divisor of a curve of genus 1 has degree $2g-2=0$, so we are not able to write down a model for C over k as we did for curves of genus 0. We are able to write down models if we assume the existence of k-divisors of a given degree.

Theorem V.4. *Let C be a curve of genus 1 defined over k. Suppose that $C(k) \neq \emptyset$. Then there is k-isomorphism*

$$\varphi : C \to E$$

where $E \subset \mathbb{P}^2$ is an elliptic curve given by a (non-singular) Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in k, \tag{1}$$

such that $\varphi(P) = \infty$.

Proof. Let $n \geq 1$. Recall that $L(nP)$ is the space of functions that are regular everywhere except for a pole at P of order *at worst n*. The Riemann–Roch Theorem tells us that $l(nP) = n$ for $n \geq 1$. We shall write k-bases for the Riemann–Roch spaces $L(nP)$ for $n = 1, \dots, 6$. Since $L(nP) \subset L((n+1)P)$, a k-basis for $L((n+1)P)$ can be obtained from a k-basis for $L(nP)$ by adding an extra element belonging to $L((n+1)P) - L(P)$.

Observe that $k \subset L(P)$. As $L(P)$ is 1-dimensional, $L(P) = k$ and $\{1\}$ is a k-basis for $L(P)$.

Next $L(2P)$ is 2-dimensional and contains $L(P) = k$ as a subspace, so we must have a basis for $L(2P)$ of the form $\{1, x\}$ where $x \in L(2P) - L(P)$; note that x has a pole of exact order 2 at P.

$L(3P)$ has a basis $\{1, x, y\}$ where y has a pole of exact order 3. Note that x^2 has a pole of exact order 4 at P, and so $x^2 \in L(4P) - L(3P)$ and so $\{1, x, y, x^2\}$ is a k-basis for $L(4P)$. Similarly $\{1, x, y, x^2, xy\}$ is a k-basis for $L(5P)$.

Now $L(6P)$ is 6-dimensional and contains the seven elements $1, x, y, x^2, xy, x^3, y^2$, which must be linearly dependent. Hence we have

$$c_1y^2 - c_2x^3 = c_3xy + c_4x^2 + c_5y + c_6x + c_7, \qquad c_i \in k, \tag{2}$$

where not all the c_i are zero. If $c_1 = c_2 = 0$ then $\{1, x, y, x^2, xy\}$ is linearly dependent, which contradicts that fact that it is a basis for $L(5D)$. Hence at least one of c_1, c_2 is non-zero. As x^3 and y^3 have poles of order 6 at P, neither belongs to $L(5P)$. However, by (2), $c_1y^2 - c_2x^3 \in L(5P)$ and so $c_1 \neq 0 \neq c_2$. Now replace x by c_1x/c_2 and y by c_1y/c_2; this does not at all affect the above as it does not change the orders of the poles at P. Simplifying now gives

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

By Theorem V.2, $\varphi := \varphi_{3P}$ is an embedding $C \hookrightarrow \mathbb{P}^2$ given by $\varphi(Q) = (x(Q) : y(Q) : 1)$ (since $x, y : 1$ is a basis for $L(3P)$). We see by the above that the image must equal E

Finally $\varphi(P) = \infty$ as x, y have poles at P. □

4. Hyperelliptic Curves

Definition V.5. A *hyperelliptic curve* over k is a curve C of genus ≥ 2 that has a degree 2 separable map π to a curve C' of genus 0.

It is natural to ask what C looks like in terms of explicit equations.

Assumption. We shall suppose that $\mathrm{char}(k) \neq 2$ and $C'(k) \neq \emptyset$. Note that the second assumption is certainly true if $C(k) \neq \emptyset$.

By Theorem V.3, $C' \cong_k \mathbb{P}^1$, and so $k(C') = k(x)$ where $k[x]$ is the coordinate ring of $\mathbb{A}^1$. Since $\pi : C \to C'$ has degree 2, the extension $k(C)/k(C')$ has degree 2. Thus $k(C) = k(x)(\sqrt{f})$ for some non-square element $f \in k(x)$. As $k[x]$ is a unique factorization domain, we can suppose that $f \in k[x]$ and square-free. Hence $k(C)$ is the field of fractions of the ring

$$k[x, y]/(y^2 - f(x));$$

in other words, it is the function field of the affine curve $y^2 = f(x)$. Since the genus is at least 2 we know that $\deg(f) \geq 4$. In fact we shall see shortly that $\deg(f) \geq 5$.

Since $y^2 = f(x)$ gives an affice model for C, we can think of C as being a curve in $\mathbb{P}^2$ with $C \cap \mathbb{A}^2 : y^2 = f(x)$. Homogenising we obtain a projective model $C : y^2 z^{n-2} = F(x, z)$ where $n = \deg(f)$. It is easy to show that this model is singular at infinity (i.e. at $C \cap \{z = 0\}$). We do not like this because of the singularity.

We shall now describe the standard way of constructing a **smooth** projective model for the hyperelliptic curve C. Let $g \in \mathbb{Z}_{\geq 0}$ be the unique integer such that $\deg(f) = 2g + 1$ or $\deg(f) = 2g + 2$. We will eventually see that g happens to be the genus of C.

To start with recall that the projective line is the union of two affine patches: $\mathbb{P}^1 = \mathbb{A}^1 \cup \mathbb{A}^1$. We give the first patch the coordinate ring $k[x]$ and the second $k[x']$. The two patches are "glued" together using the identification

$$\mathbb{A}^1 \cap \{x \neq 0\} \longleftrightarrow \mathbb{A}^1 \cap \{x' \neq 0\}, \qquad x' = \frac{1}{x}.$$

We have a degree 2 separable morphism $\pi : C \to \mathbb{P}^1$; we shall describe C by describing the parts (or patches) of C lying above the two affine patches $\mathbb{A}^1$ of $\mathbb{P}^1$.

Patch 1. This is simply given by $C_1 : y^2 = f(x)$ in $\mathbb{A}^2$, with the map $\pi : C_1 \to \mathbb{A}^1$ given by $(x, y) \mapsto x$.

Patch 2. Let $f^{\mathrm{rev}}(x') = x'^{2g+2} f(1/x')$. The second affine patch is $C_2 : y'^2 = f^{\mathrm{rev}}(x')$ in $\mathbb{A}^2$, with the map $\pi : C_2 \to \mathbb{A}^2$ given by $(x', y') \mapsto x'$.

Finally C is given by $C = C_1 \cup C_2$ where the two patches are "glued" together using the identification

$$C_1 \cap \{x \neq 0\} \longleftrightarrow C_2 \cap \{x' \neq 0\}, \qquad x' = \frac{1}{x}, \quad y' = \frac{y}{x^{g+1}}.$$

Example V.6. This construction is quite natural if we try to work out what happens at ∞ on the first affine model $y^2 = f(x)$. For concretness, look at $y^2 = x^6 + 2$. We would like to know what happens when x is 'large'. We divide out by x^6 and we obtain

$$\left(\frac{y}{x^3}\right)^2 = 1 + 2\left(\frac{1}{x}\right)^6.$$

This has the form $y'^2 = 1 + 2x'^6$. Now we can ask, how many points are there at ∞? The points at ∞ (relative to the first patch) are the points where $x' = 0$ on the second patch, so we have two points at infinity: $(x', y') = (0, \pm 1)$.

Now look at another example, $y^2 = 3x^5 + 2$. Dividing by x^5 does not give us a square on the left-hand side. So we divide by x^6 instead. We obtain

$$\left(\frac{y}{x^3}\right)^2 = 3\left(\frac{1}{x}\right) + 2\left(\frac{1}{x}\right)^6.$$

This now has the form $y' = 3x' + 2{x'}^2$. There are is now exactly one point at ∞ (relative to the first patch), which is $(x', y') = (0, 0)$.

Lemma V.7. *The curve $C = C_1 \cup C_2$ is smooth (i.e. each affine patch C_1 and C_2 is smooth). If $\deg(f)$ is even then there is exactly two points at ∞, and the ramification points of the map $\pi : C \to \mathbb{P}^1$ are the points $(x, y) \in C_1$ where $f(x) = 0$. If $\deg(f)$ is odd then there is exactly one point at ∞, and the ramification points of the map $\pi : C \to \mathbb{P}^1$ are the points $(x, y) \in C_1$ where $f(x) = 0$ and the unique point at ∞ (i.e. $(x', y') = (0, 0)$).*

Proof. The proof is mostly left as an exercise. To show that the affine patch $y^2 = f(x)$ is smooth, we note that the singularities are given by

$$y^2 = f(x), \qquad 2y = 0, \qquad f'(x) = 0.$$

Since $\mathrm{char}(k) \neq 2$ we must solve $f(x) = f'(x) = 0$. As f is squarefree, there is no solution, showing that the affine patch $y^2 = f(x)$ is smooth. □

Theorem V.8. *The genus of C is g.*

Proof. We do this by apply the Hurwitz Theorem IV.21 to the degree 2 separable morphism $\pi : C \to \mathbb{P}^1$. Write g_C for the genus of C. The Hurwitz formula gives

$$g_C = -1 + \frac{1}{2}\sum(e_P - 1).$$

As π has degree 2, $e_P = 1$ everywhere except at the ramification points where $e_P = 2$. Hence $\sum(e_P - 1)$ counts the number of ramification points. By Lemma V.7 this is $2g + 2$ regardless of whether $\deg(f)$ is even or odd. Hence $g_C = g$ as required. □

4.1. Regular Differentials on Hyperelliptic Curves. The genus of a curve C what originally defined to be the dimension of the space Ω_C^{reg} of regular differentials on C. For the hyperelliptic curve C we are studying above, $\dim \Omega_C^{\mathrm{reg}} = g = g_C$.

Proposition V.9. *The differentials*

$$\frac{dx}{y}, \frac{xdx}{y}, \ldots, \frac{x^{g-1}dx}{y}$$

form a k-basis for Ω_C^{reg}.

Proof. Since we have the number of elements right, all we have to do is prove that these differentials are regular and linearly independent. The linear independence follows immediately from the linear independence of $1, x, \ldots, x^{g-1}$ in $k[x] \subset k(x) \subset k(x)(\sqrt{f})$ which is the function field of the curve C. We leave the proof of regularity as an exercise, but before you do this, revise Example II.31 and see the Example V.10 below. □

Example V.10. Let $C : y^2 = x^7 + 1$. When we write something like this, what we mean is let C be the smooth projective curve with first affine patch $C_1 : y^2 = x^7 + 1$ and second affine patch C_2 constructed in the usual way: $C_2 : {y'}^2 = x' + {x'}^8$ with $x' = 1/x$ and $y' = y/x^4$. Note that C has genus 3. In this example we show that dx/y is regular at the unique point at ∞. To do this, note that the point at ∞ is $(x', y') = (0, 0)$ and that y' is a uniformizer. So we need to express dx/y in terms of dx'.

We start with $x' = {y'}^2 - {x'}^8$, and repeatedly substitute for x' to obtain x' as a power series in y':

$$x' = {y'}^2 - {y'}^16 + \cdots .$$

Hence

$$x = \frac{1}{x'} = {y'}^{-2} + {y'}^{12} + \cdots ,$$

so that

$$dx = (-2{y'}^{-3} + 12{y'}^{11} + \cdots)dy'.$$

However,

$$\frac{1}{y} = \frac{{x'}^4}{y'} = \frac{({y'}^2 + \cdots)^4}{y'} = {y'}^7 + \cdots .$$

Hence

$$\frac{dx}{y} = (-2{y'}^4 + \cdots)dy',$$

which shows that dx/y is regular at ∞.

5. The Canonical Map

Definition V.11. Let C be a curve of genus ≥ 2 over a field k, and let K be any canonical divisor. Let $f_0, \dots, f_{g-1}$ be a basis for the Riemann-Roch space $L(K)$. The **canonical map** is given by

$$\varphi_K : C \to \mathbb{P}^{g-1}, \qquad \varphi(P) = (f_0(P) : \ldots : f_{g-1}(P)).$$

Theorem V.12. *Let C be a curve of genus $g \geq 2$ over a field k. If C is* ***not*** *hyperelliptic then φ_K embeds C as a curve of degree $2g - 2$ curve in $\mathbb{P}^{g-1}$. If C is hyperelliptic then $\varphi_K(C)$ has genus 0 and $\varphi_K : C \to \varphi_K(C)$ has degree 2.*

Proof. We omit the proof, but observe that for $C : y^2 = f(x)$ (hyperelliptic), $\varphi_K(x, y) = (1 : x : \cdots : x^{g-1})$ which is clearly a degree 2 map since $\varphi_K(x, y) = \varphi_K(x, -y)$. □

The theorem will help us classify curves of genus 2 and 3.

6. Curves of Genus 2

Theorem V.13. *Suppose* $\mathrm{char}(k) \neq 2$. *Every curve of genus* 2 *over k is hyperelliptic and in fact has the model $y^2 = f(x)$ where $f \in k[x]$ is squarefree of degree* 5 *or* 6.

Proof. Suppose C has genus 2 but is not hyperelliptic. The canonical map $\varphi_K : C \to \mathbb{P}^1$ is an embedding and so an isomorphism, which contradicts the fact that C has genus 2. Hence C must be hyperelliptic. The rest follows from Exercise **??** below. □

Exercise V.14. Let C be a hyperelliptic curve, and let C' be the underlying curve of genus 0 (see Definition V.5). Show that if the genus of C is even then $C'(k) \neq \emptyset$.

7. Curves of Genus 3

Theorem V.15. *Let C be a curve of genus 3 over a field k with characteristic $\mathrm{char}(k) \neq 2$.*

(i) *Either C is isomorphic to a hyperelliptic curve with plane model $C : y^2 = f(x)$, where f is squarefree with degree 7 or 8,*

(ii) *or there is a morphism $\pi : C \to C'$ of degree 2 to a curve C'/k of genus 0, where $C'(k) = \emptyset$ and π is ramified at precisely 8 points,*

(iii) *or C is isomorphic to a smooth plane quartic curve in $\mathbb{P}^3$.*

Proof. (i) and (ii) are the familiar dichotomy for hyperelliptic curves; the numer of ramification points in (ii) follows from the Hurwitz Theorem.

Thus we may suppose that C is non-hyperelliptic, and all we require is a proof of (iii). By Theorem V.12, the canonical map embeds C as a curve of degree 4 in $\mathbb{P}^2$, in other words, a plane quartic curve. Since C is smooth, its image under the embedding must be smooth. □

Bibliography

[1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106**, Springer–Verlag, 1986.

[2] J. W. S. Cassels, *Diophantine equations with special reference to curves of genus* 1, J. L. M. S. **41** (1966), 193–291.