Around the Riemann-Roch Theorem

Ibrahim Emir Cicekli, Michele Tamagnone

June 2024

Contents

Chapter 1

Algebraic Varieties

Throughout this whole mémoire, k will denote an algebraically closed field. In this preliminary chapter, we recall the theory of algebraic varieties and state some preliminary results which will be useful later on. A certain familiarity with the topics of this chapter is assumed, and many facts will simply be presented without giving extensive proofs.

1.1 Varieties and Morphisms

Throughout this whole mémoire, k will denote an algebraically closed field. For n a positive integer, we will denote by $\mathbb{A}^n = k^n$ and $\mathbb{P}^n = (k^n \setminus 0)/k^\times$ the *affine n-space* and the *projective n-space* over k respectively, both endowed with the Zariski topology.

We denote the coordinates of $\mathbb{A}^n$ by $X_1, \ldots, X_n$, and those of $\mathbb{P}^n$ by $X_0, \ldots, X_n$. If I is an ideal of $k[X_1, \ldots, X_n]$ (respectively, homogeneous ideal of $k[X_0, \ldots, X_n]$), then $\mathrm{V}(I)$ denotes the closed subset of $\mathbb{A}^n$ (resp. $\mathbb{P}^n$) consisting of the common zeros of elements of I. If $X \subset \mathbb{A}^n$ (resp. $X \subset \mathbb{P}^n$), $\mathrm{I}(X)$ denotes the ideal of $k[X_1, \ldots, X_n]$ (resp. homogeneous ideal of $k[X_0, \ldots, X_n]$,) of polynomials that vanish on all points of X. By the Nullstellensatz, $\mathrm{I}(\mathrm{V}(I)) = \sqrt{I}$ for all ideals $I \subset k[X_1, \ldots, X_n]$, and there is an analogous homogeneous statement.

Definition 1.1. A nonempty irreducible subset of $\mathbb{A}^n$ or $\mathbb{P}^n$, endowed with the induced topology, is called a *quasi-projective variety* or more simply *variety.*

Closed varieties are called *affine varieties* or *projective varieties* depending if they are contained in $\mathbb{A}^n$ or $\mathbb{P}^n$ respectively. Any variety is an open subset of a projective variety, and any open subset of a variety is a variety. Any closed subset V of $\mathbb{A}^n$ or $\mathbb{P}^n$ can be written uniquely as the union of a finite number of varieties called *irreducible components* and it is a variety if and only if $\mathrm{I}(X)$ is prime.

To define a category, we need morphisms.

Definition 1.2. Let X be a variety. If $X \subset \mathbb{A}^n$, a function $f\colon X \to k$ is said to be *regular at a point* $P \in X$ if there is an open neighborhood U of P in X and polynomials $G, H \in k[X_1, \ldots, X_n]$, with H vanishing nowhere in U, such that $f(Q) = G(Q)/H(Q)$ for all $Q \in U$. If instead $X \subset \mathbb{P}^n$, we require the polynomials $G, H \in k[X_0, \dots, X_n]$ to be homogeneous of the same degree.

We say that f is *regular on* X if it is regular at every point of X. For an open subset U of X, we denote the k-algebra of all regular functions on U by $\mathcal{O}_X(U)$.

Regular functions are continuous if view $k = \mathbb{A}^1$ with the Zariski topology. If X is a variety and f a regular function on X, we denote set of zeroes of f, which is a closed subset of X, again by $\mathrm{V}(f)$.

Remark 1.3. If X is a subvariety of $\mathbb{A}^n$ and we embed $\mathbb{A}^n$ into $\mathbb{P}^n$ using an affine chart, the two definitions of regular functions obtained by viewing $X \subset \mathbb{A}^n$ or $X \subset \mathbb{P}^n$ coincide.

Definition 1.4. A *morphism* of varieties is a continuous map $\varphi\colon X \to Y$ such that for any open subset V of Y and any regular function f on U, the precomposition $f\varphi$ is regular on $f^{-1}V$. The induced map on the rings of regular functions is denoted $\varphi^*\colon \mathcal{O}_Y(V) \to \mathcal{O}_X(f^{-1}V)$.

We thus a category to work in, consisting of quasi-projective varieties and morphism.

An important fact is that this category admits products: given two quasi-projective varieties X and Y the underlying set of the product $X \times Y$ is the Cartesian product, but it is endowed with a topology finer than the product topology. It is the topology induced by the Segre embedding $\mathbb{P}^n \times \mathbb{P}^m \hookrightarrow \mathbb{P}^{nm+n+m}$. For example, the closed subsets of $\mathbb{P}^n \times \mathbb{P}^m$ are defined by the vanishing of bi-homogeneous polynomials of $k[X_0, \dots, X_n, Y_0, \dots, Y_n]$ (that is, polynomials which are homogeneous both when considered as polynomials in the X_i's and when considered as polynomials in the Y_j's.)

Let X be a variety and consider the set of couples (U, f) where $U \subset X$ is a nonempty open set and f is a regular function on U. If (V, g) is another pair, then $U \cap V$ is nonempty because X is irreducible; we introduce an equivalence relation $(U, f) \sim (V, g)$ if $f = g$ on $U \cap V$. Transitivity is given by the fact that if two regular functions coincide on an open set, then (by irreducibility) they coincide everywhere they are defined. The equivalence classes are called *germs* and are denoted by $\langle U, f\rangle$ or, without ambiguity, simply by f.

Definition 1.5. The quotient set consisting of germs of regular functions as defined above has a natural field structure. It is denoted by $k(X)$, and is called the *field of rational functions* of the variety. The set of germs of regular functions defined at a point $P \in X$ is called the *local ring of* X *at* P and is denoted by $\mathcal{O}_{X,P}$.

Observe that $\mathcal{O}_{X,P}$ is indeed a local ring: its maximal ideal consists of germs of functions that vanish at P, and is denoted by $\mathfrak{m}_P(X)$ or simply by $\mathfrak{m}_P$ whenever the variety we are talking about is clear. Evaluation at P gives a canonical isomorphism $\mathcal{O}_{X,P}/\mathfrak{m}_P = k$. For neighborhood U of P in X we have canonical isomorphisms $\mathcal{O}_{X,P} = \mathcal{O}_{U,P}$ and $K(U) = k(X)$.

We turn our focus back on affine varieties. Let $X \subset \mathbb{A}^n$ be an affine variety.

Definition 1.6. The quotient ring $k[X_1, \dots, X_n]/\,\mathrm{I}(X)$ is called the *coordinate ring* of the affine variety X; it is denoted by $k[X]$.

Proposition 1.7. *For an affine variety X, we have the following canonical isomorphisms:*

- $\mathcal{O}_X(X) = k[X]$*;*
- $k(X) = \operatorname{Frac} k[X]$*, the field of fractions of the coordinate ring;*
- *if $P \in X$ then $\mathcal{O}_{X,P} = k[X]_{\mathfrak{m}_P}$, the localization of $k[X]$ at the maximal ideal consisting of functions that vanish at P. If $P = (a_1, \dots, a_n)$ and x_i denotes the residue class of X_i in $k[X]$, then $\mathfrak{m}_P = (x_1 - a_1, \dots, x_n - a_n)$.*

Proof. These are all consequences of the Nullstellensatz. See [Har77, Thereom 3.2] □

From the first point of the above proposition we can get the following

Theorem 1.8. *There is an equivalence of categories between affine algebraic varieties and finitely generated k-algebras given by the functor $X \mapsto k[X]$.*

More generally, if X is an affine variety and Y is any quasi-projective variety there is a canonical isomorphism between morphisms $Y \to X$ and k-algebras morphisms $k[X] \to \mathcal{O}_Y(Y)$.

We extend the notion of affine variety to include any quasi-projective variety that is isomorphic to an irreducible closed subset of $\mathbb{A}^n$ for some n. An important example is contained in the following

Proposition 1.9. *Let X be an affine variety and f a regular function on X. Then the open subvariety $X \setminus \mathrm{V}(f)$ is affine, and*

$$k[X \setminus \mathrm{V}(f)] = k[X]_f,$$

the localization of $k[X]$ at the element f.

Any variety has a basis consisting of affine varieties.

There is an analogous to the coordinate ring for projective varieties, but Theorem 1.8 does not hold.

Definition 1.10. For $Y \subset \mathbb{P}^n$ a projective variety, the quotient ring $S(Y) = k[X_0, \dots, X_n]/\mathrm{I}(Y)$ has a natural graded ring structure. It is called the *homogeneous coordinate ring* or the *graded ring associated* to the projective variety Y.

Differently from the coordinate ring of an affine variety, the elements of $S(Y)$ cannot be interpreted as functions on Y (indeed $\mathcal{O}_Y(Y) = k$). The graded ring structure on $S(Y)$ is inherited from the grading of the polynomial ring $k[X_0, \dots, X_n]$ since the ideal $\mathrm{I}(Y)$ is homogeneous.

The field of rational functions $k(Y)$ consists of quotients f/g of elements of $S(Y)$ of the same degree, while the elements of the local ring $\mathcal{O}_{Y,P}$ for $P \in Y$ are of the form f/g, with $f, g \in S(Y)$ of the same degree and $g(P) \neq 0$.

1.2 Dimension of Varieties and Rational Maps

To define the dimension of a variety, we appeal to the notion of the transcendence degree in field theory. Let K be a finitely generated extension of k. We say that $x_1, \dots, x_n \in K$ are *algebraically independent* if there is no nonzero polynomial $F \in k[X_1, \dots, X_n]$ such that $F(x_1, \dots, x_n) = 0$. If furthermore K is algebraic over $k(x_1, \dots, x_n)$, then $x_1, \dots, x_n$ is called a *transcendence basis* of K over k.

Definition 1.11. The *transcendence degree* of K over k is defined as the cardinality of any transcendence basis, and is denote by $\operatorname{tr.deg}_k K$. If $\operatorname{tr.deg}_k K = n$, we also say that K is a *function field in n variables* over k.

These notions are analogous to linear independence, basis and dimension for vector spaces: $x_1, \dots, x_n$ is a minimal set such that $K|k(x_1, \dots, x_n)$ is algebraic if and only if it is a maximal set of algebraically independent elements of K. Any algebraically independent set can be completed into a transcendence basis, and any set $x_1, \dots, x_n$ such that $K|k(x_1, \dots, x_n)$ is algebraic contains a transcendence basis. The cardinality of any two transcendence basis for K over k are the same, so that Definition 1.11 is well-posed.

Definition 1.12. The *dimension* of a variety is defined as $\dim X = \operatorname{tr.deg}_k k(X)$, the transcendence degree of its field of rational functions. A *curve* is a variety of dimension one.

Remark 1.13. There is a more intrinsic definition of dimension which we could have given: usually the dimension of a variety is defined as the highest n for which there exists a chain $\varnothing \neq Z_0 \subsetneq \cdots \subsetneq Z_n$ of irreducible closed nonempty subsets of X.

Since both these definitions are left unaltered if we replace X by one of its open subsets, we may assume that X is affine. Then Noether normalization [AK13, Lemma 15.1] and the going-up theorem [AM69, Theorem 5.11] imply that $\operatorname{tr.deg}_k k(X)$ is equal to the Krull dimension of the coordinate ring $k[X]$ (i.e the length of a maximal chain of ascending prime ideals.) Since for an affine variety there is a bijective correspondence between prime ideals of the coordinate ring and nonempty irreducible closed subset, we see that the two definitions are equivalent.

In particular, a variety has dimension 0 iff it is a point and the only proper closed subsets of a curve are finite.

Rational Maps

Definition 1.14. Let X and Y be two varieties. The germ $\langle U, \psi \rangle$ of a morphism $\psi \colon U \to Y$, with U an open subset of X, is called a *rational map* between X and Y. Again, without ambiguity we also refer to it as φ and we use the notation

$$\psi \colon X \dashrightarrow Y.$$

The *domain* of ψ is the biggest open set over which it is defined. A rational map is said to be *birational* if it has a rational inverse, and in this case we say that X and Y are *birationally equivalent.*

A rational map $\psi\colon X \to Y$ is said to be *dominating* if its image is dense in Y; thanks to this assumption ψ induces a well defined morphism of field extensions over k

$$\psi^*\colon k(Y) \to k(X).$$

Vice-versa, it can be shown that any morphism $k(Y) \to k(X)$ fixing k is induced by a dominating rational map. We can reformulate these facts by saying that the functor $X \mapsto k(X)$ from the category of quasi-projective varieties with arrows birational maps to the category of extensions of k is fully faithful. Two varieties are birationally equivalent iff their function fields are isomorphic.

Theorem 1.15. *Any function field in one variable is the function field of an affine curve. Every curve is birationally equivalent to an affine plane curve.*

Proof. Let K be a function field in one variable. Since $\operatorname{tr.deg} K = 1$ any $x \in K \smallsetminus k$ is a transcendence basis for K over k, so $K|k(x)$ is a finite algebraic extension. If $\operatorname{char} k = 0$, then this extension is also separable so by the Primitive Element Theorem there is some $y \in K$ such that $K = k(x, y)$. If $F \in k(x)[Y]$ is the minimal polynomial of y, clearing denominators yields an irreducible polynomial F' with coefficients in k such that $F'(x, y) = 0$. Then $k(\mathrm{V}(F)) = \operatorname{Frac} k[X, Y]/(F) = k(x, y) = K$, so X is birationally equivalent to $\mathrm{V}(F)$. If $\operatorname{char} k = p$ then the extension $K|k(x)$ need not to be separable for all x; however [ZS75, Ch II, Theorem 31] ensures that there is a choice of x so that it is. $\square$

1.3 Ideals with a Finite Number of Zeros

To simplify the exposition later on, we give some results regarding ideals $I \subset k[X_1, \dots, X_n]$ with a finite number of zeros, i.e. such that $\mathrm{V}(I)$ is finite.

Proposition 1.16. *Let I be an ideal of $k[X_1, \dots, X_n]$. Then $\mathrm{V}(I)$ is finite if and only if $k[X_1, \dots, X_n]/I$ is a finite dimensional vector space; in this case the number of points in $\mathrm{V}(I)$ is at most $\dim_k k[X_1, \dots, X_n]/I$.*

Proof. Suppose $\mathrm{V}(I) = \{P_1, \dots, P_r\}$ is finite and let $\mathfrak{m}_i = \mathrm{I}(P_i)$. We have

$$\mathrm{V}(I) = \mathrm{V}(\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r),$$

so $\sqrt{I} = \sqrt{\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r} = \sqrt{\mathfrak{m}_1} \cap \dots \cap \sqrt{\mathfrak{m}_r} = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r$. By Noetherianity, there is an integer N such that $I \supset (\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r)^N = \mathfrak{m}_1^N \cap \dots \cap \mathfrak{m}_r^N$, and this inclusion gives a surjective homomorphism

$$k[X_1, \dots, X_n]/(\mathfrak{m}_1^N \cap \dots \cap \mathfrak{m}_r^N) \to k[X_1, \dots, X_n]/I.$$

The Chinese Remainder Theorem gives

$$\begin{aligned} &k[X_1, \dots, X_n]/(\mathfrak{m}_1^N \cap \dots \cap \mathfrak{m}_r^N) = \\ &\qquad = k[X_1, \dots, X_n]/\mathfrak{m}_1^N \times \dots \times k[X_1, \dots, X_n]/\mathfrak{m}_r^N, \end{aligned}$$

and the fact that $\dim_k k[X_1, \dots, X_n]/I$ is finite follows from the fact that each $k[X_1, \dots, X_n]/\mathfrak{m}_i^N$ is finite dimensional over k.

Vice-versa, if $\dim_k k[X_1, \dots, X_n]/I$ is finite for any finite set $P_1, \dots, P_r$ of points of $\mathrm{V}(I)$ the inclusion $I \subset \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r$ gives a surjective map

$$k[X_1, \dots, X_n]/I \to k[X_1, \dots, X_n]/\mathfrak{m}_1 \times \dots \times k[X_1, \dots, X_n]/\mathfrak{m}_r,$$

$(\mathfrak{m}_i = \mathrm{I}(P_i))$, so that $r \leq \dim_k k[X_1, \dots, X_n]/I$. $\square$

The strategy of the last proposition can be refined to prove

Proposition 1.17. *Let $I \subset 1k[X_1, \ldots, X_n]$ be an ideal with a finite number of zeros, $\mathrm{V}(I) = \{P_1, \ldots, P_r\}$. We have a canonical isomorphism*

$$k[X_1, \ldots, X_n]/I = \mathcal{O}_{\mathbb{A}^n, P_1} \times \cdots \times \mathcal{O}_{\mathbb{A}^n, P_r}$$

Proof. [Ful69, Proposition 6 of §2.9] $\square$

Chapter 2

Multiplicity and Intersection Numbers

In this chapter, we deal with the issues of intersection theory of curves in $\mathbb{P}^2$ and prove a very important ingredient to the proof of Riemann-Roch, Max Noether's Fundamental Theorem. Although in the previous chapter we assumed varieties to be irreducible, the results we will see in this chapter hold in a more general context: we want to allow reducible subsets and even multiple components. To avoid dealing with the language of schemes, we will adopt the following convention: we will call a *plane curve* any polynomial $F \in k[X, Y, Z]$, up to a nonzero multiplicative constant. While for irreducible polynomials the notion of 'plane curve' we just introduced coincides with the notion of 'projective plane curve in $\mathbb{P}^2$' as defined in Chapter 1, in general the set $\mathrm{V}(F) \subset \mathbb{P}^2$ does not determine F: for example, X and X^2 will be two different plane curves to us. Similarly, an *affine plane curve* will be a polynomial of $k[X, Y]$ up to a multiplicative constant.

For any plane curve F, we will write $P \in F$ to mean $P \in \mathrm{V}(F)$. If the curve is irreducible, $\mathcal{O}_{F,P}$ will denote $\mathcal{O}_{\mathrm{V}(F),P}$ and so on.

2.1 Multiplicity

Let F be a plane curve, and $P \in F$. We calculate the multiplicity of F at P as follows:

We write $F = F_m + F_{m+1} + \cdots + F_n$ where each F_i is a form of degree i. The multiplicity of F at $(0, 0)$ is m, the smallest degree of the forms that make up F. To extend this definition to any point $P = (a, b)$, we compute the multiplicity at zero of $F(X + a, Y + b)$, and denote it $m_P(F)$. We say that P is a *smooth* point for F, or *simple* or *nonsingular*, if $m_P(F) = 1$ and that P is a *singular* or a *multiple* point if $m_P(F) > 1$.

Multiplicity is a local property, so one expects it to be expressed in terms of the local ring of F if F is irreducible. Before stating that, we need the following result.

Theorem 2.1. *Let F be an irreducible plane curve. If $P \in F$ is a simple point, then $\mathcal{O}_{F,P}$ is a discrete valuation ring. Further, if $P \in F$ is indeed simple,* *for any line $L : aX + bY + c$ not tangent to F at P, its image $l \in \mathcal{O}_{F,P}$ is a uniformizing parameter for $\mathcal{O}_{F,P}$.*

Proof. Suppose P is a simple point on F, and L is a line through P not tangent to F.

Any two distinct lines L_1, L_2 meeting at P can be sent to two distinct lines L_1', L_2' meeting at P' under an affine transformation. Two distinct lines L_1, L_2 passing by P correspond to two linearly independent vectors v_1, v_2 in k^2, the directional vectors of respective lines. $GL_2(k)$ can send any two linearly independent vectors to any other two linearly independent vectors. We simply translate by $-P$, then send v_1, v_2 to the directional vectors of L_1', L_2' and then translate by P'. Keep also in mind that affine coordinate changes induce isomorphism on the local ring level.

Therefore, there is no harm in assuming that $P = (0,0)$, Y is a tangent to F, and that $L = X$. To show that $\mathcal{O}_{F,P}$ is a discrete valuation ring, It suffices to show that the maximal ideal $\mathfrak{m}_P(F)$ is principal. We are going to show that it is generated by x, the residue of L.

Now $F = Y + A(X,Y)$ where A is a polynomial consisting of terms higher than Y. We can group all the terms that include Y together and write $F = YG - XH^2$, where $G = 1 + \widetilde{A}(X,Y)$, and $H \in k[X]$. Then modulo F we have the following equation

$$yg = x^2 h.$$

Then $y = x^2 h g^{-1} \in (x) \subset \mathcal{O}_{F,P}$ because g doesn't vanish at P. So we have $\mathfrak{m}_P(F) = (x,y) = (x)$. $\square$

We will denote by ord_P^F or simply by ord_P the order function induced by the DVR $\mathcal{O}_{F,P}$ onto $k(F)$. Now we are ready to express multiplicity purely in terms of local rings.

Theorem 2.2. *Let P be a point on an irreducible plane curve F. Then for all sufficiently large n,*

$$m_P(F) = \dim_k \left(\mathfrak{m}_P(F)^n / \mathfrak{m}_P(F)^{n+1} \right)$$

Proof. We have the following exact sequence

$$0 \longrightarrow \mathfrak{m}_P(F)^n/\mathfrak{m}_P(F)^{n+1} \longrightarrow \mathcal{O}_{F,P}/\mathfrak{m}_P(F)^{n+1} \longrightarrow \mathcal{O}_{F,P}/\mathfrak{m}_P(F)^n \longrightarrow 0$$

So,

$$\dim_k(\mathfrak{m}_P(F)^n/\mathfrak{m}_P(F)^{n+1}) = \dim_k(\mathcal{O}_{F,P}/\mathfrak{m}_P(F)^{n+1}) - \dim_k(\mathcal{O}_{F,P}/\mathfrak{m}_P(F)^n)$$

If we can prove that $\dim_k(\mathcal{O}_{F,P}/\mathfrak{m}_P(F)^n) = n \cdot m_P(F) + s$ for some constant s and all $n \geq m_P(F)$,

$$\dim_k(\mathfrak{m}_P(F)^n/\mathfrak{m}_P(F)^{n+1}) = (n+1)m_P(F) + s - n \cdot m_P(F) + s = m_P(F).$$

We may assume $P = (0,0)$. Let $I = (x,y)$, then $\mathfrak{m}_P(F)^n = I^n \mathcal{O}_{F,P}$.

Since $\mathrm{V}(I^n) = \{0\}$, we have by Proposition 1.17

$$k[X,Y]/(I^n, F) = \mathcal{O}_{P,\mathbb{A}^2}/(I^n, F)\mathcal{O}_{P,\mathbb{A}^2} = \mathcal{O}_{F,P}/I^n\mathcal{O}_{F,P} = \mathcal{O}_{F,P}/\mathfrak{m}_P(F)^n.$$

So we calculate the dimension of $k[X,Y]/(I^n,F)$. Let $m = m_P(F)$. If $G \in I^{n-m}$, then $FG \in I^n$.

So we have two maps now, $\psi : k[X,Y]/I^{n-m} \to k[X,Y]/I^n$ given by $\psi(G) = FG$ and a projection $\pi : k[X,Y]/I^n \to k[X,Y]/(I^n,F)$. Again, we have the exact sequence

$$0 \longrightarrow k[X,Y]/I^{n-m} \xrightarrow{\psi} k[X,Y]/I^n \xrightarrow{\pi} k[X,Y]/(I^n,F) \longrightarrow 0.$$

From which we deduce

$$\begin{aligned}\dim(k[X,Y]/(I^n,F)) &= \dim(k[X,Y]/I^n) - \dim(k[X,Y]/I^{n-m}) = \\ &= nm - \frac{m(m-1)}{2}.\end{aligned}$$

for all $n \geq m$. $\square$

Smoothness of Arbitrary Curves

In analogy with Theorem 2.1, we are lead to the definition of smoothness for any not-necessarily-plane curve:

Definition 2.3. Let X be a curve, and $P \in X$. We say that P is a *smooth point* for X if the local ring $\mathcal{O}_{X,P}$ is a DVR and that X is *smooth* if all of its points are smooth.

Using Theorem 1.15, it is not hard to see that the set of singular points of X is closed, and hence finite.

2.2 Intersection Numbers

Similar to the notion of multiplicity at a point, we would like to be able to talk about the intersection of two curves algebraically. The definition at first glance is unintuitive, so let's write a list of properties one would reasonably expect from intersection of two curves.

Firstly we would like the intersection number to be an integer. So it makes sense to exclude cases where two curves intersect on a common component. We will say that F and G *intersect properly* at P if they have no common component passing through P. We will denote the intersection number at P of F and G as $I(P, F \cap G)$. Here is a list of reasonable expectations.

1. If F and G intersect properly at P, the intersection number $I(P, F \cap G)$ should be a nonnegative integer.

2. If $P \notin F \cap G$, then $I(P, F \cap G)$ should be 0.

3. The intersection number $I(P, F \cap G)$ should be invariant under change of coordinates. In other words , if T is a change of coordinates, $I(P, F \cap G) = I(Q, F^T \cap G^T)$.

4. It should be symmetric, $I(P, F \cap G) = I(P, G \cap F)$.

5. Two curves intersect transversally at the simple point P if their tangent lines are distinct. If F and G intersect transversally at a simple point P, the intersection number should be 1 at P. More generally $I(P, F \cap G) \geq m_P(F)m_P(G)$.

6. We should add intersection numbers if curves have multiple components : If $F = \prod F_i^{n_i}$, and $G = \prod G_j^{m_j}$ then $I(P, F \cap G) = \sum n_i m_j I(P, F_i \cap G_j)$.

7. If F is irreducible, the intersection number of F and G should depend on the residue of G in $k[F]$. Meaning, $I(P, F \cap G) = I(P, F \cap (AF + G))$ for all $A \in k[X, Y]$.

8. If P is a simple point of F, then $I(P, F \cap G) = \text{ord}_P^F(G)$.

9. If F and G have no common components then

$$\sum_P I(P, F \cap G) = \dim_k(k[X, Y]/(F, G))$$

Example 2.4. Even before defining the intersection number, these properties allow us to efficiently calculate it.

Let $F(x, y) = y^2 - x^3 + x$, let $G(x, y) = x$, and $P = (0, 0)$. then

$$\begin{aligned} I(P, F \cap G) &= I(P, y^2 - x^3 + x \cap x) = I(P, y^2 - x^3 + x + (x(x^2 - 1)) \cap x) \\ &= I(P, y^2 \cap x) = 2I(P, y \cap x) = 2 \end{aligned}$$

We used, in order, the properties 7, 6 and 5. We need not know how $I(P, y \cap x)$ is defined. They intersect transversally. Though, there is only one way to define an intersection number satisfying these properties.

Theorem 2.5. *There exist a unique intersection number defined for all plane curves F and G, and for all points $P \in \mathbb{A}^2$, satisfying the properties **(1-7)**. It is given by the formula*

$$I(P, F \cap G) = \dim_k(\mathcal{O}_{\mathbb{A}^2, P}/(F, G)).$$

Proof. See [Ful69, Theorem 3 of §3.3] □

2.3 Bézout's Theorem

In the previous section we focused on affine plane curves, but all the results may be lifted effortlessly to projective plane curves.

Let $F \in K[X, y, Z]$ be a plane curve and $P \in F$. When $P = [x : y : 1]$, we have $\mathcal{O}_{F,P} = \mathcal{O}_{F(x,y,1),(x,y)}$. So the results from the previous section are valid since they all depend on the local ring. For example, the multiplicity of an affine curve is expressed in terms of the local ring. Therefore for the multiplicity of a projective plane curve F at a point $P \in \mathbb{P}^2$, we can dehomogenize F at any of the three affine patches U_1, U_2 and U_3 of $\mathbb{P}^2$ and compute the multiplicity there. Since it is invariant under projective change of coordinates, multiplicity is independent of our choice of dehomogenization. For any $F \in k[X, Y, Z]$ we will write F_* to mean F dehomogenized.

The intersection number of two projective plane curves F and G at P is defined as $I(P, F \cap G) = \dim_k(\mathcal{O}_{\mathbb{A}^2,P}/(F_*, G_*))$.

We say a line L is tangent to F at P, if $I(P, F \cap L) > m_P(F)$. A point $P \in F$ is called an *ordinary multiple point* if F has $m_P(F)$ distinct tangent lines at P. We are ready to state Bézout's theorem.

Theorem 2.6 (Bézout). *Let F and G be two projective plane curves of degree m and n respectively. Assume F and G have no common components. Then,*

$$\sum_P I(P, F \cap G) = mn$$

We will give a sketch of the proof. For detail see [Ful69, § 5.3].

Since $F \cap G$ is finite by assumption, we assume none of the intersections lie at the line at infinity $Z = 0$.

Now we have $I(P, F \cap G) = I(P, F_* \cap G_*) = \dim_k(k[X, Y]/(F_*, G_*))$ by the property 9 of the intersection number. Define

$$\Gamma_* = k[X, Y]/(F_*, G_*) \quad \Gamma = k[X, Y, Z]/(F, G) \quad R = k[X, Y, Z]$$

and let Γ_d and R_d be the space of degree d forms in Γ and R respectively. The theorem is proved if $\dim(\Gamma_*) = \dim(\Gamma_d)$ and $\dim(\Gamma_d) = $ mn.

We have the following exact sequence

$$0 \longrightarrow R \xrightarrow{\psi} R \times R \xrightarrow{\varphi} R \xrightarrow{\pi} \Gamma \longrightarrow 0$$

where $\psi(C) = (GC, -FC)$ and $\varphi(A, B) = AF + BG$. This sequence restricts to the following exact sequence :

$$0 \longrightarrow R_{d-m-n} \xrightarrow{\psi} R_{d-m} \times R_{d-n} \xrightarrow{\varphi} R_d \xrightarrow{\pi} \Gamma_d \longrightarrow 0$$

This sequence proves that $\dim(\Gamma_d) = mn$. For $\dim(\Gamma_*) = \dim(\Gamma_d)$ we pick a basis $A_1, \ldots, A_{mn}$ of R_d and show that the residues $a_1, \ldots, a_{mn}$ in Γ_* form a basis.

The following corollaries are immediate from Bézout and properties of intersection number.

Corollary 2.7. *If F and G have no common component, then*

$$\sum_P m_P(F) m_P(G) \leq \deg F \deg G$$

Corollary 2.8. *If F and G are of degree m and n respectively, and they meet at mn distinct points, then all these points are simple.*

Corollary 2.9. *If two curves of degree m and n have more than mn points in common, then they have a common component.*

2.4 Max Noether's Fundamental Theorem

Definition 2.10. Let F and G be two projective plane curves of degrees m and n respectively. The *intersection cycle* of F and G is the formal sum

$$F \cdot G = \sum_{P \in \mathbb{P}^2} I(P, F \cap G) P$$

Let H be another projective plane curve, we will write $H \cdot F \geq G \cdot F$ to mean $I(P, H \cap F) \geq I(P, G \cap F)$ for all P.

Some of the properties of the intersection number carry over. Intersection cycle is symmetric, and $G \cdot FH = G \cdot F + G \cdot H$. Also, if A is of degree $n - m$, $F \cdot (G + AF) = G \cdot F$.

Suppose F, G and H are curves, and $H \cdot F \geq G \cdot F$. One might ask whether there is some curve B such that $B \cdot F = H \cdot F - G \cdot F$. If there exist an equation $H = AF + BG$, then $H \cdot F = BG \cdot F = B \cdot F + G \cdot F$.

Let P be a point on the projective plane. Let F and G be curves with no common component through P. Let H be another curve. The *Noether's conditions* are satisfied at P, with respect to F, G and H, if $H_* \in (F_*, G_*) \subset \mathcal{O}_{\mathbb{P}^2, P}$

Example 2.11. Say $F(x, y, z) = y^2z - x^3 + xz^2$, $G(x, y, z) = x$, and $H(x, y, z) = y^2z - 2x^3 + xz^2 + y^2x$. We first find the intersections.

$$G \cap F = \{[0 : 1 : 0], [0 : 0 : 1]\}$$

Since $I([0 : 0 : 1], G \cap F) = 2$, the intersection cycle is

$$G \cdot F = 2[0 : 0 : 1] + [0 : 1 : 0]$$

We know we missed no points or multiplicities thanks to Bézout.

With a bit of a calculation, we see that H and F meet at 6 distinct points. They both are of degree 3. So there must be some multiplicity.

$$H \cap F = \{[0 : 1 : 0], [0 : 0 : 1], \left[\frac{1 - \sqrt{5}}{2} : -\frac{1 - \sqrt{5}}{2} : 1\right], \left[\frac{\sqrt{5} - 1}{2} : -\frac{\sqrt{5} - 1}{2} : 1\right], \left[\frac{1 - \sqrt{5}}{2} : \frac{1 - \sqrt{5}}{2} : 1\right], \left[\frac{\sqrt{5} - 1}{2} : \frac{\sqrt{5} - 1}{2} : 1\right]\}$$

For simplicity, let us name the points with square roots P_1, P_2, P_3, P_4 according to the order in which they appear.

The intersection numbers are $I([0 : 1 : 0], H \cap F) = 4$ and $I([0 : 0 : 1], H \cap F) = 1$. So the intersection cycle is

$$H \cdot F = 1[0 : 0 : 1] + 4[0 : 1 : 0] + P_1 + P_2 + P_3 + P_4.$$

So $H \cdot F \geq G \cdot F$. And indeed, we have $H = F + (y^2 - x^2)G$. Notice how also the Noether's Conditions are satisfied.

$$H_* = 2y^2 - 2x^3 + x = 2(y^2 - x^3 + x) - x = 2F_* - G_*$$

Theorem 2.12 (Max Noether's Fundamental Theorem). *Let F, G and H be projective plane curves. Assume F and G have no common components. T*

There exist A with $\deg A = \deg H - \deg F$, and B with $\deg B = \deg H - \deg H$ such that $H = AF + BG$ if and only if Noether's Conditions are satisfied at every point $P \in F \cap G$.

Proof. If $H = AF + BG$, then $H_* = A_*F_* + B_*G_*$.

Since Noether's Conditions are local, local rings are preserved under projective coordinate changes, and F and G meet only at a finite number of points, again we are free to assume that F and G don't meet at line $Z = 0$. So that we may dehomogenize as $F_* = F(X, Y, 1)$, etc.

Noether's Conditions being satisfied at each P means that H_* is zero in $\mathcal{O}_{\mathbb{P}^2,P}/(F_*, G_*)$ for all $P \in F \cap G$. This implies that H_* is identically zero on the finite variety determined by (F_*, G_*), or in other words H_* is zero in the coordinate ring $k[X, Y]/(F_*, G_*)$. Then there is an equation $H_* = aF_* + bG_*$ for some $a, b \in k[X, Y]$. Homogenizing this equation with Z, we would get $Z^r H = AF + BG$ for some r, A, B.

The map $H \mapsto ZH$ is injective on $k[X, Y]/(F_*, G_*)$. We examine the kernel. Suppose $HZ = AF + BG$ for some A, B then

$$A(X, Y, 0)F(X, Y, 0) = -B(X, Y, 0)G(X, Y, 0).$$

But since F and G don't meet at $Z = 0$, $F(X, Y, 0)$ and $G(X, Y, 0)$ are relatively prime. Therefore $B(X, Y, 0) = F(X, Y, 0)C$ and $A(X, Y, 0) = -G(X, Y, 0)C$ for some $C \in k[X, Y]$. Set $A_1 = A + CG$ and $B_1 = B - CF$. Then $A_1(X, Y, 0) = B_1(X, Y, 0) = 0$. So $A_1 = ZA'$ and $B_1 = ZB'$ for some A', B'. Now since $ZH = A_1F + B_1G$n we have $H = A'F + B'G$. Thus the map is injective.

Going back to the equation $Z^r H = AF + BG$, we have some A', B' such that $H = A'F + B'G$. Let A'_s be the degree $s = \deg H - \deg F$ part of A', and B'_t be the degree $t = \deg H - \deg G$ part of B'. Then we have $H = A'_sF + B'_tG$. □

Notice how if F and G meet transversally at $P \in H$, then Noether's Conditions are satisfied. Because if F and G meet transversally, the tanget to G is an uniformizing parameter of $\mathcal{O}_{F,P}$.

In the next chapter, we will find another formulation of Noether's Conditions that work for all ordinary multiple points of F.

2.5 Applications of Noether's Theorem

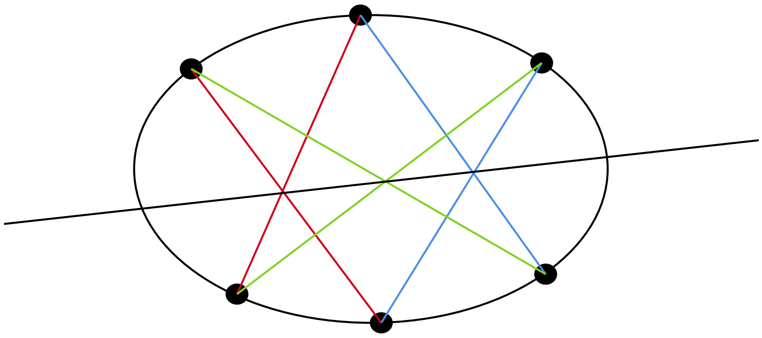
Some applications of Noether's Theorem , although not directly related to the ultimate goal Riemann-Roch theorem, are worth going into.

Proposition 2.13. *Let C and C' be two cubics. Let $C \cdot C' = \sum_{i=1}^{9} P_i$. Suppose Q is conic, and $Q \cdot C = \sum_{i=1}^{6} P_i$. Assume $P_1, \ldots, P_6$ are simple points on C. Then P_7, P_8, P_9 are collinear.*

Proof. Since Q and C meet at $6 = \deg Q \deg C$ simple (distinct) points, Noether's Conditions are satisfied. Suppose C, Q, C' are given by the forms F, G, H respectively. Then $H = AF + BG$ for some A, B with $\deg B = \deg H - \deg G = 3 - 2 = 1$. The line B is the one we seek. □

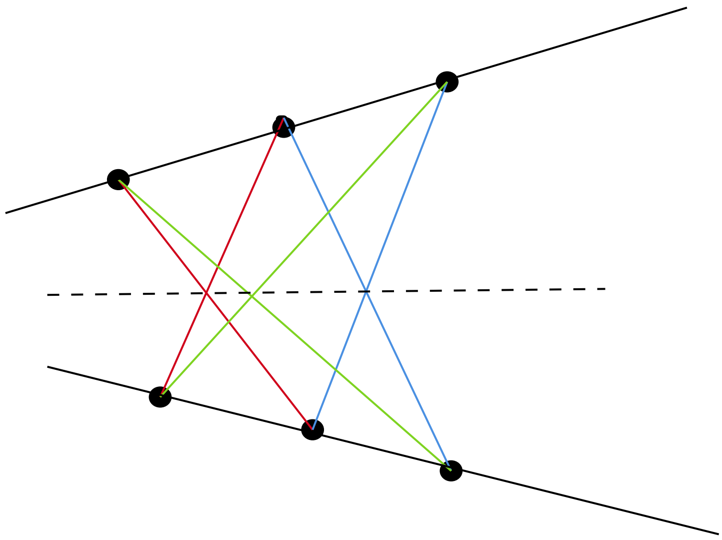
Corollary 2.14 (Pascal's Theorem). *If a hexagon is inscribed in an irreducible conic, then the opposite sides meet in collinear points.*

Proof. Let C be three sides and C' be three opposite sides, Q the conic. Apply the previous proposition. □



Corollary 2.15 (Pappus's Theorem). *Let L_1, L_2 be two lines. $P_1, P_2, P_3 \in L_1$ and $Q_1, Q_2, Q_3 \in L_2$, none of which lie on $L_1 \cap L_2$. Let L_{ij} be the line between P_i and Q_j. Let $R_k = L_{ij} \cdot L_{ji}$. Then R_1, R_2 and R_3 are collinear.*

Proof. The lines L_1, L_2 form a conic. So the proof is the same as previous corollary. $\square$



Proposition 2.16. *Let C be an irreducible cubic. Let C' and C'' be two cubics. Suppose $C' \cdot C = \sum_{i=1}^{9} P_i$ where P_i are simple but not necessarily distinct points of C. Suppose $C'' \cdot C = \sum_{i=1}^{8} P_i + Q$. Then $Q = P_9$.*

Proof. Let L be a line through P_9 not passing through Q. $L \cdot C = P_9 + R + S$. Then

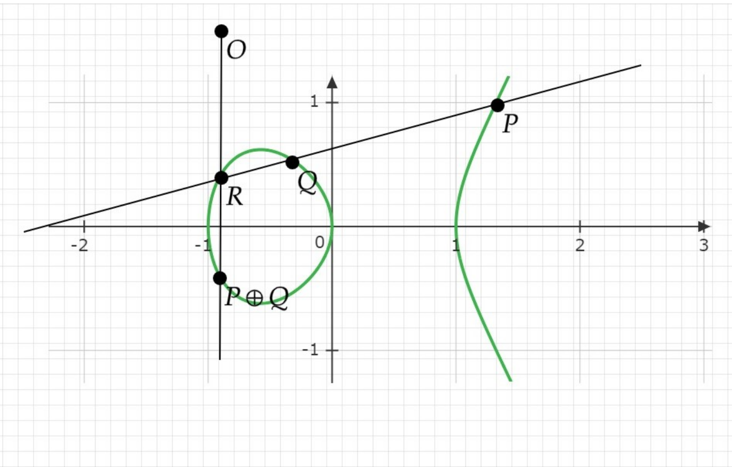
$$LC'' \cdot C = C'' \cdot C + L \cdot C = \sum_{i=1}^{8} P_i + QP_9 + R + S + = C' \cdot C + Q + R + S$$

Therefore, there is a line L' such that $L' \cdot C = Q + R + S$. But then $L = L'$. Because they are both of degree 1 sharing more than 1 common point. So $Q = P_9$. $\square$

There is a group law on cubics. Let C be a nonsingular cubic. For any two points P, Q on C there is a line L passing through them, and $L \cdot C = P + Q + R$.

And if $P = Q$ take L as the tangent at P. Let us write $f(P,Q) = R$. This is a binary operation on C indeed. But it has no identity element. So we choose a distinguished point $O \in C$ (which functions as the identity) and define $P \oplus Q = f(O, f(P,Q))$.

The figure below demonstrates this operation on $Z = 1$ patch of the cubic $C : y^2z - x^3 + xz^2$. For O, we have chosen the point at infinity $[0 : 1 : 0]$.

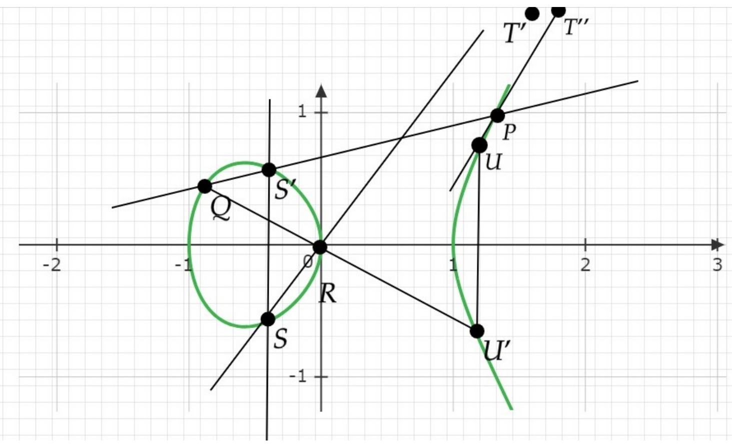


Proposition 2.17. *Let C be a nonsingular cubic and let $\oplus$ be the binary operation described as above. $(C, \oplus)$ is an abelian group.*

Proof. We show the associativity. Let P, Q, R be three points on C. Consider the following lines,

$$\begin{aligned} L_1 \cdot C &= P + Q + S' & \qquad M_1 \cdot C &= O + S + S' \\ L_2 \cdot C &= S + R + T' & \qquad M_2 \cdot C &= R + Q + U' \\ L_3 \cdot C &= O + U + U' & \qquad M_3 \cdot C &= P + U + T'' \end{aligned}$$

This configuration is depicted in the following admittedly complicated figure.



Although it is not completely useless. We could convince ourselves of the facts that $(P \oplus Q) \oplus R = f(O, T')$ and that $P \oplus (Q \oplus R) = f(O, T'')$. So , it remains to show that $T' = T''$.

Let $C' = L_1L_2L_3$, and $C'' = M_1M_2M_3$. Applying the previous proposition, we see that C' and C'' are both cubics that meet C at 8 common points. So the remaining 9th points T' and T'' should be the same.

$\square$

Chapter 3

Resolution of Singularities

In this chapter, we analyze in detail the strategies we can employ to obtain a smooth curve X from an arbitrary curve C. Since the singularities of C are only a finite amount, we want to resolve each of them in a finite number of steps.

3.1 Blowing up

The essential tool in the resolution of singularities is the blow up. The idea is to replace a point O of $\mathbb{A}^n$ with a copy of $\mathbb{P}^{n-1}$, whose elements represent the lines through O.

Up to a translation, we can assume $O = (0, \dots, 0)$ is the origin of $\mathbb{A}^n$, so that the points $[a_1 : \cdots : a_n]$ of $\mathbb{P}^{n-1}$ correspond exactly to the lines $\mathrm{V}(a_i X_j - a_j X_i \mid i, j = 1, \dots, n)$ of $\mathbb{A}^n$ through O, where $X_1, \dots, X_n$ are the coordinates of $\mathbb{A}^n$. The *blowing up of* $\mathbb{A}^n$ *at* O is the closed subset of $B \subset \mathbb{A}^n \times \mathbb{P}^{n-1}$ consisting of couples (P, L) such that $P \in L$. If $Y_1, \dots, Y_n$ are the coordinates of $\mathbb{P}^{n-1}$, then B is defined by the equations $X_i Y_j - X_j Y_i = 0$ for $i, j = 1, \dots, n$.

There is a natural projection,

$$\pi \colon B \to \mathbb{A}^n,$$

given by the restriction of the projection $\mathbb{A}^n \times \mathbb{P}^{n-1} \to \mathbb{A}^n$.

The fiber above the origin is $\pi^{-1}(O) = O \times \mathbb{P}^{n-1}$, a copy of $\mathbb{P}^{n-1}$; call it E. The fiber above a point P other than O consists of the single point (P, L) of B, where L is the unique line passing through O and P: in fact π gives an isomorphism of $B \smallsetminus E$ and $\mathbb{A}^n \smallsetminus O$, with inverse $\pi^{-1}(a_1, \dots, a_n) = ((a_1, \dots, a_n), [a_1 : \cdots : a_n])$.

The set B is irreducible, as its subspace $B \smallsetminus E$ is irreducible and dense. Indeed each point $(O, [a_1 : \cdots : a_n])$ of E lies on the line $\mathrm{V}(a_i X_j - a_j X_i, a_i Y_j - a_j Y_i \mid i, j = 1, \dots, n) \subset B$, so B is the closure of $B \smallsetminus E$ which is isomorphic to the irreducible $\mathbb{A}^n \smallsetminus O$.

Definition 3.1. If Y is a closed subvariety of $\mathbb{A}^n$, we define the *blowing up of* Y *at* O to be the closure $\widetilde{Y} = \overline{\pi^{-1}(Y \smallsetminus O)}$.

The plane case

We now focus on the case $n = 2$. Let X, Y be the coordinates of $\mathbb{A}^2$ and T, U those of $\mathbb{P}^1$. Consider an irreducible closed curve $C \subset \mathbb{A}^2$, passing through O with multiplicity $r = m_P(C)$ and distinct tangents $L_1, \ldots, L_s$ at O. Let $\widetilde{C}$ be the blowing up of C at O and $f\colon \widetilde{C} \to C$ the restriction of π to $\widetilde{C}$.

If $F \in k[X, Y]$ is an equation for C, $(F) = \mathrm{I}(C)$, the equations for the L_i are obtained by factoring the lowest-degree homogeneous component F_r of F into linear factors,

$$F_r = \prod_{i=1}^{s} (\beta_i Y - \alpha_i X)^{r_i}.$$

The blow up of $\mathbb{A}^2$ at O is given by $B = \mathrm{V}(UX - TY)$. A point $(x, y) \neq (0, 0)$ of C corresponds to the point $((x, y), [x : y])$ of $\widetilde{C}$ via f^{-1}. In the affine patch $\mathbb{P}^1 \smallsetminus \mathrm{V}(T)$ for $\mathbb{P}^1$, we may set $T = 1$ and get an isomorphism

$$\varphi\colon \mathbb{A}^2 \xrightarrow{\sim} B \smallsetminus \mathrm{V}(T), \qquad \varphi(x, u) = ((x, ux), [1 : u]).$$

We shall use this isomorphism to understand the fiber $f^{-1}(O)$ above O. The points of $\widetilde{C} \smallsetminus E$ satisfy the equations $Y = XU$ and $F(X, Y) = 0$; writing $F = \sum_{i=r}^{d} F_i$ the decomposition of F into homogeneous components, they also satisfy

$$F(X, XU) = \sum_{i=r}^{d} X^i F_i(1, U) = X^r \underbrace{\left(\sum_{i=r}^{d} X^{i-r} F_i(1, U) \right)}_{\text{let this be } \widetilde{F}(X, U)}.$$

If G divides $\widetilde{F}$ then $X^{\deg G} G(X, Y/X)$ divides F, so $\widetilde{F}$ is irreducible. Since $\varphi^{-1}(\widetilde{C} \smallsetminus E) \subset \mathrm{V}(\widetilde{F})$, by irreducibility $\varphi^{-1}(\widetilde{C}) = \mathrm{V}(\widetilde{F})$.

As $\varphi^{-1}(E) = \mathrm{V}(X)$, we have

$$\varphi^{-1}(\widetilde{C} \cap E) = \mathrm{V}(X, \widetilde{F}) = \mathrm{V}(X, F_r(1, U)) = \{(0, \alpha_i/\beta_i) \text{ , with } \beta_i \neq 0\}.$$

By a similar reasoning in the affine patch $U \neq 0$, we find

$$f^{-1}(O) = \widetilde{C} \cap E = \{(O, [\alpha_i : \beta_i])\}_{i=1,\ldots,s}.$$

So $\widetilde{C}$ consists of a copy $\widetilde{C} \smallsetminus E$ of $C \smallsetminus O$, and one point for each distinct tangent of C at O.

Remark 3.2. Letting $P_i = (0, \alpha_i/\beta_i) = \varphi^{-1}(O, [\alpha_i : \beta_i])$ for $\beta_i \neq 0$, we have an estimate on the multiplicity at P_i of the plane curve $\varphi^{-1}(\widetilde{C})$ in terms of the multiplicity r_i of the corresponding tangent L_i:

$$m_{P_i}\big(\varphi^{-1}(\widetilde{C})\big) = m_{P_i}(\widetilde{F}) \leq I\left(P_i, \widetilde{F} \cap X\right) = r_i.$$

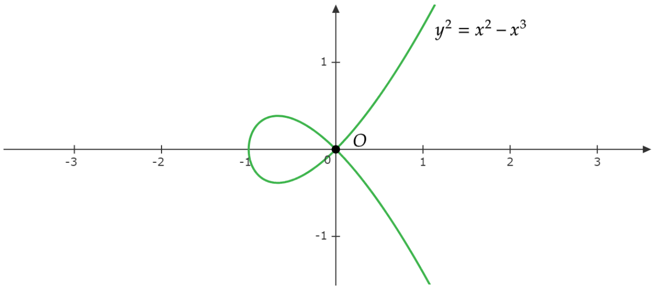
Indeed

$$I\left(P_i, \widetilde{F} \cap X\right) = I\left(P_i, \prod_{j=1}^{s} (\beta_j U - \alpha_j)^{r_j} \cap X\right) = I\left(P_i, (\beta_i U - \alpha_i)^{r_i} \cap X\right) = r_i,$$

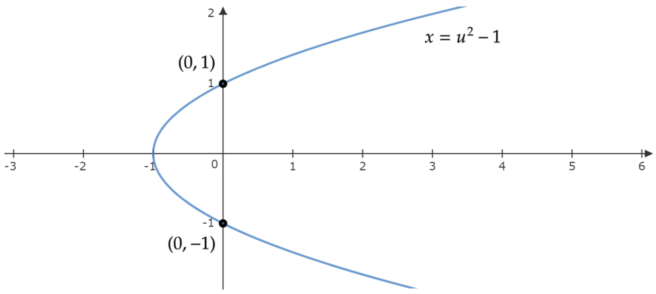
by the properties of the intersection number of Chapter 2.

The fundamental consequence of this observation is that if all tangents to C at O are distinct (that is, O is an ordinary point,) then $f^{-1}(O)$ consists of r points, which are all simple for $\widetilde{C}$.

Example 3.3. The affine plane curve of equation $Y^2 = X^2 - X^3$ represented below has a double point $O = (0,0)$.



Finding its blow up through the process described above, we obtain the curve $\mathrm{V}(UX - TY, X - U^2 + 1) \subset \mathbb{A}^2 \times \mathbb{P}^1$. The points above O are $(O, [1 : -1])$ and $(O, [1 : 1])$, corresponding to the tangents $Y = X$ and $Y = -X$. Dehomogeneizing with respect ot T and projecting onto the X, U plane we get the parabola $X = U^2 - 1$.



Proposition 3.4. *For all points $P \in C$, there exists an affine neighborhood U of P in C such that $\widetilde{U} = f^{-1}U$ is affine and the morphism $f^*\colon k[U] \to k[\widetilde{U}]$ is finite (we say that the morphism $f\colon \widetilde{C} \to C$ is finite).*

Proof. The result is obvious near points of $C \smallsetminus O$, for $f\colon \widetilde{C} \smallsetminus f^{-1}(O) \to C \smallsetminus O$ is an isomorphism. Thus we need only to focus on O. Up to an affine change of coordinates of $\mathbb{A}^2$, we may assume that the Y-axis $\mathrm{V}(X)$ is not tangent to C at O, so we can suppose all β_i to be 1, $F_r = \prod_{i=1}^{s} (Y - \alpha_i X)^{r_i}$. Since none of the points of $f^{-1}(O)$ lie in $\mathrm{V}(T)$ and $\varphi\colon \mathbb{A}^2 \to B \smallsetminus \mathrm{V}(T)$ is an isomorphism, by letting

$$\psi = f\varphi\colon\ \mathrm{V}(\widetilde{F}) \to C \qquad \psi(x,u) = (x, ux),$$

we need to find an affine open neighborhood W of O in C such that $\widetilde{W} = \psi^{-1}W$ is affine and $\psi^*\colon k[W] \to k[\widetilde{W}]$ is finite. We identify $k[C] = k[x,y]$ as a subring of $k[\widetilde{C}] = k[x,u]$ via ψ^*, that is $y = ux$. Let

$$H(Y) = F(0,Y)/Y^r \in k[X,Y],$$

and $h = H(y) = H(ux)$ its image in $k[C] \subset k[\widetilde{C}]$. Since $h(O) \neq 0$, the affine subset $C \smallsetminus \mathrm{V}(h)$ is a neighborhood of O, and $\widetilde{W} = \psi^{-1}W = \widetilde{C} \smallsetminus \mathrm{V}(h)$ is affine too.

We have $k[W] = k[x, y, 1/h]$ and $k[\widetilde{W}] = k[x, u, 1/h]$. Since $k[\widetilde{W}] = k[W][u]$, it is sufficient to find an integral relation for u over $k[C]$. To find it, observe that using the identity $y = ux$ we can write

$$0 = \widetilde{F}(x, u) = F_r(1, u) + xF_{r+1}(1, u) + \cdots + x^{d-r}F_d(1, u) = \\ = hu^r + a_1u^{r-1} + \cdots + a_r,$$

for $a_i \in k[x, y]$. After dividing by h, we are done. Remark that the relation we have found also implies $x^{r-1}k[\widetilde{W}] \subset k[W]$. □

What we have done in this section can easily be generalized to blow up any finite set of points, adding a copy of $\mathbb{P}^1$ representing the lines through each of them. It also causes no problems to consider closed curves of $\mathbb{P}^2$ instead of $\mathbb{A}^2$, with analogous definitions: the local computation in one of the affine charts will look exactly like what we have done above. Hence by Remark 3.2 we get the following

Proposition 3.5. *For any irreducible projective plane curve C with only ordinary multiple points, there exists a smooth curve $\widetilde{C}$ and a birational surjective morphism $f : \widetilde{C} \to C$.*

Thus with a single blowing up we resolve ordinary multiple points, but we have no guarantee of resolving points where tangents coincide. These last kind of singularities can still be resolved by iterating the process of the a finite number of times, but there is a small complication: for a plane curve C, the blown up curve $\widetilde{C}$ is no longer necessarily plane. It is however embedded in the surface B, which we could check to be smooth. The process of this section can be adapted to be hold for any smooth surface, appearing in local coordinates like what we have done above, but we prefer going a different route following [Ful69] by introducing the concept of quadratic transformations instead.

3.2 Quadratic Transformations

The process we describe in this section will allow us to transform a plane curve C into another plane curve $\widetilde{C}$ which has better singularities. The singularities of C will become ordinary multiple points on $\widetilde{C}$. During this process, $\widetilde{C}$ may acquire new singularities but they will all be ordinary ones, so that by we may resolve the curve via Proposition 3.5.

Before starting, let us label some objects to simplify the exposition. Let X_0, X_1, X_2 be the coordinates of $\mathbb{P}^2$. The three points $P_0 = [1 : 0 : 0]$, $P_1 = [0 : 1 : 0]$ and $P_2 = [0 : 0 : 1]$ will be called the *fundamental points*. The three lines $L_0 = \mathrm{V}(X_0)$, $L_1 = \mathrm{V}(X_1)$ and $L_2 = \mathrm{V}(X_2)$ will be called *fundamental lines*. Observe that $L_0 \cap L_1 = P_2$ and L_0 is the line through P_1 and P_2, with similar identities by permuting indices. Finally, denote the intersection of the three affine charts of $\mathbb{P}^2$ by $U = \mathbb{P}^2 \smallsetminus \mathrm{V}(X_0X_1X_2)$.

We can now introduce the main protagonist of this section: the *standard quadratic transformation* (or *standard Cremona transformation*) is the rational map

$$Q\colon \mathbb{P}^2 \dashrightarrow \mathbb{P}^2, \qquad Q[x_0 : x_1 : x_2] = [x_1x_2 : x_1x_2 : x_0x_1].$$

It is defined on $\mathbb{P}^2 \smallsetminus \{P_0, P_1, P_2\}$, which it maps onto $U \cup \{P_0, P_1, P_2\}$. Since all three coordinates are nonzero in U, if $[x_0 : x_1 : x_2] \in U$ then $Q(Q[x_0 : x_1 : x_2]) = Q[x_1x_2 : x_1x_2 : x_0x_1] = [x_0x_1x_2x_0 : x_0x_1x_2x_1 : x_0x_1x_2x_2] = [x_0 : x_1 : x_2]$ so Q is an isomorphism of U with itself and a birational map. The preimage of a fundamental point is $Q^{-1}(P_0) = L_0 \smallsetminus \{P_1, P_2\}$ (again with similar identities by permuting indices.)

Now let C be an irreducible curve in $\mathbb{P}^2$ which is not an exceptional line.

Definition 3.6. The *quadratic transform* $\widetilde{C}$ of C is defined as

$$\widetilde{C} = \overline{Q(C \cap U)} = \overline{Q^{-1}(C \cap U)}.$$

Restricting Q yields a birational morphism from $\widetilde{C} \smallsetminus \{P_0, P_1, P_2\}$ to C.

Proper transform and good position

Let $r_i = m_{P_i}(C)$, for $i = 1, 2, 3$, and $F \in k[X_0, X_1, X_2]$ be an equation for C, $d = \deg F$. The *algebraic transform* of F is $F^Q = F(X_1X_2, X_0X_2, X_0X_1)$; it has degree $2d$. Dehomogeneizing F with respect to a variable and decomposing into homogeneous components we can see that $X_i^{r_i}$ is the highest powers of X_i that divides F^Q, so that

$$F = X_0^{r_0} X_1^{r_1} X_2^{r_2} \widetilde{F},$$

for some $\widetilde{F} \in k[X_0, X_1, X_2]$ not divisible by X_i for all i. For example, writing

$$F = F_{r_0}(X_1, X_2)X_0^{d-r_0} + \cdots + F_d(X_1, X_2),$$

with F_i homogeneous of degree i, then

$$\begin{aligned} F^Q &= F_{r_0}(X_0X_2, X_0X_1)(X_1X_2)^{d-r_0} + \cdots + F_d(X_0X_2, X_0X_1) = \\ &= X_0^{r_0}\Big(F_{r_0}(X_2, X_1)(X_1X_2)^{d-r_0} + \cdots + X_0^{d-r_0}F_d(X_2, X_1)\Big), \end{aligned}$$

from which we can also see that $m_{P_0}(\widetilde{F}) = d - r_1 - r_2$ (similarly for P_1 and P_2) as the leading homogeneous coefficient of $\widetilde{F}$ at P_0 is $F_d(X_2, X_1)X_1^{-r_1}X_2^{-r_2}$:

$$\begin{aligned} \widetilde{F} &= X_1^{-r_1}X_2^{-r_2}\Big(F_{r_0}(X_2, X_1)(X_1X_2)^{d-r_0} + \cdots + X_0^{d-r_0}F_d(X_2, X_1)\Big) = \\ &= F_{r_0}(X_2, X_1)X_1^{d-r_0-r_1}X_2^{d-r_0-r_2} + \cdots + X_0^{d-r_0}F_d(X_2, X_1)X_1^{-r_1}X_2^{-r_2}. \end{aligned}$$

The polynomial $\widetilde{F}$ is called the *proper transform* of F and it has degree $\deg \widetilde{F} = 2d - r_0 - r_1 - r_2$. From $(F^Q)^Q = (X_0X_1X_2)^dF$ it follows that $\widetilde{F}$ is irreducible. Since $Q(C \cap U) \subset \mathrm{V}(\widetilde{F})$, passing to the closure we get

$$\widetilde{C} = \mathrm{V}(\widetilde{F}),$$

by irreducibility.

We now need to add some assumptions on the relative position of C and the exceptional lines. We say that C is in *good position* if no exceptional line is tangent to C at a fundamental point. We claim that if C ia in good position, then $\widetilde{C}$ is in good position as well. Indeed, the line L_0 is tangent to $\widetilde{C}$ at P_1 if and only if

$$I\left(P_1, \widetilde{F} \cap X_0\right) > m_{P_1}(\widetilde{C}) = d - r_0 - r_2,$$

and using the properties of intersection numbers

$$\begin{aligned} d - r_0 - r_2 < I\left(P_1, \sum_{i=r_0}^{d} F_i(X_2, X_1) X_0^{i-r_0} X_1^{d-r_1-i} X_2^{d-r_2-i} \cap X_0\right) = \\ = I\left(P_1, F_{r_0}(X_2, X_1) X_1^{d-r_0-r_1} X_2^{d-r_0-r_2} \cap X_0\right) = \\ = I\left(P_1, F_{r_0}(X_2, X_1) \cap X_0\right) + \underbrace{I\left(P_1, X_2^{d-r_0-r_2} \cap X_0\right)}_{=d-r_0-r_2}. \end{aligned}$$

Now $I\left(P_1, F_{r_0}(X_2, X_1) \cap X_0\right) > 0$ if and only if $F_{r_0}(X_2, X_1)$ passes through P_1, $F_{r_0}(0,1) = 0$. But this last condition is equivalent to $X_1 | F_{r_0}$ i.e. L_1 being tangent to C at P_0. By symmetry, the same holds for the other lines and points and the claim is proven.

Assume C is in good position, and let $Q_1, \ldots, Q_s$ be the points on $\widetilde{C} \cap L_0$ other than the fundamental points P_1 and P_2. We have

$$m_{Q_i}(\widetilde{C}) \leq I\left(Q_i, \widetilde{C} \cap L_0\right) \qquad \text{and} \qquad \sum_{i=1}^{s} I\left(Q_i, \widetilde{C} \cap X_0\right) = r_0, \qquad (*)$$

(with similar identities for P_1 and P_2.) The first inequality comes from the properties of intersection numbers; as above $I\left(Q_i, \widetilde{C} \cap X_0\right) = I\left(Q_i, F_{r_0}(X_2, X_1) \cap X_0\right)$ and the sum $\sum_{i=1}^{s} I\left(Q_i, F_{r_0}(X_2, X_1) \cap X_0\right) = r_0$ by Bézout. As a particular case of $(*)$, if $P_0 \notin C$ then there are no non-fundamental points on $\widetilde{C} \cap L_0$, as $r_0 = 0$.

Remark 3.7. If C is in good position and $P_0 \in C$, locally around P_0 the quadratic transformation looks like a blowing up. We wish to make this statement more precise: let $C_0 = (C \cap U) \cap \{P_0\}$, which is a neighborhood of P on C. Let $\widetilde{C}_0 = \widetilde{C} \smallsetminus \mathrm{V}(X_1 X_2)$ and

$$f \colon \widetilde{C}_0 \to C_0$$

the restriction of Q to $\widetilde{C}_0$. Let $F_* = F(1, X, Y) \in k[X, Y]$ and $C_* = \mathrm{V}(F_*) \subset \mathbb{A}^2$. Define $\widetilde{F}_* = F(1, X, UX) X^{-r_0} \in k[X, U]$, $\widetilde{C}_* = \mathrm{V}(\widetilde{F}_*)$ and

$$\psi \colon \widetilde{C}_* \to C_* \qquad \psi(x, u) = (x, ux),$$

so that ψ is the projection of the blowing up of the previous section (proof of Proposition 3.4). Then the claim we wanted to reformulate becomes: there are neighborhoods W of $(0,0)$ in C_* and $\widetilde{W} = \psi^{-1}W$ of $\mathrm{V}(X) \cap \widetilde{C}_*$ in $\widetilde{C}_*$, and isomorphisms $\varphi\colon W \to C_0$ and $\widetilde{\varphi}\colon \widetilde{W} \to \widetilde{C}_0$ such that $\varphi\psi = f\widetilde{\varphi}$, i.e. the diagram

$$\begin{array}{ccccccc} \widetilde{C}_* & \supset & \widetilde{W} & \xrightarrow[\sim]{\widetilde{\varphi}} & \widetilde{C}_0 & \subset & \widetilde{C} \\ {\scriptstyle\psi}\big\downarrow & & \big\downarrow & & \big\downarrow{\scriptstyle f} & & \\ C_* & \supset & W & \xrightarrow[\varphi]{\sim} & C_0 & \subset & C \end{array}$$

commutes. We can take $W = (C_* \smallsetminus \mathrm{V}(XY)) \cup (0,0)$ so that $\widetilde{W} = (\widetilde{C}_* \smallsetminus \mathrm{V}(U)) \cup \{(0,0)\}$; $\varphi(x,y) = [1 : x : y]$ and $\widetilde{\varphi}(x,u) = [ux : u : 1]$. Indeed

$$f\widetilde{\varphi}(x,u) = f[ux : u : 1] = [u : ux : u^2x] = [1 : x : ux] = \varphi\psi(x,u),$$

the inverse of $\widetilde{\varphi}$ is given by $[x_0 : x_1 : x_2] \mapsto (x_0/x_1, x_1/x_2)$.

Excellent position

We make another assumption on the position of C. We say that C is in *excellent position* if it is in good position and

- $r_1 = r_2 = 0$;
- L_0 intersects C transversally in d distinct (non-fundamental) points;
- L_1 and L_2 each intersect C transversally in $d - r_0$ distinct points other than P_0.

Assuming that C is in excellent position, we can now study the singularities of $\widetilde{C}$. We have the following cases.

1. *The singularities of $\widetilde{C}$ in U correspond to the singularities of C in U, the correspondence preserving multiplicity and ordinary multiple points.* In fact both these properties of a point $P \in C$ correspond to properties of the local ring $\mathcal{O}_{C,P}$: the multiplicity is $\dim_k \mathfrak{m}_P/\mathfrak{m}_P^2$, while the being an ordinary point is equivalent to the existence of $g_1, \ldots, g_m \in \mathfrak{m}_P$ such that $g_i - \lambda g_j \notin \mathfrak{m}_P^2$ for all $i \neq j, \lambda \in k$, and $\dim_k \mathcal{O}_{C,P}/(g_i) > m$, with $m = m_P(C)$ [Ful69, Problem 3.24]. Since f induces isomorphisms on local rings, it follows that the correspondence preserves multiplicities and ordinary multiple points.

2. *There are no non-fundamental points on $\widetilde{C} \cap L_1$ and $\widetilde{C} \cap L_2$. If $Q_1, \ldots, Q_s$ are the non-fundamental points on $\widetilde{C} \cap L_0$, then $m_{Q_i}(\widetilde{C}) \leq I\left(Q_i, \widetilde{C} \cap L_0\right)$ and $\sum_{i=1}^s I\left(Q_i, \widetilde{C} \cap L_0\right) = r_0$.* This follows directly from $(*)$.

3. *The fundamental points P_0, P_1 and P_2 are ordinary multiple points on $\widetilde{C}$ with multiplicities d, $d - r_0$ and $d - r_0$ respectively.* Again we apply $(*)$ but this time to $\widetilde{C}$, and we observe that $\widetilde{\widetilde{C}} = C$: for the case of P_0, since C is in excellent position $C \cap L_0$ consists of d distinct points $Q_1, \ldots, Q_d$ each with $I\left(Q_i, C \cap L_0\right) = 1$ so that

$$d = \sum_{i=1}^{d} I\left(Q_i, C \cap L_0\right) = m_{P_0}(\widetilde{C}),$$

where the last equality is due to $(*)$ ($\widetilde{C}$ is in good position because C is.) The point P_0 is ordinary by Remark 3.7: locally around P_0 the restriction $\widetilde{f}\colon C \dashrightarrow \widetilde{C}$ of Q to C looks like the blow up of $\widetilde{C}$ at P_0, and we have seen in Section 3.1 that the number of points in the fiber corresponds to the number of distinct tangent lines. Since $\widetilde{f}^{-1}(P_0) = \{Q_1, \ldots, Q_d\}$, $\widetilde{C}$ has d distinct tangent lines at P_0. Similarly for P_1 and P_2.

Even if P_0 was a non-ordinary multiple point on C, it becomes an ordinary point on $\widetilde{C}$. However, the number of non-ordinary multiple points of could still not decrease: we may introduce new not-necessarily-ordinary singularities for $\widetilde{C}$ at the points $Q_1, \ldots, Q_s$ of $\widetilde{C} \cap L_0$. To ensure that by applying a finite number of quadratic transformations the process will eventually end we need to introduce a new quantity, which will decrease whenever we introduce new multiple points.

For any irreducible plane curve C of degree d, with multiple points of multiplicity $r_P = m_P(C)$, let

$$g^*(C) = \frac{(d-1)(d-2)}{2} - \sum_P \frac{r_P(r_P - 1)}{2}.$$

This quantity is a nonnegative integer [Ful69, Theorem 2 of §5.4].

Proposition 3.8. *If C is in excellent position, then*

$$g^*(\widetilde{C}) = g^*(C) - \sum_{i=1}^{s} \frac{\widetilde{r}_i(\widetilde{r}_i - 1)}{2},$$

where $Q_1, \ldots, Q_s$ are the non-fundamental points of $\widetilde{C} \cap L_0$ and $\widetilde{r}_i = m_{Q_i}(\widetilde{C})$. In particular, if one of the Q_i is a multiple point for $\widetilde{C}$ then $g^*(\widetilde{C}) < g^*(C)$.

Proof. It is a but a straightforward computation using the properties above:

$$g^*(\widetilde{C}) = \frac{(2d - r_0 - 1)(2d - r_0 - 2)}{2} - \sum_P \frac{m_P(\widetilde{C})(m_P(\widetilde{C}) - 1)}{2},$$

and using 1–3 we split the sum over the multiple points of $\widetilde{C} \cap U$, the fundamental points P_0, P_1, P_2 and the non-fundamental points $Q_1, \ldots, Q_s$ of $\widetilde{C} \cap L_0$:

$$\begin{aligned}
g^*(\widetilde{C}) = \frac{(2d - r_0 - 1)(2d - r_0 - 2)}{2} &- \Bigg(\sum_{P \in C \cap U} \frac{m_P(\widetilde{C})(m_P(\widetilde{C}) - 1)}{2} + \\
&+ \frac{d(d-1)}{2} + 2\frac{(d - r_0)(d - r_0 - 1)}{2} + \sum_{i=1}^{s} \frac{\widetilde{r}_i(\widetilde{r}_i - 1)}{2} \Bigg) = \\
&= \frac{d(d-1)}{2} - \left(\sum_{P \in C \cap U} \frac{m_P(C)(m_P(C) - 1)}{2} + \frac{r_0(r_0 - 1)}{2} + \sum_{i=1}^{s} \frac{\widetilde{r}_i(\widetilde{r}_i - 1)}{2} \right),
\end{aligned}$$

and since the only multiple point for C outside U is P_0,

$$\begin{aligned}
g^*(\widetilde{C}) &= \frac{d(d-1)}{2} - \sum_P \frac{m_P(C)(m_P(C) - 1)}{2} - \sum_{i=1}^{s} \frac{\widetilde{r}_i(\widetilde{r}_i - 1)}{2} = \\
&= g^*(C) - \sum_{i=1}^{s} \frac{\widetilde{r}_i(\widetilde{r}_i - 1)}{2},
\end{aligned}$$

we get the wanted equality. □

3.3 Resolution of Plane Curves

We are finally ready to resolve the singularities of any plane curve. The idea is to transport a multiple point P of C to $[1:0:0]$ via a projectivity T, that is $T([1:0:0]) = P$, and apply what we have developed in the previous section. To do so, we will need C^T to be in excellent position: if this is the case, we say that $Q \circ T$ is a *quadratic transformation centered at* P.

Theorem 3.9. *By a finite sequence of quadratic transformations, any irreducible projective plane curve may be transformed into a curve whose only singularities are ordinary multiple points.*

Celarly, this result along eith Proposition 3.5 tells us how to resolve the singularities of any plane curve. The proof will rely on the existence of enough quadratic transformations centered at different points of C.

Characteristic zero

This case is made easy by the following lemmas:

Lemma 3.10. *Let* $\operatorname{char} k = 0$ *and* C *be an irreducible projective plane curve of degree* d*,* $P \in C$ *with* $m_P(C) = r$*. For all but finitely many lines* L *through* P*,* L *intersects* C *in* $d - r$ *distinct points other than* P*.*

Proof. Let $F \in k[X_0, X_1, X_2]$ be an equation for C of degree d. Since the result is invairant under projectivity we may assume $P = [1:0:0]$. Excluding only the line $\mathrm{V}(X_1)$, we may focus on the lines through P of the form $\mathrm{V}(X_2 - \lambda X_1) = \{[t:1:\lambda] \mid t \in k\} \cup \{P\}$ for $\lambda \in k$. Writing

$$F = \sum_{i=r}^{d} F_i(X_1, X_2) X_0^{d-i}$$

with F_i homogeneous of degree i, the points of $\mathrm{V}(X_2 - \lambda X_1) \cap C$ other than P correspond to the roots of the polynomial $G = F(T, 1, \lambda) \in k[T]$. All these roots are distinct if G is nonzero ($F_r(1, \lambda)$ vanishes only for finitely many λ's) and it is coprime with its derivative $dG/dT = \partial F/\partial X_0(T, 1, \lambda)$, i.e. if $\mathrm{V}(F, \partial F/\partial X_0, X_2 - \lambda X_1) = \{P\}$. However $\mathrm{V}(F, \partial F/\partial X_0)$ consists of finitely many points since F is irreducible and $\partial F/\partial X_0 \neq 0$ as $\operatorname{char} k \neq 0$, so all but finitely many choices for λ will ensure that G has distinct roots. □

Lemma 3.11. *Let* $\operatorname{char} k = 0$*,* C *be an irreducible projective plane curve of degree* d *and* P *a point on* C*. Then there exists a projectivity* T *such that* C^T *is in excellent position.*

Proof. By Lemma 3.10 we may find two lines L' and L'' that each intersect C at $d - r$ distinct points other than P. Taking any point P' on L' that is not on C, again by Lemma 3.10 we may find a line L through P' that intersects C transversally at d points and intersects L'' at a point P'' not on C. The wanted change of coordinates is the unique projectivity that maps P_0, P_1, P_2 onto P, P', P'' and L_0, L_1, L_2 onto L, L', L'' respectively. □

now, the proof if $\operatorname{char} k = 0$ is immediate. We will have problems with the case of positive characteristic.

Proof of Theorem 3.9 if $\operatorname{char} k = 0$. We take successive quadratic transformations centering each one at a non-ordinary multiple point.

After each quadratic transformation either the number of multiple points decreases or we may introduce new singularities on an exceptional line. In the latter case, by Proposition 3.8 the quantity $g^*(C)$ decreases, so we conclude in at most $\#\{\text{non-ordinary multiple points for } C\} + g^*(C)$ steps. □

The dual curve and characteristic p

Assume for the rest of the section that $\operatorname{char} k = p > 0$. The problem is that Lemma 3.10 is no longer true: assuming $P = [1 : 0 : 0]$ and using the notations of that proof, we could have that the derivative $\partial F/\partial X_0$ vanishes in $k[X_0, X_1, X_2]$.

For an irreducible plane curve C of degree d, we will call a point $P \in \mathbb{P}^2$ *terrible* if there are infinitely many lines through P that meet C in less than $d - r$ distinct points other than P, where $r = m_P(C)$. Observe that for a point to be terrible we need to have $p \mid d - r$.

Example 3.12. Let C be the curve $\mathrm{V}(X_2^{p+1} - X_0^p X_1)$. Every line of the form $\mathrm{V}(X_2 - \lambda X_1)$ intersects C at only one other point other than $[1 : 0 : 0]$, namely $[\xi : 1 : \lambda]$ where ξ is the (unique!) p-th root of λ^{p+1} in k.

To better study the case of terrible points, we adopt the following approach. The set of lines of $\mathbb{P}^2$ form a $\mathbb{P}^2$, whose coordinates we denote by U_0, U_1, U_2. If $F \in k[X_0, X_1, X_2]$ is an equation for C, $d = \deg F$, the k-algebra morphism

$$\begin{aligned} \alpha\colon k[U_0, U_1, U_2] &\to S(C) = k[X_0, X_1, X_2]/(F), \\ U_i &\mapsto \partial F/\partial X_i \end{aligned}$$

is a morphism of graded rings, so its kernel is a homogeneous ideal that defines a closed subset $\mathrm{V}(\ker \alpha)$ of $\mathbb{P}^2$ which we will denote by $C^\vee$. Since $k[U_0, U_1, U_2]/\ker \alpha$ can be identified with a subalgebra of the domain $S(C)$, it is itself a domain and $C^\vee$ is a variety. It contains all points of the form $[\partial F/\partial X_0(Q) : \partial F/\partial X_1(Q) : \partial F/\partial X_2(Q)]$ for Q a smooth point on C: indeed if $G \in \ker \alpha$

$$G\left(\frac{\partial F}{\partial X_0}(Q), \frac{\partial F}{\partial X_1}(Q), \frac{\partial F}{\partial X_2}(Q)\right) = \alpha(G)(Q) = 0$$

Since C has infinitely many smooth points, we deduce that $C^\vee$ is reduced to a single point iff C is a line. Thus for $d > 1$ the variety $C^\vee$ is a curve, which is called the *dual curve* of C.

Assume C is not a line and P is a terrible point for C of multiplicity r. Excluding those that pass through multiple points for C, there are infinitely many lines L through P that meet C in less than $d - r$ smooth points. Necessarily, those L will be the tangent to C at one of the intersection points and thus correspond to a point of $C^\vee$.

The set of lines through P forms an hyperplane $\mathbb{P}^1$ of the set of lines in $\mathbb{P}^2$; since $C^\vee$ has infinitely many points in common with this hyperplane, by irreducibility they coincide. It follows easily that there cannot be more than one terrible point for C. In particular, there is always a line that meets C at d distinct points.

Proof of Theorem 3.9 if $\operatorname{char} k = p > 0$. Lemma 3.11 is false in this case: if P is terrible for C it may be impossible to perform a quadratic transformation centered at P. However since there is at most one terrible point for C, we can make a quadratic transformation centered at another point Q which we can take to have multiplicity $m = 0$ or 1, and so that P is not on a fundamental line. If $\widetilde{C}$ is the quadratic transformation of C, then by Section 3.2 $\widetilde{C}$ has degree $\widetilde{d} = 2d - m$. Since P is terrible, p divides $d - r$ so

$$\widetilde{d} - r = 2d - m - r \equiv d - m \mod p$$

Choosing either $m = 0$ or $m = 1$ will insure that the point $\widetilde{P}$ on $\widetilde{C}$ corresponding to P will not be terrible for $\widetilde{C}$, so we may proceed as in the case of $\operatorname{char} k = 0$. We could introduce new terrible points for $\widetilde{C}$ different from $\widetilde{P}$, but again the decreasing of the quantity $g^*(C)$ allows to conclude in a finte number of steps. □

3.4 Nonsingular Models of Curves

In this final section of the chapter we generalize the results seen to an arbitrary curve, obtaining its nonsingular model, and we establish the connection between function fields in one variable and curves.

Given two local rings A and B, we say that B *dominates* A if A is a subring of B and the maximal ideal $\mathfrak{m}_A$ of A is contained in the maximal ideal $\mathfrak{m}_B$ of B, $\mathfrak{m}_A \subset \mathfrak{m}_B$.

If K is an extension of k, we say that a local ring A is a *local ring of* K if we have inclusion of subrings $k \subset A \subset K$ and $K = \operatorname{Frac} A$. Clearly for any variety X and $P \in X$, the local ring $\mathcal{O}_{X,P}$ is a local ring of $k(X)$. Similarly a *discrete valuation ring of* K is a DVR that is a local ring of K.

Theorem 3.13. *Let C be a projective curve. Suppose L is an extension of $k(C)$ and R is a DVR if L, with $R \not\supset k(C)$. Then there is a unique point $P \in C$ such that R dominates $\mathcal{O}_{C,P}$.*

Proof. Uniqueness is easy. Suppose R dominates $\mathcal{O}_{C,P}$ and $\mathcal{O}_{C,Q}$ for $P \neq Q$; there exists a function $f \in k(C)$ defined both at P and Q such that $f(P) = 0$ (i.e. $f \in \mathfrak{m}_P$) and $f(Q) = 1$ (so $1/f$ is defined at Q, $1/f \in \mathcal{O}_{C,Q}$). If ord denotes the order function on L induced by R, this means $\operatorname{ord} f > 0$ and $-\operatorname{ord} f = \operatorname{ord}(1/f) \geq 0$, absurd.

We now prove the existence. The curve C can be embedded as a closed subvariety of $\mathbb{P}^n$ for some n; if $x_0, \dots, x_n$ are the coordinates functions of C in $S(C) = k[X_0, \dots, X_n]/\operatorname{I}(C) = k[x_0, \dots, x_n]$, we may choose this embedding so that none of the x_i is zero. Let

$$N = \max_{i,j} \operatorname{ord}\left(\frac{x_i}{x_j}\right),$$

and assume by permuting coordinates that $N = \operatorname{ord}(x_j/x_0)$ for some j. Then for all i

$$\operatorname{ord}\left(\frac{x_i}{x_0}\right) = \operatorname{ord}\left(\frac{x_j}{x_0}\frac{x_i}{x_j}\right) = N - \operatorname{ord}\left(\frac{x_i}{x_j}\right) \geq 0,$$

so we have $x_i/x_0 \in R$. If C_* is the affine curve $C \smallsetminus \mathrm{V}(X_0)$ then $k[C_*] = k[x_1/x_0, \dots, x_n/x_0] \subset R$.

Let $\mathfrak{m}$ be the maximal ideal of R and J the prime ideal $\mathfrak{m} \cap k[C_*]$ of $k[C_*]$. If the closed subvariety W of C_* corresponding to J is the whole C_* then $J = 0$, so every element of $k[C_*]$ is a unit in R. But then $k(C) = \operatorname{Frac} k[C_*] \subset R$, contradicting our assumption. So W is a single point P, and R dominates $\mathcal{O}_{C,P}$. □

We have the important corollary:

Corollary 3.14. *Let $f : C' \dashrightarrow C$ be a rational map between curves, and suppose that C is projective. The domain of f contains every smooth point of C'. Hence if C' is smooth, f is a morphism.*

Proof. A rational map between curves is either dominating or constant, so we can suppose f is dominating. Then f^* embeds $k(C)$ as a subfield of $k(C')$. For a smooth point $P \in C'$, consider the DVR $\mathcal{O}_{C',P} \subset k(C')$. We have $k(C) \not\subset \mathcal{O}_{C',P}$ as if it were, the fact that the field extension $k(C')/k(C)$ is algebraic would imply that $\mathcal{O}_{C',P}$ is a field. So we can apply Theorem 3.13 to the DVR $\mathcal{O}_{C',P} \subset k(C')$, and find a point $Q \in C$ such that $\mathcal{O}_{C',P}$ dominates $f^*(\mathcal{O}_{C,Q})$. Then by [Ful69, Proposition 11 of §6.6] P belongs to the domain of f, and $f(P) = Q$. □

We can finally prove the most important result of this chapter.

Theorem 3.15 (Existence and uniqueness of the nonsingular model). *Let C be a projective curve. Then there exists a smooth projective curve X and a birational morphism $f \colon X \to C$. If $f' \colon X' \to C$ is another such morphism, then there exists a unique isomorphism $g \colon X \to X'$ such that $f'g = f$.*

Proof. Uniqueness follows from Corollary 3.14. Indeed the birational map $ff'^{-1} \colon X \to X'$ is defined everywhere as X is smooth hence it is a morphism, and so is its inverse.

For the existence, take any plane curve $\widetilde{C}$ that is birationally equivalent to C (Theorem 1.15). By theorem Theorem 3.9, this curve may be taken to only have ordinary singularities so that by blowing it up (Proposition 3.5) we obtain a smooth curve X that is birational to C. The fact that the map $f \colon X \to C$ we obtained is a morphism follows again from Corollary 3.14.

If C is a plane curve surjectivity of f follows from the construction of X. For any point $P \in C$ we may find $\widetilde{C}$ so that the map $\widetilde{C} \dashrightarrow C$ is defined at some point $\widetilde{P}$ which is mapped onto P: indeed, when applying quadratic transformations not centered at P, we may choose them so that P does not lie on an exceptional line. We are free to choose them so by the already proven uniqueness. If C is not plane, we may choose the morphism from C to a plane curve so that it is an isomorphism in a neighborhood of P, and then proceed as above. □

The curve X obtained in the Theorem 3.15 is called the *nonsingular model* of C. We identify the function field $k(X)$ with $k(C)$ by means of the isomorphism f^*. The points of X are called *places* of C and the places in the fiber $f^{-1}(P)$ above a point $P \in C$ are the *places centered at P*.

The following proposition states some properties of the nonsingular model.

Proposition 3.16. *let C be a projective plane curve and $f: X \to C$ its nonsingular model. For all points $P \in C$, there exists an arbitrarily small affine neighborhood U of P such that:*

- *$\widetilde{U} = f^{-1}U$ is affine and $k[\widetilde{U}]$ is a finite module over $k[U]$ (i.e. the morphism f is finite;)*
- *there exists a nonzero $t \in k[U]$ such that $t \cdot k[\widetilde{U}] \subset k[U]$;*
- *the k-vector space $k[\widetilde{U}]/k[U]$ is finite-dimensional.*

Proof. The first point follows from Proposition 3.4, Remark 3.7 and by choosing the quadratic transformations not centered at P in the construction of X so that P does not meet any exceptional line (again, we are allowed to do so by uniqueness of the nonsingular model.)

For the second point, if $z_1, \dots, z_n$ are generators for $k[\widetilde{U}]$ over $k[U]$, then since $k[\widetilde{U}]$ and $k[U]$ have the same fraction field $k(X) = k(C)$ (identified via f^*,) writing each z_i as a quotient of two elements of $k[U]$ and taking t to be the lcm of the denominators insures $tz_i \in k[U]$ for all i.

Multiplication by t yields a k-linear mapping $k[\widetilde{U}] \to k[U]$, which factors as an injective mapping $k[\widetilde{U}]/k[U] \to k[U]/(t)$. Thus to show the last point it is to sufficient to prove that $k[U]/(t)$ is finite-dimensional over k. Since t has finitely many zeros in U, this is a consequence of the Nullstellensatz (Proposition 1.16). □

Smooth curves and fields in one variable

Theorem 3.15 and Theorem 3.13 allow us to observe the deep connection between smooth projective curves and function fields in one variable. We will show that the two categrìories they form are equivalent, so that we find another correspondence between geometric objects and purely algebraic ones.

Let X be any smooth projective curve. If R is a DVR of $k(X)$, then by Theorem 3.13 R dominates $\mathcal{O}_{X,P}$ for some $P \in X$. Both being DVR's, it is not difficult to see that $R = \mathcal{O}_{X,P}$. Thus the map

$$P \mapsto \mathcal{O}_{X,P},$$

from X to the set of DVR's of $k(X)$ is bijective and a homeomorphism, if we endow the codomain with the cofinite topology. Since

$$\mathcal{O}_X(U) = \bigcap_{P \in U} \mathcal{O}_{X,P} \ ,$$

the structure of the variety X can be completely recovered from the field $k(X)$. On the other hand, Theorem 3.15 and Theorem 1.15 tell us that any function field in one variable is the function field of some smooth curve.

Theorem 3.17. *The functor $X \mapsto k(X)$ gives an equivalence between the category of smooth projective curves, with arrows dominant (nonconstant) morphisms, and the category of function fields in one variable.*

Another criterion for Noether's conditions

Let us go back to considering an irreducible projective plane curve C with nonsingular model $f\colon X \to C$.

For any place $Q \in X$ centered at $P \in C$, we have an order function ord_Q on the field $k(X)$, identified with $k(C)$ via f^*, defined by the DVR $\mathcal{O}_{X,P}$. If G is any plane curve (possibly reducible), let $g \in \mathcal{O}_{C,P} \subset k(C)$ denote the image of $G_* = G/L^{\deg G} \in \mathcal{O}_{\mathbb{P}^2,P}$ under the canonical morphism $\mathcal{O}_{\mathbb{P}^2,P} \to \mathcal{O}_{C,P}$, where L is any line not passing through P.

Definition 3.18. If G is any plane curve and g is defined as above, we define $\mathrm{ord}_Q(G)$ to be $\mathrm{ord}_Q(f^*g)$. Similarly, for $z \in k(C)$ we write $\mathrm{ord}_Q(z)$ for $\mathrm{ord}_Q(f^*z)$.

As usual, this does not depend on the choice of L.

The following proposition will relate the intersection number of C and G at P as the sum of the orders of G at the places centered at P:

Proposition 3.19. *Let C be any irreducible projective plane curve, $f\colon X \to C$ its nonsingular model and P a point on C. Let G be a plane curve, possibly reducible. Then*

$$I\,(P, C \cap G) = \sum_{Q \in f^{-1}(P)} \mathrm{ord}_Q(G)$$

Proof. Let g be the image of G_* in $\mathcal{O}_{C,P}$, as above. Take U as in Proposition 3.16, and so small that U does not contain any zeros or poles for g, except eventually P. Then if F is an equation for C

$$I\,(P, C \cap G) = \dim_k \mathcal{O}_{\mathbb{P}^2,P}/(F_*, G_*) = \dim_k \mathcal{O}_{C,P}/(g) = \dim_k k[U]/(g),$$

where the last equality is due to Proposition 1.17. If $\widetilde{U} = f^{-1}U$, identify then we have an injective map $k[U] \to k[\widetilde{U}]$ given by $z \mapsto f^*(gz)$. Since the quotient $k[\widetilde{U}]/f^*k[U]$ is finite-dimensional by Proposition 3.16, some linear algebra and diagram chasing tell us that

$$\dim_k k[U]/(g) = k[\widetilde{U}]/(f^*g).$$

Again by Proposition 1.17,

$$\dim_k k[\widetilde{U}]/(f^*g) = \sum_{Q \in f^{-1}(P)} \dim_k \mathcal{O}_{X,Q}/(f^*g) = \sum_{Q \in f^{-1}(P)} \mathrm{ord}_Q(G),$$

as we wanted. $\square$

Lemma 3.20. *Let $f\colon X \to C$ be the nonsingular resolution of C, P an ordinary multiple point on C of multiplicity r and $Q_1, \ldots, Q_r$ the places of X centered at P. If $z \in k(C)$ satisfies $\mathrm{ord}_{Q_i}(z) \geq r-1$ for all $i = 1, \ldots, r$, then $z \in \mathcal{O}_{C,P}$.*

Proof. Again as in the previous proof, take U as given by Proposition 3.16 and such that z is defined everywhere in U. If $\widetilde{U} = f^{-1}U$, we may also take U so that the map $f\colon \widetilde{U} \to U$ looks like the proof of Proposition 3.4; in particular $x^{r-1}k[\widetilde{U}] \subset k[U]$. By Remark 3.2, we know that $\mathrm{ord}_{Q_i}(x) = 1$, so

$$\mathrm{ord}_{Q_i}(x^{1-r}z) \geq 0$$

and $x^{1-r}z \in k[\widetilde{U}]$ is defined everywhere in $\widetilde{U}$. But $x^{r-1}(x^{1-r}z) = z \in k[U] \subset \mathcal{O}_{C,P}$ as desired. $\square$

The final result of this chapter is another criterion for verifying Noether's conditions, which will be fundamental in the next chapter.

Proposition 3.21. *Let C be an irreducible projective plane curve with equation F, and let $P \in C$ be an ordinary multiple point of multiplicity r. If $Q_1, \ldots, Q_r$ are the places of X centered at P and G, H two (possibly reducible) plane curves. If*

$$\mathrm{ord}_{Q_i}(H) \geq \mathrm{ord}_{Q_i}(G) + r - 1,$$

for all $i = 1, \ldots, r$, then Noether's conditions are satisfied at P.

Proof. Let L be a line not passing through P, $F_*, G_*, H_* \in \mathcal{O}_{\mathbb{P}^2,P}$ as usual and $g, h \in \mathcal{O}_{C,P}$ the images of G_*, H_* respectively. Then $H_* \in (F_*, G_*) \subset \mathcal{O}_{\mathbb{P}^2,P}$ is equivalent to $h \in (g) \subset \mathcal{O}_{C,P}$, which in turn is equivalent to $h/g \in \mathcal{O}_{C,P}$. Our hypothesis allow us to apply Lemma 3.20 to $z = h/g$ and conclude. $\square$

Chapter 4

Divisors and Genus

Our study of the geometry of curves will greatly be aided by the language of divisors. We will establish a first connection between rational functions with certain poles and the genus of a curve in Riemann's Theorem, which is a rougher version of Riemann-Roch.

In this chapter, C will be an irreducible projective curve, X a nonsingular model of C, $f\colon X \to C$ the birational morphism Theorem 3.15. We identify the function fields $k(X) = k(C)$ by means of f^*. A point $P \in C$ will be identified with the places of $k(X)$ and ord_P will denote the order function on $k(X)$.

4.1 Divisors

Definition 4.1. A *divisor* on X is a formal sum

$$D = \sum_{P \in X} n_p P$$

where only finitely many n_p is nonzero. The set of divisors on X is precisely the free abelian group generated by the points of X. Let us call $D(X)$ the group of divisors on X

The *degree* of a divisor D is simply the sum $\deg(D) = \sum_{P \in X} n_p$ of its coefficients. A divisor D is said to be effective if $n_P \geq 0$ for all $P \in X$.

For two divisors $D = \sum_{P \in X} n_p P$ and $K = \sum_{P \in X} m_p P$, we will write $D \geq K$ if $n_p \geq m_p$ for all $P \in X$.

Definition 4.2. Suppose C is a plane curve of degree n. For any plane curve F not containing C as a component, the divisor of F is defined to be

$$\operatorname{div} F = \sum_{P \in X} \operatorname{ord}_P(F) P.$$

The factor $\operatorname{ord}_P(F)$ makes sense because we identified the function fields of C and X at the beginning.

If $\deg(F) = m$, due to Bézout, the degree of $\operatorname{div} F$ is

$$\sum_{P \in X} \operatorname{ord}_P(F) = \sum_{P \in C} I(P, F \cap C) = mn.$$

We can define the divisor of any $z \in k(X)$ as $\operatorname{div} z = \sum_{P \in X} \operatorname{ord}_P(z) P$.

Example 4.3. Say $X = C$ is given by $F(x, y, z) = y^2z - x^3 + xz^2$. On the affine patch $z = 1$, it has the form $f(x, y) = y^2 - x^3 + x$. The points $e_1 = [1 : 0 : 1], e_2 = [-1 : 0 : 1]$ and $e_3 = [0 : 0 : 1]$ lie on this curve. So the sum $D = 2e_1 + 3e_2 + 5e_3$ is an effective divisor on X. And, the divisor D is bigger than $D' = 2e_2 - e_3$.

The line $g(x, y) = x + y$ meets C at exactly three points; e_3 and some P_1, P_2 whose values we need not know. Let's say we want to compute the divisor of g on X. Then, we need $\mathrm{ord}_{P_i}(g)$ for each i.

By previous results, we know that $\mathrm{ord}_{P_i}(g) = I(P_i, f \cap g)$. One could deduce from Bézout that each intersection number will be 1. Or, since they have no common components, one could compute k-dimension of $k[x, y]/(f, g)$ to find the intersection numbers. So, $\operatorname{div} g = P_1 + P_2 + e_3$.

Now take $h(x, y) = y$. It meets X at 3 points as well, e_1, e_2 and e_3. Meaning $\operatorname{div} h = e_1 + e_2 + e_3$ The rational function g/h therefore has the divisor $\operatorname{div} g/h = \operatorname{div} g - \operatorname{div} h = e_3 + P_1 + P_2 - e_1 - e_2 - e_3 = P_1 + P_2 - e_1 - e_2$. Notice that the degree of this divisor is 0.

The rational function given by $(x + y)/y^2$ on $z = 1$ has again 3 distinct zeros e_3, P_1, P_2, but now the orders of pole points are doubled. This is where we need to look at the line at infinity $z = 0$. X intersect $z = 0$ at $[0 : 1 : 0]$.

$$I([0 : 1 : 0], z \cap y^2z - x^3 + xz^2) = I([0 : 1 : 0], z \cap x^3) = 3I([0 : 1 : 0], z \cap x) = 3$$

So $\operatorname{div}(x + y)/y^2 = P_1 + P_2 + 3[0 : 1 : 0] - 2e_1 - 2e_2 - e_3$; and its order is again zero.

Proposition 4.4. *For any nonzero $z \in k(X)$, $\operatorname{div} z$ is a degree zero divisor.*

Proof. Say $z = f/g$ for some $f, g \in S(C)$ forms of same degree. Simply pick F and G of same degree in $k[X, Y, Z]$ whose residue are f and g respectively. Then $\deg(\operatorname{div} z) = \deg(\operatorname{div} F) - \deg(\operatorname{div} G) = 0$. □

Corollary 4.5. *For any rational function z, $\operatorname{div} z \geq 0$ means z is constant.*

Proof. If $\operatorname{div} z \geq 0$, then $z \in \mathcal{O}_{X,P}$ for all $P \in X$. For some P_0, $z(P_0) = c_0$. Then $\operatorname{div} z - c_0$ is effective and of degree nonzero positive. Which contradicts the proposition unless $z = c_0 \in k$. □

Definition 4.6. We call a divisor obtained from a rational function a *principal divisor*. Since the divisor of any rational function is of degree zero, and $\operatorname{div} fg = \operatorname{div} f + \operatorname{div} g$, principal divisors form a subgroup of $D(X)$, denoted $P(X)$.

The quotient group $C(X) = D(X)/P(X)$ is called the class group of divisors. Any two divisors that belong to the same class group are said to be *linearly equivalent*.

In other words D and D' are linearly equivalent if $D - D' = \operatorname{div} z$ for some $z \in k(X)$. We will denote this equivalence as $D \equiv D'$

Definition 4.7. Assume C has only ordinary singularities. For each $Q \in X$, set $r_Q = m_{f(Q)}(C)$. Define $E = \sum_{Q \in X}(r_Q - 1)Q$.

E is effective, and

$$\sum_{Q \in X}(r_Q - 1) = \sum_{P \in C} \#f^{-1}(P)(m_P(C) - 1) = \sum_{P \in C} m_P(C)(m_P(C) - 1).$$

Any plane curve F such that $\operatorname{div} F \geq E$ is called an adjoint curve to C.

Proposition 4.8. *A curve G is adjoint to C if and only if $m_P(G) \geq m_P(C) - 1$ for all $P \in C$.*

Proof. See [Ful69, Problem 7.19]. $\square$

Theorem 4.9 (Residue Theorem). *Suppose C has only ordinary singularities. Let E be defined as above. Suppose D and D' are effective on X and $D \equiv D'$. Suppose G is adjoint to C and of degree m such that $\operatorname{div} G = D+E+A$, for some effective divisor A. Then there is an adjoint G' of degree m suh that $\operatorname{div} G' = D' + E + A$.*

Proof. Let H and H' be curves of same degree such that $D+\operatorname{div} H = D'+\operatorname{div} H'$. Then,

$$\operatorname{div} GH = \operatorname{div} G + \operatorname{div} H = D + E + A + \operatorname{div} H = D' + E + A + \operatorname{div} H'$$

and therefore $\operatorname{div} GH \geq \operatorname{div} H'+E$. Suppose F is the form defining C. Noether's conditions are satisfied for F,H' and GH. So for some F', G' we have $GH = FF' + H'G'$, and $\deg(G') = m$. Then

$$\begin{aligned}\operatorname{div} GH &= \operatorname{div} F + \operatorname{div} F' + \operatorname{div} H' + \operatorname{div} G' \\ &= \operatorname{div} H' + \operatorname{div} G'.\end{aligned}$$

since F and F' are zero on the curve. We have $\operatorname{div} G' = \operatorname{div} GH - \operatorname{div} H' = D' + E + A$. $\square$

4.2 Vector Space Associated to a Divisor

Each divisor D picks a finite number of points P on X, and to each point it assigns an order n_p. Therefore we may ask which rational functions on X have a pole on each P with order less than n_p.

Definition 4.10. For any divisor D , the space $\mathcal{L}(D)$ is defined as

$$\mathcal{L}(D) = \{f \in k(X) \mid \operatorname{div} f + D \geq 0\} \cup \{0\},$$

it is indeed a k-vector space. Its dimension is denoted as $l(D)$.

Proposition 4.11. *Let D, D' be divisors on X.*

1. *If $D \leq D'$ then $\mathcal{L}(D) \subset \mathcal{L}(D')$ and $\dim_k(\mathcal{L}(D')/\mathcal{L}(D)) \leq \deg(D' - D)$.*
2. *$\mathcal{L}(0) = k$ and if $\deg(D) < 0$, $\mathcal{L}(D) = 0$.*
3. *$\mathcal{L}(D)$ is finite dimensional for all $D \in D(X)$. If $\deg(D) \geq 0$, then $l(D) \leq \deg(D) + 1$.*
4. *If $D \equiv D'$, then $l(D) = l(D')$.*

Proof. 1. Suppose $D' = D+P_1+\cdots+P_s$, then we have the inclusion of vector spaces $\mathcal{L}(D) \subset \mathcal{L}(D+P_1) \subset \mathcal{L}(D+P_1+P_2) \subset \cdots \subset \mathcal{L}(D+P_1+\cdots+P_s)$. If we can show that $\dim(\mathcal{L}(D + P)/\mathcal{L}(D)) \leq 1$, then, at each inclusion, the dimension increases at most by 1. So we get the desired result.

To prove $\dim(\mathcal{L}(D+P)/\mathcal{L}(D)) \leq 1$, let t be the uniformizing parameter of $\mathcal{O}_{X,P}$ and set $r = n_p$ be the coefficent of P. The map $\varphi : \mathcal{L}(D+P) \to k$ defined by $f \mapsto (t^{r+1}f)(P)$ is a well-defined linear map, since $\mathrm{ord}_P(f) \geq -r-1$. If $\varphi(f) = 0$, then $\mathrm{ord}_P(f) \geq -r$ so $f \in \mathcal{L}(D)$, $\ker(\varphi) = \mathcal{L}(D)$. Therefore φ induces an injective map $\mathcal{L}(D+P)/\mathcal{L}(D) \to k$.

2. This is an immediate consequence of the corollary to Proposition 4.4.

3. For $\deg(D) = n$, pick a point $P \in X$, and let $D' = D - (n+1)P$. So, $\mathcal{L}(D') = 0$ and by applying 1), $l(D) = \dim(\mathcal{L}(D)/\mathcal{L}(D')) \leq n+1$.

4. If $D' = D + \operatorname{div} g$, define $\varphi : \mathcal{L}(D) \to \mathcal{L}(D')$ by $\varphi(f) = fg$. The map φ is an isomorphism. So $l(D) = l(D')$.

□

We can restrict any divisor $D \in D(X)$ to a subset S of X.

Definition 4.12. If $D = \sum_{P \in X} n_p P$, and $S \subset X$. Then

$$\mathcal{L}^S(D) = \{f \in k(X) \mid \mathrm{ord}_P(f) \geq -n_P \text{ for all } P \in S\}.$$

and $\deg^S(D) = \sum_{P \in S} n_P$.

Lemma 4.13. *If $D \leq D'$, then $\mathcal{L}^S(D) \subset \mathcal{L}^S(D')$. If S is finite, then $\dim(\mathcal{L}^S(D')/\mathcal{L}^S(D)) = \deg^S(D'-D)$.*

Proof. Assume $D' = D + P$, and define $\varphi : \mathcal{L}^S(D+P) \to k$, $f \mapsto (t^{r+1}f)$ just like in Proposition 4.11. We have to show that it is surjective. It is sufficent to show that it is not the zero map. This amounts to finding a function $f \in k(X)$ with $\mathrm{ord}_P(f) = -r-1$ so that $\varphi(f) \neq 0$, and with $\mathrm{ord}_Q(f) \geq -n_Q$ so that $f \in \mathcal{L}(D+P)$.

Write $S = \{Q_1, \ldots, Q_n\}$. For each $i = 1, \ldots, n$, we can find a projective line L_i passing through Q_i but not through any $Q_j, j \neq i$. Let L_{n+1} be a projective line meeting P but not any Q_i. Further we can take these lines to be transversal to X at Q_i and P. The function

$$z = \prod_i L_i^{-n_{Q_i}} L_0^{-(\sum n_{Q_i} \;+r+1)}$$

satisfies our needs. □

For our next proposition, we will need the following lemma of algebra.

Lemma 4.14. *Let K be the field of fractions of a domain R. Let L be a finite algebraic extension of K.*

1. *For any $v \in L$, there exist some nonzero $a \in R$ such that av is integral over R.*

2. *There is a K-basis $v_1, \ldots, v_n$ of L such that each v_i is integral over R.*

Proof. 1. Let $v \in L$, there exists some polynomial with coefficents $a_i \in K$ such that $a_n v^n + \cdots + a_1 v + a_0 = 0$. Since K is the field of fractions of R, each a_i can be written as $a_i = \frac{b_i}{c_i}$ where $b_i, c_i \in R$ and c_i nonzero. Let $\gamma = \prod c_i$ the product of all c_i, $\gamma_i = \gamma/c_i$ and $t_i = b_i\gamma_i \in R$.

Notice that $\gamma a_i = \frac{\gamma}{c_i} b_i = \gamma_i b_i = t_i$. So multiplying by the equation $a_n v^n + \cdots + a_1 v + a_0 = 0$ with γ we get

$$r_n v^n + r_{n-1} v^{n-1} + \ldots r_1 v + r_0 = 0$$

Now multiply everything with r_n^{n-1} to get

$$(r_n v)^n + r_{n-1}(r_n v)^{n-1} + \cdots + r_1 r_n^{n-2}(r_n v) + r_n^{n-1} r_0 = 0$$

Therefore $r_n v$ is integral over R.

2. Say $v_i, \ldots, v_m$ is a $K-$basis of L. Then for each v_i, there is $a_i \in R$ such that $a_i v_i$ is integral over R. We claim the family $a_i v_i, \ldots, a_m v_m$ form a basis as well. Because the equation

$$\sum \lambda_i(a_i v_i) = \sum (\lambda_i a_i) v_i = 0$$

implies that each λ_i is zero since a_i are nonzero.

□

Proposition 4.15. *Let $x \in k(X)$ be non-constant. Let $Z = (x)_0$ be the divisor which contains only the zeros of z. Set $n = [k(X) : k(x)]$.*

1. *Z is an effective divisor of degree n.*

2. *There is a constant τ such that $l(rZ) \geq rn - \tau$ for all r.*

Proof. Denote $K = k(X)$. Let $Z = \sum n_P P$ and let $m = \deg(Z)$. Firstly we show $m \leq n$.

Let $S = \{P \in X \mid n_P > 0\}$. Since $-Z \leq 0$, by the above lemma,

$$\dim(\mathcal{L}^S(0)/\mathcal{L}^S(-Z)) = \deg^S(Z) = m.$$

Choose $v_1, \ldots, v_m \in \mathcal{L}^S(0)$ so that the residues $\overline{v_1}, \ldots, \overline{v_m} \in \mathcal{L}^S(0)/\mathcal{L}^S(-Z)$ form a basis. We want to show that $v_1, \ldots, v_m$ are linearly independent over $k(x)$. Then we would necessarily have $m \leq \dim_{k(x)} K = [K : k(x)] = n$.

Suppose they are not linearly independent. Then for some $g_i \in k(X)$ we have $\sum g_i v_i = 0$. By reorganizing this sum under a common denominator we would get $\sum G_i v_i = 0$ where $G_i(x) = \lambda_i + x H_i(x) \in k[x]$ with $\lambda_i \in k$ and not all λ_i zero. This would imply that $\sum \lambda_i v_i = -x \sum H_i v_i \in \mathcal{L}^S(-Z)$, but then $\sum \lambda_i \overline{v_i} = 0$. A contradiction.

We can now prove the second claim. Let $w_1, \ldots, w_n$ be a basis of K over $k(x)$. Now, the field $k(x)$ is the field of fractions of $k[x^{-1}]$. By above lemma, since w_i are algebraic over $k(x)$, they are integral over $k[x^{-1}]$

So, each w_i satisfies an equation $w_i^{n_i} + a_{i1} w_i^{n_i} + \cdots = 0$ where $a_{ij} \in k[x^{-1}]$.

The inequality $\operatorname{ord}_P(a_{ij}) < 0$ implies that $\frac{1}{x}$ has a pole at P, which means that x has a zero at P. So, if $P \notin S$, then $\operatorname{ord}_P(a_{ij}) \geq 0$. If $\operatorname{ord}_P(w_i) < 0$, and $P \notin S$, then $\operatorname{ord}_P(w_i^{n_i}) < \operatorname{ord}_P(a_{ij} w_i^{n_i - j})$. One way to see this is starting with the inequality

$$\operatorname{ord}_P(w_i) < 0 \leq \operatorname{ord}_P(a_{ij}).$$

Multiplying the left-hand side with j, which is a nonzero positive integer, to get

$$j \cdot \operatorname{ord}_P(w_i) < 0 \le \operatorname{ord}_P(a_{ij}).$$

Then adding $(n_i - j)\operatorname{ord}_P(a_{ij})$ to both sides to see that

$$n_i \operatorname{ord}_P(w_i) < \operatorname{ord}_P(a_{ij}) + (n_i - j)\operatorname{ord}_P(w_i).$$

Which implies our desired inequality. Now then, using this, and the fact that the order of a finite sum is the minimum of the order of its terms we have the following contradiction.

$$\operatorname{ord}_P(w_i^{n_i} + a_{i1}w_i^{n_i} + \dots) = \min_{i,j}\{\operatorname{ord}_P(w_i^{n_i}), \operatorname{ord}_P(a_{ij}w_i^{n_i-j})\} = \operatorname{ord}_P(w_i^{n_i}).$$

But the sum is zero, and the zero function's order is taken to be infinite.

So, the order of w_i at a point P can be negative only if $P \in S$. But then, for a big enough $t > 0$, one has $\operatorname{div} w_i + tZ \ge 0$ for all i.

For $i = 1, \dots, n$ and $j = 1, \dots, r$, $\operatorname{div} w_i x^{-j} + (r+t)Z \ge 0$. In other words $w_i x^{-j} \in \mathcal{L}((r+t)Z)$.

Since w_i are independent over $k(x)$, and $1, x^{-1}, \dots, x^{-r}$ are independent over k, the family $\{w_i x^{-j}\}$ is independent over k. So $l((r+t)Z) \ge \#\{w_i x^{-j}\} = n(r+1)$. But,

$$\begin{aligned} l((r+t)Z) = l(rZ) + \dim(\mathcal{L}((r+t)Z)/\mathcal{L}(rZ)) &\le l(rZ) + \deg((r+t)Z - rZ) \\ &= l(rZ) + tm. \end{aligned}$$

Thus, $l(rZ) \ge n(r+1) - tm = rn - \tau$. $\square$

For $m \ge n$, observe that $rn - \tau \le l(rZ) \le rm + 1$ since rZ is of positive degree (3. of Proposition 4.11). If we let r get large , we see that $m \ge n$.

4.3 Riemann's Theorem

Theorem 4.16 (Riemann's Theorem). *There is an integer g such that $l(D) \ge \deg(D) + 1 - g$ for all $D \in D(X)$. The smallest such g is called the* genus *of X. The genus is nonnegative.*

Proof. For any $D \in D(X)$, we define the quantity $s(D) = \deg(D) + 1 - l(D)$. So our aim is to find an integer g such that $s(D) \le g$.

Since $s(0) = 0$, such a g , if exists, is positive. For $D \equiv D'$, we have $s(D) = s(D')$ by 4. of Proposition 4.11.

If $D \le D'$, then $s(D) \le s(D')$ by 1. of Proposition 4.11. Now let nonconstant x be in $k(X)$, let $Z = (x)_0$, and let τ be the smallest integer that works for the proposition above. Since for all r,

$$s(rZ) = \deg(rZ) + 1 - l(rZ) \le rn + 1 - rn + \tau = \tau + 1$$

and $rZ \le (r+1)Z$, we must have $s(rZ) = \tau + 1$ for sufficently large r. Then we simply let $g = \tau + 1$.

To be able to finish the proof, we must show that for any $D \in D(X)$, there is a $D' \equiv D$, and an integer $r \ge 0$ such that $D' \le rZ$; Then we will have $s(D) = s(D') \le s(rZ) \le g$.

Let $Z = \sum n_P P$, and $D = \sum m_P P$. So we seek some f such that for $D' = D - \operatorname{div} f$, we have $D - \operatorname{div} f \leq rZ$. Term by term comparison shows that we need f satisfy $m_P - \operatorname{ord}_P(f) \leq rn_P$ for all P. Let $y = x^{-1}$, and let $T = \{P \in X \mid m_P > 0 \text{ and } \operatorname{ord}_P(y) > 0\}$.

Define $f = \prod_{Q \in T}(y - y(Q))^{m_P}$. If $\operatorname{ord}_P(y) \geq 0$, then, $m_P - \operatorname{ord}_P(f) = m_P - \sum_{Q \in T} m_Q \operatorname{ord}_P(y - y(Q)) \leq 0$. If $\operatorname{ord}_P(y) < 0$, then x has a zero at P, i.e $n_P > 0$. Since we can make r as large as we want the inequality is satisfied. $\square$

Corollary 4.17. *If $l(D_0) = \deg(D_0) + 1 - g$, then for any $D \equiv D' \geq D_0$, we have $l(D) = \deg(D) + 1 - g$.*

Proof. Let $s(D) = \deg(D) + 1 - l(D)$ just as above. Then $g \geq s(D) \geq s(D_0) = g$. $\square$

Corollary 4.18. *If $x \in k(X)$, $x \notin k$, then $g = \deg(r(x)_0) - l(r(x)_0) + 1$ for all sufficently large r.*

Corollary 4.19. *There is an integer N such that for all divisors D with $\deg D > N$, $l(D) = \deg D + 1 - g$.*

Proof. Let $D_0 \in D(X)$ such that $l(D_0) = \deg D_0 + 1 - g$, and let $N = \deg D_0 + g$. So, for any D with $\deg D \geq N$, we have $\deg(D - D_0) + 1 - g > 0$. By Riemann's Theorem, $l(D - D_0) > 0$ as well. Then there exist a nonzero $f \in \mathcal{L}(D - D_0)$ such that $D - D_0 + \operatorname{div} f \leq 0$, meaning D is linearly equivalent to a divisor bigger than D_0. The result follows from the first corollary. $\square$

Proposition 4.20 (Genus-degree formula). *Let C be a plane curve with only ordinary multiple points. Let d be its degree, $r_p = m_P(C)$:*

$$g = \frac{(d-1)(d-2)}{2} - \sum_{P \in C} \frac{r_P(r_P - 1)}{2}.$$

Proof. We can assume that X, Y, Z are projective coordinates such that $Z = 0$ intersects C in d distinct points $\{P_1, \ldots, P_d\}$. Let F be the homogenous polynomial that defines C.

Let $E = \sum_{Q \in X}(r_Q - 1)Q$, $r_Q = m_{f(Q)}(C)$ just as in the beginning of this chapter. Define

$$E_m = m \sum_{i=1}^{d} P_i - E. \tag{4.1}$$

So, $\deg(E_m) = md - \sum r_p(r_p - 1)$.

Let V_m be the space of m degree forms that are adjoint to C. We know that G is adjoint to C if and only if $m_P(G) \geq m_P(C) - 1 = r_p - 1$ for all P (Proposition 4.8). We admit the following equation (See [Ful69, Theorem 1 of §5.2] for the proof):

$$\dim V_m \geq \frac{(m+1)(m+2)}{2} - \sum \frac{r_P(r_P - 1)}{2}. \tag{$*$}$$

Where we have equality for sufficiently large m.

We define a linear map $\varphi : V_m \to \mathcal{L}(E_m)$ given by $\varphi(G) = G/Z^m$. Note that since G being adjoint to C means $\operatorname{div} G \geq E$, and $\operatorname{div} G/Z^m = \operatorname{div} G - m \operatorname{div} Z$,

$\varphi(G) \in \mathcal{L}(E_m)$ indeed. Furthermore, $\varphi(G) = 0$ means that G/Z^m is zero in $k(X)$. In which case G is divisible by F.

We show that φ is surjective. Let $f \in \mathcal{L}(E_m)$. Suppose $f = R/S$ where R and S are forms of same degree. Notice that by Lemma 3.20 Noether's Conditions are satisfied for F, S and RZ^m because, since $f \in \mathcal{L}(E_m)$, we have

$$\operatorname{div} RZ^m \geq \operatorname{div} S + E$$

which implies that at every point of C,

$$\operatorname{ord}_P(RZ^m) \geq \operatorname{ord}_P(S) + \operatorname{ord}_P(E) = \operatorname{ord}_P(S) + r_P - 1.$$

So there exist forms A, B such that $RZ^m = AS + BF$. So on C we have $f = R/S = A/Z^m$. Therefore, φ maps A to f. What we have said so far implies the following sequence is exact.

$$0 \longrightarrow W_{m-d} \longrightarrow V_m \longrightarrow \mathcal{L}(E_m) \longrightarrow 0$$

Where W_{m-d} is the space of $m-d$ degree homogeneous polynomials and the map from W_{m-d} to V_m is just multiplication by F. The dimension of $\mathcal{L}(E_m)$ is $\dim(V_m) - \dim(W_{m-d})$. Again, for a large enough m,

$$l(E_m) = \frac{(m+1)(m+2)}{2} - \sum \frac{r_P(r_P-1)}{2} - \frac{(m-d+1)(m-d+2)}{2}$$

We proceed to manipulate this equation algebraically. First we take the sum with r_p to the rightmost position and simplify the expressions with m and d.

$$\begin{aligned}
l(E_m) &= \frac{(m+1)(m+2) - (m+1-d)(m+2-d)}{2} - \sum \frac{r_P(r_P-1)}{2} \\
&= \frac{2mn + 3n - d^2}{2} - \sum \frac{r_P(r_P-1)}{2} \\
&= md + \frac{(3n-d^2)}{2} - \sum \frac{r_P(r_P-1)}{2}
\end{aligned}$$

Then we add and subtract $\sum r_P(r_P-1)$ to be able to plug in $\deg E_m$.

$$\begin{aligned}
l(E_m) &= md - \sum r_P(r_P-1) + \sum r_P(r_P-1) + \frac{(3n-d^2)}{2} - \sum \frac{r_P(r_P-1)}{2} \\
&= \deg E_m + \sum r_P(r_P-1) + \frac{(3n-d^2)}{2} - \sum \frac{r_P(r_P-1)}{2}
\end{aligned}$$

Now, after combining $\sum r_P(r_P-1)$ with $-\sum \frac{r_P(r_P-1)}{2}$ at the rightmost position, we add and subtract 1, to get the term $\frac{(d-1)(d-2)}{2}$ included in our formula.

$$\begin{aligned}
l(E_m) &= \deg E_m + 1 - 1 - \frac{(3n-d^2)}{2} + \sum \frac{r_P(r_P-1)}{2} \\
&= \deg E_m + 1 - \left(\frac{(d-1)(d-2)}{2} - \frac{r_P(r_P-1)}{2} \right)
\end{aligned}$$

But we can make $\deg E_m$ as large as we want! From the third corollary to Theorem 4.16, we have the desired equality. □

Corollary 4.21. *Let C be a plane curve of degree d, $r_p = m_P(C)$. Then,*

$$g \leq \frac{(d-1)(d-2)}{2} - \sum_{P \in C} \frac{r_P(r_P - 1)}{2}.$$

Proof. The g here is precisely the $g^*(C)$ as seen in Section 3.2. We have seen that g^* decreases as we do quadratic transformations. Any irreducible projective plane curve can be transformed into a curve with only ordinary multiple points with a finite amount of quadratic transformations. □

Remark 4.22. If E_m denotes the divisor defined in the proof of the proposition, the long exact sequence constructed above shows that any $h \in \mathcal{L}(E_m)$ can be written as $h = H/Z^m$, for H an adjoint of degree m. Remark also that we have $V_m = \mathcal{L}(E_m)$ for all $m < d$. In particular for E_{d-3} the inequality $(*)$ becomes

$$l(E_{d-3}) = \dim V_{d-3} = \frac{(d-1)(d-2)}{2} - \sum \frac{r_p(r_p - 1)}{2} = g,$$

and

$$\deg E_{d-3} = d(d-3) - \sum r_p(r_p - 1) = 2g - 2.$$

Chapter 5

The Riemann-Roch Theorem

5.1 Derivations and Algebraic Differentials

The purpose of this section is to make algebraic sense of notions one might know from differential geometry. Our rings are always commutative with unity.

Definition 5.1. Let M be an R-module. A module morphism $d : R \to M$ is called a derivation on R if $d(f+g) = d(f) + d(g)$ and $d(fg) = d(f)g + d(g)f$, for all $f, g \in R$.

So for now a derivation is a tuple (M, d). The set derivations on R onto M is denoted by $\mathrm{Der}(R, M)$. But we have a universal derivation in the sense of the following proposition.

Proposition 5.2. *There exists an R-module Ω^1_R and a derivation $d : R \to \Omega^1_R$ such that for any derivation $D : R \to M$, there exist a module morphism $\varphi : \Omega^1_R \to M$ such that $\varphi \circ d = D$.*

Proof. Let A be the R-module generated by the symbols $\{d(f) \mid f \in R\}$. We define Ω^1_R to be this module A quotiented by the following relations.

1. $d(f+g) - d(f) - d(g)$
2. $d(fg) - d(f)g - fd(g)$

Then $f \mapsto d(f)$ is a derivation on R onto Ω^1_R. For the second part, one easily sees that the map $\varphi(d(f)) = D(f)$ is a module morphism satisfying our needs. □

Therefore the sets $\mathrm{Der}(R, M) \equiv \mathrm{Hom}(\Omega^1_R, M)$ are in one-to-one correspondance.

The module Ω^1_R is called the module of algebraic differentials on R.

Definition 5.3. Let R, S be rings. Let $\varphi : S \to R$ be a ring morphism. (In other words, let R be an S -algebra). Let M be an R-module. A derivation $D \in \mathrm{Der}(R, M)$ is said to be an S-linear derivation if $D(\varphi(s)) = 0$ for all $s \in S$.

In a similar sense, there is also a universal module of S-linear differentials.

Proposition 5.4. *There exist an R-module $\Omega^1_{R|S}$ and an S-linear derivation $d : R \to \Omega^1_{R|S}$ such that for any S-linear derivation $D : R \to M$, there is $\varphi : \Omega^1_{R|S} \to M$ such that $\varphi \circ d = D$.*

Proof. The proof goes pretty much the same as Proposition 5.2. We define a module A generated by the symbols $d(f)$. Then we quotient it with the relations $d(f+g) - d(f) - d(g)$, $d(fg) - d(f)g - fd(g)$ and with $d(\varphi(s)), s \in S$. Again, φ will be defined as $\varphi(d(f)) = D(f)$. $\square$

Now, we move into the familiar context of polynomial rings.

Lemma 5.5. *Let $R = k[X_1, \dots, X_n]$. Then $\Omega^1_{R|k}$ is isomorphic to $R^{\oplus n}$.*

Proof. Consider the map $D : R \to R^{\oplus n}$ given by $D(F) = \left(\frac{\partial F}{\partial X_1}, \dots, \frac{\partial F}{\partial X_n}\right)$, where $\frac{\partial F}{\partial X_i}$ is the formal derivative of F with respect to X_i. It is easy to check that this is a k-linear derivation.

By the universal property of $\Omega^1_{R|k}$, there exist a module morphism φ : $\Omega^1_{R|k} \to R^{\oplus n}$ given by $d(f) \mapsto \left(\frac{\partial F}{\partial X_1}, \dots, \frac{\partial F}{\partial X_n}\right)$. This φ is an isomorphism. Since $\varphi(X_j) = (0, \dots, 1, \dots, 0)$, where 1 is in the j-th place, and it's inverse is given by $\psi(a_1, \cdots, a_n) = \sum_{i=1}^n a_i d(X_i)$. $\square$

Meaning, we can identify $\Omega^1_{R|k}$ with $\bigoplus_{i=1}^n k[X_1, \dots, X_n]dX_i$. Algebraic differentials on the whole space k^n therefore have the familiar form of $\sum f_i dX_i$ where f_i are polynomials in $k[X_1, \dots, X_n]$. Now we want to carry these over to the coordinate ring. For that, we use two well-known exact sequences. We will omit the proof of their exactness.

Lemma 5.6 (First Exact Sequence). *Let A, B and C be rings. Suppose there are two ring morphisms $A \to B$ and $B \to C$. The following sequence of C-modules is exact.*

$$C \otimes_B \Omega^1_{B|A} \xrightarrow{f} \Omega^1_{C|A} \xrightarrow{g} \Omega^1_{C|B} \longrightarrow 0$$

Where $f(c \otimes d(b)) = cd(b)$, and $g(d(c)) = d(c)$.

Lemma 5.7 (Second Exact Sequence). *Let R be a ring, suppose there is a ring morphism $S \to R$. Let I be an ideal of R. Set $T = R/I$. Te following sequence is exact.*

$$I/I^2 \xrightarrow{d} T \otimes_S \Omega^1_{R|S} \xrightarrow{D} \Omega^1_{T|S} \longrightarrow 0$$

Where $d(f + I^2) = 1 \otimes d(f)$, and $D(c \otimes d(b)) = cd(b)$.

Now take $R = k[X_1, \dots, X_n]$, let $I = (f_1, \dots, f_m)$ be a prime ideal of R. $T = R/I$ a coordinate ring. Then, by the preceding lemmas and the fact that tensor product distributes over direct sum,

$$T \otimes_k R = T \otimes \left(\bigoplus_{i=1}^n R dX_i\right) = \bigoplus_{i=1}^n T dX_i \equiv T^{\oplus n}.$$

Now, $\Omega^1_{T|_k}$ is precisely the cokernel of the map $D : I/I^2 \to T^{\oplus n}$. We have the following sequence (not necessarily exact)

$$R^{\oplus m} \twoheadrightarrow I/I^2 \xrightarrow{\quad d \quad} R^{\oplus n}$$

$$e_i \longmapsto f_i + I^2 \longrightarrow d(f_i) = \textstyle\sum_{j=1}^n \frac{\partial f_i}{\partial x_j}$$

So $\Omega^1_{T|_k} = \operatorname{coker}(d) = R^{\oplus n}/J$ where J is the Jacobian matrix of $(X_1, \ldots, X_n) \mapsto (f_1 \ldots, f_m)$, or if one prefers, it is $\left(\bigoplus_{i=1}^n TdX_i\right)/(d(f_i) \mid i = 1, \ldots, m)$.

Now we algebraic differentials with coefficients in the function field.

Lemma 5.8. *Let R be a domain, and K its field of fractions. Any derivation $D : R \to M$ extends uniquely to a derivation $\widetilde{D} : K \to M$*

Proof. The usual derivative of fractions formula $\widetilde{D}(x/y) = \frac{D(x)-zD(y)}{y}$. It is easy to check that this is a derivation. □

Let us turn our gaze back to curves.

Proposition 5.9. *1. Let K be an algebraic function field in one variable over k. Then $\Omega^1_{K|_k}$ is one-dimensional over K.*

2. (char$k$=0). If $x \in K$ is nonconstant, then dx is a basis for $\Omega^1_{K|_k}$.

Proof. Let $F \in k[X, Y]$ be an affine plane curve. Let $T = k[X, Y]/(F) = k[x, y]$ be it's coordinate ring, and $K = k(x, y)$ be its function field. Since F is irreducible, one may assume $\frac{\partial F}{\partial Y} \neq 0$. So F does not divide $\frac{\partial F}{\partial Y}$. Then, $\frac{\partial F}{\partial Y}(x, y) \neq 0$. We have seen that dx and dy generate $\Omega^1_{K|_k}$ over K. But,

$$0 = d(F(x, y)) = \frac{\partial F}{\partial X}(x, y)dx + \frac{\partial F}{\partial Y}(x, y)dy.$$

so $dy = udx$ where $u = -\frac{\partial F}{\partial X}(x, y)/\frac{\partial F}{\partial Y}(x, y)$. So dx alone generates $\Omega^1_{K|_k}$ over K. □

It follows that if char$k = 0$, there is a unique element $\nu \in K$ such that $df = \nu dt$. We write $\nu = \frac{df}{dt}$.

Proposition 5.10. *Let $F \in k[X, Y]$ be an affine plane curve. Let $T = k[X, Y]/(F) = k[x, y]$ be it's coordinate ring, and $K = k(x, y)$ be its function field. Let $\mathcal{O}$ be a DVR of K, and let t be an uniformizing parameter in $\mathcal{O}$. If $f \in \mathcal{O}$, then $\frac{df}{dt} \in \mathcal{O}$.*

Proof. We may assume $\mathcal{O} = \mathcal{O}_{F,P}$, and $P = (0, 0)$ a simple point. Fix a non-constant $t \in K$ and write z' instead of $\frac{dz}{dt}$.

Pick a large enough N so that $\operatorname{ord} Px' \geq -N$ and $\operatorname{ord} Py' \geq -N$. Then if $f \in k[x, y]$, then $\operatorname{ord} Pf' \geq -N$ since $f' = \frac{\partial f}{\partial X}(x, y)x' + \frac{\partial f}{\partial Y}(x, y)y'$.

Similarly, if $f \in \mathcal{O}$, write $f = g/h$ where $h(P) \neq 0$. Then, $f' = (g'h - gh')h^{-2}$. So, $\operatorname{ord} Pf' \geq -N$ again.

Now, let $f \in \mathcal{O}$. Write $f = \sum_{i<N} c_i t^i + t^N g$, where $c_i \in k$ and $g \in \mathcal{O}$.

$$f' = \sum ic_i t^{i-1} + gNt^{N-1} + t^N g'.$$

We had $\operatorname{ord} Pg' \geq -N$, so each term belongs to $\mathcal{O}$. □

5.2 Canonical Divisors

As usual, let C be an irreducible plane curve and $f\colon X \to C$ its nonsingular resolution. After the study of abstract differentials in the previous section, we are now ready to talk in more detail about differentials on X.

Definition 5.11. The $k(X)$-module $\Omega^1_{k(X)|_k}$, simply denoted Ω^1_X, is called the *module of differentials* of X; its elements may also be called *1-forms* or simply *forms*.

If $\omega \in \Omega^1_X$ and $P \in X$ is a place, we want to define the *order* of ω at P in the following manner. Let t be a uniformizing parameter in $\mathcal{O}_{X,P}$, so that we may write uniquely $\omega = g\,dt$ with $g \in k(X)$ by Proposition 5.9. We set $\operatorname{ord}_P(\omega) = \operatorname{ord}_P(g)$. If u is another uniformizing parameter with $\omega = h\,du = g\,dt$, then $h/g = du/dt$ and $g/h = dt/du$ lie in $\mathcal{O}_{X,P}$ by Proposition 5.10, so h/g has order 0 and $\operatorname{ord}_P(g) = \operatorname{ord}_P(h)$.

If $\omega \in \Omega^1_X$ is a nonzero form, its *divisor* is defined as

$$\operatorname{div}(\omega) = \sum_{P \in X} \operatorname{ord}_P(\omega) P.$$

To see that this divisor is actually well-defined (that is, it only has finitely many nonzero entries) we will have to wait until Proposition 5.13.

Any other nonzero form in Ω^1_X is of the form $g\omega$ for $0 \neq g \in k(X)$, so the its associated divisor is $\operatorname{div}\omega + \operatorname{div} g$ linearly equivalent to $\operatorname{div}\omega$. Conversely if a divisor $\operatorname{div}\omega + \operatorname{div} g$ is linearly equivalent to $\operatorname{div}\omega$, then it is the divisor of the differential form $g\omega$.

Definition 5.12. The divisor $K = \operatorname{div}\omega$ of any nonzero differential form $\omega \in \Omega^1_X$ on X is called a *canonical divisor.* Canonical divisors forms an equivalence class under linear equivalence and, in particular, all have the same degree.

Proposition 5.13. *Let C be an irreducible plane projective curve of degree $d \geq 3$ with only ordinary multiple points. Let $E = \sum_{Q \in X}(r_Q - 1)Q$ as in Section 4.1. For any plane curve G of degree $d-3$, the divisor*

$$\operatorname{div} G - E$$

is a canonical divisor (if $d = 3$, take $\operatorname{div} G = 0$.)

Proof. We may choose the coordinates X, Y, Z for $\mathbb{P}^2$ so that the following conditions hold: $Z \cap C$ consists of d distinct points $P_1, \ldots, P_d$ (eventually using the remarks of Section 3.3 in the case C has a terrible point;) $[1:0:0] \notin C$; and no tangent to C at a multiple point passes through $[1:0:0]$. Denote also by X, Y, Z the images of the coordinates functions in $S(C)$ and let $x = X/Z, y = Y/Z \in k(C) = k(X)$. Let F be an equation for C and $f_x = \partial F/\partial X(x, y, 1), f_y = \partial F/\partial Y(x, y, 1)$. Since

$$\operatorname{div} G - E \equiv \operatorname{div}\left(Z^2 \frac{\partial F}{\partial Y}\right) - E = 2\sum_{i=1}^{d} P_i + \operatorname{div}\left(\frac{\partial F}{\partial Y}\right) - E,$$

our thesis is equivalent to showing

$$\operatorname{div}(dx) - \operatorname{div}\left(\frac{\partial F}{\partial Y}\right) = -2\sum_{i=1}^{d} P_i - E. \qquad (\star)$$

Firstly, note that $0 = d(F(x,y)) = f_x dx + f_y dy$ we have

$$\operatorname{ord}_Q(dx) - \operatorname{ord}_Q(\partial F/\partial Y) = \operatorname{ord}_Q(dy) - \operatorname{ord}_Q(\partial F/\partial X)$$

for all $Q \in X$.

Now suppose Q is a place centered at $P_i \in C \cap Z$. By our assumption on the P_i's the intersection of Z with C is transverse, so $y^{-1} = Z/Y$ is a uniformizing parameter for $\mathcal{O}_{C,P_i} = \mathcal{O}_{X,Q}$ and the identity $dy = -y^2 d(y^{-1})$ shows that $\operatorname{ord}_Q(dy) = -2$. The fact that $P_i \neq [1:0:0]$, along with Euler's identity, insures that $\partial F/\partial X(P_i) \neq 0$ so bot sides of $(\star)$ have order -2 at P_i.

Suppose Q is a place centered at a point $P = [a:b:1]$. We may assume, up to a translation, $P = [0:0:1]$. If Y is tangent to C at P, since it passes also through $[1:0:0]$ by our assumption on the coordinates P must be a smooth point. So x is a uniformizing parameter and $\partial F/\partial Y(P) \neq 0$; both sides of $(\star)$ have order 0 at P.

If Y is not tangent to P at C then Remark 3.2 tells us that y is a uniformizing parameter at Q and (with a calculation, see [Ful69, Problem 7.4]) that $\operatorname{ord}_Q(f_y) = r_Q - 1$, as desired. $\square$

Thus a good choice for a canonical divisor is (with the notations of the Proposition above) $K = E_{d-3} = (d-3)\sum_{i=1}^{d} P_i - E$. Remark 4.22 then becomes

Corollary 5.14. *If K is a canonical divisor for X, then $\deg K = 2g-2$ and $l(K) \geq g$.*

We conclude this section with some examples over a field of characteristic 0.

Example 5.15. Let C be a cubic given by $F(X,Y,Z) = Y^2Z = X^3 - XZ^2$. Let us use the affine coordinates $x = X/Z$ and $y = Y/Z$ on the affine patch $Z = 1$. Let us denote C_0 the affine curve $(Z=1) \cap C$ given by $f(x,y) = y^2 - x^3 + x$.

We have already computed $\operatorname{div} y = P_1 + P_2 + P_3 - 3P_\infty$ where $P_i = [e_i : 0 : 1]$, $e_i = 0, 1, -1$.

What is then $\operatorname{div} dx$? Let us first compute $\operatorname{div} x$. For P_0, we have

$$\operatorname{ord} P_0 x = I(P_0, f \cap x) = I(P_0, y^2 \cap x) = 2I(P_0, y \cap x) = 2.$$

by the properties of intersection number. Therefore $\operatorname{div} x = 2P_0 - 2P_\infty$.

Let's compute for dx. Remember that $dx = d(x - e_i)$. Further if t is an uniformizing parameter at $\mathcal{O}_{C,P_i}$, $\operatorname{ord} P_i x - e_i$ =2 implies that $x - e_i$ locally has the form

$$x - e_i = a_2t^2 + a_3t^3 + \dots$$

so

$$d(x) = (2a_2t + 3a_3t^2 \dots)dt \tag{5.1}$$

so dx is of order 1 at every point P_i. If t is a uniformizing parameter at P_∞ however, we have,

$$x - e_i = b_{-2}t^{-2} + b_{-1}t^{-1} \dots$$

at P_∞ and therefore

$$dx = (-2b_{-2}t^{-3} + -b_{-2}t{-}2 \dots)dt.$$

So dx is of order 3 at P_∞. We may deduce that

$$\operatorname{div} dx = P_1 + P_2 + P_3 - 3P_\infty$$

which is exactly the same as that of y! Meaning the divisor of dx/y is zero. $g = \deg K = 2g - 2$ implies that $g = 1$. Smooth projective curves of genus 1 are called *elliptic curves*.

Example 5.16. Now, we attempt to write a canonical divisor for a family of special curves. Suppose $g \geq 1$.

Let
$$f(x) = a_0 x^{2g+2} + a_1 x^{2g+1} \dots a_{2g+1} x + a_{2g+2}$$
be a polynomial with $2g + 2$ distinct roots. Let C_0 be the affine curve given by $y^2 = f(x)$.

Let φ be the map $(x, y) \mapsto [1 : x : x^2 : \cdots : x^{g+1} : y]$ from C_0 to $\mathbb{P}^{g+2}$. Write $[X_0 : \cdots : X_{g+2}]$ for the homogeneous coordinates of $\mathbb{P}^{g+2}$. Let C be the closure of $\operatorname{im}\varphi$. Then C is smooth and $C \cap (X_0 \neq 0)$ is isomorphic to C. C is called a *hyperelliptic curve*. C is given by the polynomial

$$F^* = X_{g+2}^2 X_0 - \sum_{s=0}^{g+1} a_{2g+2-2s} X_s^2 X_0 - \sum_{j=0}^{g} a_{2g+2-2j-1} X_j^2 X_1.$$

One could easily check that this is smooth.

Now let

$$f^*(v) = v^{2g+2} f(1/v) = a_0 + a_1 v + \cdots + a_{2g+2} v^{2g+2}.$$

C is given by "gluing" the affine curve C_0 with the affine curve $C_1 : w^2 = f^*(v)$ with the maps

$$\begin{array}{ll} C_0 \longrightarrow C_1 & \qquad\qquad C_1 \longrightarrow C_0 \\ (x, y) \mapsto (1/x, y/x^{g+1}) & \qquad\qquad (v, w) \mapsto (1/v, w/v^{g+1}) \end{array}$$

All the points of C missing from C_0 are in C_1. (Those on $X_0 = 0$). By "gluing" we mean that at the points of C are covered by points on C_0 and C_1 and that on their intersection the maps

$$x = \frac{X_1}{X_0} = \frac{v^g}{v^{g+1}} = 1/v$$
$$y = \frac{X_{g+2}}{X_0} = \frac{w}{v^{g+1}}$$

and for the other direction,

$$v = \frac{X_{g+1}}{X_{g+2}} = \frac{x^{g+1}}{x^{g+2}} = 1/x$$
$$w = \frac{X_{g+2}}{X_{g+1}} = \frac{x^{g+2}}{x^{g+1}} = y/x^{g+1}.$$

. define a variety isomorphism.

Now since $y^2 = f(x)$, we have $2ydy = f'(x)dx$, and therefore $\frac{2dy}{f'(x)} = \frac{dx}{y}$. So it is natural to wonder the divisor of $\frac{dx}{y}$ again. By the above gluing maps we have $dx = -\frac{1}{v^2}dv$. So dx has two poles $(0, \pm 1)$, both of order 2. And

$$\frac{dx}{y} = \frac{-\frac{1}{v^2}dv}{\frac{w}{v^{g+1}}} = \frac{-v^{g-1}}{w}dv.$$

The polynomial f has $2g+2$ distinct roots. Therefore, we have $2g+2$ zeros of order 1.

$$\operatorname{div} dx/y = P_1 + \cdots + P_{2g+2} - 2(0,1) - 2(0,-1)$$

This is a canonical divisor of degree $2g-2$. Therefore C is indeed of genus g.

5.3 Riemann-Roch Theorem

We can finally achieve the main goal of the mémoire, and refine the result of Riemann's Theorem by finding the missing term in the inequality. The proof of [Ful69] which we have built to here follows the classical proof of Brill and Noether.

Theorem 5.17 (Riemann-Roch). *Let K be a canonical divisor on a smooth projective curve X. Then for any divisor D,*

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

We have already deduced the statement for divisors of large degree (greater than both the N appearing in Corollary 4.19 and $2g-2 = \deg K$, so that $l(K-D) = 0$.) The general case will follow by induction if we compare both sides of the equation when the degree increases by 1: that is, observing the change when we replace the divisor D by $D+P$ for $P \in X$. Indeed $\deg(D+P) = \deg D + 1$ and both the quantities $l(D+P)$ and $l(K-D-P)$ change vary from $l(D), l(K-D)$ by either 0 or 1. The heart of the proof is therefore contained in the following

Lemma 5.18 (Noether's Reduction). *Let D be a divisor on X such that $l(D) > 0$. If $l(K-D-P) \neq l(K-D)$, then $l(D+P) = l(D)$.*

Proof. By the machinery of Chapter 3, we may suppose X is the nonsinuglar model of an irreducible plane curve C with only ordinary multiple points, and such that P is the place corresponding to a simple point on C. We may also choose the coordinates X, Y, Z of $\mathbb{P}^2$ so that P does not lie on the line $Z = 0$, and $C \cap Z$ consists of $d = \deg C$ distinct points $P_1, \ldots, P_d$. As usual let $E_m = m \sum P_i - E$, with E defined as in Section 4.1. The quantities in the lemma depend only on the linear equivalence class of a divisor, so we may replace K by E_{d-3} (Proposition 5.13) and D by $D + \operatorname{div} g$, for nonzero $g \in \mathcal{L}(D)$ (which exists since by hypothesis $l(D) > 0$.) Hence we may also assume $D \geq 0$, which implies $\mathcal{L}(E_{d-3} - D) \subset \mathcal{L}(E_{d-3})$.

Take a nonzero $h \in \mathcal{L}(E_{d-3} - D)$ not in $\mathcal{L}(E_{d-3} - D - P)$. By Remark 4.22, it may be written as $h = G/Z^{d-3}$, for G an adjoint of degree $d-3$. Then

$$\begin{aligned} 0 \leq \operatorname{div} h + E_{d-3} - D = \operatorname{div} G - \operatorname{div} Z^{d-3} + E_{d-3} - D = \\ = \operatorname{div} G - E - D =: A. \end{aligned}$$

Remark that P does not appear in A as $h \notin \mathcal{L}(E_{d-3} - D - P)$. Since P is not terrible for C, we can take a line L such that $L \cap C$ consists of $d-1$ distinct points other than P. Letting B be the effective divisor given by the sum of these points, we have $L \cdot C = B + P$ and

$$\operatorname{div}(LG) = (D + P) + E + (A + B).$$

Now take any $f \in \mathcal{L}(D + P)$; let $D' = D + \operatorname{div} f$. Showing that $f \in \mathcal{L}(D)$ is equivalent to $D' \geq 0$.

Since the divisors $D + P$ and $D' + P = D + P + \operatorname{div} f \geq 0$ are linearly equivalent and both effective, the Theorem 4.9 applies: there is a curve H of degree $\deg H = \deg(LG) = d - 2$ such that

$$\operatorname{div} H = (D' + P) + E + (A + B).$$

However, B contains $d-1$ distinct collinear points so, by degree and Theorem 2.6, H must contain L as a component. In particular H passes through P and since P does not appear any of E, A nor B, P must appear in $D' + P$. That is $D' + P \geq P$ or $D' \geq 0$. ☐

We will also need the simple following lemma to reason by induction.

Lemma 5.19. *If D is a divisor on X such that $l(D) > 0$, then for all but a finite number of $P \in X$ we have $l(D - P) = l(D) - 1$.*

Proof. Take a nonzero $f \in \mathcal{L}(D)$, which exists since $l(D) > 0$. If P is a point not appearing in the effective divisor $\operatorname{div} f + D$, then $\operatorname{div} f + D - P \ngeq 0$, so the inclusion $\mathcal{L}(D - P) \subset \mathcal{L}(D)$ is strict. We conclude by Proposition 4.11. ☐

Proof of the Riemann-Roch Theorem. We split the proof into two cases:

Case 1: $l(K - D) = 0$. The statement becomes

$$l(D) = \deg D + 1 - g. \tag{†}$$

We proceed by induction on $l(D)$. If $l(D) = 0$, applying Riemann's Theorem to D and $K - D$ gives $0 \geq \deg D + 1 - g$ and

$$0 \geq \deg(K - D) + 1 - g = 2g - 2 + \deg D + 1 - g = \deg D + 1 - g,$$

so $\deg D + 1 - g = 0$ as wanted.

If $l(D) = 1$, we may assume D is effective. Then $g \leq l(K)$ by Corollary 5.14, $l(K) \leq l(K - D) + \deg D$ by Proposition 4.11 and $\deg D \leq g$ by Riemann's Theorem, so all inequalities are actually equalities and we get (†).

If $l(D) > 1$, by Lemma 5.19 we may choose P so that $l(D - P) = l(D) - 1$. Then Noether's Reduction implies $l(K - (D - P)) = l(K - D) = 0$ and by induction

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

proving (†).

Case 2: $l(K - D) > 0$. This case is possible only if $\deg D \leq \deg K = 2g - 2$, so we can pick a maximal D for which the thesis is false i.e. the thesis holds for all divisors off the form $D + P$,

$$l(D + P) = \deg(D + P) + 1 - g + l(K - D - P), \qquad \text{for all } P \in X.$$

We may choose P so that $l(K-D-P) = l(K-D)-1$ by Lemma 5.19. If $l(D) = 0$ the statement holds by applying case 1 (†) to the divisor $K - D$:

$$l(K-D) = \deg(K-D) + 1 - g = 2g - 2 - \deg D + 1 - g,$$

so $0 = l(D) = \deg D + 1 - g + l(W - D)$. If instead we assume $l(D) > 0$, the Reduction Lemma gives $l(D+P) = l(D)$ and hence

$$\begin{aligned} l(D) = l(D+P) &= \deg(D+P) + 1 - g + l(K-D-P) = \\ &= (\deg D + 1) + 1 - g + (l(K-D) - 1) = \deg D + 1 - g + l(K-D), \end{aligned}$$

finishing the proof. □

We can finish this chapter with some straight-forward applications of Riemann-Roch: applying it to a canonical gives an immediate improvement on the bound of Corollary 5.14.

Corollary 5.20. *If K is a canonical divisor on a smooth projective curve X, then $l(K) = g$.*

Remark 5.21. Another elementary remark is that if D is a divisor of degree $\deg D \geq 2g - 1$ and K is a canonical divisor, then $\deg(K - D) \leq (2g-2) - (2g-1) = -1$ so $l(K-D) = 0$ and the dimension $l(D)$ depends only on the genus of X and the degree of D:

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

If $\deg D \geq 2g$, applying this remark to D and $D - P$, for $P \in X$, improves Lemma 5.19:

$$l(D-P) = l(D) - 1$$

Slightly less trivial is the following bound on $l(D)$:

Corollary 5.22 (Clifford's Theorem). *Let X be a smooth projective curve. If K is a canonical divisor on X and D a divisor with $l(D) > 0$ and $\mathcal{L}(K-D) > 0$, then*

$$l(D) \leq \frac{1}{2} \deg D + 1.$$

Proof. We may assume $D \geq 0$ and $D' := K - D \geq 0$ since $l(D), l(K-D) > 0$. We can also assume $l(D-P) \neq l(D)$ for all $P \in X$, since otherwise substituting D for $D - P$ leads to a better inequality.

Hence we may choose a $g \in \mathcal{L}(D)$ such that $g \notin \mathcal{L}(D-P)$ for each P appearing in D'. Then the k-linear map

$$\varphi \colon \mathcal{L}(D')/\mathcal{L}(0) \to \mathcal{L}(K)/\mathcal{L}(D), \qquad \varphi(\overline{f}) = \overline{gf},$$

is well-defined and injective (if $0 \leq \operatorname{div}(gf) + D = \operatorname{div} f + \operatorname{div} g + D$, then $D' \leq (\operatorname{div} f + D') + (\operatorname{div} g + D)$ but no point appearing in D' appears in $\operatorname{div} g + D$, so $D' \leq \operatorname{div} f + D'$ and $\operatorname{div} f \geq 0$). This gives a bound $l(D') - 1 \leq g - l(D)$, and applying Riemann-Roch to D' concludes. □

Bibliography

[AK13] Allen Altman and Steven Kleiman. *A term of commutative algebra.* Worldwide Center of Mathematics, 2013.

[AM69] M.F. Atiyah and I.G. MacDonald. *Introduction To Commutative Algebra.* CRC Press, 1969.

[Ful69] William Fulton. *Algebraic Curves: An Introduction to Algebraic Geometry.* Mathematical Lecture Note Series. 1969.

[Har77] Robin Hartshorne. Graduate texts in mathematics. Springer, 1977.

[ZS75] O. Zariski and P. Samuel. *Commutative Algebra I.* Graduate Texts in Mathematics. Springer New York, 1975.