Projective Curves with Riemann-Roch

G14PJS

Mathematics 3rd Year Project

Spring 2019/20

School of Mathematical Sciences

University of Nottingham

Oliver Daisey

Supervisor: Dr. C Wuthrich

Project code: CW P1

Assessment type: Review

I have read and understood the School and University guidelines on plagiarism. I confirm that this work is my own, apart from the acknowledged references.

Abstract

We survey the elementary definitions and results of commutative algebra and algebraic geometry, leading up to a presentation of the Riemann-Roch theorem of curves in the smooth case. We then explore some applications of this theorem to algebraic geometry and beyond.

Contents

0.1 Introduction

Algebraic geometry, the subject of this project, is the study of sets of zeros of polynomials using algebraic techniques. The deep connection between algebra and geometry has been well known throughout the history of mathematics. The 'classical' study of algebraic geometry starts as far back as the ancient Greeks, who knew the algebraic relations that defined the conic sections (though did not have the language to express them.) Much further to the 17th century, Descartes developed his analytic coordinate system which gave an immediate correspondence between arithmetic and geometry. Newton provided a rudimentary statement and proof of Bézout's theorem in the *Principia* in 1687. The Renaissance motivated an interest in projective geometry, and the synthetic study of projective geometry started around this time. In the 19th century the subject found rich development with Riemann's insight and contributions. With Riemann's inequality together with the work of his student Gustav Roch, they formulated the powerful Riemann-Roch theorem that motivated much of the development of the subject into the 20th century and beyond. Grothendieck's theory of schemes, the language in which modern algebraic geometry is phrased, can be thought of as the environment to best generalise the Riemann-Roch theorem. The Italian school of algebraic geometry flourished in the turn of the 20th century, and conducted much study into the birational geometry of algebraic surfaces. They successfully gave a classification of algebraic surfaces, similar to the classification of algebraic curves by their genus g. References as well as a more detailed account of the history of algebraic geometry can be found in [1].

The purpose of this work is to expose a reader to the methods and techniques of algebraic geometry, by developing the theory of projective curves, divisors on them and the Riemann-Roch theorem. The common theme throughout the work is that we can better understand a geometric object by understanding the functions defined on that object. The work will have fulfilled its purpose if a reader can walk away with a better understanding of this idea than before.

For prerequisites, the reader is assumed to have a solid background in linear algebra, and ideally a first course in abstract algebra; at least, the reader should understand the notion of an abelian group. No prior knowledge of algebraic geometry is assumed.

The first section is intended as a review of the ring theory and commutative algebra that is used throughout the report. It also serves as a brief survey of the abstract algebra that we see in most modern treatments of algebraic geometry. The material is standard and some proofs have been omitted.

The second section introduces the theory of algebraic sets, projective space, function fields and local rings. Certainly the crowning jewel of this section is the Nullstellensatz, which provides a direct translation between radical ideals, an algebraic object, and algebraic sets, a geometric object. Some of the notions we introduce here are quite general and are rarely summoned throughout the rest of the text, so this section serves more as a taste at the flavour of modern algebraic geometry.

The third section is a detailed discussion of projective varieties in the case that they are plane curves. We develop the machinery of intersection numbers and state and prove Bézout's theorem, a remarkable result which acts as the geometric analogue to the fundamental theorem of algebra.

The fourth section is a lengthy discussion of divisors on smooth curves. Divisors encode the locations and orders of zeroes and poles of a function on a curve. The vector space of all functions with zeros and poles constrained by the divisors are the object of interest here, and the celebrated Riemann-Roch theorem, which we state and prove, provides a precise relationship between the dimension of this space and some invariants of the curve.

The fifth and final section is essentially a showcase of the Riemann-Roch theorem. We show that Riemann-Roch permits the famous Weierstrass form of an elliptic curve to be deduced from the geometric definition as a genus one smooth projective curve. We also discuss Clifford's theorem.

Throughout the body of the text, I sometimes reference other sources for results and proofs. These sources, as well as other books that I have used to build up my own understanding of this subject, are found at the end of the paper. I particularly recommend Fulton's [2] book for the interested reader.

I'd like to thank my supervisor, for both the guidance and discussion they provided.

“Algebra is the offer made by the devil to the mathematician. The devil says: I will give you this powerful machine, it will answer any question you like. All you need to do is give me your soul: give up geometry and you will have this marvelous machine.“

- Michael Atiyah

1 Elements of algebra

Throughout this paper, all rings are commutative with identity. We recall some standard facts from ring theory. Any textbook on algebra should cover this section; a standard reference is [3].

1.1 Rings

Definition 1.1. Let R be a set, and suppose $+ : R \times R \to R$, called addition, and $\cdot : R \times R \to R$, called multiplication, are binary operations on R such that:

1. $\langle R, + \rangle$ is an abelian group with identity 0,
2. For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$,
3. For all $a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
4. There exists $1 \in R$ such that $1 \cdot a = a$ for all $a \in R$,
5. For all $a, b \in R$, $a \cdot b = b \cdot a$.

We then say that the triple $(R, +, \cdot)$ is a *ring*, and denote this triple by R. Typically we omit the $\cdot$ symbol when writing multiplication, writing $a \cdot b$ as ab.

Example 1.1. The following are rings:

1. The integers $\mathbb{Z}$ with the operations of integer addition and multiplication.
2. The integers modulo n for an integer n. Here the set is $\mathbb{Z}/n\mathbb{Z} = \{0, 1, ..., n - 1\}$, and the operations of addition and multiplication are carried out modulo n.
3. The set of real numbers, with real number addition and multiplication, forms a ring.
4. The set of polynomials $R[X]$ in one variable, with coefficients in a ring R, forms a ring. We add polynomials and multiply them in the natural way.

Definition 1.2. Let R be a ring. We call those elements $a \in R$ for which there exists $b \in R$ such that $ab = 1$ *units*, and denote the set of units $R^{\times}$. This is a group with respect to multiplication, so a multiplicative inverse of a unit is uniquely determined, justifying the notation a^{-1} for the inverse of a under multiplication.

Definition 1.3. Let R be a ring, and suppose that for all $a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$. Then we say R is an *integral domain*. We call elements a, b for which $a, b \neq 0$ but $ab = 0$ *zero divisors*.

Definition 1.4. Suppose R is a ring such that $R^\times = R \setminus \{0\}$. We then call R a *field*.

Lemma 1.1. *Every field F is an integral domain.*

Proof. Let $a, b \in F$ and suppose $ab = 0$. Without loss of generality, suppose $a \neq 0$. Then $b = a^{-1} \cdot 0 = 0$. So F is an integral domain. □

Lemma 1.2. *Every finite integral domain R is a field.*

Proof. Write $R = \{a_1, a_2, ..., a_n\}$. Given any $0 \neq a \in R$, consider the set $aR = \{aa_1, aa_2, ..., aa_n\}$. Now $aa_i = aa_j$ if and only if $a(a_i - a_j) = 0$. Since R is an integral domain, we conclude $aa_i = aa_j$ if and only if $i = j$. This implies the sets aR and R are equal. Hence there exists some $i \in \mathbb{N}$ such that $aa_i = 1$. Hence a is a unit. □

Remark. The converse does not hold in general when R is infinite. A counterexample is the ring of integers $\mathbb{Z}$.

Definition 1.5. Let R, S be rings, and suppose $f : R \to S$ is a function such that:

1. For all $a, b \in R$, $f(a + b) = f(a) + f(b)$.

2. For all $a, b \in R$, $f(ab) = f(a)f(b)$.

3. $f(1_R) = 1_S$,

where $1_R \in R$ and $1_S \in S$ are unity in R and S respectively, and addition/multiplication on the right hand side is interpreted in the ring S. We then say f is a *ring homomorphism*. A bijective homomorphism is called an *isomorphism*. We write that rings R and S are isomorphic if there exists an isomorphism between them, and denote this relation by $R \cong S$.

Definition 1.6. We define the set $\ker f = \{x \in R \mid f(x) = 0\}$ and call it the *kernel* of f. The set $\operatorname{Im} f = \{y \in S \mid \exists x \in R : f(x) = y\}$ is called the *image* of f.

1.2 Ideals and quotients

Definition 1.7. Let R be a ring. Suppose I is a subset of R such that:

1. $\langle I, + \rangle$ is an additive subgroup of R. That is, for any $a, b \in I$, we have $a - b \in I$.

2. For all $r \in R, a \in I$, $ra \in I$. Equivalently $rI = I$ for any $r \in R$.

We then call I an *ideal* of R.

Definition 1.8. We may define an ideal I by specifying a set $S \subseteq R$ such that every element of I may be written as a finite $R-$linear combination of elements of S, that is $I = \{\sum_{i=1}^{n} a_i s_i \mid a_i \in R, s_i \in S, n \in \mathbb{N}\}$. We denote $I = (S)$ and call S a *generating set* for I. An ideal I is *finitely generated* if it can be written $I = (S)$ for some finite subset $S \subseteq R$.

Definition 1.9. If there exists $a \in R$ such that $I = (a)$, that is $I = aR = \{ar \mid r \in R\}$, we say that I is a *principal ideal.* An integral domain where every ideal is principal is called a *principal ideal domain.*

Example 1.2. The ring $\mathbb{Z}$ with normal addition and multiplication is a principal ideal domain. Let I be an ideal of $\mathbb{Z}$, and suppose $I \neq (0)$. Let n be the smallest positive integer in I. We claim $I = (n)$. For let $z \in I$, and divide z by n, using the division algorithm. We have

$$z = qn + r$$

where $0 \leq r < n$ are integers. Hence $r = z - qn \in I$. Since by assumption n is the smallest positive integer in I, we must have that $r = 0$. So $z = qn$, so $z \in (n)$.

Since any ideal of $\mathbb{Z}$ is principal, we have that $\mathbb{Z}$ is a principal ideal domain.

Remark. It is not difficult to adapt the above example to show additionally that any proper ideal of $\mathbb{Z}$ must be generated by either 0 or p for some prime p.

Definition 1.10. Let $a, b \in R$. We say that $a \mid b$ if there exists $c \in R$ such that $b = ac$. We have that $(a) \subseteq (b)$ if and only if $b \mid a$. If a, b are such that $a \mid b$ and $b \mid a$, we say that a and b are *associates.*

Lemma 1.3. *Suppose R is an integral domain. Let $a_1, a_2 \in R$, and suppose $(a_1) = (a_2)$, equivalently, $a_1 \mid a_2$ and $a_2 \mid a_1$. Then $a_1 = ua_2$ for some $u \in R^\times$.*

Proof. Since $(a_1) \subseteq (a_2)$, we have $a_1 \in (a_2)$, hence $a_1 = sa_2$ for some $s \in R$. Similarly we have $a_2 = ta_1$ for some $t \in R$. Hence $a_1 = sta_1$, so $a_1(1 - st) = 0$. Hence either $a_1 = 0$, or $1 = st$, in which case s, t are units and we are done. In case $a_1 = 0$, then $a_2 = 0$ and the claim follows. □

Remark. The above lemma shows that associates should be thought of as 'the same' element, up to a unit.

Lemma 1.4. *A ring F is a field if and only if the only ideals of F are (0) and F.*

Proof. Suppose F is a field. Let $I \subseteq F$ be a non-trivial ideal of F. Then there exists non-zero $a \in I$. Hence $aa^{-1} = 1 \in I$, so $I = F$.

For the converse, let $0 \neq a \in F$, and consider the ideal (a). Since this ideal is non-trivial, we must have $(a) = F$. But then $1 \in (a)$, so there exists some $b \in R$ such that $ab = 1$. Hence a is a unit. So F is a field. □

Corollary. *Every field is a principal ideal domain.*

Definition 1.11. Let I, J be ideals of a ring R. We may form:

1. The sum of ideals: $I + J = \{r + s \mid r \in I, s \in J\}$,

2. The product of ideals: $IJ = \{\sum_{i=1}^{n} r_i s_i \mid r_i \in I, s_i \in J, n \in \mathbb{N}\}$, which is the ideal generated by products rs for $r \in I, s \in J$,

and the resulting sets are also ideals. We can extend these definitions by induction to define $\sum_{i=1}^{n} I_i$, $\prod_{i=1}^{n} I_i$, I^n, etc.

Definition 1.12. Let I be an ideal of R. For any $a \in R$, we call the set $a + I = \{a + x \mid x \in I\}$ a *coset* of I. We call the set $R/I = \{a + I \mid a \in R\}$ the *quotient ring* of R by I. The induced ring operations $(a + I) + (b + I) = (a + b) + I$ and $(a + I)(b + I) = (ab) + I$ are well-defined, and do not depend on the choice of representatives $a, b \in R$ ([4], Section 7.3). The additive identity of the quotient ring is $0 + I = I$ and the multiplicative identity is $1 + I$.

Lemma 1.5. *Let $f : R \to S$ be a ring homomorphism. The kernel* $\ker f$ *is an ideal of R.*

Remark. The converse holds; given any ideal I of R, the natural projection $h : R \to R/I, r \mapsto r + I$ has kernel given by I.

Definition 1.13. Let k be a field. Let $c : \mathbb{Z} \to k$ be the homomorphism defined by $c(n) = n \cdot 1 = \underbrace{1 + 1 + ... + 1}_{n \text{ times}}$. Then, since $\mathbb{Z}$ is a principal ideal domain, $\ker c = (p)$ for some integer p which is either 0 or prime. We say that p is the *characteristic* of the field k.

1.3 Homomorphism theorems

Theorem 1.6. *(Ring homomorphism theorem.) Let $f : R \to S$ be a ring homomorphism. Then $R/\ker f \cong \operatorname{Im} f$.*

Proof. Denote $I = \ker f$. Let $\phi : R/\ker f \to \operatorname{Im} f$ be such that $\phi(a+I) = f(a)$. We must check that this map does not depend on the choice of representative for $a + I$. Indeed, suppose $a + I = b + I$. Then $a - b \in \ker f$, so $f(a - b) = f(a) - f(b) = 0$. Hence $f(a) = f(b)$, so $\phi(a + I) = \phi(b + I)$. Hence ϕ is a well-defined ring homomorphism.

We now show ϕ is bijective. Clearly ϕ is surjective. And ϕ is injective, for $a \in \ker \phi \iff \phi(a + I) = f(a) = 0 \iff a \in \ker f \iff a + I = I$. □

Example 1.3. Let $f : Z \to \mathbb{Z}/n\mathbb{Z}$ be defined by $f(z) = \overline{z}$, where $\overline{z}$ is the residue of z modulo n. Then $\ker f = \{z \in \mathbb{Z} \mid \overline{z} = 0\} = \{\dots, -2n, -n, 0, n, 2n, \dots\} = n\mathbb{Z}$. Hence $\mathbb{Z}/n\mathbb{Z}$ really is the quotient of $\mathbb{Z}$ by $n\mathbb{Z}$.

Theorem 1.7. *(Correspondence theorem.) Let R be a ring, $I \subseteq R$ an ideal of R. There exists a bijective correspondence between ideals of R/I and ideals of R containing I:*

$$\{\text{ideals } J \subseteq R \mid I \subseteq J\} \xleftrightarrow{\textit{one-to-one}} \{\text{ideals of } R/I\},$$

$$J \mapsto J/I,$$

$$h^{-1}(K) \leftarrow\!\shortmid K,$$

where $h : R \to R/I$ is the natural projection.

Proof. Let J be an ideal of R containing I. It is easy to verify that the quotient J/I is an ideal of R/I. Conversely, given an ideal K of R/I, the set $h^{-1}(K) \subseteq R$ is an ideal of R since it is a preimage of an ideal under a ring homomorphism. Since $0 + I \in K$, it follows that $I \subseteq h^{-1}(K)$.

The maps are inverse to each other: We have that $h^{-1}(J/I) = J$ and $h^{-1}(K)/I = K$. □

1.4 Maximal and prime ideals

Definition 1.14. Let R be a ring, and $\mathfrak{p}$ an ideal of R. If $ab \in \mathfrak{p}$ means either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ for any $a, b \in R$, we say that $\mathfrak{p}$ is a *prime ideal* of R. Let $\mathfrak{m}$ be an ideal of R. If there does not exist a proper ideal $I \subsetneq R$ such that $\mathfrak{m} \subsetneq I$, we say that $\mathfrak{m}$ is a *maximal ideal.*

Definition 1.15. Assuming Zorn's lemma, it can be shown that every ring has at least one maximal ideal ([4], Chapter 7, Proposition 11.) We say that a ring R is *local* if it has exactly one maximal ideal.

Lemma 1.8. *An ideal $\mathfrak{p} \subseteq R$ is prime if and only if $R/\mathfrak{p}$ is an integral domain.*

Proof. Suppose $\mathfrak{p}$ is prime. Suppose $(a+\mathfrak{p})(b+\mathfrak{p}) = \mathfrak{p}$, that is, $(ab)+\mathfrak{p} = \mathfrak{p}$. Then $ab \in \mathfrak{p}$, hence either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, from which either $a + \mathfrak{p} = \mathfrak{p}$ or $b + \mathfrak{p} = \mathfrak{p}$. We conclude $R/\mathfrak{p}$ is an integral domain.

Conversely, suppose $R/\mathfrak{p}$ is an integral domain. Let $a, b \in R$ and suppose $ab \in \mathfrak{p}$. Then $(ab) + \mathfrak{p} = (a + \mathfrak{p})(b + \mathfrak{p}) = \mathfrak{p}$. Since $R/\mathfrak{p}$ is an integral domain, either $a + \mathfrak{p} = \mathfrak{p}$ or $b + \mathfrak{p} = \mathfrak{p}$. It follows either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Hence $\mathfrak{p}$ is prime. □

Lemma 1.9. *An ideal $\mathfrak{m} \subsetneq R$ is maximal if and only if $R/\mathfrak{m}$ is a field.*

Proof. Ideals of $R/\mathfrak{m}$ are in one-to-one correspondence with ideals of R containing $\mathfrak{m}$ (Theorem 1.7.) But if $\mathfrak{m}$ is maximal, the only ideals containing $\mathfrak{m}$ are $\mathfrak{m}$ and R. Hence the only proper ideal of $R/\mathfrak{m}$ is the trivial ideal, and hence $R/\mathfrak{m}$ is a field. The converse follows similarly. □

Lemma 1.10. *Every maximal ideal is prime.*

Proof. Suppose $\mathfrak{m}$ is a maximal ideal of the ring R. By Lemma 1.9, the ring $R/\mathfrak{m}$ is a field. By Lemma 1.1, $R/\mathfrak{m}$ is an integral domain. By Lemma 1.8, $\mathfrak{m}$ is prime. □

Definition 1.16. Let $I \subseteq R$ be an ideal. We define $\sqrt{I} = \{r \in R \mid \exists n \in \mathbb{N} : r^n \in I\}$, and call it the *radical* of I. If $I = \sqrt{I}$, we say that I is a *radical ideal.*

Lemma 1.11. *Prime ideals are radical.*

Proof. Suppose I is prime. Obviously we have the inclusion $I \subseteq \sqrt{I}$. Now suppose $x \in \sqrt{I}$. Then there exists $n \in \mathbb{N}$ such that $x^n = (x^{n-1})x \in I$. By the primality of I, either $x \in I$ (in which case we are done), or $x^{n-1} \in I$. Suppose the latter. Then by writing $x^{n-1} = (x^{n-2})x \in I$, we may proceed as before to get either $x \in I$ (in which case we are done), or $x^{n-2} \in I$. By induction, we conclude $x \in I$. □

1.5 Polynomial rings

Definition 1.17. Let R be a ring. Define $R[x] = \{a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \mid a_n, a_{n-1}, ..., a_1, a_0 \in R\}$ Then $R[x]$ becomes a ring under the natural polynomial addition and multiplication. We call $R[x]$ the *ring of polynomials in x.*

Note. We inductively define $R[x, y] = (R[x])[y]$, so it makes sense to define the polynomial ring $R[x_1, ..., x_n]$.

Example 1.4. Let S be a ring such that $R \subseteq S$. We may *evaluate* any $f \in R[x]$ at any $s \in S$ by replacing x with s and performing multiplication/addition in the ring S. Hence we have a homomorphism

$$ev_s : R[x] \to S, f \mapsto f(s)$$

with kernel $\ker ev_s = \{f \in R[x] \mid f(s) = 0\}$.

Definition 1.18. Let k be a field; we say that k is *algebraically closed* if every non-constant polynomial $f \in k[x]$ has a root in k; that is there exists $a \in k$ such that $f(a) = 0$. It then follows that every polynomial $f \in k[x]$ can be written

$$f(x) = u \prod_{i=1}^{n} (x - a_i)$$

where $u \in k, u \neq 0$ and the a_i are the roots of f, possibly repeated.

Definition 1.19. Let $F \in k[x_1, ..., x_n]$. We say that F is *homogeneous* if every monomial forming F has the same degree.

Example 1.5. $F = X^2Y - Z^3 + XYZ$ is homogeneous, but $G = X^3 - Y$ is not homogeneous.

Definition 1.20. Let $f \in k[X, Y]$. Then we define the *homogenisation* of f to be the homogeneous polynomial in $k[X, Y, Z]$ obtained by substituting $X \mapsto X/Z$, $Y \mapsto Y/Z$ and multiplying through by a large enough factor of Z to clear denominators. Conversely, given a homogeneous polynomial F in $k[X, Y, Z]$ we obtain a polynomial in $k[X, Y]$ by setting Z to 1. We write $f = F_* = F(X, Y, 1)$ and call f the *dehomogenisation* of F (with respect to Z).

1.6 Noetherian rings

Definition 1.21. Let R be a ring. We say that R is *Noetherian* if it satisfies any of the following equivalent properties ([3], Proposition 6.1):

1. For any ascending chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$ of ideals of R, there exists some $n \in \mathbb{N}$ such that $I_i = I_{i+1}$ for any $i \geq n$.

2. Every ideal of R is finitely generated.

3. Given any non-empty collection $\mathcal{M}$ of ideals of R, there exists a maximal element with respect to inclusion. That is, there exists $I \in \mathcal{M}$ such that for any $J \in \mathcal{M}$ with $J \neq I$ we have $I \not\subset J$.

Remark. Principal ideal domains are Noetherian, because each ideal is principal and hence finitely generated.

Theorem 1.12. *(Hilbert's basis theorem.) If R is Noetherian, then the polynomial ring $R[x_1, ..., x_n]$ is Noetherian.*

Proof. We show that any ideal of $R[x]$ is finitely generated, from which the theorem follows by induction. Let I be an ideal of $R[x]$. Define for each $n \in \mathbb{N}_{\geq 0}$ the ideal

$J_n = \{a \in R \mid \text{there exists a polynomial } ax^n + a_{n-1}x^{n-1} + ... + a_0 \in I, a_{n-1}, ..., a_0 \in R\}$. Then clearly $J_n \subseteq J_{n+1}$. Hence we obtain an increasing sequence of ideals

$$J_0 \subseteq J_1 \subseteq J_2 \subseteq J_3 \subseteq ...$$

of R, which must stabilise by the Noetherian condition. So there exists an integer $k \in \mathbb{N}_{\geq 0}$ such that $J_i = J_{i+1}$ for all $i \geq k$. Let $\{c_j^{(n)} \mid 1 \leq j \leq l_n\}$ be a set of generators for J_n, which is possible to be chosen as finite again due to the Noetherian condition. Next, for each $c_j^{(n)}$ choose a polynomial $f_j^{(n)}(x) = c_j^{(n)}x^n + a_{n-1}x^{n-1} + ... + a_0 \in I$ where $a_{n-1}, ..., a_0 \in R$. We now show that $\{f_j^{(n)}(x) \mid 0 \leq n \leq k, 1 \leq j \leq l_n\}$ is a generating set for I. Let $f(x) = ax^m + a_{m-1}x^{m-1} + ... + a_0 \in I$ be arbitrary. If $m \geq k$ then $c_j^{(m)} \in J_m = J_k$ and so there exists $a_j \in R$ such that

$$a = \sum_{j=1}^{l_k} a_j c_j^{(k)}$$

Hence

$$f(x) - \sum_{j=1}^{l_k} a_j f_j^{(k)} x^{m-k}$$

is a polynomial of degree strictly less than m. If $m < k$ then we may write

$$a = \sum_{j=1}^{l_m} a_j c_j^{(m)}$$

and hence

$$f(x) - \sum_{j=1}^{l_m} a_j f_j^{(m)}$$

has smaller degree than $f(x)$. Since we may always reduce the degree of f by subtracting appropriate $R[x]-$linear combinations of the $f_j^{(n)}$, we conclude by induction that f is an $R[x]-$linear combination of the $f_j^{(n)}$, and hence I is finitely generated. □

The Noetherian property passes to quotients, too:

Theorem 1.13. *Let R be Noetherian, and I an ideal of R. Then R/I is Noetherian.*

Proof. Let

$$J_0 \subsetneq J_1 \subsetneq J_2 \subsetneq ...$$

be an increasing sequence of ideals of R/I. By Theorem 1.7, this corresponds to an increasing sequence

$$I \subseteq I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq ...$$

of ideals of R. This sequence must terminate, since R is Noetherian. So the sequence in R/I must terminate as well. □

1.7 Localisations

Definition 1.22. Let R be a ring. Suppose $S \subseteq R$ is such that:

1. $0 \notin$ S.

2. $1 \in$ S.

3. For any $a, b \in S$, $ab \in S$.

We then say that S is a *multiplicatively closed subset* of R.

Definition 1.23. Let S be a multiplicatively closed subset of R. We define the ring $S^{-1}R = \{a/b \mid a \in R, b \in S\}$ with addition $a/b + c/d = (ad + bc)/bd$ and multiplication $(a/b)(c/d) = ac/bd$. We call it the *ring of fractions of R with respect to S*. Two fractions a/b and c/d are equal if and only if there exists $s \in S$ such that $(ad - bc)s = 0$.

Remark. If R is an integral domain, then $S = R \setminus \{0\}$ is a multiplicatively closed subset. The ring $S^{-1}R$ is then called the *field of fractions of R*. Here $a/b = c/d$ if and only if $ad = bc$. In this case the map $R \to S^{-1}R, f \mapsto f/1$ is an injection. Hence we may regard R as a subring of its field of fractions.

Example 1.6. The rational numbers $\mathbb{Q}$ can be constructed as the field of fractions of the integers $\mathbb{Z}$.

Lemma 1.14. *If $\mathfrak{p} \subseteq R$ is a prime ideal, the set $S = R \setminus \mathfrak{p}$ is a multiplicatively closed subset of R.*

Definition 1.24. Let $\mathfrak{p}$ be a prime ideal of R. We call the ring of fractions of R with respect to $R \setminus \mathfrak{p}$ the *localisation of R at $\mathfrak{p}$*. We denote it by $R_{\mathfrak{p}}$.

1.8 Discrete valuation rings

Definition 1.25. A *discrete valuation ring* (DVR) is a local principal ideal domain which is not a field.

Definition 1.26. Let R be a DVR, and suppose the maximal ideal $\mathfrak{m} = (t)$. We call t a *uniformising parameter* for R.

Remark. The maximal ideal $\mathfrak{m}$ consists of all non-units of R.

Lemma 1.15. *Let R be a discrete valuation ring, and let t_1, t_2 be uniformising parameters for R. Then $t_1 = ut_2$ where $u \in R^\times$.*

Proof. Let $\mathfrak{m}$ be the maximal ideal of R. We have $\mathfrak{m} = (t_1) = (t_2)$. Now R is an integral domain, hence we may apply Lemma 1.3 to get $t_1 = ut_2$ for some $u \in R^\times$. □

Theorem 1.16. *Suppose R is a DVR and t a uniformising parameter for R. Then any $x \in R$ with $x \neq 0$ can be uniquely written in the form $x = ut^n$ where $u \in R^\times$ and $n \in \mathbb{N}_{\geq 0}$.*

Proof. Existence. If x is a unit clearly $u = x, n = 0$ is a representation of x in the required shape, so suppose that x is not a unit. Then $x \in \mathfrak{m} = (t)$, so there exists $r_1 \in R$ such that $x = r_1 t$. Now either r_1 is a unit, in which case we are done, or r_1 is not a unit, so $r_1 \in \mathfrak{m}$ and hence we may write $r_1 = r_2 t$ for some $r_2 \in R$. Continuing in this fashion, we deduce that there must exist $n \in \mathbb{N}$ such that $r_n \in R^\times$. Otherwise, we would induce an ascending chain of ideals

$$(r_1) \subsetneq (r_2) \subsetneq (r_3) \subsetneq ...$$

which would not terminate, contradicting the Noetherian property of R. Hence $x = r_1 t = r_2 t^2 = ... = r_n t^n$ with $r_n \in R^\times$ and we are done.

Uniqueness. Suppose $x = ut^n = vt^m$ are two representations of x, where $u, v \in R^\times$, $n, m \in \mathbb{N}_{\geq 0}$, and suppose without loss of generality that $m \geq n$. Then $t^n(u - vt^{m-n}) = 0$, from which we deduce $uv^{-1} = t^{m-n}$ is a unit. Hence $m - n = 0$, so $m = n$, and finally $u = v$. □

Definition 1.27. Given any $x = ut^n$ in a DVR, we call n the *order* of x, and it is does not depend on the choice of uniformising parameter (check this.)

1.9 Modules over rings

Modules provide a unifying algebraic structure to discuss abelian groups, rings and vector spaces.

Definition 1.28. Let R be a ring and M an abelian group. Suppose $\cdot : R \to M$ is a map, called scalar multiplication, such that for all $r, s \in R$, $m, n \in M$:

1. $r \cdot (m + n) = r \cdot m + r \cdot n$.
2. $(r + s) \cdot m = r \cdot m + s \cdot m$.
3. $(rs) \cdot m = r \cdot (s \cdot m)$.
4. $1 \cdot x = x$.

Then $(M, R, \cdot)$ is called a *module* over R. We say that M is an $R-$*module.* We typically omit the $\cdot$ notation.

Example 1.7.

1. Any abelian group G may be considered as a $\mathbb{Z}-$module by defining the scalar multiplication:
$$n \cdot g = \begin{cases} \underbrace{g + ... + g}_{n \text{ times}}, & n \geq 0 \\ \underbrace{-g - ... - g}_{n \text{ times}}, & n < 0 \end{cases}$$
2. A vector space V over a field k is a $k-$module.
3. A ring is a module over itself.

Remark. One should think of an $R-$module as a vector space where we relax the condition that R is a field, into merely being a ring.

Definition 1.29. Let M be an $R-$module. Suppose N is a subgroup of M such that N is closed under scalar multiplication from R. We then say N is an *R-submodule* of M.

Definition 1.30. Let M be an $R-$module and N an $R-$submodule of M. We define the *quotient module* M/N as the set of cosets $\{m + N \mid m \in M\}$ with addition $(m + N) + (m' + N) = (m + m') + N$ and scalar multiplication $a(m + N) = (am) + N$.

Remark. The homomorphism and correspondence theorems from the section on rings pass over to modules in the same way, with rings substituted for $R-$modules and ideals for $R-$submodules.

1.10 Exact sequences

Let V_1, V_2, V_3 be vector spaces over a field k, and ϕ, ψ linear maps over k. We say that the sequence

$$V_1 \xrightarrow{\phi} V_2 \xrightarrow{\psi} V_3$$

of $k-$linear maps is *exact* if $\operatorname{Im}\phi = \ker\psi$. Similarly the sequence

$$V_0 \xrightarrow{\phi_1} V_1 \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_{n-1}} V_{n-1} \xrightarrow{\phi_n} V_n$$

is called *exact* if $\operatorname{Im}\phi_i = \ker\phi_{i+1}$ for all $1 \leq i < n$.

Lemma 1.17. *The sequence*

$$0 \longrightarrow V_1 \xrightarrow{\phi} V_2 \xrightarrow{\psi} V_3 \longrightarrow 0$$

is exact if and only if ϕ is injective and ψ is surjective.

Remark. A sequence of the above form is called a *short exact sequence.*

Example 1.8. Let V be a vector space over k, W a subspace of V and consider the sequence

$$0 \longrightarrow W \longrightarrow V \xrightarrow{h} V/W \longrightarrow 0$$

where h is the natural projection onto V/W, and the map $W \to V$ is inclusion. This sequence is exact. Conversely, given any exact sequence

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$$

of vector spaces, we may regard U as a subspace of V. Hence U is the kernel of the map $\phi : V \to W$, and therefore $W = V/U$.

Remark. By virtue of the above example, a heuristic for thinking about short exact sequences is

$$0 \longrightarrow \text{subobject} \longrightarrow \text{primary object} \longrightarrow \text{quotient object} \longrightarrow 0.$$

Lemma 1.18. *Let V_1, V_2, V_3 be finite-dimensional vector spaces, and suppose the sequence*

$$0 \longrightarrow V_1 \xrightarrow{\phi} V_2 \xrightarrow{\psi} V_3 \longrightarrow 0$$

is exact. Then $\dim V_1 + \dim V_3 = \dim V_2$.

Proof. Since we have a short exact sequence, we see that $\dim\ker\phi = 0$ and $\dim\operatorname{Im}\psi = \dim V_3$. By the rank-nullity theorem of linear algebra, $\dim\ker\phi + \dim\operatorname{Im}\phi = \dim V_1$, $\dim\ker\psi + \dim\operatorname{Im}\psi = \dim V_2$. Applying the equalities due to exactness, we see $\dim\operatorname{Im}\phi = \dim V_1$, $\dim\ker\psi + \dim V_3 = \dim V_2$. Now $\operatorname{Im}\phi = \ker\psi$, hence $\dim V_1 + \dim V_3 = \dim V_2$. □

A similar proof of the above yields the following:

Lemma 1.19. *Let $V_1, V_2, V_3, ..., V_n$ be finite-dimensional vector spaces, and suppose the sequence*

$$0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow ... \longrightarrow V_{n-1} \longrightarrow V_n \longrightarrow 0$$

is exact. Then $\sum_{i=1}^{n}(-1)^{i+1}V_i = 0$.

2 Elements of algebraic geometry

Throughout, we assume k is an algebraically closed field.

2.1 Affine space

Definition 2.1. We denote $\mathbb{A}^n = \{(x_1, ..., x_n) \mid x_i \in k\}$. An *algebraic set* is a subset $X \subseteq \mathbb{A}^n$ whose elements are given by the zero set of an arbitrary set of polynomials $S \subseteq k[x_1, ..., x_n]$. We denote this zero set by $\mathbb{V}(S)$.

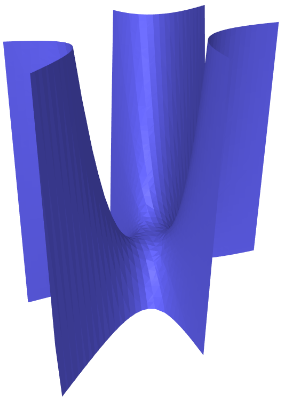

Figure 1: An algebraic set in $\mathbb{A}^3$.

Definition 2.2. We say an algebraic set X is *irreducible* if whenever X_1, X_2 are algebraic sets such that $X = X_1 \cup X_2$, then either $X_1 = X$ or $X_2 = X$. We call an irreducible algebraic set an *affine algebraic variety.*

Definition 2.3. Let X be an arbitrary subset of $\mathbb{A}^n$. We write

$$\mathbb{I}(X) = \{f \in k[x_1, ..., x_n] \mid f(a_1, ..., a_n) = 0 \text{ for all } (a_1, ..., a_n) \in X\}$$

and call it the *ideal of* X.

Lemma 2.1. *$\mathbb{I}(X)$ is an ideal of the polynomial ring $k[x_1, ..., x_n]$.*

Lemma 2.2. *An algebraic set X is irreducible (equivalently an affine algebraic variety) if and only if the ideal $\mathbb{I}(X)$ is prime.*

Proof. Suppose X is irreducible. Let $f, g \in k[x_1, ..., x_n]$, and suppose $fg \in \mathbb{I}(X)$. Then $(fg) \subseteq \mathbb{I}(X)$. Hence we have the inclusions $X = \mathbb{V}(\mathbb{I}(X)) \subseteq \mathbb{V}(fg) = \mathbb{V}(f) \cup \mathbb{V}(g)$. Therefore, we have that $X = (\mathbb{V}(f) \cap X) \cup (\mathbb{V}(g) \cap X)$. The irreducibility of X implies without loss of generality that $X = \mathbb{V}(f) \cap X$, so $X \subseteq \mathbb{V}(f)$. We conclude $f \in \mathbb{I}(X)$.

Conversely, suppose $\mathbb{I}(X)$ is prime. Suppose $X = X_1 \cup X_2$. Then we have that $\mathbb{I}(X) = \mathbb{I}(X_1) \cap \mathbb{I}(X_2)$. Now, if $\mathbb{I}(X) = \mathbb{I}(X_1)$ then $X_1 = X$, and then we are done. Otherwise, there exists $f \in \mathbb{I}(X_1) \backslash \mathbb{I}(X)$ and for any $g \in \mathbb{I}(X_2)$, $fg \in \mathbb{I}(X_1) \cap \mathbb{I}(X_2) = \mathbb{I}(X)$, from which we conclude $g \in \mathbb{I}(X)$ by the primality of $\mathbb{I}(X)$. Hence $\mathbb{I}(X_2) \subseteq \mathbb{I}(X) \subseteq \mathbb{I}(X_2)$, so $\mathbb{I}(X) = \mathbb{I}(X_2)$. Hence $X = X_2$. We conclude X is irreducible. □

Lemma 2.3. *Let $X, Y \subseteq \mathbb{A}^n$, $I, J \subseteq k[x_1, ..., x_n]$ be sets. The maps $\mathbb{I}$ and $\mathbb{V}$ reverse inclusions:*

1. *If $X \subseteq Y$ then $\mathbb{I}(Y) \subseteq \mathbb{I}(X)$.*

2. *If $I \subseteq J$ then $\mathbb{V}(J) \subseteq \mathbb{V}(I)$.*

Proof. Suppose $f \in \mathbb{I}(Y)$. Then f is a polynomial which vanishes on all of Y, and hence all of X, since $X \subseteq Y$. Hence $f \in \mathbb{I}(X)$.

Suppose $x = (a_1, ..., a_n) \in \mathbb{V}(J)$. Then $f(x) = 0$ for every $f \in J$, and hence for every $f \in I$, since $I \subseteq J$. Hence $x \in \mathbb{V}(I)$. □

Lemma 2.4. *We have the follow inclusions and equalities (Galois correspondence!):*

1. *$X = \mathbb{V}(\mathbb{I}(X))$.*

2. *$I \subseteq \mathbb{I}(\mathbb{V}(I))$.*

Definition 2.4. We define a topology on $\mathbb{A}^n$, whose closed sets are the algebraic sets. That is, a set $X \subseteq \mathbb{A}^n$ is closed if and only if it may be written $X = \mathbb{V}(I)$ for some ideal $I \subseteq k[x_1, ..., x_n]$. We call this topology the *Zariski topology*. Subvarieties of $\mathbb{A}^n$ get the induced subspace topology.

Definition 2.5. For each polynomial $f \in k[x_1, ..., x_n]$ we obtain a map $f : \mathbb{A}^n \to k$ by evaluating f at points of $\mathbb{A}^n$. Suppose $X \subseteq \mathbb{A}^n$. The restriction of f to X induces a polynomial map $f \mid_X : X \to k$. Let $\pi : k[x_1, ..., x_n] \to k[x_1, ..., x_n] \mid_X$, $f \mapsto f \mid_X$. Then $\ker(\pi) = \mathbb{I}(X)$.

Hence by the ring homomorphism theorem, $k[x_1, ..., x_n] \mid_X \cong k[x_1, ..., x_n]/\mathbb{I}(X)$. We denote this ring by $\Gamma(X)$ and call it the *coordinate ring* of X.

Theorem 2.5. *(Weak Nullstellensatz.) Let $I \subseteq k[x_1, ..., x_n]$ be an ideal and suppose $\mathbb{V}(I) = \emptyset$. Then $I = k[x_1, ..., x_n]$.*

Proof. A proof is found in ([2], 1.7.) □

Theorem 2.6. *(Nullstellensatz.) Let $I \subseteq k[x_1, ..., x_n]$ be an ideal. Then $\sqrt{I} = \mathbb{I}(\mathbb{V}(I))$, where $\sqrt{I}$ is the radical of I.*

Proof. We show the inclusion $\sqrt{I} \subseteq \mathbb{I}(\mathbb{V}(I))$ first: Let $f \in \sqrt{I}$. Then there exists $m \in \mathbb{N}$ such that $f^m \in I$. Hence $f^m \in \mathbb{I}(\mathbb{V}(I))$ by Lemma 2.4. Since the zero sets of f^m and f are equal, we have $f \in \mathbb{I}(\mathbb{V}(I))$.

Now we show the reverse inclusion; the method is due to Rabinowitsch. Since $k[x_1, ..., x_n]$ is Noetherian (Theorem 1.12), there exists $f_1, ..., f_s \in k[x_1, ..., x_n]$ such that $I = (f_1, ..., f_s)$. Let $f \in \mathbb{I}(\mathbb{V}(I))$, and define the ideal

$$I' = (f_1, ..., f_s, 1 - yf) \subseteq k[x_1, ..., x_n, y].$$

We want to show $\mathbb{V}(I')$ is empty. To this end, suppose for contradiction that $\mathbb{V}(I') \neq \emptyset$; hence choose $(a_1, ..., a_n, a_{n+1}) \in \mathbb{V}(I')$. We have $(a_1, ..., a_n) \in \mathbb{V}(I)$. Since $f \in I$, $f(a_1, ..., a_n) = 0$. Hence $(1 - yf)(a_1, ..., a_n, a_{n+1}) = 1 - a_{n+1}f(a_1, ..., a_n) = 1 - 0 = 1 \neq 0$, a contradiction. So $\mathbb{V}(I') = \emptyset$, hence by Theorem 2.5, $I' = k[x_1, ..., x_n, y]$. In particular $1 \in I'$, so there exists $h_1, ..., h_s, p \in k[x_1, ..., x_n, y]$ such that

$$1 = h_1 f_1 + ... + h_s f_s + p(1 - yf).$$

Now set $y = 1/f(x_1, ..., x_n)$. We obtain

$$1 = h_1(x_1, ..., x_n, 1/f)f_1 + ... + h_s(x_1, ..., x_n, 1/f)f_s$$

and hence by multiplying through by a high enough power f^m to clear the denominators yields

$$f^m = h'_1(x_1, ..., x_n)f_1 + ... + h'_s(x_1, ..., x_n)f_s$$

and hence $f^m \in (f_1, ..., f_s)$. So $f \in \sqrt{I}$. □

Corollary. *There are bijective order-reversing correspondences between:*

1. *Algebraic sets in k^n and radical ideals in $k[x_1, ..., x_n]$.*

2. *Affine algebraic varieties in k^n and prime ideals in $k[x_1, ..., x_n]$.*

Theorem 2.7. *Every algebraic set is a finite union of affine algebraic varieties.*

Proof. Let X be an algebraic set. If X is irreducible, we are done. Otherwise, there exists algebraic sets $X_1, X_1' \subsetneq X$ with $X = X_1 \cup X_1'$. If both X_1 and X_1' are irreducible then we are done, otherwise without loss of generality we may similarly write $X_1 = X_2 \cup X_2'$ with $X_2, X_2' \subsetneq X_1$. Continuing in this fashion we obtain a strictly decreasing chain of algebraic sets

$$X \supsetneq X_1 \supsetneq X_2 \supsetneq ...$$

which by the Nullstellensatz (Theorem 2.6) corresponds to a strictly increasing chain of ideals $I \subsetneq I_1 \subsetneq I_2 \subsetneq ...$ of $k[x_1, ..., x_n]$, which must terminate by the Noetherian property. Hence the chain of algebraic sets must terminate too. Hence we may write X as a finite union of irreducible algebraic sets. □

2.2 Projective space

Definition 2.6. Let k be a field. Let $\mathbb{P}^n(k)$ be the set of all $1-$dimensional subspaces of k^{n+1}. We call $\mathbb{P}^n(k)$ *projective space*, calling $\mathbb{P}^1(k)$ the projective line, $\mathbb{P}^2(k)$ the projective plane, etc.

Remark. Equivalently, one can define projective space $\mathbb{P}^n(k)$ as the quotient of k^{n+1} by the equivalence relation $(a_0, a_1, ..., a_n) \sim (b_0, b_1, ..., b_n)$ if and only if there exists $\lambda \in k^\times$ such that $(a_0, a_1, ..., a_n) = (\lambda b_0, \lambda b_1, ..., \lambda b_n)$. We denote the equivalence class of $(a_0, a_1, ..., a_n)$ by $[a_0 : a_1 : ... : a_n]$. These are *projective coordinates.*

Definition 2.7. For each $0 \leq i \leq n$, let $U_i = \{[a_0 : a_1 : ... : a_n] \in \mathbb{P}^n \mid a_i \neq 0\}$. Then $\mathbb{P}^n = \bigcup_{i=0}^n U_i$. We call each U_i an *affine patch* of $\mathbb{P}^n$.

Note. Let $x \in U_j$. Then we may write $x = [a_0/a_j : a_1/a_j : ... : 1 : ... : a_n/a_j]$ (the jth coordinate is 1), and so for each $x \in U_j$ we choose the representative $(a_0/a_j, a_1/a_j, ..., 1, ..., a_n/a_j)$.

This representative is called the *local affine coordinates* for x. With this convention adopted we then have

$$U_j = \{(a_0, a_1, ..., 1, ..., a_n) \mid a_0, a_1, ..., a_n \in k\} \cong \mathbb{A}^n$$

$$\mathbb{P}^n \setminus U_j = \{[a_0, a_1, ..., 0, ..., a_n] \mid a_0, a_1, ..., a_n \in k\} \cong \mathbb{P}^{n-1}.$$

Hence we may write $\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{P}^{n-1}$. The $\mathbb{P}^{n-1}$ in this decomposition is called the *hyperplane at infnity.*

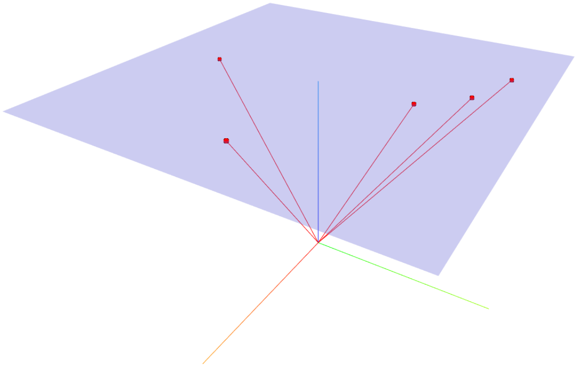

Figure 2: An example of an affine patch of $\mathbb{P}^2$ by considering the intersection of lines through the origin in k^3 with a fixed plane which does not pass through the origin. We identify each line with its intersection point on the plane, and this sets up a one-to-one correspondence of $\mathbb{A}^2$ with those lines. The only lines in k^3 which fail to get a representative are the lines which are parallel to the plane. From the plane's point of view, these lines correspond to 'points at infinity'.

Remark. Similar to the affine case, we may define *projective algebraic sets* and the *ideal of a projective algebraic set*, but for this to be well-defined, we need to restrict our defining polynomials to be homogeneous.

Definition 2.8. We say that $X \subseteq \mathbb{P}^n$ is a *projective algebraic set* if $X = \{x \in \mathbb{P}^n \mid f(x) = 0 \text{ for all } x \in S\}$, where $S \subseteq k[x_0, ..., x_n]$ is a set of homogeneous polynomials of degree d. We write $X = \mathbb{V}(S)$.

Definition 2.9. Let $X \subseteq \mathbb{P}^n$. We define $\mathbb{I}(X)$ to be the set of all homogeneous polynomials in $k[x_0, ..., x_n]$ which vanish at all $x \in X$. It is an ideal, called the *(projective) ideal of* X.

Definition 2.10. Let $X \subseteq \mathbb{A}^n$ be an affine algebraic variety. We may consider X as a subset of $\mathbb{P}^n$ by the map $(x_1, ..., x_n) \mapsto [1 : x_1 : ... : x_n]$. The *projective closure* X^* of X is defined to be the closure (in the topological sense) of X in $\mathbb{P}^n$. If $X = \mathbb{V}(I)$, then $X^* = \mathbb{V}(I^*)$, where I^* is the ideal generated by all homogenisations of elements of I. If $I = (F)$ then $I^* = (F^*)$ where F^* is the homogenisation of F ([2], Chapter 4.)

Example 2.1. Let $X = \mathbb{V}(x^2 - y) \subset \mathbb{A}^n$. Then $X^* = \mathbb{V}(X^2 - YZ) \subset \mathbb{P}^2$. The points at infinity of $X^2 - YZ$ may be obtained by setting $Z = 0$. Then $X = 0$, so $[0 : 1 : 0]$ is the only point at infinity. Hence we can write

$$X^* = \mathbb{V}(x^2 - y) \sqcup \{[0 : 1 : 0]\}$$

and so we can view the projective closure as adding in points at infinity, in line with Definition 2.7.

Definition 2.11. Suppose $T : k^{n+1} \to k^{n+1}$ is a linear map that takes lines through the origin to lines through the origin. Then T determines a map $\mathbb{P}^n \to \mathbb{P}^n$, which we call a *projective change of coordinates*, or a *projective transformation.*

2.3 Functions on varieties

Definition 2.12. Let $X \subseteq \mathbb{A}^n$ be an algebraic set. Recall the *coordinate ring* $\Gamma(X)$ as in Definition 2.5. We call elements of $\Gamma(X)$ *regular functions on* X.

Definition 2.13. Let $X \subseteq \mathbb{A}^n, Y \subseteq \mathbb{A}^m$ be affine algebraic sets. A *regular map* $f : X \to Y$ is a map which may be written $f = (f_1, ..., f_m)$ where each $f_i \in \Gamma(X)$. We say X and Y are *isomorphic* if there exists bijective regular $f : X \to Y$ with regular inverse.

Remark. If we restrict the f_i to be linear polynomials, and suppose f is bijective, then we say that f determines an *affine change of coordinates*, or *affine transformation* of X (equivalently, Y.) Every affine transformation consists of a translation and a linear transformation. The set of all affine transformations with function composition forms a group structure.

Definition 2.14. Let X be an affine algebraic variety. Since X is irreducible, $\mathbb{I}(X)$ is prime, so $\Gamma(X)$ is an integral domain (Lemma 1.8.) Denote by $k(X)$ the field of fractions of $\Gamma(X)$. We call $k(X)$ the *function field* of X. Elements of $k(X)$ are called *rational functions on X*.

Definition 2.15. Let X be an affine algebraic variety, $p \in X$. Define the ring $\mathcal{O}_p(X) = \{f/g \mid f, g \in \Gamma(X), g(p) \neq 0\}$, with natural addition and multiplication inherited from $k(X)$. We call $\mathcal{O}_p(X)$ the *local ring* of X at p.

Remark. Let $p = (p_1, p_2, \ldots, p_n)$. Then $\mathcal{O}_p(X)$ is the localisation of $\Gamma(X)$ at the maximal ideal $(x_1 - p_1)(x_2 - p_2) \ldots (x_n - p_n)$.

Definition 2.16. If X is a projective variety and $p \in X$, we define $\mathcal{O}_p(X)$ as $\mathcal{O}_p(X \cap U)$, where U is an affine chart containing p. This does not depend on the choice of affine chart; for two choices of affine charts, the corresponding local rings are naturally isomorphic ([2], 5.1).

Definition 2.17. Let $\phi \in k(X)$. We say that ϕ is *regular at $p \in X$* if $\phi \in \mathcal{O}_p(X)$.

Theorem 2.8. *Let X be an affine algebraic variety. A function $\phi \in k(X)$ is a regular function if and only if it is regular at every $p \in X$.*

Proof. This amounts to showing that $\bigcap_{p \in X} \mathcal{O}_p(X) = \Gamma(X)$. Clearly $\Gamma(X) \subseteq \bigcap_{p \in X} \mathcal{O}_p(X)$, since $\Gamma(X)$ is an integral domain. Now let $\phi \in \bigcap_{p \in X} \mathcal{O}_p(X)$, and suppose for a contradiction that $\phi \notin \Gamma(X)$. Define the ideal $I_\phi = \{f \in \Gamma(X) \mid f\phi \in \Gamma(X)\}$. Then I_ϕ is proper, since $1 \notin I_\phi$. Hence there must be a maximal ideal $\mathfrak{m}$ containing I_ϕ. Let q be the corresponding point in X (Nullstellensatz), so $\phi \in \mathcal{O}_q(X)$. Now there must exist $g \in \Gamma(X)$ with $g(q) \neq 0$ and $g\phi \in \Gamma(X)$. Hence $g \notin \mathfrak{m}$, $g \in I_\phi$. But this contradicts $I_\phi \subseteq \mathfrak{m}$. □

We need a theorem for a result in the next section, but its proof is found in [2], 2.10, Corollary 2.

Theorem 2.9. *Let I be an ideal of $k[x_1, ..., x_n]$. If $\mathbb{V}(I) = P$, then $k[x_1, ..., x_n]/I$ is isomorphic to $\mathcal{O}_P(\mathbb{A}^n)/I\mathcal{O}_p(\mathbb{A}^n)$.*

3 Projective plane curves

The primary reference for this section is [2], Chapters 3 and 5.

3.1 Multiplicities and local rings

Definition 3.1. Let $F \in k[X,Y,Z]$ be a homogeneous polynomial. We say $\mathbb{V}(F)$ is a *projective plane curve.* A projective plane curve of degree 1 is called a line, of degree 2 is called a conic, of degree 3 a cubic, of degree 4 a quartic, etc.

Note. Unless otherwise stated, we assume F is irreducible. Hence we will write $\mathcal{O}_P(F)$ instead of $\mathcal{O}_P(\mathbb{V}(F))$ and so on. We will frequently swap notation for curves and polynomials, writing F instead of $C = \mathbb{V}(F)$ and vice versa.

Definition 3.2. Let C be a projective plane curve, and $C = \mathbb{V}(F)$, where $F \in k[X,Y,Z]$. Let $p \in C$. We say that C is *nonsingular* or *simple* at p if none of the partial derivatives $\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z}$ vanish at p. Otherwise p is a *singular* or *multiple* point. The curve C is *smooth* if every point in C is simple.

Definition 3.3. Let $C = \mathbb{V}(F)$ be a projective plane curve, and suppose F has degree n. Let $p \in C$, and suppose U is an affine chart containing p, such that $p \mapsto (0,0)$ in this chart. Let f be the dehomogenisation of F with respect to this coordinate chart. Write

$$f = f_m + f_{m+1} + ... + f_n$$

where each f_i is homogeneous of degree i, and $m \leq n$. We call the integer m the *multiplicity* of F at p, and write $m = m_p(C)$. The form f_m can be factored into irreducible components as

$$f_m = \prod L_i^{r_i}$$

where the L_i are distinct lines, r_i their multiplicities. We call the L_i the *tangent lines* to C at p, with the r_i being their *tangent multiplicities.*

Remark. Suppose without loss of generality that p is contained in U_z, and $p \mapsto (a,b)$ in this chart. Then to find the multiplicity of F and the tangents lines at p, we apply the above definition to the polynomial

$$g = f(x+a, y+b).$$

Theorem 3.1. *Let F be a smooth projective plane curve. Then for any $p \in \mathbb{V}(F)$, $\mathcal{O}_p(F)$ is a discrete valuation ring. As a uniformising parameter, one can choose the image in $\Gamma(F)$ of any line $L = aX + bY + cZ$ which is not tangent to F at p.*

Proof. Pass over to an affine chart containing p and then use [2], Chapter 3, page 34. It does not depend on the choice of affine chart by the usual considerations. □

Remark. More is true; $\mathcal{O}_p(F)$ is a DVR if and only if p is simple, as the referenced result above shows.

Definition 3.4. Let C be a projective plane curve, and suppose $p \in C$ is a simple point. Let $f \in \mathcal{O}_p(C)$, and t a uniformising parameter for $\mathcal{O}_p(C)$. Then we may write $f = ut^n$ for some unique $u \in \mathcal{O}_p(C)^\times$ and $n \in \mathbb{Z}$. We define $\operatorname{ord}_p(C) = n$. By our results in Section 1, this does not depend on the choice of t.

We now state some properties of the order function. The proofs are easy and are left as a useful exercise:

Lemma 3.2. *The order function satisfies the following properties for all non-zero $f, g \in k(C)$:*

1. $\operatorname{ord}_p(fg) = \operatorname{ord}_p(f) + \operatorname{ord}_p(g)$.

2. $\operatorname{ord}_p(f) \geq 0 \iff f \in \mathcal{O}_p(C)$.

3. $\operatorname{ord}_p(f) = 0 \iff f \in \mathcal{O}_p(C)^\times$.

Furthermore, if $\operatorname{ord}_p(f) \geq 0$ *for every $p \in C$, then equivalently* $\operatorname{ord}_p(f) = 0$ *for every $p \in C$ and hence $f \in k$.*

The multiplicity of a curve at a point depends only on the local ring at the point:

Theorem 3.3. *Let $C = \mathbb{V}(F)$ be a projective plane curve, $p \in C$. Let $\mathcal{O} = \mathcal{O}_p(C)$ be the local ring at p with maximal ideal $\mathfrak{m}$. Then for all sufficiently large n,*

$$m_p(C) = \dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}).$$

Remark. Before we prove the theorem, we will work out an example of calculating a dimension of a polynomial ring. The result is used in the proof.

Example 3.1. Let $I = (x, y) \subset k[x, y]$, and $n \in \mathbb{N}$. Let us calculate the dimension $\dim_k(k[x, y]/I^n)$. Elements of $k[x, y]$ whose residues are 0 are finite sums of monomials of the form $x^i y^j$, where $i + j \geq n$. Hence as basis elements we can choose all monomials of the form $x^i y^j$ where $i + j < n$, of which there are $n(n + 1)/2$ such monomials in $k[x, y]$.

Indeed, given $f \in k[x, y]$, write $f = \sum_{i,j} a_{ij} x^i y^j$. Then taking I^n-residues, we see all the monomials of the form $x^i y^j$ where $i+j \geq n$ are killed by I^n, so the claimed basis spans $k[x, y]/I^n$. And we have linear independence, for suppose there exists a linear relation $\sum_{i,j,i+j\leq n} c_{ij} x^i y^j = 0$. Then the polynomial $f(x, y) = \sum_{i,j,i+j\leq n} c_{ij} x^i y^j$ is identically zero, and so must be the zero polynomial, i.e., $c_{ij} = 0$ for all i, j.

Proof. Let us pass over to an affine chart containing p. Suppose without loss of generality that this chart is U_z and that $p = (0, 0)$ in this chart. Then we may write $\mathfrak{m}^n = I^n\mathcal{O}$, where $I = (x, y)$ is an ideal of $k[x, y]$. Now $\mathbb{V}(I^n) = \{p\}$. Hence by Theorem 2.9,

$$k[x, y]/(I^n, F) \cong \mathcal{O}_p(\mathbb{A}^2)/(I^n, F)\mathcal{O}_p(\mathbb{A}^2) \cong \mathcal{O}_p(F)/I^n\mathcal{O}_p(F) = \mathcal{O}/\mathfrak{m}^n.$$

where we used the fact that $\mathcal{O}_p(\mathbb{A}^2)/(I^n, F)\mathcal{O}_p(\mathbb{A}^2) = \mathcal{O}_p(F)/I^n\mathcal{O}_p(F)$, since the image of F in $\Gamma(F)$ is zero. Hence it is enough to calculate the dimension of $k[x, y]/(I^n, F)$ over k. Let us denote $m = m_p(C)$. The sequence

$$\begin{tikzcd} 0 \arrow[r] & k[x,y]/I^{n-m} \arrow[r, "\psi"] & k[x,y]/I^n \arrow[r, "\phi"] & k[x,y]/(I^n,F) \arrow[r] & 0 \end{tikzcd}$$

is exact, where $\psi(G+I^{n-m}) = FG+I^n$ and ϕ is a natural homomorphism. Using Lemma 1.18, we get that

$$\dim_k(\mathcal{O}/\mathfrak{m}^n) = \dim_k(k[x, y]/(I^n, F)) = n(n+1)/2-(n-m)(n-m+1)/2 = mn-m(m+1)/2$$

and finally, from the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathfrak{m}^n/\mathfrak{m}^{n+1} \arrow[r] & \mathcal{O}/\mathfrak{m}^{n+1} \arrow[r] & \mathcal{O}/\mathfrak{m}^n \arrow[r] & 0 \end{tikzcd}$$

we see that

$$\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = m(n + 1) - m(m + 1)/2 - mn + m(m + 1)/2 = m$$

as required. □

3.2 Intersection numbers

Given two curves F and G, we want to classify the types of points in $\mathbb{V}(F) \cap \mathbb{V}(G)$. One way to achieve this is via the intersection number, which we now discuss.

Definition 3.5. Let F, G be projective plane curves (not necessarily irreducible.) Suppose $p \in \mathbb{P}^2$, and let U be an affine chart containing p. Denote by f, g respectively the dehomogenisations of F and G with respect to this affine chart U. We define

$$I(p, F \cap G) = \dim_k(\mathcal{O}_p(U)/(f, g))$$

and call it the *intersection number* of F and G at p.

Remark. As usual, this definition does not depend on the choice of affine chart containing p, since it involves the dimension of a local ring. The definition may seem unintuitive at first glance, so we now list some properties that this intersection number satisfies.

Theorem 3.4. *The intersection number $I(p, F \cap G)$ satisfies the following properties:*

1. *$I(p, F \cap G)$ is a non-negative integer, unless $p \in \mathbb{V}(\gcd(F, G))$, in which case $I(p, F \cap G) = \infty$.*

2. *$I(p, F \cap G) = 0$ if and only if $p \notin \mathbb{V}(F) \cap \mathbb{V}(G)$.*

3. *If F, G are distinct lines then at the point of intersection p, $\mathbb{V}(p, F \cap G) = 1$.*

4. *$I(p, F \cap G) = I(p, G \cap F)$.*

5. *$I(p, F \cap G) = \sum_{i,j} a_i b_j I(p, F_i \cap G_j)$ where $F = \prod_i F_i^{r_i}$, $G = \prod_j G_j^{s_j}$ are the factorisations of F and G into irreducible components.*

6. *$I(p, F \cap G) = I(p, F \cap (G + HF))$ for any $H \in k[X, Y, Z]$.*

Proof. We prove only property 5; the remaining properties' proofs may be found by consulting [2], 3.3, Theorem 3.

We will show that for any F, G, H, $I(p, F \cap GH) = I(p, F \cap G) + I(p, F \cap H)$, as then the result follows by induction. Assume that F and GH are coprime, for otherwise property 1 will apply to complete the proof. Let us define the $k-$linear homomorphism

$\phi : \mathcal{O}/(F, GH) \to \mathcal{O}/(F, G)$ in the natural way and the $k-$linear homomorphism $\psi : \mathcal{O}/(F, H) \to \mathcal{O}/(F, GH)$ by $\psi(a + (F, H)) = Ga + (F, H)$.

Now ψ is injective, as we will now show. Denote by $\overline{Z}$ the coset $Z + (F, H)$, and suppose $\psi(\overline{Z}) = 0$. Then $GZ \in (F, H)$, so we may write

$$GZ = uF + vH$$

for some $u, v \in \mathcal{O}$. Now let $S \in k[X, Y, Z]$ with $S(p) \neq 0$, and denote $A = Su, B = Sv, C = SZ$. Then multiplying through by S in the above equation, we get

$$GSZ = SuF + SvH$$

and hence

$$G(C - BH) = AF.$$

By assumption, F and G have no common factors. Hence F must divide $C - BH$, which means we can write $C - BH = DF$ for some $D \in k[X, Y, Z]$. So $C = BH + DF$, hence

$$Z = (B/S)H + (D/S)F$$

which shows $\overline{Z} = 0$, as required. Next, ϕ is clearly surjective. Hence the sequence of vector spaces

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{O}/(F, H) \arrow[r, "\psi"] & \mathcal{O}/(F, GH) \arrow[r, "\phi"] & \mathcal{O}/(F, G) \arrow[r] & 0 \end{tikzcd}$$

is exact. Counting dimensions with Lemma 1.18, we obtain the result. □

Example 3.2. Let us compute the intersection number of $F = X^2, G = YZ$ at $p = [0 : 0 : 1]$. Using property 5, we have that $I(p, F \cap G) = 2I(p, X \cap Y) + 2I(p, X \cap Z)$. Clearly $I(p, X \cap Z) = 0$. And since X, Y are distinct lines we have that $I(p, X \cap Y) = 1$. Hence $I(p, F \cap G) = 2$.

Alternatively, we could look at the affine chart U_z, where p is identified with $(0, 0)$, and the dehomogenisations of F and G in this chart are $f = x^2$, $g = y$ respectively. Consider the ring $\mathcal{O}_p(U_z)/(f, g)$. As a basis, one can take $\{1, x\}$, since higher degree terms in x or y are killed by the ideal (f, g). Hence $\dim_k \mathcal{O}_p(U_z)/(f, g) = 2$.

Lemma 3.5. *Suppose p is a simple point on the projective plane curve $C = \mathbb{V}(F)$. Then $I(p, C \cap G) = \text{ord}_p(G)$, where $\text{ord}_p(G)$ is the order of G in the local ring $\mathcal{O}_p(C)$.*

Proof. Let g denote the image of G in the local ring $\mathcal{O}_p(C)$, and let U be an affine chart containing p. Then $\mathrm{ord}_p(C) = \dim_k(\mathcal{O}_p(C)/(g)) = \dim_k(\mathcal{O}_p(U)/(F, G))$, since the rings $\mathcal{O}_p(C)/(g), \mathcal{O}_p(U)/(F, g)$ are isomorphic. Hence $\mathrm{ord}_p(C) = I(p, C \cap G)$. □

Lemma 3.6. *Suppose f and g are distinct affine plane curves. Then*

$$\sum_p I(p, f \cap g) = \dim_k(k[x, y]/(f, g)).$$

Proof. [2], 2.9, Corollary 1. □

Lemma 3.7. *Suppose f and g are distinct projective curves. Then $I(p, F \cap G) \geq m_p(F)m_p(G)$, with equality if and only if F and G have distinct tangent lines at p.*

Proof. This is item 5 of [2], 3.3. □

3.3 Bézout's theorem

This subsection is devoted to the statement, proof and corollaries of Bézout's theorem, which is one of the cornerstones of projective geometry and the primary reason we prefer projective varieties over affine ones. We denote by F, G the curves $\mathbb{V}(F), \mathbb{V}(G)$ respectively.

Theorem 3.8. *(Bézout's theorem.) Let F, G be projective plane curves of degree m and n respectively, and let us suppose F and G have no common factors. Then*

$$\sum_{p \in V} I(p, F \cap G) = mn.$$

Proof. We follow a similar style to [2]'s treatment of Bézout's theorem.

Let us assume that all of the points in $F \cap G$ can be written $[x : y : 1]$ for some $x, y \in k$. This assumption preserves generality, since any two projective curves without common components intersect at a finite number of points, so we can transform those p that lie on $Z = 0$ by a projective transformation. Then it follows that, denoting f, g for the dehomogenisations of F and G with respect to U_z,

$$\sum_{p \in F \cap G} I(p, F \cap G) = \sum_{p \in f \cap g} I(p, f \cap g) = \dim_k(k[x, y]/(f, g))$$

by Lemma 3.6. Now let us denote $\Gamma_* = k[x,y]/(f,g)$, $\Gamma = k[X,Y,Z]/(F,G)$, and $R = k[X,Y,Z]$. Let us denote Γ_d, R_d for the vector space of homogeneous polynomials of degree d in Γ, R respectively. Now we are going to show that there exists some sufficiently large d such that $\dim_k \Gamma_* = \dim_k \Gamma_d = mn$. Then the theorem is proved by the equality above.

1. Let $d \geq m+n$; we will show $\dim_k \Gamma_d = mn$. Let $h : R \to \Gamma$ be the natural projection. The product of rings $R \times R$ carries the natural ring structure induced by R, so let $\phi : R \times R \to R$ be such that $\phi(U,V) = UF + VG$. and let $\psi : R \to R \times R$ be such that $\psi(W) = (GW, -FW)$. It is a routine verification, remembering that F and G are coprime, to check that the following sequence of vector spaces is exact:

   $$0 \longrightarrow R \xrightarrow{\psi} R \times R \xrightarrow{\phi} R \xrightarrow{h} \Gamma \longrightarrow 0.$$

   Now let us restrict each of the maps in the exact sequence to forms of given degrees. The following sequence is then exact:

   $$0 \longrightarrow R_{d-m-n} \xrightarrow{\psi} R_{d-m} \times R_{d-n} \xrightarrow{\phi} R_d \xrightarrow{h} \Gamma_d \longrightarrow 0.$$

   It is not difficult to calculate $\dim_k R_d = \frac{(d+1)(d+2)}{2}$. Hence using Lemma 1.19, and after some tedious algebra, we obtain $\dim_k \Gamma_d = mn$.

2. Let

   $$\alpha : \Gamma \to \Gamma,$$
   $$H + (F,G) \mapsto ZH + (F,G).$$

   Let us denote by J_0 the polynomial $J(X,Y,1)$ where $J \in \Gamma$. Since $\mathbb{V}(F,G,Z) = \emptyset$, then certainly F_0, G_0 are coprime. We claim that α is injective. Indeed, suppose $\alpha(H+(F,G)) = 0$. Then $ZH = AF+BG$ for some $A, B \in \Gamma$. Hence $A_0F_0 = -B_0G_0$, so, remembering that F_0 and G_0 are coprime, there exists some $C \in \Gamma$ such that $B_0 = F_0C$ and $A_0 = -G_0C$. Let us denote $A_1 = A + CG$, $B_1 = B - CF$. Then clearly $(A_1)_0 = (B_1)_0 = 0$. Hence we may write $A_1 = ZA', B_1 = ZB'$ for some $A', B' \in \Gamma$. Then $H = A'F + B'G$, so $H \in (F,G)$, i.e. $H = 0$ in Γ, as required.

3. Assume $d \geq m+n$ and let $\{\overline{A_1}, ..., \overline{A_{mn}}\}$ be a basis for Γ_d. Let a_i be the dehomogenisation of A_i with respect to U_z, and $\overline{a_i}$ the residue of a_i in Γ_*. We claim that $\{\overline{a_1}, ..., \overline{a_{mn}}\}$ is a basis for Γ_*.

   The map α in step 2 is an isomorphism of vector spaces from Γ_d onto Γ_{d+1}, provided $d \geq m+n$, since these two spaces have the same dimension, so any injection between them is an isomorphism. Hence the residues of $Z^r A_1, ..., Z^r A_{mn}$ in Γ_{d+r} form a basis for all $r \geq 0$.

   The $\overline{a_i}$ span Γ_*, for let $h = \overline{H} \in \Gamma_*$ where $H \in k[x, y]$. Then there is some N such that $Z^n H^*$, where H^* is the homogenisation of H with respect to Z, has degree $d+r$, Hence $Z^n H^* = \sum_{i=1}^{mn} \lambda_i Z^r A_i + BF + CG$ for some $\lambda_i \in k$ and $B, C \in k[X, Y, Z]$. Hence $H = (Z^n H^*)_* = \sum \lambda_i a_i + B_* F_* + C_* G_*$. Hence $h = \sum_{i=1}^{mn} \lambda_i \overline{a_i}$.

   The $\overline{a_i}$ are linearly independent. Suppose $\sum_{i=1}^{mn} \lambda_i \overline{a_i} = 0$. Then $\sum_{i=1}^{mn} \lambda_i a_i = Bf + Cg$. Hence $Z^r \sum_{i=1}^{mn} \lambda_i a_i = Z^s B^* F + Z^t C^* G$ for some r, s, t. Then $\sum_{i=1}^{mn} \lambda_i \overline{Z^r A_i} = 0$ in the space Γ_{d+r}. We know the $\overline{Z^r A_i}$ form a basis. Hence each $\lambda_i = 0$.

□

Example 3.3. To illustrate Bézout's theorem in practice, let $f = x^2 + y^2 - z^2$ and $g = x - y$. Then the two projective plane curves defined by these polynomials intersect when $x = y$ and $2x^2 - z^2 = 0$, that is when $(\sqrt{2}x + z)(\sqrt{2}x - z) = 0$, that is at the points $p = [1 : 1 : -\sqrt{2}], q = [1 : 1 : \sqrt{2}]$. So only these points have non-vanishing intersection number.

Let $t \in \mathbb{P}^2$. Let us compute $I(t, f \cap g)$. We have

$$I(t, (x^2+y^2-z^2) \cap (x-y)) = I(t, (2y^2-z^2) \cap (x-y)) = I(t, ((\sqrt{2}x+z)(\sqrt{2}x-z)) \cap (x-y))$$

by application of property 6 of intersection numbers, subtracting $(x+y)$ times g from f. Now, by property 5,

$$I(t, (x^2+y^2-z^2) \cap (x-y)) = I(t, (\sqrt{2}x+z) \cap (x-y)) + I(t, (\sqrt{2}x-z) \cap (x-y)).$$

Now we appeal to property 3. Since p is the point of intersection of $x - y$ with $\sqrt{2}x - z$, only the second term evaluates to 1 at p, whilst the first term is 0 at p. Similarly, the first term evaluates to 1 at q, and the second term is 0 at q. Hence

$$I(p, f \cap g) = 1, I(q, f \cap g) = 1$$

and hence

$$\sum_{t \in \mathbb{P}^2} I(t, f \cap g) = 2 = \deg(f) \cdot \deg(g)$$

as claimed by Bézout's theorem.

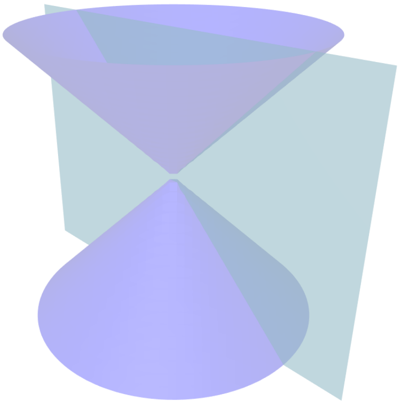

Figure 3: The geometric setup of Example 3.3 in $\mathbb{A}^3$. The intersection consists of two lines through the origin, so two projective points. The plane is not tangent to the cone so we expect the intersection number at each projective point to be 1.

Corollary. *Suppose F, G are distinct projective plane curves. Then*

$$\sum_{p \in \mathbb{P}^2} m_p(F) m_p(G) \leq \deg(F) \cdot \deg(G).$$

Proof. Use Bézout's theorem and Lemma 3.7. □

Corollary. *Suppose F is a smooth projective curve; then it is irreducible.*

Proof. Suppose for a contradiction that F is reducible, and let $F = GH$ be a non-trivial factorisation. On the one hand, the curves G, H intersect somewhere in $\mathbb{P}^2$, by Bézout's theorem. So F has a root, which is a root of both G and H. On the other hand, the singular points $[X_1 : X_2 : ... : X_n]$ of F satisfy, for each $i = 1, 2, ..., n$,

$$\frac{\partial F}{\partial X_i} = G \frac{\partial H}{\partial X_i} + H \frac{\partial G}{\partial X_i} = 0$$

and so any point in the intersection of G and H must be singular. But this contradicts the fact that F is smooth. □

Remark. The converse does not hold in general; For example, suppose $F = X^3 - ZY^2$. Here F is irreducible, which could be verified by Eisenstein's criterion using Z. But the partial derivatives all vanish at $[0 : 0 : 1]$, so the curve is not smooth.

4 Divisors on curves

Let $C = \mathbb{V}(F)$ be a projective plane curve in $\mathbb{P}^2$. We assume that C is smooth and irreducible unless otherwise stated.

Definition 4.1. A *divisor* on C is an element of the free abelian group on the points of C. That is,

$$D = n_1 p_1 + n_2 p_2 + ... + n_k p_k$$

where the $p_i \in C$ and $n_1, ..., n_k$ are a finite collection of integer coefficients.

Definition 4.2. We call $\deg D = \sum_{i=1}^{k} n_i$ the *degree* of the divisor D.

Definition 4.3. Let $D = n_1 p_1 + ... + n_k p_k$ be a divisor. We say that D is *effective*, writing $D \geq 0$, if each $n_i \geq 0$. Given two divisors D_1 and D_2 on C, we say that $D_1 \geq D_2$ if and only if the divisor $D_1 - D_2$ is effective. This sets up a partial ordering on the set of all divisors of $\mathbb{V}(F)$.

4.1 Divisors of functions

Definition 4.4. Let $f \in k(C)$ be an element of the function field of C. We define the *divisor of f* by

$$\operatorname{div}(f) = \sum_{p \in C} \operatorname{ord}_p(f) p$$

where $\operatorname{ord}_p(f)$ is the order function defined by the discrete valuation ring $\mathcal{O}_p(F)$.

Lemma 4.1. *Let $f \in k(C)$. Then* $\deg \operatorname{div}(f) = 0$.

Proof. Suppose C has degree n. Let $f = g/h$ where g, h are homogeneous polynomials in $k[x, y, z]$ of common degree m. Then $\operatorname{div}(f) = \operatorname{div}(g) - \operatorname{div}(h)$, and $\operatorname{div}(g), \operatorname{div}(h)$ have the same degree mn by Bézout's theorem. □

Example 4.1. Let $F = Y^2 Z - X^3 - XZ^2$. Then F is a smooth irreducible projective plane curve. Let $C = \mathbb{V}(F)$ and $f = Y/Z$. Let us compute $\operatorname{div}(f)$. We need only consider those $p = [X : Y : Z]$ such that $Y = 0$ or $Z = 0$. Otherwise Y/Z is a unit in the local ring at p, hence $\operatorname{ord}_p(Y/Z) = 0$.

To consider where $Y = 0$, we move to local coordinates in the affine chart $U_z = \{[X : Y : Z] \mid Z \neq 0\}$ by $x = X/Z, y = Y/Z$. Then in these local coordinates the equation of the curve is

$$F_* = y^2 - x^3 - x.$$

In this chart, $y = 0$ when $x(x^2 + 1) = 0$, so either $x = 0$ or $x = \pm i$. Hence the zeros are $[0 : 0 : 1], [i : 0 : 1], [-i : 0 : 1]$. The tangent to F_* at $(0, 0)$ is given by the lowest degree form, which is x. So y is a uniformiser of $\mathcal{O}_{(0,0)}(F_*)$. Hence $\text{ord}_{(0,0)}(y) = 1$. Similarly, by appropriate coordinate changes, one can deduce $\text{ord}_{(i,0)}(y) = 1$ and $\text{ord}_{(-i,0)}(y) = 1$. Hence the effective part of the divisor,

$$\text{div}(Y/Z)_+ = [0 : 0 : 1] + [i : 0 : 1] + [-i : 0 : 1].$$

Now let us consider when $Z = 0$. We will use local coordinates in the chart U_y. Here the equation of the curve becomes

$$F_* = z - x^3 - xz^2.$$

For $z = 0$, we need $x = 0$. So $(0, 0)$ is the only zero of z (in this chart.) The tangent to the curve at $(0, 0)$ is $z = 0$, so x is a uniformising parameter. From the equation of the curve we have

$$z = x^3 + xz^2 = x^3 + x(x^3 + xz^2)^2 = x^3(1 + (x^4 + 2x^2z^2 + z^4))$$

and $1 + x^4 + 2x^2z^2 + z^4$ is a unit in the local ring $\mathcal{O}_{(0,0)}(C)$. So $\text{ord}_{(0,0)}(z) = 3$. We know there cannot be other poles, since we expect $\deg \text{div}(Y/Z) = 0$. Hence

$$\text{div}(Y/Z) = [0 : 0 : 1] + [i : 0 : 1] + [-i : 0 : 1] - 3[0 : 1 : 0].$$

4.2 The vector space $L(D)$

Definition 4.5. Let D be a divisor on C. We define

$$L(D) = \{F \in k(C) \mid F = 0 \text{ or } \text{div}(F) + D \geq 0\}.$$

We have that $L(D)$ is a vector space over k. We let $l(D)$ denote the dimension of this vector space.

Remark. Write $D = \sum_{p \in C} n_p p$. One should think of $L(D)$ as those functions in $k(C)$ which have poles of order at most n_p for points p with $n_p > 0$ in D, and which have zeroes of order at least $-n_p$ at points p with $n_p < 0$ in D.

Lemma 4.2. *If* $\deg(D) < 0$*, then* $L(D) = \{0\}$.

Proof. Given any non-zero $f \in k(C)$, we have $\deg \operatorname{div}(f) = 0$. Hence $\deg(D + \operatorname{div}(f)) < 0$, so $D + \operatorname{div}(f)$ cannot be effective. □

Theorem 4.3. *If* $D \leq D'$*, then* $L(D) \subseteq L(D')$ *and*

$$\dim_k(L(D')/L(D)) \leq \deg(D' - D).$$

Proof. (Adapted from [2], 8.2, Proposition 3, (1).) The first claim is easy. For the second, write $D' = D + P_1 + ... + P_s$, so that $L(D) \subseteq L(D + P_1) \subseteq ... \subseteq L(D + P_1 + ... + P_s)$. We will show that for any point P,

$$\dim_k(L(D + P)/L(D)) \leq 1.$$

Then the result will follow, since $\dim_k(L(D')/L(D)) = \dim_k(L(D+P_1+...+P_s)/L(D+P_1+...+P_{s-1})) + \dim_k(L(D+P_1+...+P_{s-1})/L(D+P_1+...+P_{s-2})) + ... + \dim_k(L(D+P)/L(D)) \leq 1 \times s = \deg(D' - D)$ ([2], Problem 2.49.)

Let t be a uniformising parameter in $\mathcal{O}_P(C)$ and let $r = n_P$ be the coefficient of P in D. We define the following linear map:

$$\begin{aligned} \phi : L(D + P) &\to k \\ f &\mapsto (t^{r+1} f)(P). \end{aligned}$$

We must check that ϕ is well-defined. Indeed, let $f \in L(D + P)$. Then $\operatorname{ord}_P(f) \geq -(r + 1)$. Hence $t^{r+1} f$ is a well-defined element of $\mathcal{O}_P(C)$. Clearly ϕ is $k-$linear, and $\ker \phi = L(D)$. Hence there exists a one-to-one mapping $L(D + P)/L(D) \to k$. Hence $\dim_k L(D + P)/L(D) \leq 1$. □

Corollary. *Given any divisor* D*, if* $\deg(D) \geq 0$*, then* $l(D) \leq \deg(D) + 1$*. In particular,* $L(D)$ *is finite dimensional.*

Proof. Write $\deg(D) = n \geq 0$. Let $P \in C$, and let $D' = D - (n+1)P$. Then $\deg(D') < 0$, so $L(D') = \{0\}$ by Lemma 4.2. Then since $D' \leq D$, by the above we must have

$$\dim_k(L(D)/L(D')) \leq \deg(D - D') = n + 1 = \deg(D) + 1.$$

Hence $l(D) = \deg(D) + 1$. □

It turns out that Theorem 4.3 is stronger when divisors are restricted to *finite subsets* of C. Let $D = \sum_{p \in C} n_p p$ be a divisor on C, and $S \subset C$. If we define $\deg^S(D) = \sum_{p \in S} n_p$ and $L^S(D) = \{f \in k(C) \mid \mathrm{ord}_P(f) \geq -n_p \text{ for all } p \in S\}$, then we get the following:

Lemma 4.4. *Let $S \subset C$. If $D \leq D'$ are divisors, then $L^S(D) \subseteq L^S(D')$ and, provided S is finite,*

$$\dim_k(L^S(D')/L^S(D)) = \deg^S(D' - D).$$

Proof. We follow the same tactic as in the proof of Theorem 4.3, so define $\phi : L(D+P) \to k$ by $\phi(f) = (t^{r+1}f)(P)$. We will show ϕ is surjective by choosing $f \in k(C)$ such that $\mathrm{ord}_P(f) = -(r+1)$, so $\phi(f) \neq 0$, and $\mathrm{ord}_Q(f) \geq -n_Q$ for all $Q \in S$, so $f \in L^S(D+P)$. But since S is finite, we may apply [2], Problem 7.21(b) to obtain such f. □

4.3 Linear equivalence

Definition 4.6. Let D, D' be be divisors on C. Then D and D' are said to be *linearly equivalent* if $D' = D + \mathrm{div}(f)$ for some $f \in k(C)$. If D, D' are linearly equivalent we write $D \equiv D'$.

Theorem 4.5. *Let D, D', D_1, D_1' be divisors.*

1. *The relation $\equiv$ is an equivalence relation.*
2. *$D \equiv 0$ if and only if $D \equiv \mathrm{div}(f)$ for some $f \in k(C)$.*
3. *If $D \equiv D'$, then $\deg D = \deg D'$.*
4. *If $D \equiv D'$ and $D_1 \equiv D_1'$, then $D + D_1 \equiv D' + D_1'$.*

Proof. 1. For reflexivity, take $f = 0$. Symmetry is obvious. Suppose $D \equiv D'$ and $D' \equiv D''$. Then $D = D' + \mathrm{div}(f)$, $D' = D'' + \mathrm{div}(g)$ for some $f, g \in k(C)$. Then $D = D'' + \mathrm{div}(f) + \mathrm{div}(g) = D'' + \mathrm{div}(f+g)$, so $D \equiv D''$.

2. $\Longrightarrow$ is immediate. Suppose $D \equiv \text{div}(f)$ for some $f \in k(C)$. Then $D = \text{div}(f) + \text{div}(g)$ for some $g \in k(C)$, so $D = 0 + \text{div}(f + g)$. Hence $D \equiv 0$.

3. Suppose $D \equiv D'$. Write $D = D' + \text{div}(f)$ for some $f \in k(C)$. Then counting degrees on each side, $\deg(D) = \deg(D' + \text{div}(f)) = \deg(D') + \deg(\text{div}(f)) = \deg(D')$.

4. Write $D = D' + \text{div}(f)$, $D_1 = D_1' + \text{div}(g)$. Then $D + D_1 = D' + D_1' + \text{div}(f + g)$, so $D + D_1 \equiv D' + D_1'$.

□

Lemma 4.6. *If $D \equiv D'$, then $L(D) \cong L(D')$.*

Proof. Write $D' = D + \text{div}(g)$. Define the linear map

$$\psi : L(D) \to L(D')$$
$$f \mapsto fg.$$

Then ψ is a well-defined isomorphism of vector spaces ([2], 8.2, Proposition 3, (4)). □

4.4 Hyperplane divisors

For a certain class of divisors, we can calculate $l(D)$ explicitly.

Definition 4.7. We define a *hyperplane divisor* H on C as $H = \text{div}(\ell)$ for some linear homogeneous polynomial ℓ.

Lemma 4.7. *Any two hyperplane divisors H, H' are linearly equivalent.*

Proof. Let ℓ, ℓ' be such that $\text{div}(\ell) = H, \text{div}(\ell') = H'$. Then $H - H' = \text{div}(\ell) - \text{div}(\ell') = \text{div}(\ell/\ell')$ is principal. □

The following theorem will be useful in this subsection; the proof is given in [2], Chapter 5, page 61.

Theorem 4.8. *(Max Noether's $AF + BG$ theorem.) Let $F, G \in k[x, y, z]$ be homogeneous polynomials defining plane curves with no common component, with $\mathbb{V}(F)$ smooth. Suppose U is a homogeneous polynomial such that for every $p \in \mathbb{V}(F) \cap \mathbb{V}(G)$,*

$$I(p, F \cap U) \geq I(p, F \cap G).$$

Then there exists homogeneous polynomials A, B such that $U = AF + BG$.

Lemma 4.9. *Let $f = u/v \in L(mH)$, where u, v are homogeneous polynomials of the same degree m. Then there exists a homogeneous polynomial g of common degree m such that $f = g/\ell^m$.*

Proof. Write $C = \mathbb{V}(F)$ and let $p \in \mathbb{V}(F) \cap \mathbb{V}(v)$. Then, since $\operatorname{div}(u/v) = \operatorname{div}(u) - \operatorname{div}(v)$ and $\operatorname{div}(u/v) + mH = \operatorname{div}(u/v) + \operatorname{div}(\ell^m) \geq 0$, we must have $\operatorname{div}(u) \geq \operatorname{div}(v) + \operatorname{div}(\ell^m)$. It then follows that $I(p, F \cap u\ell^m) \geq I(p, F \cap v)$ since $\operatorname{ord}_p(v) \leq \operatorname{ord}_p(u\ell^m)$. Hence by Theorem 4.8, there exists homogeneous A, B such that $u\ell^m = AF + Bv$. Now by passing over to $k(C)$, we must have $u\ell^m = Bv$ and hence $f = u/v = B/\ell^m$. □

Remark. The above shows us that the non-zero elements of $L(mD)$ consist of rational functions of the form f/ℓ^m where f is homogeneous of degree m, and F does not divide f. By counting arguments, we can determine the cardinality of a basis.

Theorem 4.10. *Let H be a hyperplane divisor, $m \in \mathbb{N}$. Then*

$$l(mH) = md - g_a + 1$$

where $g_a = (d-1)(d-2)/2$ is the algebraic genus of C, d the degree of C.

Proof. There are $\binom{m+2}{m}$ homogeneous polynomials in x, y, z of degree m, where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is "n choose k". From these polynomials, $\binom{m-d+2}{m-d}$ of them are divisible by F, which may be observed by writing such a polynomial $f = Fg$ where F does not divide the homogeneous g of degree $m-d$, and considering a basis for all such g. Hence a basis contains

$$\binom{m+2}{m} - \binom{m-d+2}{m-d} = \frac{(m+1)(m+2)}{2} - \frac{(m-d+1)(m-d+2)}{2}$$

elements, and by expanding, one obtains the result. □

Definition 4.8. Let G be a plane curve, and suppose G has only ordinary multiple points. Define the divisor

$$E = \sum_{p \in G} (m_p(G) - 1)p.$$

Then any plane curve H such that $\operatorname{div}(H) \geq E$ is called an *adjoint* of G.

Remark. In the case that G is nonsingular (like our model curve C in this section), then every plane curve H is adjoint to C.

Theorem 4.11. *(Residue theorem.) Let G and E be as in Definition 4.8. Let D, D' be effective divisors on G, with $D \equiv D'$. Suppose H is an adjoint to G such that there exists an effective divisor A with*

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

Then there exists an adjoint H' of degree m such that $\operatorname{div}(H') = D' + E + A$.

Proof. Take M_1, M_2 to be curves of equal degree such that $D + \operatorname{div}(M_1) = D' + \operatorname{div}(M_2)$. Then we have

$$\operatorname{div}(GM_1) = \operatorname{div}(G) + \operatorname{div}(M_1) = D + E + A + (D' - D + \operatorname{div}(M_2)) = \operatorname{div}(M_2) + D' + E + A.$$

and hence $\operatorname{div}(GM_1) \geq \operatorname{div}(M_2) + E$. Now letting F be the homogeneous polynomial defining G, and applying [2], 7.5, Proposition 3 to F, M_2 and HM_1, we see that the conditions of Theorem 4.8 are satisfied. Hence there exists F', H' such that

$$HM_1 = F'F + H'M_2$$

where $\deg(H') = m$. Now, calculating divisors,

$$\operatorname{div}(M_2) = \operatorname{div}(HM_1) - \operatorname{div}(M_2) = D' + E + A$$

as required. □

4.5 Riemann's theorem

We can tighten the bound given as a corollary of Theorem 4.3.

Theorem 4.12. *(Riemann's theorem.) There exists a non-negative integer g such that*

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

for all divisors D on C. The smallest such g is called the genus of C, and it is a non-negative integer depending only on C.

Proof. Following the notation of [2] 8.3, let $s(D) = \deg(D) + 1 - l(D)$. Then we just need to find g such that $s(D) \leq g$ for all divisors D on C. First, $s(0) = \deg(0) + 1 - l(0) = 1 - 1 = 0$. So $g \geq 0$, provided g exists. Next, suppose $D \equiv D'$. Then $s(D) - s(D') = \deg(D) + 1 - l(D) - \deg(D') - 1 + l(D') = (\deg(D) - \deg(D')) - (l(D) - L(D')) = 0$ (Lemma 4.6 and Theorem 4.5, 3.), so $s(D) = s(D')$. Also, suppose $D \leq D'$. Then from Theorem 4.3, we have $\dim_k(L(D')/L(D)) \leq \deg(D' - D)$, so $l(D') - l(D) \leq \deg(D' - D)$, so $\deg(D) - l(D) \leq \deg(D') - l(D')$. Therefore $s(D) \leq s(D')$.

Clearly if H is a hyperplane divisor, then $S(mH) = g_a$ for all $m \in \mathbb{N}$, and if $f \in \Gamma(C)$ has degree m, then $\operatorname{div}(f) \equiv mH$ since $\operatorname{div}(f) - mH = \operatorname{div}(f) - \operatorname{div}(\ell^m) = \operatorname{div}(f/\ell^m)$ is principal. Hence $\deg \operatorname{div} f = md$. Now let $p_1 = [a_1 : b_1 : c_1], p_2 = [a_2 : b_2 : c_2], ..., p_k = [a_k : b_k : c_k]$ be points in C, and suppose without loss of generality that $a_i, b_i \neq 0$ for all $1 \leq i \leq k$ (otherwise a projective change of coordinates will achieve this.) Define

$$f(x, y, z) = (a_1 y - b_1 x)(a_2 y - b_2 x) \dots (a_k y - b_k x).$$

Then $\operatorname{div}(f) \geq p_1 + ... + p_k$. Now let H be any hyperplane divisor on C, and then by the above $\operatorname{div}(f) \equiv kH$.

Let D be any divisor on C. Let H be any hyperplane divisor. Write $D = \sum_{i=1}^{n} n_i p_i$. Use $p_1, ..., p_n$ in the above to obtain a function f. Then there must exist a finite set of points $q_1, ..., q_l$ such that $D + \sum q_l \equiv mH$ for some sufficiently large $m \in \mathbb{N}$. Hence $s(D + \sum q_l) = s(mH)$, so $s(D) \leq s(mH)$. Since for any hyperplane divisor H we have $s(mH) = g_a$ (Theorem 4.10), we have $s(D) \leq g_a$ for any divisor D on C. □

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

Proof. We noted that mH satisfies $s(mH) = g_a$. Let $N = \deg(mH) + g_a$. Then if $\deg(D) \geq N$ we have that $\deg(D - mH) + 1 - g = \deg(D) - \deg(mH) + 1 - g_a > 0$. Hence, by Theorem 4.12, $l(D - mH) > 0$. Hence there must exist some non-zero $f \in L(D - mH)$, so some f such that $D + \operatorname{div}(f) \geq mH$. Now let $D' = D + \operatorname{div}(f)$. Then $D \equiv D' \geq mH$, so by the proof of Theorem 4.12, $l(D) = \deg(D) + 1 - g$. □

Remark. The algebraic genus g_a and the genus g in Theorem 4.12 are equal when the curve C is smooth, but generally they are different, as the following theorem illustrates.

Theorem 4.13. *Suppose C has at most ordinary multiple points. The genus g of C as in Theorem 4.12 is given by*

$$g = g_a - \sum_{p \in C} \frac{m_p(C)(m_p(C)+1)}{2}.$$

Proof. ([2], 8.3, Proposition 5.) □

4.6 Differentials on curves

This section closely follows [2], 8.4.

Definition 4.9. Let R be a ring containing k and let M be an $R-$module. Let $D : R \to M$ be a $k-$linear map such that $D(xy) = xD(y) + yD(x)$ for all $x, y \in R$. We say that D is a *derivation* of R into M.

Note. It follows that for any $F \in k[x_1, ..., x_n]$ and $x_1, ..., x_n \in R$,

$$D(f(x_1, ..., x_n)) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i} D(x_i).$$

Lemma 4.14. *Suppose R is an integral domain with field of fractions K. Let M be a vector space over K. Then any derivation*

$$D : R \to M$$

extends uniquely to a derivation

$$D' : K \to M$$

such that the diagram commutes:

$$\begin{tikzcd} R \arrow[r, "D"] \arrow[d, "i"] & M \\ K \arrow[ur, "D'"] & \end{tikzcd}$$

where i is the inclusion map into the field of fractions.

Proof. Let $f = g/h$ with $g, h \in R$, $h \neq 0$. Then $fh = g$, so we must have $D'(x) = D'(yz) = yD'(z) + zD'(y)$, hence $D(x) = yD'(z) + zD(y)$. Therefore $D'(z) = y^{-1}(D(x) - zD(y))$, which verifies uniqueness. By defining D' as in this formula, it is simple to see that D' is a derivation. □

Construction 4.1. Let F be the free $R-$module generated by the set $\{(x) \mid x \in R\}$ (each (x) is a formal symbol). Let K be the submodule of F generated by the union of the following subsets:

1. $\{(x+y) - (x) - (y) \mid x, y \in R\}$.

2. $\{(\lambda x) - \lambda(x) \mid x \in R, \lambda \in K\}$.

3. $\{(xy) - x(y) - y(x) \mid x, y \in R\}$.

Let $\Omega_k(R) = F/K$ be the quotient of F by K, and denote by dx the image of (x) in F/K. Let

$$d : R \to \Omega_k(R)$$
$$x \mapsto dx.$$

We call $\Omega_k(R)$ the *module of differentials* of R over k. We see $d : R \to \Omega_k(R)$ is a derivation.

Lemma 4.15. *Let M be an $R-$module. Let $D : R \to M$ be a derivation. Then there exists a unique $R-$linear map $\phi : \Omega_k(R) \to M$ that makes the following diagram commute:*

$$\begin{tikzcd}
R \arrow[r, "D"] \arrow[d, "d"'] & M \\
\Omega_k(R) \arrow[ur, dashed, "\exists\phi"] &
\end{tikzcd}$$

Proof. If we define $\dot{\phi} : F \to M$ from F in Construction 4.1 by $\dot{\phi}(\sum x_i(y_i)) = \sum x_i D(y_i)$, then since $\dot{\phi}(K) = 0$, we obtain a unique $R-$linear map $\phi : \Omega_k(R) \to M$ that makes

$$\begin{tikzcd}
F \arrow[r, "\dot{\phi}"] \arrow[d, "d"'] & M \\
\Omega_k(R) \arrow[ur, "\phi"] &
\end{tikzcd}$$

commute. □

Remark. From an earlier note we have

$$d(G(x_1, ..., x_n)) = \sum_{i=1}^{n} \frac{\partial G(x_1, ..., x_n)}{\partial x_i} dx_i$$

for all $x_1, ..., x_n \in R$ and $G \in k[x_1, ..., x_n]$. Hence if $R = k[x_1, ..., x_n]$, then $\Omega_k(R)$ is generated by the differentials $dx_1, ..., dx_n$.

If R is an integral domain with quotient field K, then from Lemma 4.14 we have for any $z \in K$, $z = x/y$,

$$dz = y^{-1}(dx - (z/y)dy).$$

Theorem 4.16. *Let C be a projective plane curve, $K = k(C)$. Then the space of differentials $\Omega_k(K)$ is a $1-$dimensional vector space over k, with basis $\{dx\}$.*

Proof. [2], 8.4, Proposition 6. □

Definition 4.10. Applying Theorem 4.16, we see that any two differentials are linearly dependent; that is for any $f, t \in K$ with $t \notin k$ there must exist unique $v \in K$ such that $df = vdt$. We write $v = \frac{df}{dt}$ and say v is the *derivative* of f with respect to t.

Lemma 4.17. *Let $\mathcal{O}$ be a discrete valuation ring of K, and let t be a uniformising parameter in $\mathcal{O}$. If $f \in \mathcal{O}$, then $\frac{df}{dt} \in \mathcal{O}$.*

Proof. [2], 8.4, Proposition 7. □

4.7 Canonical divisors

Let C be a smooth irreducible projective curve, $K = k(C)$, and let $\Omega = \Omega_k(K)$. Let $\omega \in \Omega$, and $p \in C$. Let t be a uniformising parameter in $\mathcal{O}_p(C)$. Write $\omega = fdt$.

Definition 4.11. We define the *order* of ω at $p \in C$, denoted $\text{ord}_p(\omega)$, by the value of $\text{ord}_p(f)$ in the equality above. This definition does not depend on the choice of uniformising paramter, for suppose $s \in \mathcal{O}_p(C)$ is another choice, so $fdt = gds$. Then $f/g = ds/dt$, which lies in $\mathcal{O}_p(C)$ by Lemma 4.17. Likewise $dt/ds \in \mathcal{O}_p(C)$, and hence $\text{ord}_p(f) = \text{ord}_p(g)$.

Definition 4.12. We define the *divisor* of ω by

$$\text{div}(\omega) = \sum_{p \in C} \text{ord}_p(C)p.$$

Lemma 4.18. *All canonical divisors on C are linearly equivalent.*

Proof. Suppose $\omega, \omega' \in \Omega$. By Theorem 4.16, we have $\omega' = f\omega$ for some $f \in K$. Hence $\operatorname{div}(\omega') = \operatorname{div}(f) + \operatorname{div}(\omega)$, and so $\operatorname{div}(\omega') \equiv \operatorname{div}(\omega)$. □

Remark. In fact, all the of the canonical divisors form entirely one equivalence class, for suppose $W \equiv \operatorname{div}(\omega)$ for some divisor W. Then $W = \operatorname{div}(\omega) + \operatorname{div}(f) = \operatorname{div}(f\omega)$, so W is a canonical divisor.

Corollary. *All canonical divisors have the same degree.*

Lemma 4.19. *Let C be a projective curve of degree $n \geq 3$, and assume C has only ordinary multiple points. Let*

$$E = \sum_{p \in C} (m_p(C) - 1)p.$$

Let G be any homogeneous polynomial of degree $n - 3$. Then $\operatorname{div}(G) - E$ *is a canonical divisor.*

Proof. We follow the style of [2], 8.5, Proposition 8. Let X, Y, Z be coordinates for $\mathbb{P}^2$ such that: The line $Z = 0$ intersects C at distinct points $p_1, ..., p_n$ with intersection multipliticites $I(p_i, C \cap Z) = 1$ for each i, the point $[1 : 0 : 0] \notin C$, and no tangent to C at a multiple point passes through the point $[1 : 0 : 0]$. We pass to the affine chart U_z by the coordinate change $x = X/Z$, $y = Y/Z$. Let F be such that $\mathbb{V}(F) = C$, and define

$$f_x = \frac{\partial F}{\partial X}, f_y = \frac{\partial F}{\partial Y}.$$

Let $E_m = m \sum_{i=1}^{n} p_i - E$. Observe that, provided $\deg(G) = \deg(G') = n - 3$, we have $\deg(G) - E \equiv \deg(G') - E$. Hence it suffices to show $\operatorname{div}(\omega) \equiv E_{n-3}$ by showing

$$\operatorname{div}(\omega) = E_{n-3} + \operatorname{div}(f_y),$$

and since $\frac{\partial f}{\partial y} = \frac{\partial F}{\partial Y}/Z^{n-1}$, is equivalent to showing

$$\operatorname{div}(dx) - \operatorname{div}(F_Y) = -2\sum_{i=1}^{n} p_i - E.$$

By the chain rule, $dx = -(f_y/f_x)dy = -(F_Y/F_X)dy$. Hence for any $p \in C$,

$$\operatorname{ord}_p(dx) - \operatorname{ord}_p(F_Y) = \operatorname{ord}_p(dy) - \operatorname{ord}_p(F_X).$$

which implies

$$\mathrm{div}(dx) - \mathrm{div}(F_Y) = \mathrm{div}(dy) - \mathrm{div}(F_X)$$

so we can show

$$\mathrm{div}(dy) - \mathrm{div}(F_X) = -2\sum_{i=1}^{n} p_i - E. \tag{4.1}$$

First let us suppose $p = p_i$ for some $1 \leq i \leq n$. Then $y^{-1} = Z/Y$ is not tangent to C at p, so it is a uniformising parameter for $\mathcal{O}_p(C)$. Since $dy = -y^2 d(y^{-1})$, we have $\mathrm{ord}_p(dy) = \mathrm{ord}_p(-y^2) = -2$. Now $F_X(p) \neq 0$ (otherwise, $F_Y(p) = 0$, but since Z is not tangent to F at p, this is a contradiction.) So boths sides of Equation 4.1 have the same order -2.

Now suppose p is a point not equal to one of $p_1, ..., p_n$, so we can write $p = [a : b : 1] \in C$. Since $dx = d(x - a)$ and derivatives do not change with translations, we may assume that $p = [0 : 0 : 1]$. Then there are two cases to consider:

1. Y is tangent to C at p. Then by assumption, p cannot be a multiple point. Hence $x = X/Z$ is a uniformising parameter, and $F_Y(p) \neq 0$. So $\mathrm{ord}_p(dx) = \mathrm{ord}_p(F_Y) = 0$.
2. Y is not tangent to C at p. Then we can choose y as a uniformising parameter for $\mathcal{O}_p(C)$. Hence $\mathrm{ord}_p(dy) = 0$ and $\mathrm{ord}_p(f_x) = m_p(C)^{-1}$.

□

Corollary. *If ω is a canonical divisor, then* $\deg(\omega) = 2g - 2$ *and* $l(\omega) \geq g$.

Proof. Any two canonical divisors are linearly equivalent, so it's enough to see what happens with $\omega = E_{n-3}$ as in the above lemma. Then by a corollary to Theorem 4.13 ([2], 8.2, Corollary 3(b)), we obtain the result. □

4.8 Riemann-Roch theorem

The Riemann-Roch theorem strengthens Riemann's theorem by finding the missing term to create an equality. We state and prove the theorem in the case that C is smooth; however, it remains true even when C has singular points ([2], 8.5.). We need a few preliminary facts before proving the theorem, though.

Lemma 4.20. *(Noether's reduction lemma.) Let D be a divisor on C, and suppose $L(D) \subsetneq L(D+p)$. Then $L(\omega - D - p) = L(\omega - D)$.*

Proof. By hypothesis, there exists $f \in k(C)$ such that $\operatorname{div}(f)+D+p \geq 0$, but $\operatorname{div}(f)+D \not\geq 0$, which means we have $\operatorname{ord}_p(f) = -\operatorname{ord}_p(D+p)$. Suppose for a contradiction that $L(\omega - D - p) \subsetneq L(\omega - D)$. Then similarly we have $g \in k(C)$ such that $\operatorname{div}(g) + \omega - D \geq 0$ and $\operatorname{ord}_p(g) = -\operatorname{ord}_p(\omega - D)$. Now

$$\operatorname{div}(fg\omega) + p = \operatorname{div}(f) + p + \operatorname{div}(g) + \operatorname{div}(\omega) = \operatorname{div}(f) + D + p + \operatorname{div}(g) + \operatorname{div}(\omega) - D \geq 0,$$

so $fg\omega$ has a pole of order 1 at p, and no other poles. This is a contradiction; we expect the sum of the residues of w to be zero ([5], Theorem 4.) □

Corollary. *Under the assumptions of the lemma, since $l(D+p) - l(D) \leq 1$ we get*

$$l(D+p) - l(D) + l(\omega - D) - l(\omega - d - p) \leq 1,$$

and an easy induction yields

$$l(D + \sum_{i=1}^{k} p_i) - l(D) + l(\omega - D) - l(\omega - d - \sum_{i=1}^{k} p_i) \leq k$$

where $p_1, ..., p_k \in C$.

Theorem 4.21. *(Riemann-Roch.) Let C be a smooth projective curve of degree d. Let ω be a canonical divisor on C. Then for any divisor D on C,*

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

Proof. Let $n > 0$ be a positive integer so large that $\deg(\omega - nH) < 0$ and hence $l(\omega - nH) = 0$. Then by the proof of Theorem 4.12, there exists $m > n$ and a set of points $p_1, ..., p_k \in C$ such that

$$D + \sum_{i=1}^{k} p_i \equiv mH.$$

Hence $\deg(D) = \deg(mH) - \deg\left(\sum_{i=1}^{k} p_I\right) = md - k$. Now using the corollary to Lemma 4.20, we have that

$$l(D + \sum_{i=1}^{k} p_i) - l(D) + l(\omega - D) - l(\omega - d - \sum_{i=1}^{k} p_i) \leq k$$

and, since linear equivalence preserves the dimension of L and $l(\omega - mH) = 0$, we get

$$l(mH) - l(D) + l(\omega - D) \leq k.$$

Now recall from Theorem 4.10 the result that $l(mH) = m\deg(C) - g + 1$ (since C is smooth, $g = g_a$). Applying this to the above inequality we find

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

Now in the above, take $\omega - D$ as the divisor D. We have

$$\begin{aligned} l(\omega - D) - l(D) \geq \deg(\omega - D) - g + 1 &= \deg(\omega) - \deg(D) - g + 1 \\ &= g - 1 - \deg(D) \end{aligned}$$

where we used the fact $\deg(\omega) = 2g - 2$. Hence we have

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

Combining the two inequalities, we obtain the Riemann-Roch theorem, $l(D) - l(\omega - D) = \deg(D) + 1 - g$. □

Corollary. *We have the following:*

1. *Let ω be a canonical divisor; then $l(\omega) = g$.*

2. *If D is a divisor such that $\deg(D) \geq 2g - 1$, then $l(D) = \deg(D) + 1 - g$.*

3. *Let $p \in C$. Then provided $\deg(D) \geq 2g$, we have $l(D - p) = l(D) - 1$.*

Proof. 1. Immediate, using the fact $\deg(\omega) = 2g - 2$.

2. This implies that $\deg(\omega - D) < 0$, and hence $l(\omega - D) = 0$.

3. Taking D to have such large degree kills the dimensions $l(\omega - D)$ and $l(\omega - (D - p))$. Now Riemann-Roch says

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

and

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

and hence $l(D - p) = l(D) - 1$.

□

5 Applications of Riemann-Roch

In this ultimate chapter, we discuss some important consequences of the Riemann-Roch theorem to demonstrate its utility.

5.1 Clifford's theorem

Clifford's theorem is due to William K. Clifford, who published the result in 1878. As an application of Riemann-Roch, we may deduce the result:

Theorem 5.1. *(Clifford's theorem.) Let C be an algebraic curve. Let D be an effective divisor on C such that $\omega - D$ is effective for some canonical divisor ω on C. Then*

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

Proof. Let D' be an effective divisor such that $D + D' = \omega$. Suppose that $l(D-p) \subsetneq l(D)$ for any $p \in C$, for otherwise $D-p$ has smaller degree than D, so we could use $D-p$ to obtain a stronger inequality. With this assumption, let $h \in L(D)$ be such that $h \notin L(D-p)$ for each $p \leq D'$. Then the k-linear map

$$\begin{aligned} \phi : L(D')/L(0) &\to L(\omega)/L(D) \\ f + L(0) &\mapsto fh + L(D) \end{aligned}$$

is injective: Suppose $\phi(f + L(0)) = 0$. Then it can be shown that f has no poles. Hence $f \in k = L(0)$.

Since ϕ is injective, we have $l(D') - 1 \leq g - l(D)$, using Corollary 4.8, 1. Now Riemann-Roch says for $D' = \omega - D$,

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

Hence

$$l(D) - \deg(D) - 2 \leq -l(D)$$

from which the result follows easily. □

5.2 Elliptic curves

An excellent introduction to elliptic curves is found in [6]. The purpose of this section is to show how Riemann-Roch produces the standard (Weierstrass) form for an elliptic curve.

Definition 5.1. An elliptic curve is a smooth projective algebraic curve of genus one, with a specified point O.

Remark. Since the elliptic curve naturally carries a group structure, we usually specifiy a point O in the definition to act as the identity. The details for this are in [6].

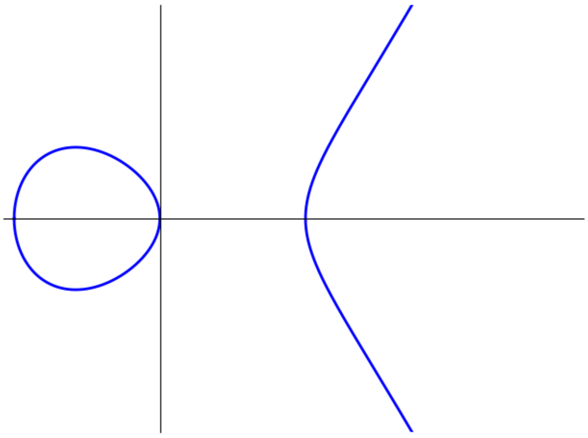

Figure 4: An elliptic curve.

Let C be an elliptic curve. If D is a divisor of strictly positive degree on C, then by Corollary 4.8 item 2, we have that $l(D) = \deg(D)$. Let p be a given point on C. Then since

$$l(p) = \deg(p) = 1$$

we must have $L(p) = k$, so $L(p)$ has basis $\{1\}$. Similarly,

$$l(2P) = 2,$$

so $L(2p) = k \oplus xk$, where $\mathrm{ord}_p(x) = -2$, and $\mathrm{ord}_q(x) \geq 0$ for any $q \neq p$. So $L(2p)$ has basis $\{1, x\}$. Continuing, we see that $L(3P)$ has basis $\{1, x, y\}$ where $\mathrm{ord}_p(y) = 3$ and $\mathrm{ord}_q(y) \geq 0$ for $q \neq p$, and $L(4P)$ has basis $\{1, x, y, x^2\}$. Finally, $L(5P)$ has basis $\{1, x, y, x^2, xy\}$. But

$$l(6P) = 6$$

and, since x^3 and y^2 both have order -6 at p, the set

$$\{1, x, y, x^2, xy, x^3, y^2\}$$

must be linearly dependent. Hence there exists $a_0, ..., a_6 \in k$ such that

$$a_0 + a_1x + a_2y + a_3x^2 + a_4xy + a_5x^3 + a_6y^2 = 0.$$

Both of a_6, a_5 must be non-zero in this relation, because $\{1, x, y, x^2, xy\}$ form a basis for $L(5P)$. Hence after normalising and rearranging, we get

$$y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6.$$

Assuming the characteristic of k is not equal to either of 2 or 3, some substitutions give

$$y^2 = x^3 + ax + b$$

which is the Weierstrass form of the elliptic curve.

6 Conclusions

In summary, we have studied algebraic curves using the machinery of abstract algebra. We have introduced new tools to study curves: Divisors, the intersection number, multiplicities, and we have derived powerful results like Bézout's theorem and the Riemann-Roch theorem, which we proved in the smooth case, yet the theorem holds in much more generality. To show this requires more technology than this report could sustain, however (see Hartshorne's classic book, [7].)

Overall, the project was quite successful, and the goals were met. An original goal for this project was to apply the Riemann-Roch theorem to some of the classical results of projective geometry, such as Desargues's and Pascal's theorems (see the first few chapters of [8] for more information) to see if alternative proofs would emerge. Both time and space constraints did not permit this. But it is a possible further route which I would be greatly interested in pursuing in future.

By introducing the nonsingular model of a curve, we have the set up to prove Riemann-Roch for a curve with ordinary multiple points; this is the approach taken by Fulton in [2]. The blowup of singularities is something I was interested in including; again, time and space constraints disqualified this. But an interested reader should certainly consult Fulton's book for a treatment of this construction.

After finishing this report, a curious reader could go on to read more about algebraic geometry as it applies to varieties of any dimension. The techniques introduced in the study of curves are generalised nicely in this case. This could even lead on to scheme theory, which is the language that modern algebraic geometry is phrased in. A possible source for this is Shafarevich's and Reid's book [9]. A more advanced reader could consult Hartshorne's book [7], which is much heavier on the algebra.

“Algebraic geometry seems to have acquired the reputation of being esoteric, exclusive, and very abstract, with adherents who are secretly plotting to take over all the rest of mathematics. In one respect this last point is accurate.“

- David Mumford

References

[1] J. Dieudonné, "The historical development of algebraic geometry," *The American Mathematical Monthly*, vol. 79, no. 8, pp. 827–866, 1972.

[2] W. Fulton, *Algebraic Curves.* Redwood City, CA: Addison-Wesley Pub. Co., 1989.

[3] M. Atiyah, *Introduction to commutative algebra.* CRC Press, 2018.

[4] D. S. Dummit and R. M. Foote, *Abstract algebra*, vol. 3. Wiley Hoboken, 2004.

[5] J. Tate, "Residues of differentials on curves," in *Annales scientifiques de l'École Normale Supérieure*, vol. 1, pp. 149–159, 1968.

[6] J. H. Silverman and J. T. Tate, *Rational points on elliptic curves*, vol. 9. Springer, 1992.

[7] R. Hartshorne, *Algebraic geometry*, vol. 52. Springer Science & Business Media, 2013.

[8] H. S. M. Coxeter, *Projective geometry.* Springer Science & Business Media, 2003.

[9] I. R. Shafarevich and M. Reid, *Basic algebraic geometry*, vol. 2. Springer, 1994.

[10] T. A. Garrity, *Algebraic geometry: a problem solving approach*, vol. 66. American Mathematical Soc., 2013.