Project

on

Topics in Algebraic Curves

Submitted by

Samprit Ghosh

Roll No. :[redacted]

Under the Supervision of

Prof. Sudhir R. Ghorpade

DEPARTMENT OF MATHEMATICS

INDIAN INSTITUTE OF TECHNOLOGY BOMBAY

May 2016

Introduction

This report consists of two major parts containing two most important theorems in the area. First part or Stage-I was done in 3rd semester (July - Dec 2015) and the second part or Stage-II, in 4th semester (Jan - May 2016).

In the first part we initially describe the projective plane and algebraic curves in the projective plane. We then discuss intersection of curves, eventually proving the "first major theorem" in algebraic geometry, Bezout's Theorem. The techniques used in the proof are very elementary. We have broadly followed the outline of the proof given in the form of a long exercise in the appendix of the book "Rational points on elliptic curves" by Silverman and Tate. We have also looked at Hensel's lemma and Abhyankar's proof of Newton's Theorem in the concluding part of this section.

In the second part we mostly focus on studying Riemann-Roch Theorem. We have initially introduced places and valuations of algebraic function fields. To get a better understanding we have devoted a section to our usual rational function field. We looked at Weak Approximation theorem and have introduced divisors. Using divisors we have constructed a finite dimensional vector space called the Riemann-Roch space and have used its dimention to define genus of an algebraic function field. We have proved Riemann's theorem and have introduced the concept of Adeles and Weil differentials. Eventually we have proved the Duality theorem and have obtained Riemann-Roch theorem as a direct consequence of it. Towards the end of this part of the project we studied Riemann surfaces and the close relation between irreducible plane algebraic curves and Riemann surfaces. We have also included an appendix on properties of manifolds and stated the classification theorem of compact surfaces.

Acknowledgement

Every project big or small is successful largely due to the effort of a number of wonderful people who have always given their valuable advice or lent a helping hand. I express my sincere gratitude to Prof. Sudhir R. Ghorpade to provide me an opportunity to do this project and be my supervisor. I am very much thankful to him for his constant guidance and encouragement. I would also like to thank Mrinmoy Dutta (PhD student) for his suggestions and kind help. Last but not the least I thank my friends who have been there to discuss, suggest and contradict where necessary during the preparation of this project work.

Samprit Ghosh
May 2016.

Contents

Chapter 1

Preliminaries

1.1 Projective Plane

In this section we are mostly concerned about intersection of curves. We introduce the relevant definitions and give what may be regarded as the first theorem of algebraic geometry, namely Bezout's theorem.
Let us first introduce the Projective plane. We give to definitions of the projective plane. One geometric and another algebraic.
In order to motivate our first description of the projective plane, we consider a geometric question. We know that two points in the usual (x, y)-plane determine a unique line. Similarly, two lines in the plane determine a unique point, if they are not parallel. Our motivation is to construct a plane where every line meets at a unique point. Since the plane itself doesn't contain the required points, we add extra points to it. How many extra points shall we add? For example, would it suffice to use one extra point P and say that any two parallel lines intersect at P ? The answer is no. As then suppose we take L_1, L_2 to be two intersecting lines meeting at Q. Take lines $L_1^{'}, L_2^{'}$ parallel to L_1, L_2 respectively, Thus $L_1^{'}, L_1$ meet at P and $L_2^{'}, L_2$ also meet at P. So that L_1, L_2 have two points in common namely P and Q , which we do not want to happen. So we really need to add a point for each *'direction'*. Logically we could define a direction in this sense to be an equivalence class of parallel lines i.e. all lines parallel to a given line. Let us denote the usual Euclidean plane by

$$\mathbb{A}^2 = \{(x, y) : x, y \in \mathbb{R}\}$$

Then we dfine the projective plane to be

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \{\text{the set of directions in } \mathbb{A}^2\}$$

The extra points in $\mathbb{P}^2$ associated to directions, that is the points in $\mathbb{P}^2$ that are not in $\mathbb{A}^2$, are often called *points at infinity*. So line in $\mathbb{P}^2$ then consists of a line in $\mathbb{A}^2$ together with the point at infinity specified by its direction. Finally, the set of all points at infinity is itself considered to be a line, which we denote by L_∞. Thus constructed the projective plane in this geometric way eliminates the need to make a distinction between parallel and non-parallel lines.

Let us now construct the projective plane algebraiclly. One motivation is related to the famous Fermat's equation of finding rational solutions of

$$x^n + y^n = 1 \tag{1.1}$$

Suppose $\frac{a}{b}$ and $\frac{c}{d}$ be solution such that $b, d > 0$ and $(a, b) = 1 = (c, d)$. So we have

$$a^n d^n + b^n c^n = b^n d^n$$

Hence $b^n | a^n d^n \Rightarrow b^n | d^n \Rightarrow b | d$. Similarly $d^n | b^n c^n \Rightarrow d^n | b^n \Rightarrow d | b$. So $b = \pm d$, but both are positive so $b = d$. Thus any solution of the Fermat's equation has the form $(\frac{a}{d}, \frac{c}{d})$. And thus gives a solution in integers (a, c, d) to the the equation

$$X^n + Y^n = Z^n \tag{1.2}$$

Also any integer solution (a, c, d) of the above eqaution with $d \neq 0$ is a solution of the previous equation. However for this equation, if (a, b, c) is a solution then for $t \neq 0$, (ta, tb, tc) is also a solution which gives rise to the same solution of equation (1). But not all solutions of equation (2) gives rise to a solution of (1) e.g. for odd n, $(1, -1, 0)$ and $(-1, 1, 0)$ do not give solutions to (1). These corresponds to solutions of (1) that lie *"at infinity"*. We now give our second definition of the projective plane. We define an equivalence relation to the set of triples (a, b, c) where $a, b, c\ in \mathbb{R}$ and a,b,c not all 0 by

$$(a, b, c) \sim (a', b', c') \quad \text{if} \;\; a = ta',\; b = tb',\; c = tc' \text{ for some non-zero t.}$$

Then the projective plane, $\mathbb{P}^2$ is the set of all equivalence classes. i.e.

$$\mathbb{P}^2 = \frac{\{(a, b, c) : a, b, c \;\text{ not all zero}\}}{\sim}$$

Thus infact one can generalise the definition for any field k and $n \geq 1$, the projective n-space to be

$$\mathbb{P}^n_k = \frac{\{(a_0, a_1, a_2, \ldots, a_n) \in k^{n+1} : \text{ not all } a_i \text{ 's are } 0\}}{\sim}$$

where

$$(a_0, a_1, a_2, \ldots, a_n) \sim (a_0^{'}, a_1^{'}, a_2^{'}, \ldots, a_n^{'}) \;\text{ if } a_i = ta_i,\; \forall i = 0, 1, ..., n \;\; ; \; t \neq 0.$$

So, a point in $\mathbb{A}^2$ is given by a pair (a, b) where a is the x-coordinate and b is the y-coordinate. In $\mathbb{P}^2$ such a point can be associated to all tuples (ta, tb, t) where $t \neq 0$, in particular we can take $(a, b, 1)$ to be a representative of the equivalence class. We call any such triple (ta, tb, t) *homogeneous* (X, Y, Z)-coordinates of (a, b).

Since we have two definitions of the projective plane, we intend to show an equivalence. First to give a more precise understanding of *directions* we observe that any line in $\mathbb{A}^2$ is parallel to a unique line through the origin. So we take lines passing through the origin as representatives of the corresponding equivalence classes related to directions. Now lines through origin are given by,

$$ly = mx$$

with l, m not both zero. However it is possible that two pairs (l, m) & (l', m') may give the same line. That happens if $\exists t \neq 0$ such that $l = tl',\; m = tm'$. Thus set of directions is described by pairs (l, m) with the above notion of equivalence. From the algebraic definition we see that set of directions is nothing but $\mathbb{P}^1$. Thus from the geomtric definition it allows us to write

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$$

. Now from the algebraic definition, for any $(a, b, c) \in \mathbb{P}^2$ with $c \neq 0$ is in the same equivalence class of $(\frac{a}{c}, \frac{b}{c}, 1)$ which can be identified with the point $(\frac{a}{c}, \frac{b}{c})$ of $\mathbb{A}^2$ and we have already seen that any $(a, b) \in \mathbb{A}^2$ can be identified as $(a, b, 1) \in \mathbb{P}^2$. So all points in $\mathbb{P}^2$ with non-zero homogeneous Z-coordinate can be identified with $\mathbb{A}^2$. And the remaining points in $\mathbb{P}^2$ namely, points with Z-cordinate 0 are just a copy of $\mathbb{P}^1$. As for $(a, b), (a', b') \in \mathbb{P}^1$ can be identified with $(a, b, 0), (a', b', 0) \in \mathbb{P}^2$ and $(a, b) \sim (a', b')$ in $\mathbb{P}^1 \Leftrightarrow (a, b, 0) \sim (a', b', 0)$ in $\mathbb{P}^2$. So that from algebraic definition we also have

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$$

1.2 Curves in the Projective Plane

Our geometric construction of the projective plane was based on trying to make every distinct pair of straight lines intersect at exacly one point. We now wish to discuss intersection of curves of higher degree. So first let us make some definitions. Let k be any field, we call $\mathbb{A}^n = \{(a_1, a_2, \ldots, a_n) \ : \ a_i \in k \ \forall i = 1, 2, ..., n\}$ the affine n-space.

Definition 1.2.1. *An* ***algebraic curve*** *in the affine plane* $\mathbb{A}^2$ *is defined to be the set of zeroes to a non-constant polynomial equation in two variables*

$$f(X, Y) = 0$$

In order to define curves in the projective plane $\mathbb{P}^2$ we need to use polynomial in three variables.

Definition 1.2.2. *A polynomial* $F(X_1, X_2, \ldots, X_n) \in k[X_1, X_2, \ldots, X_n]$ *is said to be* ***homogeneous*** *of degree* d *if it satisfies the identity* $F(tX_1, tX_2, \ldots, tX_n) = t^d F(X_1, X_2, \ldots, X_n)$.

Definition 1.2.3. *A* ***Projective curve*** C *in* $\mathbb{P}^2$ *is defined to be the set of solutions to a non-constant polynomial equation*

$$C \ : \ F(X, Y, Z) = 0$$

where F *is a non-constant homogeneous polynomial.*

If $P = [a, b, c] \in C$ is a point on C with $c \neq 0$ then $[a, b, c]$ can be identified with the point $(\frac{a}{c}, \frac{b}{c}) \in \mathbb{A}^2$. In fact if F is homogeneous of degree d then $F(a, b, c) = 0 = \frac{1}{c^d} F(\frac{a}{c}, \frac{b}{c}, 1)$. Let us define $f(x, y) := F(x, y, 1)$. define a map

$$\Phi : \{[a, b, c] \in C : c \neq 0\} \longrightarrow \{(x, y) \in \mathbb{A}^2 : f(x, y) = 0\}$$

$$[a, b, c] \longmapsto \left(\frac{a}{c}, \frac{b}{c}\right)$$

Clearly Φ is well-defined. For any (a, b) with $f(a, b) = 0, \ F(a, b, 1) = 0$. So $\Phi([a, b, 1]) = (a, b)$ so Φ is onto. If $\Phi([a_1, b_1, c_1]) = \Phi([a_2, b_2, c_2]) \Rightarrow \left(\frac{a_1}{c_1}, \frac{b_1}{c_1}\right) = \left(\frac{a_2}{c_2}, \frac{b_2}{c_2}\right) \Rightarrow a_1 = (\frac{c_1}{c_2}) a_2$; $b_1 = (\frac{c_1}{c_2}) b_2$ as $c_1, c_2 \neq 0$ and $c_1 = (\frac{c_1}{c_2}) c_2$ so $[a_1, b_1, c_1] = [a_2, b_2, c_2]$ and Φ is 1-1. And thus we get a bijection. $f(x, y) = 0$ is called the *affine part* of the projective curve C.
It remains to look at the points $[a, b, c] \in C$ with $c = 0$. These are points that lies on the line at infinity. Thus the points satisfying the equation $F(X, Y, 0) = 0$ are precisely those points of C which lies at infinity.

Chapter 2

Intersection of Curves

The *degree* of a curve C is defined to be the degree of the defining polynomial. For any field k, we know that $k[X, Y]$ is an UFD, and therefore every polynomial can be factored into irreducible components uniquely (upto multiplication by a non-zero scalar). Two curves C_1 and C_2 are said to be *devoid of common components* if their irreducible components are distinct.

Lemma 2.0.1. *If C_1 and C_2 are two curves devoid of common components and the underlying field k is algebraically closed, then $C_1 \cap C_2$ consists of a finite set of points.*

Proof. Suppose $C_1 \ : \ f(X, Y) = 0$ and $C_2 \ : \ g(X, Y) = 0$ have no common factor in $k[X, Y]$. Then by Gauss's lemma they don't have any common factor in $(k(X))[Y]$. This is a PID so there exists rational functions $a_0(X, Y), \ b_0(X, Y) \in k(X)[Y]$ i.e. polynomials in Y with coefficiesnts as rational functions in X such that

$$a_0(X, Y)f(X, Y) + b_0(X, Y)g(X, Y) = 1$$

Upon clearing the denominator we get,

$$\Rightarrow \hat{a}(X, Y)f(X, Y) + \hat{b}(X, Y)g(X, Y) = \hat{c}(X)$$

where $\hat{c}$ is a non-constant polynomial in $k[X]$.

So that there are only finitely many x_i's for which (x_i, y) can be in $C_1 \cap C_2$ (Other wise $\hat{c}(X)$ will have infinitely many roots but $\hat{c}(X)$ is a polynomial). Similarly we can consider $(k(Y))[X]$ do the same to get that there can be only finitely many y-components y_j such that $(x, y_j) \in C_1 \cap C_2$. Therefore $C_1 \cap C_2$ is finite.

□

Let $C_1, \ C_2$ be two projective curves devoid of common components. To each point $P \in \mathbb{P}^2$ we assign an *intersection multiplicity* $I(P, C_1 \cap C_2)$. This is a nonnegative integer which reflects the extent to which $C_1, \ C_2$ are tangent to one another at P. We would like our intersecion number to have properties like $I(P, C_1 \cap C_2) = 0 \Leftrightarrow \ P \notin C_1 \cap C_2$. We define intersection multiplicity more formally and subsequently give what Abhyankar mentions as 'the very first theorem of algebraic geometry' namely Bezout's theorem.

2.1 Intersection Multiplicity

To define intersection multiplicity we introduce the notion of the local ring $\mathcal{O}_P$ of a point $P \in \mathbb{A}^2$. Let $k(X, Y)$, the field of rational functions over k in variables X, Y be the fraction field of $k[X, Y]$. For a point $P = (a, b) \in \mathbb{A}^2$ and a rational function $\phi(X, Y) = \frac{f(X,Y)}{g(X,Y)} \in k(X, Y)$ we say that ϕ is *defined* at P if $g(a, b) \neq 0$.

Lemma 2.1.1. *Consider the set $\mathcal{O}_P$ of P defined by*

$$\mathcal{O}_P = \{\phi \in k(X, Y) : \phi \text{ is defined at } P\}$$

Then $\mathcal{O}_P$ is a local ring.

Proof. Since $g_1(a, b) \neq 0 \neq g_2(a, b) \Rightarrow g_1g_2(a, b) \neq 0$ it follows that $\frac{f_1}{g_1}, \frac{f_2}{g_2} \in \mathcal{O}_P \Rightarrow \frac{f_1}{g_1} - \frac{f_2}{g_2} = \frac{f_1g_2 - f_2g_1}{g_1g_2} \in \mathcal{O}_P$ and $\frac{f_1f_2}{g_1g_2} \in \mathcal{O}_P$, so that $\mathcal{O}_P$ is a subring of $k(X, Y)$.
Now consider the evaluation map

$$ev : \mathcal{O}_P \longrightarrow k \quad \text{given by}$$

$$\phi \longmapsto \phi(P)$$

Observe that this map is identity on k and therefore onto. Also $ev(\phi+\psi) = (\phi+\psi)(P) = \phi(P)+\psi(P) = ev(\phi) + ev(\psi)$ and $ev(\phi\psi) = (\phi\psi)(P) = \phi(P)\psi(P) = ev(\phi)ev(\psi)$ so that ev is an onto homomorphism. Let

$$\mathcal{M}_P = \{\phi \in \mathcal{O}_P : \phi(P) = 0\} = ker\ ev$$

Then $\mathcal{M}_P$ is an ideal of $\mathcal{O}_P$ and $\mathcal{O}_P/\mathcal{M}_P \cong k$. Since k is a field, $\mathcal{M}_P$ is a maximal ideal. Suppose $\phi \in \mathcal{O}_P$ but $\phi \notin \mathcal{M}_P \Rightarrow \phi(P) \neq 0$ in k hence, if $\phi(X, Y) = \frac{f(X,Y)}{g(X,Y)}$ then $f(a, b) \neq 0$, so $\frac{g(X,Y)}{f(X,Y)} \in \mathcal{O}_P$ and $\frac{g(X,Y)}{f(X,Y)}\phi = 1$ so that ϕ is a unit. Therfore $\mathcal{M}_P$ contains all proper ideals of $\mathcal{O}_P$ and thus is the unique maximal ideal. So $\mathcal{O}_P$ is a local ring. □

Definition 2.1.2. *Let $C_1 : f_1(X, Y) = 0,\ C_2 : f_2(X, Y) = 0$ be two curves. Let $(f_1, f_2)_P = \mathcal{O}_Pf_1+\mathcal{O}_Pf_2$ be the ideal generated by f_1 and f_2 in $\mathcal{O}_P$. Regard $\mathcal{O}_P/(f_1, f_2)$ as a k-vector space. Then the* ***intersection multiplicity*** *of C_1 and C_2 at P is defined to be*

$$I(P, C_1 \cap C_2) = dim\,(\mathcal{O}_P/(f_1, f_2)_P)$$

Thus we see that the intersection multiplicity is either a non-negative integer or ∞. Before moving forward we note some properties of the intersection multiplicity.

Proposition 2.1.3. *Let $C :\ f(X, Y) = 0$ be a curve given by a non-zero plynomial f in $k[X, Y]$, such that $f(P) = f(a, b) = 0$. Then $I(P, C \cap C) = \infty$*

Proof. Suppose $P = (a, b)$. The ideal $(f, f)_P = (f)_P$. Suppose $I(P, C \cap C) < \infty$ i.e. to say $\mathcal{O}_P/(f)_P$ is finite dimensional. Let for any polynomial g in $k[X, Y]$, $\overline{g} := g + (f)_P$ in $\mathcal{O}_P/(f)_P$. Now all of $\overline{1},\ \overline{(X - a)},\ \overline{(X - a)^2}, \ldots$ can't be linearly independent. So $\exists\ d > 0$, and $a_0, a_1, \ldots a_d \in k$ not all zero such that

$$a_0 + a_1\overline{(X - a)} + \ldots + a_d\overline{(X - a)^d} = \overline{0}$$

That is to say, there exists a non-zero polynomial $G(X)$ such that $\overline{G}(X) = (f)_P \Rightarrow G(X) \in (f)_P \Rightarrow G(X) = \frac{g_1(X,Y)}{g_2(X,Y)}f(X, Y)$ such that $g_2(a, b) \neq 0$. Now as $f(a, b) = 0$, so $G(a) = 0$. Let $G(X) =$

$(X-a)^r\hat{G}(X)$ such that $\hat{G}(a) \neq 0$. Similarly we can do the above on $\overline{1},\ \overline{(Y-b)},\ \overline{(Y-b)^2},\ldots$ to get $H(Y) \in (f)_P$ such that $H(Y) = (Y-b)^s\hat{H}(Y)$ for $s > 0$ and $\hat{H}(b) \neq 0$. So

$$(X-a)^r\hat{G}(X) = \frac{g_1(X,Y)}{g_2(X,Y)}f(X,Y) \tag{2.1}$$

$$(Y-b)^s\hat{H}(Y) = \frac{h_1(X,Y)}{h_2(X,Y)}f(X,Y) \tag{2.2}$$

$$\text{So,}\quad g_1(X,Y)h_2(X,Y)(Y-b)^s\hat{H}(Y) = g_2(X,Y)h_1(X,Y)(X-a)^r\hat{G}(X)$$

Now we have polynomials in both sides. As $k[X,Y]$ is an UFD, we see that,
$(X-a)^r|g_1(X,Y)$. Since $h_2(a,b) \neq 0 \Rightarrow (X-a)^r \nmid h_2(X,Y)$ and being a polynomial in Y ,$(X-a)^r \nmid (Y-b)^s\hat{H}(Y)$. Now we cancel $(X-a)^r$ in equation (2.1) and see that

$$\hat{G}(X) = \frac{\hat{g}_1(X,Y)}{g_2(X,Y)}f(X,Y)$$

Evaluating at (a,b), the right hand side is zero but the left hand side is not. This is a contradiction. So we must have $I(P, C\cap C) = \infty$. □

Proposition 2.1.4. *If $C_1,\ C_2$ has a common component C such that $P \in C$, then $I(P, C_1\cap C_2) = \infty$ and conversely.*

Proof. Let $C_1 : f_1(X,Y) = 0$ and $C_2 : f_2(X,Y) = 0$ and $C : f(X,Y) = 0$. Therefore f is a common factor of f_1, f_2, therefore $(f_1,f_2)_P \subset (f)_P$. So

$$\mathit{dim}\,\frac{\mathcal{O}_P}{(f_1,f_2)_P} \geq \mathit{dim}\,\frac{\mathcal{O}_P}{(f)_P} = I(P, C\cap C) = \infty$$

by previous proposition. So $I(P, C_1\cap C_2) = \infty$.
Conversely, suppose f_1, f_2 have no common factor f such that $f(a,b) = 0$ for $P := (a,b)$. We will show that $I(P, C_1\cap C_2)$ is finite. Observe that we can in fact assume that $f_1,\ f_2$ has no common factor at all in $k[X,Y]$ and it doesn't affect the question. Since if $f_1,\ f_2$ have a common factor $g \in k[X,Y]$ such that $g(a,b) \neq 0$ then g is a unit in $\mathcal{O}_P$. So $(f_1,f_2)_P = (f_1/g, f_2/g)_P$ and thus we can simply remove those factors without altering the $\mathit{dim}\,(\mathcal{O}_P/(f_1,f_2))$. So suppose f_1, f_2 have no common factors in $k[X,Y]$. Then following lemma (2.0.1) $\exists\ g_1, g_2, g_3 \in k[X]$ such that

$$g_1(X)f_1(X,Y) + g_2(X)f_2(X,Y) = g_3(X)$$

As $f_1(a,b) = 0 = f_2(a,b) \Rightarrow g_3(a) = 0 \Rightarrow g_3(X) = (X-a)^r\hat{g}_3(X)$ for some $r > 0$ and $\hat{g}_3(a) \neq 0$. Since $\hat{g}_3(a) \neq 0,\ g_3(X)$ is a unit in $\mathcal{O}_P$ and hence $(X-a)^r \in (f_1,f_2)_P$ for some $r > 0$, Similarly working with Y we will get $s > 0$ such that $(Y-b)^s \in (f_1,f_2)_P$. So as ideals, $((X-a)^r, (Y-b)^s)_P \subseteq (f_1,f_2)_P$. Let $C_1' : (X-a)^r = 0,\ C_2' : (Y-b)^s = 0$. So,

$$I(P, C_1\cap C_2) = \mathit{dim}\,\left(\frac{\mathcal{O}_P}{(f_1,f_2)_P}\right) \leq \mathit{dim}\,\left(\frac{\mathcal{O}_P}{((X-a)^r,(Y-b)^s)_P}\right) = I(P, C_1'\cap C_2')$$

Now observe that the ideal $((X-a)^r, (Y-b)^s)$ of $k[X,Y]$ can be characterised as follows:

$$((X-a)^r, (Y-b)^s) = \{f \in k[X,Y] : \left(\frac{\partial^{i+j}f}{\partial^i X\partial^j Y}\right)(a,b) = 0,\ 0 \leq i < r, 0 \leq j < s\}$$

Again using this one can show,

$$((X-a)^r,(Y-b)^s)_P = \{f \in \mathcal{O}_P : \left(\frac{\partial^{i+j} f}{\partial^i X \partial^j Y}\right)(a,b) = 0,\ 0 \le i < r, 0 \le j < s\}$$

Thus if we consider the map,

$$Ev : \mathcal{O}_P \longrightarrow k^{rs}$$

defined by evaluating the partial derivatives at (a,b) in an odered tuple, then this gives a surjective map (as we can construct a rational function with prescribed values of partial derivatives at a point), whose kernel is the ideal $((X-a)^r,(Y-b)^s)_P$. So that

$$\left(\frac{\mathcal{O}_P}{((X-a)^r,(Y-b)^s)_P}\right) \cong k^{rs}$$

Therefore $I(P, C_1' \cap C_2') = rs$ and thus $I(P, C_1 \cap C_2) \le rs.$ □

Proposition 2.1.5. *The intersection multiplicity $I(P, C_1 \cap C_2)$ is zero if and only if at least one of C_1 and C_2 doesnot contain P.*

Proof. If $f_1(a,b) = 0 = f_2(a,b)$, then both $f_1,\ f_2$ is in $\mathcal{M}_P$. So that the ideal $(f_1,f_2)_P \subseteq \mathcal{M}_P$ and therefore is a proper ideal of $\mathcal{O}_P$. Thus $\mathcal{O}_P/(f_1,f_2)_P$ is a nonzero vector space, hence its dimension is either a positive integer or infinity, but not zero. Hence $I(P, C_1 \cap C_2) = 0 \Rightarrow$ at least one of $f_1,\ f_2$ is non zero at P.
Conversely, If one of $f_1,\ f_2$ is non-zero at P, then that is a unit in $\mathcal{O}_P$ and hence the ideal $(f_1,f_2)_P$ is unital i.e. the whole ring. So $\mathcal{O}_P/(f_1,f_2)_P$ is the zero vector space, hence its dimension $I(P, C_1 \cap C_2) = 0$. □

2.2 Bezout's Theorem

We now formally state Bezout's theorem.

Theorem 2.2.1. ***(Bezout's Theorem)***
Let C_1, C_2 be two projective curves defined over an algebraically closed field k, devoid of common components. Then

$$\sum_P I(P, C_1 \cap C_2) = (\mathit{deg}\, C_1)(\mathit{deg}\, C_2)$$

Observe that by proposition (2.1.5) the sum can also be taken over only those points P which are in $C_1 \cap C_2$. So that the Bezout's theorem can be interpreted as follows : a curve of degree m and a curve of degree n intersect each other in precisely mn points when counted properly! We give a proof of Bezout's theorm by proving a number of lemmas the first few of which focusses on the affine case. From now on k will be taken as an algebraically closed field untill otherwise stated.

Lemma 2.2.2. *Let $C_1 : f_1(X,Y) = 0$ and $C_2 : f_2(X,Y) = 0$ be two curves in the affine plane $\mathbb{A}^2$ devoid of common components. Then the number of points in $C_1 \cap C_2 \cap \mathbb{A}^2$ satisfy the inequality*

$$\#(C_1 \cap C_2 \cap \mathbb{A}^2) \le \mathit{dim}\left(\frac{k[X,Y]}{(f_1,f_2)}\right)$$

Proof. By lemma (2.0.1) $\#(C_1 \cap C_2 \cap \mathbb{A}^2)$ is finite. Let $P_1, P_2, \ldots, P_m$ be m different points in it. Suppose $P_i = (a_i, b_i)$. Observe that, for fixed i, $\forall j \neq i$, both $(a_i - a_j)$ and $(b_i - b_j)$ cannot be zero. Therefore $\exists$ scalars c_j such that $(b_i - b_j) - c_j(a_i - a_j) \neq 0$. We construct polynomials $h_i = h_i(X, Y)$, such that $h_i(P_j) = \delta^i_j$ in the following way:

$$h_i(X, Y) = \prod_{j \neq i} \frac{Y - c_j X - b_j + c_j a_j}{b_i - c_j a_i - b_j + c_j a_j}$$

Observe that thus constructed polynomials give m linearly independent vectors in $\frac{k[X,Y]}{(f_1,f_2)}$. Because if for scalars $d_1, d_2, \ldots, d_m$

$$d_1 h_1 + d_2 h_2 + \ldots + d_m h_m = \overline{0} = g_1 f_1 + g_2 f_2$$

for some $g_1, g_2 \in k[X, Y]$, evaluating at P_i gives, $d_i = g_1(P_i) f_1(P_i) + g_2(P_i) f_2(P_i) = 0$ as P_i's are points in $C_1 \cap C_2$ for all $i = 1, 2, \ldots, m$. Therefore $m \leq$ ***dim*** $\left(\frac{k[X,Y]}{(f_1,f_2)}\right)$.

□

Lemma 2.2.3. *Let $C_1 : f_1(X, Y) = 0$ and $C_2 : f_2(X, Y) = 0$ be two curves in the affine plane $\mathbb{A}^2$ devoid of common components having degrees $n_1,\ n_2$ respectively. Then*

$$\textit{dim} \left(\frac{k[X, Y]}{(f_1, f_2)}\right) \leq n_1 n_2$$

Proof. For each integer $d \geq 0$ we define,

$$R_d := \text{ vector space of polynomials } f(X, Y) \text{ of degree } \leq d$$

$$W_d := R_{d-n_1} f_1 + R_{d-n_2} f_2$$

Thus W_d is the k-vector space of polynomials of the form $f = g_1 f_1 + g_2 f_2$ with deg $g_i \leq d - n_i$ for $i = 1, 2$. Observe $W_d = 0$ if $d < max\{n_1, n_2\}$, and $W_d \subset (f_1, f_2)$.

$$\text{Let } \phi(d) = \frac{1}{2}(d + 1)(d + 2). \text{ We will show that } \ \dim R_d = \phi(d).$$

Observe that the set of monomials $S := \{x^i y^j \ : \ i + j = d,\ i, j \geq 0\}$ are linearly independent in R_d and $R_d = R_{d-1} \oplus span(S)$.
So that, dim R_d = dim R_{d-1}+ dim $span(S)$ = dimR_{d-1}+d+1. We know that dim R_0 = dim k = 1 = $\phi(0)$.
If dim $R_{d-1} = \phi(d-1)$, then dim R_d = $\phi(d-1) + d + 1 = \frac{1}{2}(d)(d+1) + d + 1 = \frac{1}{2}(d+1)(d+2) = \phi(d)$.
Hence by induction for all $d \geq 0$, dim $R_d = \phi(d)$.
Next observe that for $d \geq n_1 + n_2$,

$$R_{d-n_1} f_1 \cap R_{d-n_2} f_2 = R_{d-n_1-n_2} f_1 f_2$$

For if g be a polynomial in the intersection, $g = g_1 f_1 = g_2 f_2$ for some $g_1, g_2 \in k[X, Y]$ with deg $g_i \leq d - n_i$ for $i = 1, 2$. Now as f_1, f_2 do not have any common factor and $k[X, Y]$ is an UFD $f_2 | g_1$ so that $g_1 = \hat{g_1} f_2$ and thus deg $\hat{g_1} \leq d - n_1 - n_2$. Therefore $g = \hat{g_1} f_1 f_2 \in R_{d-n_1-n_2} f_1 f_2$. Again for $h \in R_{d-n_1-n_2} f_1 f_2,\ h = h_1 f_1 f_2$ such that deg $h_1 \leq d - n_1 - n_2$.
Thus deg $(h_1 f_1) \leq d - n_2$ and deg $(h_1 f_2) \leq d - n_1$. So $h \in R_{d-n_1} f_1 \cap R_{d-n_2} f_2$. Hence the equality.
Now dim (R_m) = dim $R_m f$ for any non-zero polynomial f as $g \mapsto gf$ gives an isomorphism between $R_m \sim R_m f$. So,

$$dim\ (W_d) = dim\ (R_{d-n_1} f_1 + R_{d-n_2} f_2) = dim(R_{d-n_1} f_1) + dim(R_{d-n_2} f_2) - dim(R_{d-n_1-n_2} f_1 f_2)$$

So, $dim(R_d) - dim(W_d) = \phi(d) - \phi(d-n_1) - \phi(d-n_2) + \phi(d-n_1-n_2) = n_1n_2$

Lastly we prove that if $r_1, r_2, \dots r_{n_1n_2+1}$ are elements of $k[X,Y]$ then they cannot be linearly independent modulo (f_1, f_2). Let us choose d large enough so that, $r_j \in R_d \;\; \forall j$. Now let $\{m_1, m_2, \dots, m_s\}$ be a basis of W_d where dim $W_d = s$.
From the fact that $dim(R_d) - dim(W_d) = n_1n_2$.
$m_1, m_2, \dots, m_s, r_1, r_2, \dots, r_{n_1n_2+1}$ can't all be linearly independent in R_d. So that we will get a $m \in W_d$ which is a non-trivial linear combination of r_i's. That is, $\sum t_ir_i = m \in W_d \subset (f_1, f_2)$ and hence r_i's are linearly dependent modulo (f_1, f_2). So we have dim $\left(\frac{k[X,Y]}{(f_1,f_2)}\right) \leq n_1n_2$. $\square$

Next we would like to know when this inequality is an equality.
Consider any polynomial $F(X,Y) \in k[X,Y]$ of degree n. Then F can be written as follows :

$$F(X,Y) = F_n(X,Y) + F_{n-1}(X,Y) + \cdots + F_0(X,Y)$$

where each polynomial $F_j(X,Y)$ is a homogeneous polynomial of degree j. Since F is of degree n, $F_n(X,Y)$ is a non-zero polynomial. F_n is called the *degree form*. Now the homogeneous polynomial of degree n in two variables X, Y

$$F_n(X,Y) = a_0Y^n + a_1Y^{n-1}X + \cdots + a_nX^n$$

can also be regarded as a polynomial in one variable

$$\frac{F_n(X,Y)}{X^n} = a_0\left(\frac{Y}{X}\right)^n + \cdots + a_n = a_0\prod_{i=1}^{n}\left(\frac{Y}{X} - \alpha_i\right) = \frac{a_0}{X^n}\prod_{1=1}^{n}(Y - \alpha_iX)$$

assuming $a_0 \neq 0$ and k algebraically closed. Thus the homogeneous polynomial can always be written as the product of n linear factors (without assuming $a_0 \neq 0$).

$$F_n(X,Y) = a_0Y^n + a_1Y^{n-1}X + \cdots + a_nX^n = \prod_{i=1}^{n}(\mu_iX - \lambda_iY)$$

We have already seen in the previous section that given a projective curve $C: \;\; F(X,Y,Z) = 0$, we can then write C as a union of in its affine part C_0 and points at infinity. Where

$$C_0: \;\; f(x,y) = F(x,y,1) = 0$$

and the points at infinity are the oints with $Z = 0$. The process of replacing a homogeneous polynomial by a non-homogeneous one is called *dehomozenization* (here with respect to the variable Z). We now focus on the reverse process.
Suppose we begin with an affine curve $C_0: \;\; f(x,y) = 0$, we want to find a projective curve C whose affine part is C_0. Let $f(x,y) = \sum a_{ij}x^iy^j$ be of degree d, i.e. $maxi + j = d$. We define *homogenization* of f as follows :

$$F(X,Y,Z) = \sum_{i,j} a_{ij}X^iY^jZ^{d-i-j}$$

From definition it is clear that F is a homogeneous polynomial of degree d and $F(x,y,1) = f(x,y)$. Also observe that $F(X,Y,0)$ is not identically 0, so that F doesn't contain the entire line at infinity. Thus homogenization and dehomogenization gives an one-to-one correspondence between affine curves and projective curves which do not contain the entire line at infinity.
Thus observe that for a given affine curve $C: \;\; f(x,y) = 0$, its points at infinity are given by : *degree*

form of f = 0, as all other lesser degree terms will contain Z after homogenization. We have seen if f is of degree n, degree form of f can be factored as

$$f_n(x, y) = \prod_{i=1}^{n}(a_i x - b_i y)$$

So points at infinity of f are points with homogeneous coordinates

$$[X, Y, Z] = [b_i, a_i, 0]$$

We now state our next lemma.

Lemma 2.2.4. *If C_1 and C_2 do not meet at infinity we will have equality in lemma (2.2.2) , i.e.*

$$\textit{dim}\left(\frac{k[X, Y]}{(f_1, f_2)}\right) = n_1 n_2$$

Proof. $C_1,\ C_2$ donot meet at infinity implies that their degree forms f_1^* and f_2^* (say) do not have a common factor.
Claim : For $d \geq n_1 + n_2, \quad (f_1, f_2) \cap R_d = W_d$
Suppose $g \in (f_1, f_2) \cap R_d \Rightarrow g = g_1 f_1 + g_2 f_2$ with $g_1,\ g_2$ of smallest possible degree. If deg $g_1 > d - n_1$ then looking at the terms of highest degree shows that, $g_1^* f_1^* + g_2^* f_2^* = 0$.
Now $f_1^*,\ f_2^*$ are relatively prime. Therefore $f_2^* | g_1^* \Rightarrow g_1^* = h f_2^*$. Clearly h is a homogeneous polynomial. And as $g_1^* - h f_2^* = 0$, therefore deg $(g_1 - h f_2) <$ deg (g_1).
Now $h f_1^* f_2^* + g_2^* f_2^* = 0 \Rightarrow h f_1^* + g_2^* = 0$ implies $h f_1^*$ and g^* are homogeneous of same degree and as their addition yeilds 0, we must have, deg $(h f_1 + g_2) <$ deg (g_2).
But $(g_1 - h f_2) f_1 + (h f_1 + g_2) f_2 = g_1 f_1 + g_2 f_2 = g$, contradicts the minimality of degrees of g_1, g_2. Thus we must have, deg $g_1 \leq d - n_1$. Similarly we ge deg $g_2 \leq d - n_2$ so that $g \in W_d$. Thus $(f_1, f_2) \cap R_d \subseteq W_d$. And from definition we see that $W_d \subseteq (f_1, f_2) \cap R_d$. Hence our claim is established.
We have seen that dim R_d - dim $W_d = n_1 n_2$, i.e. there are $n_1 n_2$ elements in R_d that are linearly independent modulo W_d. Now those elements are also elements of $k[X, Y]$ and by our claim, are linearly independent modulo (f_1, f_2). Hence dim $\left(\frac{k[X,Y]}{(f_1,f_2)}\right) \geq n_1 n_2$. From (2.2.2) we get the other way inequality. Thus the equality is established. □

Previously we have peorved that, intersection multiplicity is finite. Now we give an upperbound to it strengthenning the inequality of lemma(2.2.3).

Lemma 2.2.5.

$$I(P, C_1 \cap C_2) = \textit{dim}\left(\frac{\mathcal{O}_P}{(f_1, f_2)_P}\right) \leq \textit{dim}\left(\frac{k[X, Y]}{(f_1, f_2)}\right)$$

Proof. Any finite set of elements $\frac{g_1}{h_1}, \frac{g_2}{h_2}, \cdots, \frac{g_r}{h_r}$ in $\mathcal{O}_P$ can be written over a common denominator { As we can choose $h = \prod_i h_i$; then $h(P) \neq 0$. And $\forall j = 1, 2, \ldots, r$ choose $\overline{h_j} = \prod_{i \neq j} h_i$, then $\frac{g_j}{h_j} = \frac{g_j \overline{h_j}}{h}$}. Suppose $\frac{r_1}{l}, \frac{r_2}{l}, \cdots, \frac{r_m}{l}$ be any linearly independent set in in $\mathcal{O}_P/(f_1, f_2)_P$, $l(P) \neq 0$. We will show that $r_1, r_2, \ldots, r_m$ are linearly independent in $k[X, Y]$ modulo (f_1, f_2). Suppose not. Let for $c_1, c_2, \ldots, c_m \in k$,

$$c_1 \overline{r_1} + c_2 \overline{r_2} + \cdots + c_m \overline{r_m} = \overline{0}$$

$$\Rightarrow c_1 r_1 + c_2 r_2 + \cdot + c_m r_m = t_1 f_1 + t_2 f_2 \quad \text{for some } t_1, t_2 \in k[X, Y]$$

$$\Rightarrow c_1 \frac{r_1}{l} + c_2 \frac{r_2}{l} + \cdots + c_m \frac{r_m}{l} = \frac{t_1}{l} f_1 + \frac{t_2}{l} f_2 \in (f_1, f_2)_P \;\text{ as } l(P) \neq 0$$

This implies that $c_i = 0,\ \forall i = 1, 2, \dots m$. Hence, for any linearly independent set in the left hand side we can obtain a linearly independent set of same cardinality of the right hand side. So the lemma is proved

$\square$

Lemma 2.2.6.

$$\mathcal{O}_P = k[X, Y] + (f_1, f_2)_P$$

Proof. Suppose $\frac{g_1}{h},\ \frac{g_2}{h}, \cdots, \frac{g_m}{h}$ span $\mathcal{O}_P$ modulo $(f_1, f_2)_P$, then $h(P) \neq 0 \Rightarrow h$ is invertible in $\mathcal{O}_P$. Thus for any $\phi \in \mathcal{O}_P$, $\phi h^{-1} \in \mathcal{O}_P$ and we can write

$$\phi h^{-1} \equiv c_1 \frac{g_1}{h} + c_2 \frac{g_2}{h} + \cdots + c_m \frac{g_m}{h} \ \ (\bmod\ (f_1, f_2)_P)$$

$$\Rightarrow \phi \equiv c_1 g_1 + c_2 g_2 + \cdots + c_m g_m \ \ (\bmod\ (f_1, f_2)_P)$$

for scalars $c_1, c_2, \cdots c_m \in k$. Thus the polynomials g_i span $\mathcal{O}_P$ modulo $(f_1, f_2)_P$.

$\square$

Lemma 2.2.7. $r \geq$ *dim* $(\mathcal{O}_P/(f_1, f_2)_P) \ \Rightarrow \ \mathcal{M}_P^r \subseteq (f_1, f_2)_P$.

Proof. Let $t_1, t_2, \dots, t_r \in \mathcal{M}_P$, we will show that the product $t_1 t_2 ... t_r \in (f_1, f_2)_P$. Define the sequence of ideals

$$J_i = t_1 t_2 \cdots t_i \mathcal{O}_P + (f_1, f_2)_P \ \ \forall i = 1, 2, \dots, r \ \text{ and } J_{r+1} = (f_1, f_2)_P$$

Then we get $\mathcal{M}_P \subset J_1 \subset J_2 \subset \cdots \subset J_r \subset J_{r+1} = (f_1, f_2)_P$. Since $r \geq$dim $(\mathcal{O}_P/(f_1, f_2)_P)$ all of the above can't be strict inclusions. So, $J_i = J_{i+1}$ for some i. If $i = r$ we are done. If $i < r$, then

$$t_1 t_2 \dots t_i = t_1 t_2 \dots t_{i+1} \phi + \psi \ \text{ for some } \phi \in \mathcal{O}_P,\ \psi \in (f_1, f_2)_P$$

$$\Rightarrow t_1 t_2 \dots t_i (1 - t_{i+1\phi}) = \psi$$

Now $t_{i+1} \in \mathcal{M}_P \Rightarrow t_{i+1}(P) = 0$, so $(1 - t_{i+1}\phi)(P) \neq 0$ and hence is invertible in $\mathcal{O}_P$. Therefore $t_1 t_2 \dots t_r = \psi (1 - t_{i+1}\phi)^{-1} t_{i+1} \dots t_r \in (f_1, f_2)_P$ and hence $\mathcal{M}_P^r \subseteq (\mathcal{O}_P/(f_1, f_2)_P)$ $\square$

Lemma 2.2.8. *If $P \in C_1 \cap C_2 \in \mathbb{A}^2$ and $\phi \in \mathcal{O}_P$ then $\exists$ a polynomial $g \in k[X, Y]$ such that*

$$g \equiv \phi\, (\ \textit{mod}\ (f_1, f_2)_P)$$

$$\textit{and } g \equiv 0\, (\ \textit{mod}\ (f_1, f_2)_Q) \quad \textit{for all } Q \neq P,\ Q \in C_1 \cap C_2 \cap \mathbb{A}^2$$

Proof. We have already shown that number of points in $C_1 \cap C_2 \cap \mathbb{A}^2$ is finite. By lemma 2.2.2 we know that $\exists h \in k[X, Y]$ such that $h(P) = 1$ and $h(Q) = 0$ for all $Q \neq P$ and $Q \in C_1 \cap C_2 \cap \mathbb{A}^2$. Now $h(P) \neq 0 \Rightarrow h^{-1} \in \mathcal{O}_P$ and $h \in \mathcal{M}_Q$. Now for large r, by lemma (2.2.7) $h^r \in (f_1, f_2)_Q\ \forall Q \neq P$. For any $\phi \in \mathcal{O}_P$ consider ϕh^{-r}. By lemma 2.2.6 $\exists$ a polynomial $f \in k[X, Y]$ such that $\phi h^{-r} \equiv f$ (mod $(f_1, f_2)_P$). Let $g = f h^r$, then g is a polynomial that satisfies the conditions.

$\square$

Lemma 2.2.9.

$$\textit{dim}\ \left(\frac{k[X, Y]}{(f_1, f_2)}\right) = \sum_P I(P, C_1 \cap C_2)$$

Proof. Suppose $P_1, P_2, \cdots, P_m$ be the points in $C_1 \cap C_2 \cap \mathbb{A}^2$. Consider the natural map,

$$\Psi : k[X,Y] \longrightarrow \prod_{P \in C_1 \cap C_2 \cap \mathbb{A}^2} \frac{\mathcal{O}_P}{(f_1, f_2)_P}$$

$$f \longmapsto (f \bmod (f_1, f_2)_{P_1}\ ,\ \cdots\ ,\ f \bmod (f_1, f_2)_{P_m})$$

This is a surjective map as, for any $(\overline{\phi_1}, \overline{\phi_2}, \cdots, \overline{\phi_m})$, by lemma 2.2.8 $\exists g_i \in k[X,Y]$ such that $g_i \equiv \phi_i \left(\bmod (f_1, f_2)_{P_i} \right)$ and $g_i \equiv 0 \left(\bmod (f_1, f_2)_{P_j} \right)$ for $j \neq i$. Let $g = \sum_i g_i$.
Then $g \equiv \phi_i \left(\bmod (f_1, f_2)_{P_i} \right)$ for all i and thus $\Psi(g) = (\overline{\phi_1}, \overline{\phi_2}, \cdots, \overline{\phi_m})$. Next we show that ker $\Psi = (f_1, f_2)$. Now clearly $(f_1, f_2) \subset$ ker Ψ. Showing the other way around is a bit tricky. Let $f \in$ ker Ψ. Consider the following set.

$$L_f := \{g \in k[X,Y]\ :\ gf \in (f_1, f_2)\}$$

We will show that $1 \in L_f$. Now L_f is clearly an ideal of $k[X,Y]$ and $(f_1, f_2) \subset L_f \subset k[X,Y]$. Therefore dim $(k[X,Y]/L_f) \leq$ dim $(k[X,Y]/(f_1, f_2)) < \infty$. Now observe that for any P_i, $f \equiv 0 \bmod (f_1.f_2)_{P_i}$, i.e. to say, $f = \frac{g_{1i}}{h_{1i}} f_1 + \frac{g_{2i}}{h_{2i}} f_2$ with $h_{1i}(P_i) \neq 0,\ \ h_{2i}(P_i) \neq 0$. Thus $h_{1i} h_{2i} f \in (f_1, f_2)$ along with $h_{1i} h_{2i} \neq 0$. Again for any $P \in \mathbb{A}^2$ such that $P \notin C_1 \cap C_2$ then one of $f_i(P) \neq 0$ for $i = 1, 2$ and clearly $f_i f \in (f_1, f_2)$. So we can conclude,

Result: For all points $P \in \mathbb{A}^2$, $\exists$ a polynomial $G \in L_f$ such that $G(P) \neq 0$.

Now assume that $1 \notin L_f$. We will give a contradiction.
Since $k[X,Y]/L_f$ is finite dimensional, so all powers of X can't be linearly independent modulo L_f. Thus there exists $n > 0$ and scalars $a_i \in k$ so that $X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in L_f$. Since k is algebraically closed, we can write

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0 = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

If $1 \in L_f + \langle X - \alpha_i \rangle$ for all i then taking product we can deduce that $1 \in L_f$ contrary to our assumption. So that $\exists\ \alpha_j \in k$ such that $1 \notin L_f + \langle X - \alpha_j \rangle$. Similarly, as $L_f \subset L_f + \langle X - \alpha_j \rangle$ and hence $k[X,Y]/L_f + \langle X - \alpha_j \rangle$ is finite dimensional and all powers of Y cannot be linearly independent modulo $L_f + \langle X - \alpha_j \rangle$. Following the steps above we get a $\beta_k \in k$ such that $1 \notin L_f + \langle X - \alpha_j \rangle + \langle Y - \beta_k \rangle$. Now by our above result for $(\alpha_j, \beta_k) \in \mathbb{A}^2$ $\exists g \in L_f$ such that $g(\alpha_j, \beta_k) \neq 0$, hence is an unit in k. But

$$g(X,Y) = g(\alpha_j + (X - \alpha_j), \beta_k + (Y - \beta_k))$$
$$= g(\alpha_j, \beta_k) + g_1(X,Y)(X - \alpha_j) + g_2(X,Y)(Y - \beta_k)$$
$$\Rightarrow g(\alpha_j, \beta_k) \in L_f + \langle X - \alpha_j \rangle + \langle Y - \beta_k \rangle$$

This is a contradiction! So $1 \in L_f$ and hence ker $\Psi = (f_1, f_2)$. So,

$$\begin{aligned} \textit{dim} \left(\frac{k[X,Y]}{(f_1, f_2)} \right) &= \textit{dim} \left(\prod_{P \in C_1 \cap C_2 \cap \mathbb{A}^2} \frac{\mathcal{O}_P}{(f_1, f_2)_P} \right) \\ &= \sum_P \textit{dim}\ (\mathcal{O}_P/(f_1, f_2)_P) \\ &= \sum_P I(P, C_1 \cap C_2) \end{aligned}$$

$\square$

Thus from lemma (2.2.4) we already have an weaker version of Bezout's theorem. If $C_1,\ C_2$ do not meet at infinity, then $\sum\limits_P I(P, C_1 \cap C_2) = n_1 n_2 = (\deg C_1)(\deg C_2)$. For the more general version we show that the definition of intersection multiplicity does not change when we make a projective transformation. In order to do so we first have to define $\mathcal{O}_P, \mathcal{M}_P, (f_1, f_2)_P$ in terms of homogeneous coordinates so that they make sense for points P at infinity. To see what to do we put as usual $X\frac{\mathcal{X}}{\mathcal{Z}}$ and $Y = \frac{|y}{\mathcal{Z}}$ and we view $k[X, Y] = k[\frac{\mathcal{X}}{\mathcal{Z}}, \frac{\mathcal{Y}}{\mathcal{Z}}]$ as a subring of the field of rational functions $k(\mathcal{X}, \mathcal{Y}, \mathcal{Z})$ in variables $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$. The $k(X, Y)$ becomes identified with the set of all rational functions $\Phi = \frac{F}{G}$ that are *homogeneous of degree 0* in the sense that $F,\ G$ are homogeneous of same degree. Indeed for $\phi \in k(X, Y)$ we have

$$\phi(X, Y) = \frac{f(X, Y)}{g(X, Y)} = \frac{\mathcal{Z}^n f(\frac{\mathcal{X}}{\mathcal{Z}}, \frac{\mathcal{Y}}{\mathcal{Z}})}{\mathcal{Z}^n g(\frac{\mathcal{X}}{\mathcal{Z}}, \frac{\mathcal{Y}}{\mathcal{Z}})} = \frac{F(\mathcal{X}, \mathcal{Y}, \mathcal{Z})}{G(\mathcal{X}, \mathcal{Y}, \mathcal{Z})} = \Phi(\mathcal{X}, \mathcal{Y}, \mathcal{Z})$$

say, where $F,\ G$ are homogeneous of same degree

$$n = \max\ \{\ \deg f, \deg g\}$$

On the other hand if $\Phi = \frac{F}{G}$ is homogeneous of degree 0, then $\Phi(t\mathcal{X}, t\mathcal{Y}, t\mathcal{Z}) = \Phi(\mathcal{X}, \mathcal{Y}, \mathcal{Z})$ and

$$\Phi(\mathcal{X}, \mathcal{Y}, \mathcal{Z}) = \Phi(X, Y, 1) \in k(X, Y)$$

We now give the definitions :

If $P = [A, B, C]$ is a point in $\mathbb{P}^2$ and $\Phi = \frac{F}{G} \in k(X, Y)$, then we say Φ is *defined* at P if $G(A, B, C) \neq 0$. If Φ is defined at P, we put $\Phi(P) = \frac{F(A,B,C)}{G(A,B,C)}$, and this is well-defined as the ratio is independent of the coordinate triple, $F,\ G$ being homogeneous of same degree. Next we define :

$$\mathcal{O}_P = \{\Phi \in k(X, Y)\ :\ \Phi \text{ is defined at } P$$

$$\mathcal{M}_P = \{\Phi \in k(X, Y)\ :\ \Phi(P) = 0\}$$

Now let $C_1\ :\ \ F_1(\mathcal{X}, \mathcal{Y}, \mathcal{Z}) = 0$ and $C_2\ :\ \ F_2(\mathcal{X}, \mathcal{Y}, \mathcal{Z}) = 0$ be two projective curves without any common components. let $f_1(X, Y)$ and $f_2(X, Y)$ define their affine parts respectively. Observe that we cannot simply define $(F_1, F_2)_P$ as the ideal generated by $F_1,\ F_2$ in $\mathcal{O}_P$ as then all elements may not be homogeneous of degree 0. We define,

$$(F_1, F_2)_P = \{F/G \in \mathcal{O}_P\ :\ F \text{ is of the form } F = H_1F_1 + H_2F_2$$

Now suppose $P \in \mathbb{A}^2$, then $(F_1, F_2)_P = (f_1, f_2)_P$. Because for $\Phi = \frac{F_1H_1 + F_2H_2}{G} \in (F_1, F_2)_P$

$$\begin{aligned}
\frac{F_1(\mathcal{X}, \mathcal{Y}, \mathcal{Z})H_1(\mathcal{X}, \mathcal{Y}, \mathcal{Z}) + F_2(\mathcal{X}, \mathcal{Y}, \mathcal{Z})H_2(\mathcal{X}, \mathcal{Y}, \mathcal{Z})}{G(\mathcal{X}, \mathcal{Y}, \mathcal{Z})} &= \frac{F_1(X, Y, 1)H_1(X, Y, 1) + F_2(X, Y, 1)H_2(X, Y, 1)}{G(X, Y, 1)} \\
&= \frac{h_1(X, Y)}{g(X, Y)} f_1(X, Y) + \frac{h_2(X, Y)}{g(X, Y)} f_2(X, Y) \in (f_1, f_2)_P
\end{aligned}$$

Converse holds trivially. Therefore we define intersection multiplicity for any $P \in \mathbb{P}^2$ as

$$I(P, C_1 \cap C_2) = \ \dim\ \left(\frac{\mathcal{O}_P}{(F_1, F_2)_P}\right)$$

To prove the general case the strategy we are going to use is the following : We show that there is a line L in $\mathbb{P}^2$ which doesnot meet $C_1 \cap C_2$ and then we can take a coordinate system in which the new line is our line at infinity and thereby reduce the problem to the case already proved.

Lemma 2.2.10. *For any given finite set S of points in $\mathbb{P}^2$, there is a line L not meeting S.*

Proof. If S only consists of points of $\mathbb{A}^2$, then we can take the line to be $\mathcal{Z} = 0$. If S consists of only points at infinity, then we can choose a point $[A', B', 0] \notin S$, A', B' not both zero and we can take a line in $\mathbb{A}^2$ with direction given by $[A', B', 0]$, i.e. to say we can take the line in $\mathbb{P}^2$ given by, $A'\mathcal{Y} - B'\mathcal{X} = 0$. This works fine as required L. Now let us suppose that S contains both, points at infinity and points in $\mathbb{A}^2$. Again we pick a point $[A, B, 0] \notin S$, we can do it as k is algebraically closed, hence infinite. Consider all lines in $\mathbb{A}^2$ with direction given by $[A, B, 0]$ i.e. consider all lines in $\mathbb{A}^2$ given by $AY - BX + C = 0$. We choose C such that none of the affine points satisfy the equation, i.e. to say if $[a_1, b_1, 1]$, $[a_2, b_2, 1]$, $\cdots$, $[a_r, b_r, 1] \in S$, we choose C such that $C \neq Ba_i - Ab_i$, $\forall i = 1, 2, \ldots, r$. Then the line given by $A\mathcal{Y} - B\mathcal{X} + C\mathcal{Z} = 0$ is our required line. $\square$

Lemma 2.2.11. *$C_1 \cap C_2$ is finite.*

Proof. We know that if a prozective curve do not contain the entir line at infinity as a component then it can only have a finite number of points at infinity (recall the factorization of the degree form in the affine case). Now since C_1, C_2 are devoid of common components thus both of them can't have the line at infinity as a component. So that $C_1 \cap C_2 \cap L_\infty$ is always finite. We have already seen $C_1 \cap C_2 \cap \mathbb{A}^2$ is finite. Hence $C_1 \cap C_2$ is finite. $\square$

Now by lemma (2.2.10) there is a line that does not intersect $C_1 \cap C_2$. We can take a new coordinate system where this line is the line at infinity. This completes the proof of Bezout's theorem in all its details.

Chapter 3

Newton's Theorem

Let us first consider the following examples :

Example 3.0.1.
$$f(X,Y) = (1-X)Y^2 + XY + 2X^3$$
dividing by $(1-X)$ we get $Y^2 + \frac{X}{1-X}Y + \frac{2X^3}{1-X}$, Now
$$\frac{X}{1-X} = (X + X^2 + X^3 + \cdots)$$
$$\frac{2X^3}{1-X} = 2X^2(X + X^2 + X^3 + \cdots)$$
This way the coefficients are power series in X. Let us consider another example
$$g(X,Y) = X^2(1-X)Y^2 + XY + 2$$
division by $X^2(1-X)$ gives $Y^2 + \frac{X}{X^2(1-X)}Y + \frac{2}{X^2-X^3}$
$$\frac{X}{X^2(1-X)} = X^{-1} + 1 + X + \cdots$$
and so on. Here the coefficients are what is known as *meromorphic series* in X.

A meromorphic series in one variable X may defined as a power series with finitely many terms having negative exponents in X. One can then extend the notion of *order* of a power series to that of a meromorphic series as the degree of the smallest degree term present. If k be a field, we denote the field of meromorphic series with coefficients in k in variable X by $k((X))$.
Newton's theorm gives a way of factorising a monic polynomial in Y whose coefficients are in $k((X))$.

Theorem 3.0.2. ***(Newton's Theorem)***
Let k be an algebraically closed field of characteritic 0 (or char not dividing $n!$), and let
$$F(X,Y) = Y^n + a_1(X)Y^{n-1} + \cdots + a_n(X) \quad \in k((X))[Y]$$
be a monic poynomial of degree $n > 0$ in Y with coefficients in $k((X))$. Then $\exists m > 0$, which is not divisible by char k, such that
$$F(T^m, Y) = \prod_{i=1}^{n} [Y - \eta_i(T)] \quad \textit{with} \;\; \eta_i(T) \in k((T))$$

The theorem was first proved by Newton (1736) with the use of Newton polygon. We give here the proof by Abhyankar (1990) which makes use of Hensel's lemma. First we try to prove the theorem when the coefficients are in $k[[X]]$ which is given by Hensel's lemma. Briefly, Hensel's lemma states that if $F \in k[[X]][Y]$ and $F(0,Y)$ factors, then so does F.

3.1 Hensel's Lemma

Lemma 3.1.1. *Let k be a field and let*

$$F(X,Y) = Y^n + a_1(X)Y^{n-1} + \cdots + a_n(X) \quad \in k[[X]][Y]$$

be a monic polynomial with degree $n > 0$ in Y. Assume that $F(0,Y) = \overline{G}(Y)\overline{H}(Y)$ where,

$$\overline{G}(Y) = Y^r + \hat{b_1}Y^{r-1} + \cdots + \hat{b_r} \quad \in k[Y] \quad \textit{and}$$

$$\overline{H}(Y) = Y^s + \hat{c}_1Y^{s-1} + \cdots + \hat{c}_s \quad \in k[Y]$$

are monic polynomials of degrees $r > 0$ and $s > 0$ such that $gcd(\overline{G}(Y), \overline{H}(Y)) = 1$. Then $\exists$ unique monic polynomials

$$G(X,Y) = Y^r + b_1(X)Y^{r-1} + \cdots + b_r(X) \in k[[X]][Y] \quad \textit{and}$$

$$H(X,Y) = Y^s + c_1(X)Y^{s-1} + \cdots + c_s(X) \in k[[X]][Y]$$

of degrees r and s and coefficients $b_i(X)$, $c_j(X)$ in $k[[X]]$ for $i = 1,\ldots,r$; $j = 1,\ldots,s$ such that $G(0,Y) = \overline{G}(Y)$, $H(0,Y) = \overline{H}(Y)$, and $F(X,Y) = G(X,Y)H(X,Y)$.

Proof. We write $F(X,Y)$ as a power series in X with coefficients as polynomials in Y.

$$F(X,Y) = F_0(Y) + F_1(Y)X + \cdots + F_q(Y)X^q + \cdots$$

where $F_0(Y) = F(0,Y) \in k[Y]$ is monic with degree n and deg $F_q < n$ for all $q > 0$. We want to find

$$G = G_0(Y) + G_1(Y)X + \cdots + G_i(Y)X^i + \cdots, \quad \text{and}$$

$$H = H_0(Y) + H_1(Y)X + \cdots + H_j(Y)X^j + \cdots \quad \text{where}$$

$$G_0 = G_0(Y) = \overline{G}(Y) \in k[Y] \text{ is monic with deg } G_0 = r$$

$$H_0 = H_0(Y) = \overline{H}(Y) \in k[Y] \text{ is monic with deg } H_0 = s$$

$$G_i = G_i(Y) = \in k[Y] \text{ with deg } G_i < r, \ \forall\, i > 0$$

$$H_j = H_j(Y) \in k[Y] \text{ with deg } H_j < s, \ \forall\, j > 0$$

such that $F = GH$. So that,

$$F_q = \sum_{i+j=q} G_iH_j \quad \text{for all } q \geq 0.$$

We prove by inductuion on q. The case $q = 0$ is obvious from the given condition. Let $q > 0$. Suppose we have found G_i and H_j in $k[Y]$, with deg $G_i < r$ and deg $H_j < s$ for $0 \leq i < q$ and $0 \leq j < q$ satisfying the equations above. Now we need to find G_q and H_q in $k[Y]$ with deg $G_q < r$ and deg $H_q < s$ satisfying the equation

$$F_q = \sum_{i+j=q} G_iH_j$$

The equation can be written as

$$G_0H_q + H_0G_q = U_q = F_q - \sum_{i+j=q,\, i,j<q} G_iH_j$$

Clearly, deg $U_q < n$. Since $gcd(G_0, H_0) = 1$, we can write $G_0H^* + H_0G^* = 1$ for some $G^*,\ H^* \in k[Y]$. Multiplying both sides by U_q, we get, $G_0H^*U_q + H_0G^*U_q = U_q$. Applying division algorithm we can write $U_qH^* = E_qH_0 + H_q$ with deg $H_q < s$. Set $G_q = U_qG^* + E_qG_0 \ \in k[Y]$ since deg $U_q < n$ we see that G_q thus obtained has degree $< r$. It follows that $U_q = G_0H_q + G_qH_0$. Thus by induction we have $F_q = \sum\limits_{i+j=q} G_iH_j$ for all $q \geq 0$ with deg $G_i < r$ and deg $H_j < s$ for all $i, j > 0$. So we have proved existence of G and H having the desired properties. To prove uniqueness, it is enough to note that

$$\begin{aligned}
&G_0H_q + G_qH_0 = G_0H_q^{'} + G_q^{'}H_0 \quad \text{for any } G_q^{'}, H_q^{'} \in k[Y] \\
&\Rightarrow G_0(H_q - H_q^{'}) = (G_q^{'} - G_q)H_0 \\
&\Rightarrow G_0 | (G_q^{'} - G_q) \quad \text{(as } G_0 \text{ and } H_0 \text{ are coprime)} \\
&\Rightarrow G_q^{'} - G_q = 0 \quad \text{(as deg } (G_q^{'} - G_q) < \text{deg } G_0 \text{ are coprime)} \\
&\Rightarrow G_q^{'} = G_q \quad \text{and so } H_q^{'} = H_q.
\end{aligned}$$

This completes the proof of Hensel's lemma. □

3.2 Abhyankar's Proof of Newton's theorem

We want to reduce to the case where Hensel's lemma can be applied. We make use of multiplication process i.e. if $\alpha_1, \alpha_2 \cdots, \alpha_n$ are roots of F, to find a polynomial whose roots are $\delta\alpha_1, \delta\alpha_2, \cdots, \delta\alpha_n$ for some non-zero element δ ; and the addition process, i.e. to find a polynomial whose roots are $\alpha_1 + \epsilon, \alpha_2 + \epsilon, \cdots, \alpha_n + \epsilon$. We first apply Shreedharacharya's trick of completing the n^{th} power. This amounts to making the addition process with $\epsilon = \frac{a(X)}{n}$ to get

$$\begin{aligned}
\tilde{F}(X, Y) &= F\left(X, Y + \frac{a_1(X)}{n}\right) \\
&= Y^n + \tilde{a_1}(X)Y^{n-1} + \cdots + \tilde{a_i}(X)Y^{n-i} + \cdots + \tilde{a_n}(X)
\end{aligned}$$

with $\tilde{a_i(X)} \in k((X))$ for all i and $\tilde{a_1}(X) = 0$. Now if the coefficient of Y^{n-1} is zero to begin with it remains zero after the multiplication process also. Next we transform $\tilde{F}$ into a monic polynomial with coefficients as power series. To do that we first note that, for any non-zero element $\delta = X^d$

$$\begin{aligned}
&F^*(X, Y) \\
&= X^{-dn}F(X, X^dY) \\
&= Y^n + a_1(X)X^{-d}Y^{n-1} + \cdots + a_i(X)X^{-di}Y^{n-i} + \cdots + a_n(X)X^{-dn}
\end{aligned}$$

We want to choose d so that the coefficients $a_i(X)X^{-di}$ are "power series" in X and atleast one of them has a non-zero value at $X = 0$. i.e. to say we want ord $a_i(X)X^{-di} \geq 0$ for all i with equality for atleast one value of i. Thus we have to take

$$d = \begin{matrix} min \\ 1 \leq i \leq n \end{matrix} \left(\frac{\text{ord } a_i(X)}{i}\right)$$

Thus found d may not be an integer but it certainly is a rational number. Let $d = \frac{\lambda}{\mu}$ with $\mu > 0$. Let $X = X'^{\mu}$ and

$$\begin{aligned} F'(X', Y) &= X'^{-\lambda n} F(X'^{\mu}, X'^{\lambda} Y) \\ &= Y^n + a_1'(X') Y^{n-1} + \cdots + a_i'(X') Y^{n-i} + \cdots + a_n'(X') \end{aligned}$$

where $a_i'(X') = X'^{-\lambda i} a_i(X'^{\mu}) \in k[[X']]$ for all i and $a_i'(0) \neq 0$ for some i. Thus by first applying Shreedharacharya's trick and then multiplication process we transform F into a monic polynomial, say $\widehat{F}(X', Y)$, of degree n in Y with coefficients in $k[[X']]$ such that the coefficient of Y^{n-1} is identically 0. But the value of the coefficient of Y^{n-i} is non-zero for some i. Therefore $\widehat{F}(0, Y)$ can be split into two non-constant coprime factors in $k[Y]$. Now Hensel's lemma can be applied to factor $\widehat{F}(X', Y)$ into polynomials of smaller degrees in Y. Since characterictic of k does not divide $n!$ we can use induction on Y- degree to factor $\widehat{F}$ into linear factors. Thus once $\widehat{F}$ is factored we can factor $F(X, Y)$ by a substitution of the form $X = T^m$. This proves Newton's theorem.

Chapter 4

Places and valuations

4.1 Places

Definition 4.1.1. *An algebraic function field F/K of one variable over K is an extension field $F \supseteq K$ such that F is a finite algebraic extension of $K(x)$ for some element $x \in F$ which is transcendental over K.*

Example 4.1.2. The simplest example of an algebraic function field is the rational function field; $F = K(X)$ for some $X \in F$ which is transcendental over K. Each element $0 \neq z \in K(X)$ has a unique representation

$$z = a \cdot \prod_i p_i(X)^{n_i}$$

where $0 \neq a \in K$ and each $p_i(X) \in K[X]$ is monic and irreducible, $n \in \mathcal{Z}$.

A function field F/K is often represented as a simple algebraic field extension of a rational function field $K(x)$; i.e., $F = K(x, y)$ where $\phi(y) = 0$ for some irreducible polynomial $\phi(T) \in K(x)[T]$.

If F/K is a non-rational function field, it is not so clear, whether every element $0 \neq z \in F$ admits a decomposition into irreducibles. It is not even clear what we mean by an irreducible element of F. In order to formulate these problems to arbitrary function fields we introduce valuation rings and places.

Definition 4.1.3. *A valuation ring of the function field F/K is a ring $\mathcal{O} \subsetneq F$ with the following properties:*
(1) $K \subsetneq \mathcal{O} \subsetneq F$, and
(2) for every $z \in F$ we have that $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

Let $\mathcal{O}^\times$ denote the set of units of $\mathcal{O}$. Let $P = \mathcal{O} \setminus \mathcal{O}^\times$. Then for $x \in P$ and $z \in \mathcal{O},\ xz \notin \mathcal{O}^\times$ as otherwise x will be a unit. So $xz \in P$. Let $x, y \in P$ then either $xy^{-1} \in \mathcal{O}$ or $yx^{-1} \in \mathcal{O}$. Without loss of generality assume that $xy^{-1} \in \mathcal{O} \implies 1 + xy^{-1} \in \mathcal{O}$. So that $x + y = y(1 + xy^{-1}) \in P$. Hence P is the ideal of all non-unit elements of $\mathcal{O}$. Thus $\mathcal{O}$ is a local ring.

The set $\bar{K} := \{z \in F \mid z \text{ is algebraic over K}\}$ is a subfield of F , since sums, products and inverses of algebraic elements are also algebraic. $\bar{K}$ is called the field of constants of F/K. We have $K \subseteq \bar{K} \subsetneq F$, and it is clear that F/K is a function field over $\bar{K}$. We say that K is algebraically closed in F (or K is the full constant field of F) if $\bar{K} = K$.

Remark 4.1.4. For the field $\bar{K}$ of constants of F/K we have $\bar{K} \subseteq \mathcal{O}$ and $\bar{K} \cap P = \{0\}$.
Let $z \in \bar{K}$. Assume that $z \notin \mathcal{O}$. Then $z^{-1} \in \mathcal{O}$. Since z^{-1} is algebraic over K, there are elements $a_1, \ldots, a_r \in K$ with $a_r(z^{-1})^r + \ldots + a_1 z^{-1} + 1 = 0$, hence $z^{-1}(a_r(z^{-1})^{r-1} + \ldots + a_1) = -1$. Therefore $z = -(a_r(z^{-1})^{r-1} + \ldots + a_1) \in K[z^{-1}] \subseteq \mathcal{O}$, so $z \in \mathcal{O}$. This is a contradiction to the assumption $z \notin \mathcal{O}$. Hence we have shown that $\bar{K} \subseteq \mathcal{O}$. Let $0 \neq y \in \bar{K} \cap P$. then $y^{-1} \in \bar{K}$ and hence $1 = y.y^{-1} \in P$, we get a contradiction! Hence the intersection must be trivial.

Theorem 4.1.5. *Let $\mathcal{O}$ be a valuation ring of the algebraic function field F/K and let P be its unique maximal ideal. Then P is principal. Further if $P = \pi\mathcal{O}$ then each $0 \neq z \in F$ has a unique representation of the form $z = \pi^n u$ for some $n \in \mathcal{Z}$ and $u \in \mathcal{O}^\times$. Also every non-zero ideal I is of the form $I = \pi^n\mathcal{O}$ for some $n \in \mathbb{N}$ and hence $\mathcal{O}$ is a P.I.D.*

A ring having the above properties is called a discrete valuation ring. We prove a lemma before going to the proof of the theorem.

Lemma 4.1.6. *Let $\mathcal{O},\ P$ as in theorem and $0 \neq x \in P$. Let $x_1, x_2, \ldots, x_n \in P$ be such that $x_1 = x$ and $x_i \in x_{i+1}P$ for $i = 1, \ldots, n-1$, Then we have*

$$n \leq [F : K(x)] < \infty.$$

Proof. By Remark [4.1.4] x is transcendental. Now by definition F is a finite algebraic extention of $K(y)$ for some transcendental y. Thus x must satisfy a non-constant polynomial $f(X, Y)$ over $K(y)$. Now f can't be independent of y as x is given to be transcendental over K. Another way of stating this is y satisfies a non-constant polynomial f over $K(x)$. So that $[K(x, y) : K(x)] < \infty$. Again since

$$[F : K(x, y)] \cdot [K(x, y) : K(y)] = [F : K(y)] < \infty.$$

Hence $[F : K(x, y)] < \infty$ and therefore,

$$[F : K(x)] = [F : K(x, y)] \cdot [K(x, y) : K(x)] < \infty$$

(Observe that this is true for any transcendental element of F.)
So we have $F/K(x)$ is a finite extension. It is sufficient to prove that x_i's are linearly independent over $K(x)$. Suppose $\sum_{i=1}^{n} f_i(x)x_i = 0$ with each $f_i(x) \in K(x)$. We can clear denominators and assume that each f_i is a polynomial in x. We can further assume x does not divide all of them. Put $a_i := f_i(0)$ so that $a_j \neq 0$ for some j. Choose j such that $a_i = 0\ \forall i > j$. Now,

$$-f_j(x)x_j = \sum_{i \neq j} f_i(x)x_i$$

with each $f_i(x) \in \mathcal{O}$ as $x \in P \subseteq \mathcal{O}$. $f_i(x) = xg_i(x)\ \ \forall i > j$ and $x_i \in x_j P$ for $i < j$. Thus we have,

$$-f_j(x) = \sum_{i<j} f_i(x)x_i x_j^{-1} + \sum_{i>j} xg_i(x)x_i x_j^{-1}$$

All summands of the right hand side belong to P, therefore $f_j(x) \in P$. On the other hand $f_j(x) = a_j + g_j(x) \implies a_j = f_j(x) - xg_j(x) \in P \implies a_j \in P \cap K$ contradictory to Remark [4.1.4] as $a_j \neq 0$. So $x_1, x_2, \ldots, x_n$ are linearly independent and the inequality holds.

$\square$

Proof. of the Theorem : Assume that $\mathcal{O}$ is not principal. Choose $x_1 \in P$, as $P \neq x_1\mathcal{O}$, choose $x_2 \in P \setminus x_1\mathcal{O}$. Then $x_2 x_1^{-1} \notin \mathcal{O}$ and hence $x_2^{-1}x_1 \in P \implies x_1 \in x_2 P$. By induction one obtains an infinite sequence $x_1, x_2, \ldots$ in P such that $x_i \in x_{i+1}P \ \ \forall i$ which is contradictory to our previous lemma.

As z or z^{-1} is in $\mathcal{O}$ we can assume that $z \in \mathcal{O}$. If $z \in \mathcal{O}^\times$ then $z = \pi^0 z$. Let $z \in P$. There is a maximal $m \geq 1$ with $z \in \pi^m\mathcal{O}$, since the length of a sequence

$$x_1 = z,\ x_2 = \pi^{m-1},\ x_3 = \pi^{m-2},\ \cdots, x_m = \pi$$

is bounded by our previous lemma. So $z = \pi^m u$ where $u \in \mathcal{O}$. Now u must be a unit as otherwise if $u \in P$ then $u = \pi t$ and thus $z = \pi^{m+1}t$ contradictory to the maximality of m. It is clear that such a representation is unique as otherwise some positive power of π will be a unit.

Let I be a non-zero ideal of $\mathcal{O}$. The set $A := \{r \in \mathbb{N} \mid \pi^r \in I\}$ is non-empty (in fact, if $0 \neq x \in I$ then $x = \pi^r u$ with $u \in \mathcal{O}^\times$ and therefore $\pi^r = xu^{-1} \in I$). Put $n := min(A)$. We claim that $I = \pi^n\mathcal{O}$. The inclusion $I \supseteq \pi^n\mathcal{O}$ is trivial since $\pi^n \in I$. Conversely let $0 \neq y \in I$. We have $y = \pi^s w$ with $w \in \mathcal{O}^\times$ and $s \geq 0$, so $\pi^s \in I$ and $s \geq n$. It follows that $y = \pi^n \pi^{s-n} w \in \pi^n\mathcal{O}$.

□

Definition 4.1.7.
*(a) A **place** P of the function field F/K is the maximal ideal of some valuation ring $\mathcal{O}$ of F/K. Every element $t \in P$ such that $P = t\mathcal{O}$ is called a prime element or a uniformizing parameter for P.*
(b) $\mathbb{P}_F := \{P \mid P$ is a place of $F/K\}$.

Observe for $z \in F$, z or $z^{-1} \in \mathcal{O}$. If $z \in P \implies z^{-1} \notin \mathcal{O}$. Again if $z^{-1} \notin \mathcal{O}$ then $z \in \mathcal{O}$ and z is not a unit, so $z \in P$. So $\mathcal{O}$ is completely determined by P, namely $\mathcal{O} := \{z \in F \mid z^{-1} \notin P\}$. Hence $\mathcal{O}_P = \mathcal{O}$ is called the *valuation ring of the place P*.

Definition 4.1.8. *A discrete valuation of F/K is a function $v : F \to \mathbb{Z} \cup \{\infty\}$ with the following properties*
(1) $v(x) = \infty \Leftrightarrow x = 0$.
(2) $v(xy) = v(x) + v(y)$ for all $x, y \in F$.
(3) $v(x + y) \geq min\{v(x),\ v(y)\}$ for all $x, y \in F$.
(4) There exists an element $z \in F$ with $v(z) = 1$.
(5) $v(a) = 0$ for all $0 \neq a \in K$.

One can define a norm using this valuation. Fix a real number $0 < c < 1$. Define the function $|\ \ |_v : F \to \mathbb{R}$ by

$$|z|_v = \begin{cases} c^{v(z)} & \text{if } z \neq 0 \\ 0 & \text{if } z = 0 \end{cases}$$

Lemma 4.1.9. ***(Strict Triangle inequality)*** *Let v be a discrete valuation of F/K and let $x, y \in F$ with $v(x) \neq v(y)$. Then $v(x + y) = min\{v(x),\ v(y)\}$.*

Proof. Observe that $v(ay) = v(y)$ for $0 \neq a \in K$ (by (2) and (5)), in particular $v(-y) = v(y)$. Since $v(x) \neq v(y)$ we can assume $v(x) < v(y)$. Suppose that $v(x+y) \neq min\{v(x),\ v(y)\}$, so $v(x+y) > v(x)$ by (3). Then we obtain $v(x) = v((x + y) - y) \geq min\{v(x + y),\ v(y)\} > v(x)$, a contradiction! □

Definition 4.1.10. *For $P \in \mathbb{P}_F$ we define a valuation $v_P : F \to \mathbb{Z} \cup \{\infty\}$ as follows :*
Choose a uniformizing parameter π for P. By theorem [4.1.5] every $0 \neq z \in F$ has a unique representation $z = \pi^n u$ with $u \in \mathcal{O}^\times$ and $n \in \mathcal{Z}$. Define $v_P(z) = n$ and $v_P(0) = \infty$.

v_P is easily seen to be a valuation. Observe the definition doesn't depend on the choice of π, for let $P = \pi\mathcal{O} = \pi'\mathcal{O}$. Then $\pi = \pi'^n u'$ for some $u' \in \mathcal{O}^\times$ and $\pi' = \pi^m u$ for some $u \in \mathcal{O}^\times$. Thus $\pi = \pi^{mn} u^m u'$, so $mn = 1$ as m, n are both positive, $m = n = 1$ and thus $z = \pi^n w \implies z = \pi'^n w'$

Remark 4.1.11.

$$\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\},$$
$$\mathcal{O}_P^\times = \{z \in F \mid v_P(z) = 0\},$$
$$P = \{z \in F \mid v_P(z) > 0\}.$$

Observe if $z \in P$ then clearly $v_P(z) > 0$. Conversely if $v_P(z) > 0$ then $z = \pi^n u \in \pi\mathcal{O} = P$ as $n > 0$, hence the third assertion. If $z \in \mathcal{O}^\times$ then $v_P(z) = 0$. Conversely, let $v_P(z) = 0$. Consider $z^{-1} \in F$, $v_P(1) = 0 = v_P(z \cdot z^{-1}) = v_P(z) + v_P(z^{-1}) \implies v_P(z^{-1}) = 0$. Now z or $z^{-1} \in \mathcal{O}$. Say $z \in \mathcal{O}$. But from previous part z can't be in P. So $z \in \mathcal{O}^\times$. Thus the second and consequently the first assertion follows.

Remark 4.1.12. An element $x \in F$ is a uniformizing parameter for P if and only if $v_P(x) = 1$.

Theorem 4.1.13. *Suppose that v is a discrete valuation of F/K. Then the set $P := \{z \in F \mid v(z) > 0\}$ is a place of F/K, and $\mathcal{O}_P = \{z \in F \mid v(z) \geq 0\}$ is the corresponding valuation ring.*

Proof. Let $0 \neq z \in F$. Then $v(z) \geq 0$ or $v(z^{-1}) = -v(z) \geq 0$. So z or $z^{-1} \in \mathcal{O}_P$ and hence $\mathcal{O}_P$ is a valuation ring. It is easy to see that the defined P is an ideal of $\mathcal{O}_P$. We need only show that units in $\mathcal{O}_P$ has valuation 0. Which is obvious, for if $z,\ z^{-1} \in \mathcal{O}_P$ then $0 = v(1) = v(zz^{-1}) = v(z) + v(z^{-1})$. Now as both $v(z),\ v(z^{-1}) \geq 0$, hence $v(z) = 0 = v(z^{-1})$. So P is the ideal of all non-units, and hence is a place of F/K. □

Theorem 4.1.14. *Every valuation ring $\mathcal{O}_P$ of F/K is a maximal proper subring of F.*

Proof. Let $\mathcal{O}$ be a valuation ring of F/K, P its maximal ideal, v_P the discrete valuation associated to P and $z \in F \backslash \mathcal{O}$. We have to show that $F = \mathcal{O}[z]$. Consider an arbitrary element $y \in F$; then $v_P(yz^{-k}) \geq 0$ for sufficiently large $k \geq 0$ (note that $v_P(z^{-1}) > 0$ since $z \notin \mathcal{O}$). Consequently $w := yz^{-k} \in \mathcal{O}$ and $y = wz^k \in \mathcal{O}[z]$. □

Definition 4.1.15. *Let $P \in \mathbb{P}_F$.*
(a) $F_P := \mathcal{O}_P/P$ is the residue class field of P . The map $x \mapsto x + P$ for $x \in \mathcal{O}_P$ and otherwise $x \mapsto \infty$ from F to $F_P \cup \{\infty\}$ is called the residue class map with respect to P .
(b) deg P $:= [F_P : K]$ is called the degree of P . A place of degree one is also called a rational place of F/K.

We know that $K \subseteq \mathcal{O}_P$ and $K \cap P = 0$, so the residue class map induces a canonical embedding of K into F_P . Henceforth we shall always consider K as a subfield of F_P via this embedding. Hence (b) makes sense.

Proposition 4.1.16. *If P is a place of F/K and $0 \neq x \in P$ then*

$$\textit{deg } P \leq [F : K(x)] < \infty$$

.

Proof. It is sufficient to show that any elements $z_1, \dots, z_n \in \mathcal{O}_P$, whose residue classes are linearly independent over K, are linearly independent over $K(x)$. Suppose there is a non-trivial linear combination

$$\sum_{i=1}^{n} \phi_i(x) z_i = 0 \tag{4.1}$$

with $\phi_i(x) \in K(x)$. W.l.o.g. we assume that the $\phi_i(x)$ are polynomials in x and not all of them are divisible by x; i.e., $\phi_i(x) = a_i + x g_i(x)$ with $a_i \in K$ and $g_i(x) \in K[x]$, not all $a_i = 0$. Since $x \in P$ and $g_i(x) \in \mathcal{O}_P$, $\phi_i(x) + P = a_i + P = a_i$. Applying the residue class map to (4.1) we obtain,

$$0 + P = \sum_{i=1}^{n} (\phi_i(x) + P)(z_i + P) = \sum_{i=1}^{n} a_i (z_i + P)$$

This contradicts the linear independence of $z_1 + P, z_2 + P, \dots, z_n + P$ over K. □

Remark 4.1.17. Let P be a rational place of F/K i.e., deg P = 1. Then we have $F_P = K$, and the residue class map maps $F \to K \cup \{\infty\}$. We can read an element $z \in F$ as a function

$$z : \begin{cases} \mathbb{P}_F & \to K \cup \{\infty\} \\ P & \mapsto z + P \end{cases} \tag{4.2}$$

We will use $z(P) = z + P$. This is why F/K is called a function field. The elements of K, interpreted as functions in the sense of (4.2), are constant functions. For this reason K is called the constant field of F . Also the following terminology is justified.

Definition 4.1.18. *Let $z \in F$ and $P \in \mathbb{P}_F$. If $v_P(z) = m > 0$, P is said to be a zero of z of order m; if $v_P(z) = -m < 0$, P is said to be a pole of z of order m.*

Next we focus on existence of places of F/K.

Theorem 4.1.19. *Let F/K be a function field and let R be a subring of F with $K \subseteq R \subseteq F$. Suppose that I is a non-zero proper ideal of R. Then there is a place $P \in \mathbb{P}_F$ such that $I \subseteq P$ and $R \subseteq \mathcal{O}_P$.*

Proof. Consider the set

$$\mathcal{F} := \{S \mid S \text{ is a subring of } F \text{ with } R \subseteq S \text{ and } IS \neq S\}$$

As $R \in \mathcal{F}$, $\mathcal{F} \neq \emptyset$. $\mathcal{F}$ is partially ordered with respect to inclusion. Consider any chain $\{C_i\}$ in $\mathcal{F}$. Let $C = \bigcup_i C_i$. We will show that $IC \neq C$. Suppose they are equal. Then $1 = \sum_{j=1}^{k} a_j c_j$ for some $a_j \in I$ and $c_j \in C$. Since $\{C_i\}$ is a chain, there exists r such that $c_1, c_2, \dots c_n \in C_r$. But then $1 \in IC_r$, a contradiction. Thus by Zorn's lemma $\mathcal{F}$ contains a maximal element say $\mathcal{O}$. We want to show that $\mathcal{O}$ is a valuation ring of F/K.
Since $I\mathcal{O} \neq \mathcal{O}$, $I \subseteq \mathcal{O} \setminus \mathcal{O}^\times$. Suppose there exists an element $z \in F$ with niether z nor $z^{-1} \in \mathcal{O}$. Then $I\mathcal{O}[z] = \mathcal{O}[z]$ and $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$. Thus we can find $a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_m \in I\mathcal{O}$ such that,

$$1 = a_0 + a_1 z + \dots + a_n z^n \tag{4.3}$$

$$1 = b_0 + b_1 z^{-1} + \dots + b_m z^{-m} \tag{4.4}$$

We can assume that $n,\ m$ as in (4.3) and (4.4) are minimal. Suppose $m \leq n$. We multiply (4.3) by $1 - b_0$ and (4.4) by $a_n z^n$ and obtain

$$1 - b_0 = (1 - b_0)a_0 + (1 - b_0)a_1 z + \dots + (1 - b_0)a_n z^n \qquad \text{and}$$

$$0 = (b_0 - 1)a_n z^n + b_1 a_n z^{n-1} + \cdots b_m a_n z^{n-m}$$

Adding this equations we get, $1 = c_0 + c_1 z + \cdots + c_{n-1} z^{n-1}$. this is a contradiction to the minimality of n. Thus $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$. Hence $\mathcal{O}$ is a valuation ring of F/K

□

Corollary 4.1.20. *Let F/K be a function field, $z \in F$ transcendental over K. Then z has at least one zero and one pole. In particular $\mathbb{P}_F \neq \emptyset$.*

Proof. Consider the ring $R = K[z]$ and the ideal $I = zK[z]$. By previous theorem, there is a place $P \in \mathbb{P}_F$ with $z \in P$, hence P is a zero of z. The same argument proves that z^{-1} has a zero $Q \in \mathbb{P}_F$. Then Q is a pole of z. □

4.2 The Field of Rational Functions

For a better understanding of places in arbitrary function fields, we first investigate it in the cae of rational function field $F = K(X)$. Given an irreducible monic polynomial $p(X) \in K[X]$ we consider the valuation ring

$$\mathcal{O}_{p(X)} := \left\{ \frac{f(X)}{g(X)} \middle| \; f(X),\ g(X) \in K[X],\ p(X) \nmid g(X) \right\}$$

of $K(X)/K$ with maximal ideal

$$P_{p(X)} := \left\{ \frac{f(X)}{g(X)} \middle| \; f(X),\ g(X) \in K[X],\ p(X) \nmid g(X),\ p(X) \mid f(X) \right\} \tag{4.5}$$

There is another valuation ring of $K(X)/K$, namely

$$\mathcal{O}_\infty = \left\{ \frac{f(X)}{g(X)} \middle| \; f(X),\ g(X) \in K[X],\ \deg f(X) \leq \deg g(X) \right\}$$

With maximal ideal P_∞ when the inequality is strict. This is called *infinite place* of $K(X)$.

Proposition 4.2.1. *Let $F = K(X)$ be the rational function field.*
(a) Let $P = P_p(X) \in \mathbb{P}_{K(X)}$ be the place defined in (4.5) , where $p(X) \in K[X]$ is an irreducible polynomial. Then $p(X)$ is a uniformizing parameter for P , and the corresponding valuation v_P can be described as follows: if $z \in K(X)\ \{0\}$ is written in the form $z = p(X)^n \cdot (f(x)/g(x))$ with $n \in \mathcal{Z}$, $f(X), g(X) \in K[X]$, $p(X) \nmid f(X)$ and $p(X) \nmid g(X)$, then $v_P(z) = n$. The residue class field $K(X)_P = \mathcal{O}_P/P$ is isomorphic to $K[X]/(p(X))$; an isomorphism is given by

$$\phi \;:\; \begin{cases} K[X]/(p(X)) & \rightarrow \quad K(X)_P, \\ f(X) \textit{ mod } p(X) & \mapsto \quad f(X)(P) \end{cases}$$

Consequently deg $P =$ deg $p(X)$.

(b) In the special case $p(X) = X - \alpha$ with $\alpha \in K$ the degree of $P = P_\alpha$ is one, and the residue class map is given by

$$z(P) = z(\alpha) \quad \textit{for } z \in K(X)$$

where $z(\alpha)$ is defined as follows: write $z = f(X)/g(X)$ with relatively prime polynomials $f(X), g(X) \in K[X]$. Then

$$z(\alpha) = \begin{cases} f(\alpha)/g(\alpha) & \textit{if } g(\alpha) \neq 0 \\ \infty & \textit{if } g(\alpha) = 0. \end{cases}$$

Proof. (a) We only prove the assertion about the residue class field. Rest is clear. First we consider the ring homomorphism

$$\varphi : K[X] \to K(X)_P \quad \text{given by}$$
$$f(X) \mapsto f(X)(P)$$

Now ker $\varphi = (p(X))$. Again φ is surjective, for, if $z \in \mathcal{O}_{p(x)}$ we can write $z = u(X)/v(X)$ with $u(X), v(X) \in K[X]$ such that $p(X) \nmid v(X)$. Thus there are gcd $(p(X), v(X)) = 1$, so $\exists\ a(X), b(X) \in K[X]$ with $a(X)p(X) + b(X)v(X) = 1$, therefore

$$z = 1 \cdot z = \frac{a(X)b(X)}{v(X)} p(X) + b(X)u(X)$$

and $z(P) = (b(x)u(x))(P)$ is in the image of φ. Thus φ induces an isomorphism ϕ of $K[X]/(p(X))$ onto $K(X)_P$.

(b) Now $P = P_\alpha$ with $\alpha \in K$. If $f(X) \in K[X]$ then $(X - \alpha) \mid (f(X) - f(\alpha))$, hence $f(X)(P) = (f(X)f(\alpha))(P) + f(\alpha)(P) = f(\alpha)$. An arbitrary element $z \in \mathcal{O}_P$ can be written as $z = f(X)/g(X)$ with polynomials $f(X), g(X) \in K[X]$ and $(x\alpha) \nmid g(X)$, therefore $g(X)(P) = g(\alpha) \neq 0$ and

$$z(P) = \frac{f(X)(P)}{g(X)(P)} = \frac{f(\alpha)}{g(\alpha)} = z(\alpha)$$

□

Proposition 4.2.2. *let $P = P_\infty$ be the infinite place of $K(X)/K$. Then deg $P_\infty = 1$. A uniformizing parameter for P_∞ is $\pi = 1/X$. The corresponding discrete valuation v_∞ is given by*

$$v_\infty(f(X)/g(X)) = \textit{ deg } g(X) \textit{ deg } f(X)$$

, where $f(X), g(X) \in K[X]$. The residue class map corresponding to P_∞ is determined by $z(P_\infty) = z(\infty)$ for $z \in K(X)$, where $z(\infty)$ is defined as: if

$$z = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0} \quad \textit{with } a_n, b_m \neq 0$$

then

$$z(\infty) = \begin{cases} \frac{a_n}{b_m} & \textit{if } \ n = m, \\ 0 & \textit{if } \ n < m, \\ \infty & \textit{if } \ n > m. \end{cases}$$

Proof. We will only show that $1/X$ is a uniformizing parameter for P_∞ . Clearly we have that $1/X \in P_\infty$. Consider some element $z = f(x)/g(x) \in P_\infty$ i.e., deg $f <$ deg g. Then $z = \frac{1}{X} \cdot \frac{Xf}{g}$ with deg $(Xf) \leq$ deg g. This proves that $z \in (1/X)\mathcal{O}_\infty$, hence $1/X$ generates the ideal P_∞. The rest of the proposition follows. □

Remark 4.2.3. K is the full constant field of $K(X)/K$.

Proof. Choose a place P of $K(X)/K$ of degree one (e.g. $P = P_\alpha$ with $\alpha \in K$). The field $\bar{K}$ of constants of $K(X)$ is embedded into the residue class field $K(X)_P$, hence $K \subseteq \bar{K} \subseteq K(X)_P = K$. $\square$

Theorem 4.2.4. *The only places of the rational function field $K(X)/K$ are the places $P_{p(X)}$ and P_∞.*

Proof. Let P be a place of $K(X)/K$. We prove the theorem for following two cases :
Case - I : $X \in \mathcal{O}_P$. Then $K[X] \subseteq \mathcal{O}_P$. Let $I = K[X] \cap P$. This is an ideal of $K[X]$, in fact for polynomials f, g if $fg \in I \implies fg \in P$. P is a maximal ideal hence prime, so $f \in P$ or $g \in P \implies f \in I$ or $g \in I$. So I is a prime ideal. The residue class map induces an embedding $K[X]/I \hookrightarrow K(X)_P$ and thus $I \neq \{0\}$. Thus there is a irreducible monic polynomial $p(X)$ such that $I = (p(X))$ in $K[X]$. For every $g(X) \in K[X]$ with $p(X) \nmid g(X)$, $g(X) \notin I$, so $g(X) \notin P \implies 1/g(X) \in \mathcal{O}_P$. We conclude that

$$\mathcal{O}_{p(X)} = \left\{ \frac{f(X)}{g(X)} \middle| \; f(X),\; g(X) \in K[X],\; p(X) \nmid g(X) \right\} \subseteq \mathcal{O}_P$$

As we have already shown, valuation rings are maximal proper subrings of $K(X)$, we must have

$$\mathcal{O}_P = \mathcal{O}_{p(X)} \quad \text{and hence } P = P_{p(X)}$$

Case - II: Now suppose $X \notin \mathcal{O}_P$. Then we must have $X^{-1} \in \mathcal{O}_P$ and hence $K[X^{-1}] \subseteq \mathcal{O}_P$. Further $X^{-1} \in P$ and thus $X^{-1} \in P \cap K[X^{-1}]$ and $P \cap K[X^{-1}] = X^{-1}K[X^{-1}]$. As in case I,

$$\begin{aligned}
\mathcal{O}_P &\supseteq \left\{ \frac{f(X^{-1})}{g(X^{-1})} \middle| \; f(X^{-1}),\; g(X^{-1}) \in K[X^{-1}],\; X^{-1} \nmid g(X^{-1}) \right\} \\
&= \left\{ \frac{a_0 + a_1 X^{-1} + \cdots + a_n X^{-n}}{b_0 + b_1 X^{-1} + \cdots + b_m X^{-m}} \middle| \; b_0 \neq 0 \right\} \\
&= \left\{ \frac{a_0 X^{m+n} + \cdots + a_n X^m}{b_0 X^{m+n} + \cdots + b_m X^n} \middle| \; b_0 \neq 0 \right\} \\
&= \left\{ \frac{u(X)}{v(X)} \middle| u(X), v(X) \in K[X],\; \deg u(X) \leq \deg v(X) \right\} \\
&= \mathcal{O}_\infty.
\end{aligned}$$

Again by maximality argument, $\mathcal{O}_P = \mathcal{O}_\infty$ and $P = P_\infty$. $\square$

4.3 Independence of Valuations

Essentially the main result of this section says the following: If $v_1, \ldots, v_n$ are pairwise distinct discrete valuations of F/K and $z \in F$, and if we know the values $v_1(z), \ldots, v_{n-1}(z)$, then we cannot conclude anything about $v_n(z)$.

Theorem 4.3.1. ***(Weak Approximation Theorem).*** *Let F/K be a function field, $P_1, ..., P_n \in \mathbb{P}_{\mathbb{F}}$ pairwise distinct places of F/K, $x_1, ..., x_n \in F$ and $r_1, ..., r_n \in \mathcal{Z}$. Then there is some $x \in F$ such that*

$$v_{P_i}(x - x_i) = r_i \;\; for \;\; i = 1, ..., n.$$

Proof. We do the proof following several steps. For simplicity we write v_i instead of v_{P_i}.

Step 1. There is some $u \in F$ with $v_1(u) > 0$ and $v_i(u) < 0$ for $i = 2, ..., n$.
Proof of Step 1. By induction. For $n = 2$ we observe that $\mathcal{O}_{P_1} \subsetneq \mathcal{O}_{P_2}$ and vice versa, since valuation

rings are maximal proper subrings of F. Therefore we can find $y_1 \in \mathcal{O}_{P_1} \setminus \mathcal{O}_{P_2}$ and $y_2 \in \mathcal{O}_{P_2} \setminus \mathcal{O}_{P_1}$. Then $v_1(y_1) \geq 0,\ v_2(y_1) < 0,\ v_1(y_2) < 0$ and $v_2(y_2) \geq 0$. The element $u := y_1/y_2$ has the property $v_1(u) > 0\ , v_2(u) < 0$ as desired.

For $n > 2$ we have by induction hypothesis an element y with $v_1(y) > 0, v_2(y) < 0, ..., v_{n-1}(y) < 0$. If $v_n(y) < 0$ the proof is finished. In case $v_n(y) \geq 0$ we choose z with $v_1(z) > 0, v_n(z) < 0$ and put $u := y + z^r$. Here $r \geq 1$ is chosen in such a manner that $r \cdot v_i(z) \neq v_i(y)$ for $i = 1, ..., n-1$ (this is obviously possible). It follows that $v_1(u) \geq min\{v_1(y), r \cdot v_1(z)\} > 0$ and $v_i(u) = min\{v_i(y), r \cdot v_i(z)\} < 0$ for $i = 2, ..., n$ (observe that the Strict Triangle Inequality applies).

Step 2. There is some $w \in F$ such that $v_1(w-1) > r_1$ and $v_i(w) > r_i$ for $i = 2, ..., n$.
Proof of Step 2. Choose u as in Step 1 and put $w := (1+u^s)^{-1}$. We have, for sufficiently large $s \in \mathbb{N},\ v_1(w-1) = v_1(-u^s(1+u^s)^{-1}) = s \cdot v_1(u) > r_1$, and $v_i(w) = -v_i(1+u^s) = -s \cdot v_i(u) > r_i$ for $i = 2, ..., n$.
Step 3. Given $y_1, ..., y_n \in F$, there is an element $z \in F$ with $v_i(z - y_i) > r_i$ for $i = 1, ..., n$.
Proof of Step 3. Choose $s \in \mathcal{Z}$ such that $v_i(y_j) \geq s$ for all $i, j \in \{1, ..., n\}$.
By Step 2 there are $w_1, ..., w_n$ with

$$v_i(w_i - 1) > r_i - s \text{ and } v_i(w_j) > r_i - s \text{ for } j \neq i.$$

Then $z := \sum_{j=1}^{n} y_j w_j$ has the desired properties.
Now we are in a position to finish the proof of Theorem 1.3.1. By Step 3 we can find $z \in F$ with $v_i(z - x_i) > r_i,\ i = 1, ..., n$. Next we choose z_i with $v_i(z_i) = r_i$ (this is trivially done). Again by Step 3 there is z' with $v_i(z' - z_i) > r_i$ for $i = 1, ..., n$. It follows that

$$v_i(z') = v_i((z' - z_i) + z_i) = min\{v_i(z' - z_i), v_i(z_i)\} = r_i.$$

Let $x := z + z'$. Then

$$v_i(x - x_i) = v_i((z - x_i) + z') = min\{v_i(z - x_i), v_i(z')\} = r_i.$$

□

Corollary 4.3.2. *Every function field has infinitely many places.*

Proof. Suppose there are only finitely many places, say $P_1, ..., P_n$. By Weak Approximation theorem we can find a non-zero element $x \in F$ with $v_{P_i}(x) > 0$ for $i = 1, ..., n$. Then x is transcendental over K since it has zeros. But x has no pole; this is a contradiction to Corollary 4.1.20. □

Proposition 4.3.3. *Let F/K be a function field and let $P_1, ..., P_r$ be zeros of the element $x \in F$. Then*

$$\sum_{i=1}^{r} v_{P_i}(x) \cdot degP_i \leq [F : K(x)].$$

Proof. We set $v_i := v_{P_i},\ f_i :=$ deg P_i and $e_i := v_i(x)$. Using Weak approximation theorem for each i (i.e. choose $x_i = 0,\ r_i = 1,\ r_j = 0\ \forall j \neq i$) we can get for all i, an element t_i with

$$v_i(t_i) = 1 \text{ and } v_k(t_i) = 0 \ \text{ for } k \neq i.$$

Next we choose $s_{i1}, ..., s_{if_i} \in \mathcal{O}_{P_i}$ such that $s_{i1}(P_i), ..., s_{if_i}(P_i)$ form a basis of the residue class field F_{P_i} over K. By a weak application of Theorem 4.3.1 we can find $z_{ij} \in F$ such that the following holds for all i, j :

$$v_i(s_{ij} - z_{ij}) > 0 \ \text{ and } \ v_k(z_{ij}) \geq e_k \ \text{ for } k \neq i.$$

We claim that the elements

$$t_i^a \cdot z_{ij}, 1 \le i \le r, 1 \le j \le f_i, 0 \le a < e_i$$

are linearly independent over $K(x)$. Their number is equal to $\sum_{i=1}^{r} f_i e_i = \sum_{i=1}^{r} v_{P_i}(x) \cdot \deg P_i$, so the proposition will follow from this claim.
Suppose there is a non-trivial linear combination

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \phi_{ija}(x) t_i^a z_{ij} = 0 \tag{4.6}$$

over $K(x)$. W.l.o.g. we can assume that $\phi_{ija}(x) \in K[x]$ and not all $\phi_{ija}(x)$ are divisible by x. Then there are indices $k \in \{1, ..., r\}$ and $c \in \{0, ..., e_k - 1\}$ such that

$$x | \phi_{kja}(x) \text{ for all } a < c \text{ and all } j \in \{1, ..., f_k\}, \text{ and}$$

$$x \nmid \phi_{kjc}(x) \text{ for some } j \in \{1, ..., f_k\}$$

Multiplying (4.6) by t_k^{-c} we obtain

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \phi_{ija}(x) t_i^a t_k^{-c} z_{ij} = 0 \tag{4.7}$$

For $i \neq k$ all summands of (4.7) are in P_k, since

$$v_k(\phi_{ija}(x) t_i^a t_k^{-c} z_{ij}) = v_k(\phi_{ija}(x)) + a v_k(t_i) - c v_k(t_k) + v_k(z_{ij})$$

$$\ge 0 + 0 - c + e_k > 0.$$

For $i = k$ and $a < c$ we have

$$v_k(\phi_{ija}(x) t_k^{a-c} z_{ij}) \ge e_k + a - c \ge e_k - c > 0.$$

(Note that $x | \phi_{kja}(x)$ and therefore $v_k(\phi_{kja}(x)) \ge e_k$.) For $i = k$ and $a > c$,

$$v_k(\phi_{ija}(x) t_k^{a-c} z_{ij}) \ge a - c > 0.$$

Combining the above with (1.15) gives

$$\sum_{j=1}^{f_k} \phi_{kjc}(x) z_{kj} \in P_k.$$

Observe that $\phi_{kjc}(x)(P_k) \in K$, and not all $\phi_{kjc}(x)(P_k) = 0$ (by (1.14)), so (1.16) yields a non-trivial linear combination

$$\sum_{j=1}^{f_k} \phi_{kjc}(x)(P_k) \cdot z_{kj}(P_k) = 0$$

over K. This is a contradiction, as $z_{k1}(P_k), ..., z_{kf_k}(P_k)$ form a basis of F_{P_k}/K. □

Corollary 4.3.4. *In a function field F/K every element $0 \neq x \in F$ has only finitely many zeros and poles.*

Proof. If x is constant, x has neither zeros nor poles. If x is transcendental over K, the number of zeros is $\le [F : K(x)]$. The same argument shows that x^{-1} has only a finite number of zeros. □

Chapter 5

Divisors

From now on, F/K will always denote an algebraic function field of one variable such that K is the full constant field of F/K.

Definition 5.0.1. *The divisor group of F/K is defined as the (additively written) free abelian group which is generated by the places of F/K; it is denoted by Div(F). The elements of Div(F) are called divisors of F/K. In other words, a divisor is a formal sum*

$$D = \sum_{P \in \mathbb{P}_F} n_P P \quad \textit{with} \quad n_P \in \mathbb{Z}, \textit{ and all but finitely many } n_P = 0.$$

The support of D is defined as

$$\textit{supp } D := \{P \in \mathbb{P}_F \mid n_P \neq 0\}.$$

It will often be found convenient to write

$$D = \sum_{P \in S} n_P P,$$

where $S \subseteq \mathbb{P}_F$ is a finite set with $S \supseteq$ supp D . A divisor of the form $D = P$ with $P \in \mathbb{P}_F$ is called a prime divisor. Two divisors $D = \sum n_P P$ and $D' = \sum n'_P P$ are added coefficientwise,

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P)P.$$

The zero element of the divisor group Div(F) is the divisor

$$0 := \sum_{P \in \mathbb{P}_F} r_P P \ \ , \ \ \textit{all } \ r_P = 0.$$

For $Q \in \mathbb{P}_F$ and $D = \sum n_P P \in$ Div(F) we define $v_Q(D) := n_Q$, therefore

$$\textit{supp } D = \{P \in \mathbb{P}_F | v_P(D) \neq 0\} \ \textit{ and } D = \sum_{P \in \textit{supp } D} v_P(D) \cdot P.$$

A partial ordering on Div(F) is defined by

$$D_1 \leq D_2 : \Longleftrightarrow \ v_P(D_1) \leq v_P(D_2) \textit{ for all } P \in \mathbb{P}_F.$$

If $D_1 \leq D_2$ and $D_1 \neq D_2$ we will also write $D_1 < D_2$. A divisor $D \geq 0$ is called positive (or effective). The degree of a divisor is defined as

$$\textit{deg } D := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot \textit{deg } P,$$

and this yields a homomorphism deg : Div$(F) \to \mathcal{Z}$.

By Corollary 4.3.4 a nonzero element $x \in F$ has only finitely many zeros and poles in $\mathbb{P}_F$. Thus the following definition makes sense.

Definition 5.0.2. *Let $0 \neq x \in F$ and denote by Z (resp. N) the set of zeros (resp. poles) of x in $\mathbb{P}_F$. Then we define*

$$(x)_0 := \sum_{P \in Z} v_P(x)P, \text{ the zero devisor of } x,$$

$$(x)_\infty := \sum_{P \in N} (-v_P(x))P, \text{ the pole divisor of } x,$$

$$(x) := (x)_0 - (x)_\infty, \text{ the principal divisor of } x.$$

Clearly $(x)_0 \geq 0, (x)_\infty \geq 0$ and

$$(x) = \sum_{P \in \mathbb{P}_F} v_P(x)P$$

The elements $0 \neq x \in F$ which are constant are characterized by

$$x \in K \iff (x) = 0.$$

The forward part follows immediately. For the othe implication, note the general assumption made previously that K is algebraically closed in F.

Definition 5.0.3. *The set of divisors*

$$\textit{Princ}\ (F) := \{(x) \mid 0 \neq x \in F\}$$

is called the group of principal divisors of F/K. This is a subgroup of Div (F), since for $0 \neq x, y \in F,\ (xy) = (x) + (y)$. The factor group

$$\textit{Cl}\ (F) := \textit{Div}\ (F)/\ \textit{Princ}\ (F)$$

is called the divisor class group of F/K. For a divisor $D \in$ Div (F), the corresponding element in the factor group Cl (F) is denoted by $[D]$, the divisor class of D. Two divisors $D, D' \in$ Div (F) are said to be equivalent, written

$$D \sim D'$$

if $[D] = [D']$ i.e., $D = D' + (x)$ for some $x \in F \setminus \{0\}$. This is easily verified to be an equivalence relation.

5.1 Riemann-Roch Space

Definition 5.1.1. *For a divisor $A \in$ Div(F) we define the Riemann-Roch space associated to A by*

$$\mathscr{L}(A) := \{x \in F \mid (x) \geq -A\} \cup \{0\}.$$

This definition has the following interpretation: if

$$A = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$$

with $n_i > 0, m_j > 0$ then $\mathscr{L}(A)$ consists of all elements $x \in F$ such that

- x has zeros of order $\geq m_j$ at Q_j, for $j = 1, ..., s$, and
- x may have poles only at the places $P_1, ..., P_r$, with the pole order at P_i being bounded by n_i ($i = 1, ..., r$).

Remark 5.1.2. Let $A \in \text{Div}(F)$. Then

1. $x \in \mathscr{L}(A)$ if and only if $v_P(x) \geq -v_P(A)$ for all $P \in \mathbb{P}_F$.
2. $\mathscr{L}(A) \neq \{0\}$ if and only if there is a divisor $A' \sim A$ with $A' \geq 0$.

The proof of 1 follows directly from definition. For 2 suppose $A = \sum n_P P$, for some nonzero $x \in F$, $(x) \geq -A$. Let $A' = A + (x)$, then by definition, $A' \sim A$. Computing coefficientwise, $v_P(x) \geq -n_P \implies v_P(x) + n_P \geq 0 \implies A' \geq 0$. Conversely suppose such a divisor A' exists. If $A = A' \geq 0$, Then clearly $1 \in \mathscr{L}$ as $(1) = 0 \geq -A$. If $A \neq A'$ then, since $A' \sim A$, $A' = A + (x)$ for some $(x) \in F \setminus \{0\}$.

Lemma 5.1.3. *Let $A \in Div(F)$. Then we have:*

1. *$\mathscr{L}(A)$ is a vector space over K.*
2. *If A' is a divisor equivalent to A, then $\mathscr{L}(A) \simeq \mathscr{L}(A')$ (isomorphic as vector spaces over K).*

Proof. (1) Let $x, y \in \mathscr{L}(A)$ and $a \in K$. Then for all $P \in \mathbb{P}_F, v_P(x + y) \geq min\{v_P(x), v_P(y)\} \geq -v_P(A)$ and $v_P(ax) = v_P(a) + v_P(x) \geq -v_P(A)$. So $x + y$ and ax are in $\mathscr{L}(A)$ by previous remark.

(2) By assumption, $A = A' + (z)$ with $0 \neq z \in F$. Consider the mapping

$$\phi : \begin{cases} \mathscr{L}(A) \longrightarrow F \\ x \longmapsto xz \end{cases}$$

This is a K-linear mapping. Now $v_P(xz) = v_P(x) + v_P(z) \geq -v_P(A) + v_P(z) = -(v_P(A) - v_P(z)) = -v_P(A')$. So the image is contained in $\mathscr{L}(A')$. In the same manner,

$$\phi' : \begin{cases} \mathscr{L}(A') \longrightarrow F \\ x \longmapsto xz^{-1} \end{cases}$$

is K-linear from $\mathscr{L}(A')$ to $\mathscr{L}(A)$. These mappings are inverse to each other, hence ϕ is an isomorphism between $\mathscr{L}(A)$ and $\mathscr{L}(A')$. $\square$

Lemma 5.1.4. (a) $\mathscr{L}(0) = K$.
(b) *If $A < 0$ then $\mathscr{L}(A) = \{0\}$.*

Proof. (a) We have $(x) = 0$ for $0 \neq x \in K$, therefore $K \subseteq \mathscr{L}(0)$. Conversely, if $0 \neq x \in \mathscr{L}(0)$ then $(x) \geq 0$. This means that x has no pole, so $x \in K$ by Corollary 4.1.20.
(b) Assume there exists an element $0 \neq x \in \mathscr{L}(A)$. Then $(x) \geq -A > 0$, which implies that x has at least one zero but no pole. This is impossible. $\square$

Lemma 5.1.5. *Let A, B be divisors of F/K with $A \leq B$. Then we have $\mathscr{L}(A) \subseteq \mathscr{L}(B)$ and*

$$dim\ (\mathscr{L}(B)/\mathscr{L}(A)) \leq deg\ B - deg\ A.$$

Proof. If $A \leq B$ then $-A \geq -B$ and so if $x \in \mathscr{L}(A) \implies (x) \geq -A \geq -B \implies x \in \mathscr{L}(B)$ and thus $\mathscr{L}(A) \subseteq \mathscr{L}(B)$. In order to prove the other assertion we can assume that $B = A + P$ for some $P \in \mathbb{P}_F$; the general case follows then by induction. Choose an element $t \in F$ with $v_P(t) = v_P(B) = v_P(A) + 1$. For $x \in \mathscr{L}(B)$ we have $v_P(x) \geq -v_P(B) = -v_P(t)$, so $xt \in \mathcal{O}_P$. Thus we obtain a K-linear map

$$\psi : \begin{cases} \mathscr{L}(B) \longrightarrow F_P \\ x \longmapsto (xt)(P) \end{cases}$$

An element x is in the kernel of ψ if and only if $v_P(xt) > 0$; i.e., $v_P(x) \geq -v_P(A)$. Consequently Ker(ψ) = $\mathscr{L}(A)$, and ψ induces a K-linear injective mapping from $\mathscr{L}(B)/\mathscr{L}(A)$ to F_P . It follows that

$$\dim(\mathscr{L}(B)/\mathscr{L}(A)) \leq \dim F_P = \deg P = \deg B - \deg A.$$

□

Proposition 5.1.6. *For each divisor $A \in Div(F)$ the space $\mathscr{L}(A)$ is a finite dimensional vector space over K. More precisely: if $A = A_+ - A_-$ with positive divisors A_+ and A_-, then*

$$dim\ \mathscr{L}(A) \leq degA_+ + 1.$$

Proof. Since $\mathscr{L}(A) \subseteq \mathscr{L}(A_+)$, it is sufficient to show that

$$\dim \mathscr{L}(A_+) \leq \deg A_+ + 1.$$

We have $0 \leq A_+$, so Lemma 5.1.5 yields dim $(\mathscr{L}(A_+)/\mathscr{L}(0)) \leq$ deg A_+. Since $\mathscr{L}(0) = K$ we conclude that dim $\mathscr{L}(A_+) =$ dim $(\mathscr{L}(A_+)/\mathscr{L}(0)) + 1 \leq degA_+ + 1$. □

Definition 5.1.7. *For $A \in$ Div (F) the integer $l(A) :=$ dim $\mathscr{L}(A)$ is called the dimension of the divisor A.*

Theorem 5.1.8. *All principal divisors have degree zero. More precisely: let $x \in F \setminus K$ and $(x)_0$ (resp. $(x)_\infty$) denote the zero (resp. pole) divisor of x. Then deg*

$$deg\ (x)_0 = deg\ (x)_\infty = [F : K(x)].$$

Proof. Set $n := [F : K(x)]$ and

$$B := (x)_\infty = \sum_{i=1}^{r} -v_{P_i}(x)P_i,$$

where $P_1, ..., P_r$ are all the poles of x. Then

$$\deg B = \sum_{i=1}^{r} v_{P_i}(x^{-1}) \cdot \deg P_i \leq [F : K(x)] = n$$

by Proposition 1.3.3, and thus we need only show that $n \leq$ deg B. Choose a basis $u_1, ..., u_n$ of $F/K(x)$ and a divisor $C \geq 0$ such that $(u_i) \geq -C$ for $i = 1, ..., n$. We have

$$\ell(lB + C) \geq n(l + 1) \text{ for all } l \geq 0$$

which follows immediately from the fact that $x^i u_j \in \mathcal{L}(lB + C)$ for $0 \leq i \leq l, 1 \leq j \leq n$ (observe that these elements are linearly independent over K since $u_1, ..., u_n$ are linearly independent over $K(x)$). Setting $c :=$ deg C we obtain $n(l + 1) \leq \ell(lB + C) \leq l \cdot \deg B + c + 1$ by Proposition 1.4.9. Thus

$$l(\deg Bn) \geq n - c - 1$$

for all $l \in \mathbb{N}$. The right hand side of (1.19) is independent of l, therefore (1.19) is possible only when $\deg B \geq n$. We have thus proved that $\deg(x)_\infty = [F : K(x)]$. Since $(x)_0 = (x^{-1})_\infty$, we conclude that $\deg(x)_0 = \deg(x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)]$. □

Corollary 5.1.9. 1. *Let A, A' be divisors with $A \sim A'$. Then we have $\ell(A) = \ell(A')$ and deg $A =$ deg A'.*

2. *If deg$A < 0$ then $\ell(A) = 0$.*
3. *For a divisor A of degree zero TFAE :*
   (a) A *is principal.*
   (b) $\ell(A) \geq 1$.
   (c) $\ell(A) = 1$

Proof. 1. follows immediately from Lemma 5.1.3 and last theorem.

2. Suppose that $\ell(A) > 0$. By Remark 2.0.5. there is some divisor $A' \sim A$ with $A' \geq 0$, hence deg $A =$ deg $A' \geq 0$.
3. $(1) \Rightarrow (2)$: If $A = (x)$ is principal then $x^{-1} \in \mathscr{L}(A)$, so $\ell(A) \geq 1$.
   $(2) \Rightarrow (3)$: Assume now that $\ell(A) \geq 1$ and deg$A = 0$. Then $A \sim A'$ for some $A' \geq 0$ (Remark 5.1.3 (2)). The conditions $A' \geq 0$ and deg$A' = 0$ imply that $A' = 0$, hence $\ell(A) = \ell(A') = \ell(0) = 1$, by Lemma 5.1.4.
   $(3) \Rightarrow (1)$: Suppose that $\ell(A) = 1$ and deg$A = 0$. Choose $0 \neq z \in \mathscr{L}(A)$, then $(z) + A \geq 0$. Since deg$((z) + A) = 0$, it follows that $(z) + A = 0$, therefore $A = -(z) = (z^{-1})$ is principal.

□

Example 5.1.10. Once again we consider the rational function field $F = K(X)$. For $0 \neq z \in K(X)$ we have $z = a \cdot f(X)/g(X)$ with $a \in K \setminus \{0\}$, $f(X), g(X) \in K[X]$ monic and relatively prime. Let

$$f(X) = \prod_{i=1}^{r} p_i(X)^{n_i} \quad , \qquad g(X) = \prod_{j=1}^{s} q_i(X)^{m_i}$$

with pairwise distinct irreducible monic polynomials $p_i(X), q_j(X) \in K[X]$. Then the principal divisor of z in Div$(K(x))$ appears thus :

$$(z) = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j + (\text{deg } g(X) - \text{degX} f(x)) P_\infty$$

where P_i (resp. Q_j) are the places corresponding to $p_i(X)$ (resp. $q_j(x)$). Therefore in arbitrary function fields, principal divisors can be considered as a substitute for the decomposition into irreducible polynomials that occurs in the rational function field.
Again we consider an arbitrary algebraic function field F/K. We have seen that the inequality

$$\ell(A) \leq 1 + \text{deg} A$$

holds for all divisors $A \geq 0$. In fact the above inequality holds for every divisor of degree ≥ 0. In order to verify this, we can assume that $\ell(A) > 0$. Then $A \sim A'$ for some $A' \geq 0$ by Remark 5.1.2, so $\ell(A) = \ell(A') \leq 1 + \text{deg}A' = 1 + \text{deg}A$ by Corollary 5.1.9.
Next we want to prove the existence of a lower bound for $\ell(A)$.

Proposition 5.1.11. *There is a constant $\gamma \in \mathbb{Z}$ such that for all divisors $A \in$ Div (F) the following holds:*

$$degA - \ell(A) \leq \gamma.$$

The emphasis here lies on the fact that γ is independent of the divisor A; it depends only on the function field F/K.

Proof. To begin with, observe that

$$A_1 \leq A_2 \Rightarrow \deg A_1 - \ell(A_1) \leq \deg A_2 - \ell(A_2)$$

by Lemma 5.1.5 . We fix an element $x \in F \setminus K$ and consider the specific divisor $B := (x)_\infty$. As in the proof of Theorem 2.0.11 there exists a divisor $C \geq 0$ (depending on x) such that $\ell(lB+C) \geq (l+1)\cdot \deg B$ for all $l \geq 0$. On the other hand, $\ell(lB+C) \leq \ell(lB) + \deg C$ by Lemma 5.1.5. Combining these inequalities we find

$$\ell(lB) \geq (l+1)\deg B - \deg C = \deg(lB) + ([F : K(x)] - \deg C).$$

Therefore

$$\deg(lB) - \ell(lB) \leq \gamma \quad \text{for all} \quad l > 0 \tag{5.1}$$

with some $\gamma \in \mathcal{Z}$. We want to show that (5.1) holds even when we substitute for lB any $A \in \mathrm{Div}(F)$ (with the above γ).

Claim: Given a divisor A, there exist divisors $A_1,\ D$ and an integer $l \geq 0$ such that $A \leq A_1,\ A_1 \sim D$ and $D \leq lB$. Using this claim, Proposition 5.1.11 will follow easily :

$$\begin{aligned} \deg A - \ell(A) &\leq \deg A_1 - \ell(A_1) \\ &= \deg D - \ell(D) \\ &\leq \deg(lB) - \ell(lB) \\ &\leq \gamma \end{aligned}$$

Proof of the claim: Choose $A_1 \geq A$ such that $A_1 \geq 0$. Then

$$\begin{aligned} \ell(lB - A_1) &\geq \ell(lB) - \deg A_1 \\ &\geq \deg(lB) - \gamma - \deg A_1 \\ &> 0 \end{aligned}$$

for sufficiently large l. Thus there is some element $0 \neq z \in \mathscr{L}(lB - A_1)$. Setting $D := A_1 - (z)$ we obtain $A_1 \sim D$ and $D \leq A_1 - (A_1 - lB) = lB$ as desired. □

5.2 Genus and Riemann's Theorem

Definition 5.2.1. *The **genus** g of F/K is defined by*

$$g := \max\{\deg A - \ell(A) + 1 \mid A \in \mathrm{Div}(F)\}.$$

Observe by previous proposition the definition makes sense.

Corollary 5.2.2. *The genus of F/K is a non-negative integer.*

Proof. In the definition of g, put $A = 0$. Then $\deg(0) - \ell(0) + 1 = 0$, hence $g \geq 0$. □

Theorem 5.2.3. ***(Riemann's Theorem):*** *Let F/K be a function field of genus g. Then we have:*
(a) *For all divisors $A \in Div(F)$,*

$$\ell(A) \geq degA + 1 - g.$$

(b) *There is an integer c , depending only on the function field F/K, such that*

$$\ell(A) = deg\ A + 1 - g,$$

whenever deg $A \geq c$.

Proof. (a) This is just the definition of the genus.
(b) Choose a divisor A_0 with $g = \text{deg } A_0 - \ell(A_0) + 1$ (From definition 5.2.1, $\exists$ a divisor for which the maximum occurs) and set $c := \text{deg } A_0 + g$. If deg$A \geq c$ then

$$\ell(A - A_0) \geq deg\ (A - A_0) + 1 - g \geq c - \text{deg } A_0 + 1 - g = 1.$$

So there is an element $0 \neq z \in \mathscr{L}(A - A_0)$. Consider the divisor $A' := A + (z)$ which is $\geq A_0$. We have

$$\begin{aligned} \text{deg}A - \ell(A) &= \text{deg } A' - \ell(A') \\ &\geq \text{deg } A_0 - \ell(A_0) \\ &= g - 1 \end{aligned}$$

Hence $\ell(A) \leq \text{deg } A + 1 - g$. □

Example 5.2.4. We want to show that the rational function field $K(X)/K$ has genus $g = 0$. In order to prove this, let P_∞ denote the pole divisor of X. Consider for $r \geq 0$ the vector space $\mathscr{L}(rP_\infty)$. Obviously the elements $1, x, ..., x^r$ are in $\mathscr{L}(rP_\infty)$, hence

$$r + 1 \leq \ell(rP_\infty) = \text{deg}(rP_\infty) + 1 - g = r + 1 - g$$

for sufficiently large r. Thus $g \leq 0$. Since $g \geq 0$ holds for every function field, the assertion follows.

Chapter 6

The Riemann-Roch Theorem

6.1 Adele

In this section F/K denotes an algebraic function field of genus g.

Definition 6.1.1. *For $A \in$ Div (F) the integer*

$$i(A) := \ell(A) - \textit{deg } A + g - 1$$

is called the index of specialty of A.

Riemanns Theorem states that $i(A)$ is a non-negative integer, and $i(A) = 0$ if deg A is sufficiently large. In the present chapter we will provide several interpretations for $i(A)$ as the dimension of certain vector spaces. To this end we introduce the notion of an *adele*.

Definition 6.1.2. *An adele of F/K is a mapping*

$$\alpha : \begin{cases} \mathbb{P}_F & \to F \\ P & \mapsto \alpha_P, \end{cases}$$

such that $\alpha_P \in \mathcal{O}_P$ for almost all $P \in \mathbb{P}_F$. We regard an adele as an element of the direct product $\prod_{P \in \mathbb{P}_F} F$ and therefore use the notation $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ or, even shorter, $\alpha = (\alpha_P)$. The set

$$\mathcal{A}_F := \{\alpha \mid \alpha \textit{ is an adele of } F/K\}$$

is called the adele space of F/K. It is regarded as a vector space over K in the obvious manner (actually $\mathcal{A}_F$ can be regarded as a ring, but the ring structure will never be used).

The principal adele of an element $x \in F$ is the adele all of whose components are equal to x (note that this definition makes sense since x has only finitely many poles). This gives an embedding $F \hookrightarrow \mathcal{A}_F$. The valuations v_P of F/K extend naturally to $\mathcal{A}_F$ by setting $v_P(\alpha) := v_P(\alpha_P)$ (where α_P is the P-component of the adele α). By definition we have that $v_P(\alpha) \geq 0$ for almost all $P \in \mathbb{P}_F$.

Definition 6.1.3. *For $A \in$ Div (F) we define*

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F \mid v_P(\alpha) \geq -v_P(A) \textit{ for all } P \in \mathbb{P}_F\}.$$

This is a K-subspace of $\mathcal{A}_F$.

Theorem 6.1.4. *For every divisor A the index of specialty is*

$$i(A) = dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F))$$

.

Proof. We proceed in several steps.

Step 1 : Let $A_1, A_2 \in \text{Div}\ (F)$ and $A_1 \le A_2$. Then $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ and

$$\text{dim}\ (\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) = \text{deg}\ A_2 - \ \text{deg}\ A_1. \tag{6.1}$$

Proof of Step 1 : $\mathcal{A}_F(A_1) \subset \mathcal{A}_F(A_2)$ is trivial. It is sufficient to prove (6.1) in the case $A_2 = A_1 + P$ with $P \in \mathbb{P}_F$ (the general case follows by induction). Choose $t \in F$ with $v_P(t) = v_P(A_1) + 1$ and consider the K-linear map

$$\varphi : \begin{cases} \mathcal{A}_F(A_2) & \to F_P \\ \alpha & \mapsto (t\alpha_P)(P). \end{cases}$$

The map φ is surjective and that the kernel of φ is $\mathcal{A}_F(A_1)$. Consequently,

$$\text{deg}\ A_2 - \text{deg}\ A_1 = \text{deg}\ P = [F_P : K] = \text{dim}\ (\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1))$$

Step 2 : Let $A_1, A_2 \in \text{Div}\ (F)$ and $A_1 \le A_2$ as before. Then

$$\text{dim}\ \ ((\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F))\ = (\text{deg}\ A_2 - \ell(A_2)) - (\text{deg}\ A_1 - \ell(A_1)). \tag{6.2}$$

Proof of Step 2 : We have an exact sequence of linear mappings

$$0 \longrightarrow \mathscr{L}(A_2)/\mathscr{L}(A_1) \xrightarrow{\sigma_1} \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \xrightarrow{\sigma_2} (\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F) \longrightarrow 0 \tag{6.3}$$

where σ_1 and σ_2 are defined in the obvious manner. In fact, the only non-trivial assertion is that the kernel of σ_2 is contained in the image of σ_1 . In order to prove this, let $\alpha \in \mathcal{A}_F(A_2)$ with $\sigma_2(\alpha + \mathcal{A}_F(A_1)) = 0$. Then $\alpha \in \mathcal{A}_F(A_1) + F$, so there is some $x \in F$ with $\alpha - x \in \mathcal{A}_F(A_1)$. As $\mathcal{A}_F(A_1) \subset \mathcal{A}_F(A_2)$ we conclude that $x \in \mathcal{A}_F(A_2) \cap F = \mathscr{L}(A_2)$. Therefore $\alpha + \mathcal{A}_F(A_1) = x + \mathcal{A}_F(A_1) = \sigma_1(x + \mathscr{L}(A_1))$ lies in the image of σ_1 . From the exactness of (6.3) we obtain

$$\begin{aligned} &\text{dim}\ (\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F) \\ &= \text{dim}\ (\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) - \text{dim}\ (\mathscr{L}(A_2)/\mathscr{L}(A_1)) \\ &= (\text{deg}\ A_2 - \text{deg}\ A_1) - (\ell(A_2) - \ell(A_1)) \qquad \text{(using (6.2))}. \end{aligned}$$

Step 3 : If B is a divisor with $\ell(B) = \text{deg}\ B + 1 - g$, then

$$\mathcal{A}_F = \mathcal{A}_F(B) + F \tag{6.4}$$

Proof of Step 3 : To begin with, observe that for $B_1 \ge B$ we have (by Lemma 5.1.5)

$$\ell(B_1) \le \text{deg}\ B_1 + \ell(B) - \text{deg}\ B = \text{deg}\ B_1 + 1 - g$$

On the other hand, $\ell(B_1) \geq \deg B_1 + 1 - g$ by Riemanns Theorem. Therefore

$$\ell(B_1) = \deg B_1 + 1 - g \quad \text{for each } B_1 \geq B. \tag{6.5}$$

(Now we prove (6.4). Let $\alpha \in \mathcal{A}_F$. Obviously one can find a divisor $B_1 \geq B$ such that $\alpha \in \mathcal{A}_F(B_1)$. By (6.2) and (6.5),

$$\begin{aligned}\dim\, (\mathcal{A}_F(B_1) + F)/(\mathcal{A}_F(B) + F) &= (\deg B_1 - \ell(B_1)) - (\deg B - \ell(B)) \\ &= (g-1) - (g-1) = 0.\end{aligned}$$

This implies $\mathcal{A}_F(B) + F = \mathcal{A}_F(B_1) + F$. Since $\alpha \in \mathcal{A}_F(B_1)$ it follows that $\alpha \in \mathcal{A}_F(B) + F$, and (6.4) is proved.

End of the proof of Theorem : Now we consider an arbitrary divisor A. By Riemanns Theorem there exists some divisor $A_1 \geq A$ such that $\ell(A_1) = \deg A_1 + 1 - g$. By (6.4), $\mathcal{A}_F = \mathcal{A}_F(A_1) + F$, and in view of (6.2) we obtain

$$\begin{aligned}\dim\, (\mathcal{A}_F/(\mathcal{A}_F(A) + F)) &= \dim\, (\mathcal{A}_F(A_1) + F)/(\mathcal{A}_F(A) + F) \\ &= (\deg A_1 - \ell(A_1)) - (\deg A - \ell(A)) \\ &= (g-1) + \ell(A) - degA \\ &= i(A).\end{aligned}$$

□

Corollary 6.1.5. $g = dim(\mathcal{A}_F/(\mathcal{A}_F(0) + F))$.

Proof. $i(0) = \ell(0) - deg(0) + g - 1 = 1 - 0 + g - 1 = g.$ □

Thus we get for all $A \in$ Div (F)

$$\ell(A) = \deg A + 1 - g + \dim\, (\mathcal{A}_F/(\mathcal{A}_F(A) + F). \tag{6.6}$$

This is a preliminary version of the Riemann-Roch Theorem which we shall prove later in this section. Next we introduce the concept of Weil differentials which will lead to a second interpretation for the index of specialty of a divisor.

6.2 Weil differential

Definition 6.2.1. *A Weil differential of F/K is a K-linear map $\omega : \mathcal{A}_F \to K$ vanishing on $\mathcal{A}_F(A) + F$ for some divisor $A \in$ Div (F). We call*

$$\Omega_F := \{\omega \mid \omega \textit{ is a Weil differential of } F/K\}$$

the module of Weil differentials of F/K. For $A \in$Div (F) let

$$\Omega_F(A) := \{\omega \in \Omega_F \mid \omega \textit{ vanishes on } \mathcal{A}_F(A) + F\}$$

We regard Ω_F as a K-vector space in the obvious manner (in fact, if ω_1 vanishes on $\mathcal{A}_F(A_1) + F$ and ω_2 vanishes on $\mathcal{A}_F(A_2) + F$ then $\omega_1 + \omega_2$ vanishes on $\mathcal{A}_F(A_3) + F$ for every divisor A_3 with $A_3 \leq A_1$ and $A_3 \leq A_2$, and $a\omega_1$ vanishes on $\mathcal{A}_F(A_1) + F$ for $a \in K$). Clearly $\Omega_F(A)$ is a subspace of Ω_F.

Lemma 6.2.2. *For $A \in$ Div (F) we have dim $\Omega_F(A) = i(A)$.*

Proof. $\Omega_F(A)$ is in a natural way isomorphic to the space of linear forms on $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$. Since $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$ is finite-dimensional and of dimension $i(A)$, our lemma follows immediately.

□

A simple consequence of Lemma 6.2.2 is that $\Omega_F \neq 0$. To see this, choose a divisor A of degree ≤ 2. Then

$$\dim \Omega_F(A) = i(A) = \ell(A) - degA + g - 1 \geq 1,$$

hence $\Omega_F(A) \neq 0$.

Definition 6.2.3. *For $x \in F$ and $\omega \in \Omega_F$ we define $x\omega : \mathcal{A}_F \to K$ by*

$$(x\omega)(\alpha) := \omega(x\alpha)$$

It is easily checked that $x\omega$ is again a Weil differential of F/K. In fact, if ω vanishes on $\mathcal{A}_F(A) + F$ then $x\omega$ vanishes on $\mathcal{A}_F(A + (x)) + F$. Clearly our definition gives Ω_F the structure of a vector space over F .

Proposition 6.2.4. *Ω_F is a one-dimensional vector space over F.*

Proof. Choose $0 \neq w_1 \in \Omega_F$ (we already know that $\Omega_F \neq 0$). It has to be shown that for every $\omega_2 \in \Omega_F$ there is some $z \in F$ with $\omega_2 = z\omega_1$. We can assume that $\omega_2 \neq 0$. Choose $A_1, A_2 \in$ Div(F) such that $\omega_1 \in \Omega_F(A_1)$ and $\omega_2 \in \Omega_F(A_2)$. For a divisor B (which will be specified later) we consider the K-linear injective maps

$$\varphi_i : \begin{cases} \mathscr{L}(A_i + B) \longrightarrow \Omega_F(-B) \\ x \longmapsto x\omega_i \end{cases} \qquad (i = 1, 2)$$

Claim : For an appropriate choice of the divisor B holds

$$\varphi_1(\mathscr{L}(A_1 + B)) \cap \varphi_2(\mathscr{L}(A_2 + B)) \neq \{0\}.$$

Using this claim, the proof of the proposition can be finished very quickly:
we choose $x_1 \in \mathscr{L}(A_1 + B)$ and $x_2 \in \mathscr{L}(A_2 + B)$ such that $x_1\omega_1 = x_2\omega_2 \neq 0$. Then $\omega_2 = (x_1x_2^{-1})\omega_1$ as desired.
Proof of the Claim. We start with a simple and well-known fact from linear algebra: if U_1, U_2 are subspaces of a finite-dimensional vector space V then

$$\text{dim}(U_1 \cap U_2) \geq \text{dim}U_1 + \text{dim}U_2 - \text{dim}V. \tag{6.7}$$

Now let $B > 0$ be a divisor of sufficiently large degree such that

$$\ell(A_i + B) = \text{deg}(A_i + B) + 1 - g$$

for $i = 1, 2$ (this is possible by Riemann's Theorem). We set $U_i := \varphi_i(\mathscr{L}(A_i + B)) \subseteq \Omega_F(-B)$. Since

$$\begin{aligned} \text{dim}\Omega_F(-B) &= i(-B) = \text{dim}(-B) - deg(-B) + g - 1 \\ &= \text{deg}B - 1 + g, \end{aligned}$$

we obtain

$$\begin{aligned}&\mathrm{dim}U_1 + \mathrm{dim}U_2 - \ \mathrm{dim}\Omega_F(-B)\\ &= \mathrm{deg}(A_1 + B) + 1 - g + \mathrm{deg}(A_2 + B) + 1 - g - (\mathrm{deg}B + g - 1)\\ &= \mathrm{deg}B + (\mathrm{deg}A_1 + \mathrm{deg}A_2 + 3(1 - g)).\end{aligned}$$

The term in brackets is independent of B, so

$$\mathrm{dim}U_1 + \mathrm{dim}U_2 - \mathrm{dim}\Omega_F(-B) > 0$$

if deg$B$ is sufficiently large. By (6.7) it follows that $U_1 \cap U_2 \neq \{0\}$ which proves our claim. □

We want to attach a divisor to each Weil differential $\omega \neq 0$. Thus we consider (for a fixed ω) the set of divisors

$$M(\omega) := \{A \in \mathrm{Div}(F) \mid \omega \text{ vanishes on } \mathcal{A}_F(A) + F\}.$$

Lemma 6.2.5. *Let $0 \neq \omega \in \Omega_F$. Then there is a uniquely determined divisor $W \in M(\omega)$ such that $A \leq W$ for all $A \in M(\omega)$.*

Proof. By Riemanns Theorem there exists a constant c, depending only on the function field F/K, with the property $i(A) = 0$ for all $A \in \mathrm{Div}(F)$ of degree $\geq c$. Since $\dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)) = i(A)$, we have that deg$A < c$ for all $A \in M(\omega)$. So we can choose a divisor $W \in M(\omega)$ of maximal degree.
Suppose W does not have the property of our lemma. Then there exists a divisor $A_0 \in M(\omega)$ with $A_0 \nleq W$, i.e. $v_Q(A_0) > v_Q(W)$ for some $Q \in \mathbb{P}_F$. We claim that

$$W + Q \in M(\omega) \tag{6.8}$$

which is a contradiction to the maximality of W. In fact, consider an adele $\alpha = (\alpha_P) \in \mathcal{A}_F(W + Q)$. We can write $\alpha = \alpha' + \alpha''$ with

$$\alpha'_P = \begin{cases} \alpha_P \; for \; P \neq Q \\ 0 \; for \; P = Q \end{cases} \qquad and \quad \alpha''_P = \begin{cases} 0 \; for \; P \neq Q \\ \alpha_Q \; for \; P = Q \end{cases}$$

Then $\alpha' \in \mathcal{A}_F(W)$ and $\alpha'' \in \mathcal{A}_F(A_0)$, therefore $\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0$. Hence ω vanishes on $\mathcal{A}_F(W + Q) + F$, and (6.8) is proved. The uniqueness of W is now obvious. □

Definition 6.2.6. 1. *The divisor (ω) of a Weil differential $\omega \neq 0$ is the uniquely determined divisor of F/K satisfying*

   (a) ω vanishes on $\mathcal{A}_F((\omega)) + F$, and

   (b) if ω vanishes on $\mathcal{A}_F(A) + F$ then $A \leq (\omega)$.

   For $0 \neq \omega \in \Omega_F$ and $P \in \mathbb{P}_F$ we define $v_P(\omega) := v_P((\omega))$.

2. *A place P is said to be a zero (resp. pole) of ω if $v_P(\omega) > 0$ (resp. $v_P(\omega) < 0$). The Weil differential ω is called regular at P if $v_P(\omega) \geq 0$, and ω is said to be regular (or holomorphic) if it is regular at all places $P \in \mathbb{P}_F$.*

3. *A divisor W is called a canonical divisor of F/K if $W = (\omega)$ for some $\omega \in \Omega_F$.*

Remark 6.2.7. It follows immediately from the definitions that

$$\Omega_F(A) = \{\omega \in \Omega_F \mid \omega = 0 \text{ or } (\omega) \geq A\}$$

and

$$\Omega_F(0) = \{\omega \in \Omega_F \mid \omega \text{ is regular }\}.$$

As a consequence of Lemma 3.2.2 and Definition 3.1.1 we obtain

$$\dim \Omega_F(0) = g.$$

Proposition 6.2.8. *1. For $0 \neq x \in F$ and $0 \neq \omega \in \Omega_F$ we have $(x\omega) = (x) + (\omega)$.*

2. Any two canonical divisors of F/K are equivalent.

It follows from this proposition that the canonical divisors of F/K form a whole class $[W]$ in the divisor class group Cl(F); this divisor class is called the canonical class of F/K.

Proof. If ω vanishes on $\mathcal{A}_F(A) + F$ then $x\omega$ vanishes on $\mathcal{A}_F(A + (x)) + F$, consequently

$$(\omega) + (x) \leq (x\omega).$$

Likewise $(x\omega) + (x^{-1}) \leq (x^{-1}x\omega) = (\omega)$. Combining these inequalities we obtain

$$(\omega) + (x) \leq (x\omega) \leq -(x^{-1}) + (\omega) = (\omega) + (x).$$

This proves (a). (b) follows from (a) and Proposition 3.2.4. □

Theorem 6.2.9. ***(Duality Theorem).*** *Let A be an arbitrary divisor and $W = (\omega)$ be a canonical divisor of F/K. Then the mapping*

$$\mu = \begin{cases} \mathscr{L}(W - A) \longrightarrow \Omega_F(A) \\ x \longmapsto x\omega \end{cases}$$

is an isomorphism of K-vector spaces. In particular,

$$i(A) = \ell(W - A).$$

Proof. For $x \in \mathscr{L}(W - A)$ we have

$$(x\omega) = (x) + (\omega) \geq -(W - A) + W = A,$$

hence $x\omega \in \Omega_F(A)$ by Remark 3.2.7. Therefore μ maps $\mathscr{L}(W - A)$ into $\Omega_F(A)$. Clearly μ is linear and injective. In order to show that μ is surjective, we consider a Weil differential $\omega_1 \in \Omega_F(A)$. By Proposition 3.2.4 we can write $\omega_1 = x\omega$ with some $x \in F$. Since

$$(x) + W = (x) + (\omega) = (x\omega) = (\omega_1) \geq A,$$

we obtain $(x) \geq -(W - A)$, so $x \in \mathscr{L}(W - A)$ and $\omega_1 = \mu(x)$. We have thus proved that dim$\Omega_F(A) = \ell(W - A)$. Since dim$\Omega_F(A) = i(A)$ by Lemma 3.2.2, this implies $i(A) = \ell(W - A)$. □

Theorem 6.2.10. ***(Riemann-Roch Theorem).*** *Let W be a canonical divisor of F/K. Then for each divisor $A \in Div(F)$,*

$$\ell(A) = degA + 1 - g + \ell(W - A).$$

Proof. This is an immediate consequence of Theorem 3.2.9 and the definition of $i(A)$. $\square$

Corollary 6.2.11. *For a canonical divisor W we have*

$$\textit{deg}\, W = 2g - 2 \ \textit{ and } \ \ell(W) = g.$$

Proof. For $A = 0$, the Riemann-Roch Theorem give

$$1 = \ell(0) = \text{deg}\, 0 + 1 - g + \ell(W - 0).$$

Thus $\ell(W) = g$. Setting $A = W$ we obtain

$$g = \ell(W) = \text{deg}\, W + 1 - g + \ell(W - W) = \text{deg}\, W + 2 - g.$$

Therefore deg $W = 2g - 2$. $\square$

From Riemann's Theorem we already know there is an integer c such that $i(A) = 0$ for deg $A \geq c$. We now give a more precise description of this constant.

Theorem 6.2.12. *If $A \in$ Div (F) with deg $A \geq 2g - 1$ then, $\ell(A) =$ deg $A + 1 - g$*

Proof. We have $\ell(A) =$ deg $A + 1 - g + \ell(W - A)$ where W is a canonical divisor. Since deg $A \geq 2g - 1$ and deg $W = 2g - 2$, we conclude deg $(W - A) < 0$. Hence $\ell(W - A) = 0$ $\square$

Chapter 7

Riemann Surfaces

There is a close relationship between the study of algebraic curves and that of compact Riemann surfaces. We will introduce a powerful tool in the study of algebraic curves called *Normalization*, but first let us give basic definitions and topological properties of Riemann surfaces.

Definition 7.0.1. *A Riemann surface is a connected Hausdorff topological space C together with an open covering $\{U_\alpha\}$ of C and a family of mappings*

$$z_\alpha : U_\alpha \to \mathbb{C}$$

such that
(I) each $z_\alpha : U_\alpha \to \mathbb{C}$ is a homeomorphism of U_α onto an open subset $z_\alpha(U_\alpha)$ of $\mathbb{C}$.
(II) if $U_\alpha \cap U_\beta \neq \emptyset$ then the function

$$z_\beta \circ z_\alpha^{-1} : z_\alpha(U_\alpha \cap U_\beta) \to z_\beta(U_\alpha \cap U_\beta)$$

is biholomorphic (i.e., the function itself as well as its inverse are both holomorphic).

So a Riemann surface is an one-dimensional, connected, complex manifold [1]. We call such (U_α, z_α) a *local holomorhic coordinate or a coordinate chart.* The main topic of our study is going to be compact Riemann surfaces.

Example 7.0.2. The extended complex numbers $\Sigma = \mathbb{C} \cup \{\infty\}$ (one point compactification of complex numbers) is obviously a compact, connected, Hausdorff space. Now consider

$$U_1 = \Sigma \setminus \{\infty\} = \mathbb{C}, \qquad\qquad U_2 = \Sigma \setminus \{0\}$$

and the mappings,

$$\begin{aligned} z_1 : U_1 &\to \mathbb{C} \\ z &\mapsto z \\ z_2 : U_2 &\to \mathbb{C} \\ z &\mapsto \begin{cases} 0, & z = \infty \\ 1/z, & z \neq \infty \end{cases} \end{aligned}$$

Clearly $z_1 \circ z_2^{-1} : \mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\}$ given by $z \mapsto \frac{1}{z}$ is biholomorphic.

[1] Refer to Appendix-I for more details on manifolds.

Since we can identify the unit sphere S^2 with Σ through stereographic projection, S therefore also naturally becomes a Riemann surface, called the Riemann sphere.
Any holomorphic function which maps an open set U of $\mathbb{C}$ into an open set V of $\mathbb{C}$,

$$\omega = f(z) \qquad\qquad (\omega = u + \iota v, \ \ z = x + \iota y)$$

is at the same time a continously differentiable map from the open set U of $\mathbb{R}^2$ into the open set V of $\mathbb{R}^2$. From this we see that any compact Riemann surface is also a compact, differentiable real 2-manifold, i.e. a compact smooth surface. Also we know that any dimensional complex manifold is is orientable as a real manifold [2]. Thus any compact Riemann surface is a compact, orientable, 2-dimensional real smooth surface. So any compact Riemann surface is homeomorphic to a sphere with handles [3].

Definition 7.0.3. *Any compact Riemann surface is homeomorphic to a sphere with handles. The number of handles, g (≥ 0), is called the genus of the Riemann surface.*

7.1 Holomorphic and Meromorphic functions

A Riemann surface, locally is just an open set in $\mathbb{C}$. So using local coordinates one can define certain complex function theory on Riemann surfaces.

Definition 7.1.1. *Let C be a Riemann surface and $\{(U_i, z_i)\}$ be its holomorphic coordinate covering. A meromorphic (resp. holomorphic) function f on C is by definition a family of mappings $f_i : U_i \to \Sigma$ satisfying the following conditions :*

(a) if $U_i \cap U_j \neq \emptyset$ then, $f_i = f_j$ on $U_i \cap U_j \ \ \forall\, i, j$.
(b) $\forall\ i,\ f_i \circ z_i^{-1}$ are all meromorphic (resp. holomorphic) functions.

Observe that as $z_i(U_i) \subseteq \mathbb{C},\ f_i \circ z_i^{-1} : z_i(U_i) \to \Sigma$ is well defined and the definition makes sense. The holomorphic functions on C together with usual definition of addition and mutiplication forms a ring denoted by $\mathcal{O}(C)$. Its quotient field is the field of meromorphic functions, called the meromorphic function field on C denoted by $K(C)$. in a similar fashion one can define holomorphic function from one Riemann surface to another.
Certain theorems on holomorphic functions are inherited immediately from theory of holomorphic functions on open sets on the complex plane.

Theorem 7.1.2. ***(Uniqueness theorem)*** *Let f be a holomorphic function defined on a Riemann surface C. If the zero set of f has a limit point on C, then f is identically zero on X.*

Proof. Let E denote the zero set of f and α be a limit point of E. Consider all charts U_i containing α. Then in the local case, $f_i \circ z_i^{-1}$ is zero on the set $z_i(E \cap U_i)$ which has $z_i(\alpha)$ as a limit point (as z_i is a homeomorphism). So that f_i is identically zero on U_i. Let $A = \cup_{\alpha \in U_i} U_i$ and $B = \cup_{\alpha \notin U_j} U_j$ then A and B are open sets of C such that $C = A \cup B$. Since C is connected $A \cap B \neq \emptyset$, and A $\square$

Definition 7.1.3. *Let $C,\ C'$ are Riemann surfaces with $\{(U_i, z_i)\}$ and $\{(U'_a, z'_a)\}$ are their holomorphic coordinate covering respectively. Then a holomorphic mapping $f : C \to C'$ is by definition a family of continuous mappings*

$$f_i : U_i \to C'$$

[2]Refer to the Orientability section of Appendix-I
[3]Refer to the Classifcation section of Appendix - I

such that $(\forall i)$
(a) $f_i = f_j$ *on* $U_i \cap U_j$ *for* $U_i \cap U_j \neq \emptyset$*;*
(b) $z'_a \circ f_i \circ z_i^{-1}$ *is a holomorphic function on* $z_i(f^{-1}(U'_a) \cap U_i)$ *whenver* $f^{-1}(U'_a) \cap U_i \neq \emptyset$*.*

Theorem 7.1.4. ***(Open Mapping Theorem)*** *Let* X *and* Y *be Riemann surfaces. If* $f : X \to Y$ *is a non-constant holomorphic map, then* f *is an open map.*

Proof. Let $f : X \to Y$ be a non-constant holomorphic function, hence by uniqueness result it is non-constant on each chart. Consider any chart (U_i, ϕ_i) of X and (V_j, ψ_j) on Y. By definition $\psi_j \circ f \circ \phi_i^{-1} = g$ (say) is holomorphic on $\phi_i(U_i \cap f^{-1}(V_j))$ in our usual sense. since $\phi_i, \ \psi_j$ are homeomorphisms, f is non-constant implies g is also non constant. Then by open mapping theorem of complex numbers, g is an open map. This implies $\psi_j^{-1} \circ g \circ \phi_i = f|_{U_i}$ is an open map. Thus f is open map on every coordinate chart of X. his implies that f must be open on the arbitrary union of domains of coordinate charts on X. Thus f must be open on all of X. $\square$

Theorem 7.1.5. *Let* X *be a compact Riemann surface.* $f : X \to \mathbb{C}$ *be holomorphic, then* f *is constant.*

Proof. Suppose f is not constant. Then by last theorem, f is an open map. This in turn implies $f(X)$ is open. Since X is compact and f is continuous, $f(X)$ is compact and hence is closed in $\mathbb{C}$ (a Hausdorff space). Since $\mathbb{C}$ is connected $f(X) = \mathbb{C}$. But this is a contradiction as this implies $\mathbb{C}$ is compact. Thus f must be constant. $\square$

Definition 7.1.6. *Suppose* C *is a compact Riemann surface, with* $f \in K(C)$*. Let* $p \in C$*. Select a local coordinate* z *in a neighbourhood of the point* p *such that* $z(p) = 0$*. Then in a neighbourhood of* p*,*

$$f = z^{\nu} h(z)$$

where $h(z)$ *is a holomorphic function,* $h(0) \neq 0$ *and* $\nu \in \mathcal{Z}$*. The values of* ν *in the above expression is the same for any local coordinate* z *of* p *for which* $z(p) = 0$ *and is uniquely determined by* f*. Denote* $\nu = \nu_p(f)$*. If* $\nu_p(f) > 0$ *then* p *is called a zero of* f *and* $\nu_p(f)$ *is called the order or the multiplicity of the zero* p*. When* $\nu_p(f) < 0$*,* p *is called a pole of* f *and* $|\nu_p(f)|$ *is called the order or multiplicity of the pole* p*.*

7.2 Holomorphic and Meromorphic differentials

In this section we will discuss differentials on a Riemann surface C.

Definition 7.2.1. *Suppose* C *is a Riemann surface. Then a holomorphic (resp. meromorphic) differential* ω *is by definition a family* $\{(U_i, z_i, \omega_i)\}$ *such that :*
(a) $\{(U_i, z_i)\}$ *is a holomorphic covering of* C *and*

$$\omega_i = f_i(z_i) dz_i$$

where $f_i \in \mathcal{O}(U_i)$ *(resp.* $K(U_i)$*).*
(b) If $z_i = \phi_{ij}(z_j)$ *is the coordinate transformation on* $U_i \cap U_j (\neq \emptyset)$ *then*

$$f_i(\phi_{ij}(z_j)) \frac{d\phi_{ij}(z_j)}{dz_j} = f_j(z_j)$$

i.e. the local representation of the differential changes according to the chain rule

$$f_i(\phi_{ij}(z_j)) d\phi_{ij}(z_j) = f_j(z_j) dz_j$$

We use $\Omega^1(C)$ (resp. $K^1(C)$) to denote the set of holomorphic (resp. meromorphic) differentials on C. Suppose $f = \{(U_i, z_i, f_i(z_i))\} \in K(C)$. Then the following defines a meromorphic differential $df \in K^1(C)$, where

$$df = \left\{ \left(U_i, z_i, df_i(z_i) = \frac{df_i(z_i)}{dz_i} dz_i \right) \right\}$$

Definition 7.2.2. *We call df, as defined above, the differential of the meromorphic function f.*

Definition 7.2.3. *Suppose C is a Riemann surface with*

$$\omega = \{(U_i, z_i, f_i(z_i)dz_i)\} \in K^1(C), \qquad p \in U_i \cap U_j$$

Then

$$\nu_p(f_i) = \nu_p\left(f_i(\phi_{ij}(z_j)) \frac{d\phi_{ij}(z_j)}{dz_j} \right) = \nu_p(f_j)$$

So that we can define

$$\nu_p(\omega) = \nu_p(f_i), \qquad p \in U_i$$

If $\nu_p(\omega) > 0$ then p is called a zero of ω and if $\nu_p(\omega) < 0$ then p is called a pole of ω.

Definition 7.2.4. *Suppose C is a Riemann surface with*

$$\omega = \{(U_i, z_i, f_i(z_i)dz_i)\} \in K^1(C),$$

and γ be a piecewise smooth curve on C not containing the poles of ω and $\gamma = \cup_i \gamma_i$ is a partition of γ satisfying $\gamma_i \subset U_i$, we define the integral

$$\int_\gamma \omega = \sum_i \int_{\gamma_i} f_i(z_i)dz_i$$

Observe that this definition is well-defined because suppose $\gamma = \cup_i \gamma_i'$ be any other partition. Then by change of variables formula,

$$\int_{\gamma_i \cap \gamma_j'} f_i(z_i)dz_i = \int_{\gamma_i \cap \gamma_j'} f_i(z_i)dz_i$$

so that

$$\begin{aligned}
\sum_i \int_{\gamma_i} f_i(z_i)dz_i &= \sum_i \sum_j \int_{\gamma_i \cap \gamma_j'} f_i(z_i)dz_i \\
&= \sum_j \sum_i \int_{\gamma_i \cap \gamma_j'} f_j(z_j)dz_j \\
&= \sum_j \int_{\gamma_j'} f_j(z_j)dz_j.
\end{aligned}$$

Theorem 7.2.5. ***(Stoke's Theorem)*** *Suppose C is a Riemann surface with $\Omega \subset C$ an open set, $\overline{\Omega}$ compact, $\partial\Omega = \gamma$, a piecewise smooth curve, and ω a holomorphic differential on an open set containing $\overline{\Omega}$. Then*

$$\int_{\partial\Omega} \omega = 0.$$

Proof. Suitably subdivide Ω into a disjoint union $\Omega = \cup_i \Omega_i$ such that for each i, $\Omega_i \subset U_i$ and $\partial\Omega_i$ is a piecewise smooth curve. By using local coordinate representations and applying Cauchy's theorem we get,

$$\int_{\partial\Omega_i} \omega = 0$$

and therefore,

$$\sum_i \int_{\partial\Omega_i} \omega = 0.$$

But observe that while adding up, contribution of the boundaries $\partial\Omega_i$ cancels out other than those arcs contributing to $\partial\Omega$, thus we have

$$\int_{\partial\Omega} \omega = \sum_i \int_{\partial\Omega_i} \omega = 0.$$

□

Definition 7.2.6. *Suppose C is a Riemann surface with $\omega \in K^1(C)$, $p \in C$, γ_p a small circle around the point p and ω has no other poles other than p on the disc surrounded by γ_p (p itself may or may not be a pole). Then we define the residue of a point p of ω to be*

$$Res_p(\omega) = \frac{1}{2\pi\iota} \oint_{\gamma_p} \omega$$

From Stoke's theorem this definition is independent of the choice of γ_p.

Theorem 7.2.7. ***(Residue Theorem)*** *Let C is a compact Riemann surface. For $\omega \in K^1(C)$, we have*

$$\sum_{p \in C} Res_p(\omega) = 0$$

Proof. Since C is compact, ω can have only finitely many poles on C. Say $p_1, p_2, \ldots, p_m$ are the poles. Choose mutually disjoint small discs $\Delta_1, \Delta_2, \ldots, \Delta_m$ satisfying conditions of Definition 7.2.6. Now for any point p other than these p_i's one can choose a suitable circle so that ω is holomorphic on the disc and hence from stoke's theorem the residue at p is 0. Thus residue at the points p_i's only contribute to the sum. Let $\Omega = C \setminus \bigcup \Delta_i$. We can choose a suitable orientation for the $\partial\Delta_i$'s so that $\partial\Omega = -\bigcup_i \partial\Delta_i$. Again applying Stoke's theorem we get,

$$\begin{aligned} 2\pi\iota \sum_{p \in C} Res_p(\omega) &= 2\pi\iota \sum_{i=1}^{m} Res_{p_i}(\omega) \\ &= \sum_{i=1}^{m} \int_{\partial\Delta_i} \omega \\ &= -\int_{\partial\Omega} \omega \\ &= 0. \end{aligned}$$

□

Theorem 7.2.8. *Let C be a Compact Riemann surface. If $f \in K(C)$ is a non-constant function, then*

$$\sum_{p \in C} \nu_p(f) = 0$$

This implies that the number of zeroes of f is equal to the number of poles of f counted properly (i.e. counting multiplicities).

Proof. Use $\omega = \frac{df}{f}$. □

7.3 Differential forms

A function $f : \mathbb{C} \to \mathbb{C}$ can be also thought of as a mapping $f : \mathbb{R}^2 \to \mathbb{C}$ as $f(x, y) = u(x, y) + \iota v(x, y)$. We fix the following notation :

$$dz = dx + \iota dy, \qquad d\bar{z} = dx - \iota dy$$

$$\frac{\partial f}{\partial z} = \frac{1}{2}\left(\frac{\partial f}{\partial x} - \iota\frac{\partial f}{\partial y}\right),$$

$$\frac{\partial f}{\partial \bar{z}} = \frac{1}{2}\left(\frac{\partial f}{\partial x} + \iota\frac{\partial f}{\partial y}\right),$$

$$df = \frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy = \frac{\partial f}{\partial z}dz + \frac{\partial f}{\partial \bar{z}}d\bar{z}$$

Clearly, $\partial f/\partial\bar{z} = 0$ is equivalent to the Cauchy-Riemann equations. So f is holomorphic if and only if

$$\frac{\partial f}{\partial \bar{z}} = 0$$

For a vector space V one can define a bilinear, anti-symmetric exterior product " $\wedge$ " as follows :

$$\begin{aligned}
&(av_1) \wedge v_2 = a(v_1 \wedge v_2) \\
&(v_1 + v_1') \wedge v_2 = v_1 \wedge v_2 + v_1' \wedge v_2 \\
&v_2 \wedge v_1 = -v_1 \wedge v_2.
\end{aligned}$$

Using the previous notation, we have the following relation between the exterior product of the real differentials $dx,\ dy$ and that of the complex differentials $dz,\ d\bar{z}$

$$dz \wedge d\bar{z} = -2\iota\ dx \wedge dy$$

Definition 7.3.1. *Let C be a Riemann surface with holomorphic coordinate covering $\{(U_i, z_i)\}$. A differential 1-form λ on C is given by a family of local expressions*

$$\lambda_i = f_i(z_i, \bar{z}_i)dz_i + g_i(z_i, \bar{z}_i)d\bar{z}_i$$

where f_i, g_i are smooth functions which obey the following transformation laws :

$$f_i(\phi_{ij}(z_j), \overline{\phi_{ij}(z_j)})\frac{d\phi_{ij}(z_j)}{dz_j} = f_j(z_j, \bar{z}_j),$$

$$g_i(\phi_{ij}(z_j), \overline{\phi_{ij}(z_j)})\frac{d\phi_{ij}(z_j)}{dz_j} = g_j(z_j, \bar{z}_j).$$

We define the exterior derivative $d\lambda$ of the differential 1-form $\lambda = \{f_i dz_i + g_i d\bar{z}_i\}$ as

$$\begin{aligned} d\lambda &= \{df_i \wedge dz_i + dg_i \wedge d\bar{z}_i\} \\ &= \left\{ \left(\frac{\partial g_i}{\partial z_i} - \frac{\partial f_i}{\partial \bar{z}_i} \right) dz_i \wedge d\bar{z}_i \right\} \end{aligned}$$

The differential 1-form λ on C is called a ***closed*** 1-form if $d\lambda = 0$. If there exists a smooth function f such that $\lambda = df$, then λ is called an ***exact*** 1-form.

Remark 7.3.2. From

$$\frac{\partial^2 f}{\partial z \partial \bar{z}} = \frac{\partial^2 f}{\partial \bar{z} \partial z}$$

we have,

$$\begin{aligned} d(df) &= d\left(\frac{\partial f}{\partial z} dz + \frac{\partial f}{\partial \bar{z}} d\bar{z} \right) \\ &= \frac{\partial^2 f}{\partial \bar{z} \partial z} d\bar{z} \wedge dz + \frac{\partial^2 f}{\partial z \partial \bar{z}} dz \wedge d\bar{z} \\ &= \left(\frac{\partial^2 f}{\partial z \partial \bar{z}} - \frac{\partial^2 f}{\partial \bar{z} \partial z} \right) dz \wedge d\bar{z} \ = 0. \end{aligned}$$

Thus any exact form is always closed.

Chapter 8

Normalization

8.1 Singularities of plane algebraic curves

Consider the plane algebraic curve $C = \{[x, y, z] \in P^2\mathbb{C} \mid F(x, y, z) = 0\}$. The points P are the called singularities or singular points of C, at which

$$\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0$$

Let us look at what happens at the singularities. Suppose P is any point on the plane algebraic curve C, and choose coordinates of $P^2\mathbb{C}$ such that $P = [0, 0, 1]$. Moreover, suppose the equation of is $F(x, y, z) = 0$, and let $f(x, y) = F(x, y, 1)$. Then, the curve corresponding to $f(x, y) = 0$ is $C \ \cap \mathbb{C}^2$. Here $\mathbb{C}^2$ is canonically embedded in $P^2\mathbb{C}$ as usual. Write $f(x, y)$ as the sum of homogeneous polynomials in ascending degrees

$$f(x, y) = f_k(x, y) + f_{k+1}(x, y) + \cdots + f_d(x, y)$$

where $f_j(x, y)$ is a homomgeneous polynomial of degree j and $f_k \not\equiv 0$. Since $f(0, 0) = 0$ we have $k \geq 1$. If $k = 1$ then $f_1(x, y) = ax + by \not\equiv 0$ i.e.

$$\left.\frac{\partial f}{\partial x}\right|_{(0,0)} = a \neq 0 \quad \text{or} \quad \left.\frac{\partial f}{\partial y}\right|_{(0,0)} = b \neq 0$$

This implies that $P = (0, 0)$ is a smooth point of C, and has a tangent line at P

$$f_1(x, y) = ax + by = 0$$

We therefore call P a *simple point* of C. In order for P to be a singularity of C, it is necessary and sufficient to have $k \geq 2$. If $k = 2$, we call P a double point. If the two tangents at P are distinct we call it a node otherwise a cusp. In general, if

$$f_0 \equiv f_1 \equiv \cdots \equiv f_{k-1} \equiv 0 \quad \text{and } f_k \not\equiv 0 \quad \text{at } P \text{ on } C$$

then C has k tangent lines at P (multiple tangents counted with the appropriate multiplicity) which are given by

$$f_k(x, y) = 0$$

and we call P a k-tuple point of C.

Definition 8.1.1. *P is called an ordinary k-tuple point of if P is a k-tuple point of C and the k tangent lines at this point are distinct.*

8.2 The connectedness of irreducible plane algebraic curves

We want to show the set S of singular points of an algebraic curve is a finite set. For this, we must discuss the eliminant and discriminant of polynomials.

Lemma 8.2.1. *Suppose D is a unique factorization domain (U.F.D.), and*

$$f(x) = a_0x^m + \cdots a_m \qquad a_0 \neq 0$$
$$g(x) = b_0x^n + \cdots b_n \qquad b_0 \neq 0$$

are polynomials over D. Then a necessary and sufficient condition for f and g to possess a nontrivial common factor is that there exist two polynomials $F,\ G \in D[x]$, not both equal to 0, which satisfy

$$deg\ F < m, \quad deg\ G < n, \quad fG = gF.$$

Proof. From the well-known Gauss Lemma of algebra, $D[x]$ is also a U.F.D. Suppose h is a nontrivial common factor of f and g. Then

$$f = Fh, \quad F \in D[x], \quad \deg F < m,$$
$$g = Gh, \quad G \in D[x], \quad \deg G < n.$$

That is we get $fG = gF$.

Conversely, if there exist two polynomials $F,\ G \in D[x]$, not both 0, which satisfy

$$\deg F < m, \quad \deg G < n, \quad fG = gF,$$

then the nontrivial factors of f cannot all be factors of F (since deg F <deg f). Since $D[x]$ is a U.F.D., there must be a nontrivial factor of f which divides g. □

The polynomials F and G in the preceding lemma can be written ex- explicitly as

$$F(x) = A_0x^{m-1} + \cdots + A_{m-1}$$
$$G(x) = B_0x^{n-1} + \cdots + B_{n-1}$$

Comparing the coefficients of both sides of $fG = gF$, we get

$$a_0B_0 = b_0A_0,$$
$$a_1B_0 + a_0B_1 = b_1A_0 + b_0A_1$$
$$\cdots\cdots$$
$$a_mB_{n-1} = b_nA_{m-1}$$

We can think of the above expression as a system of homogeneous linear equations in $B_0, ..., B_{n-1},\ A_0, ..., A_{m-1}$, so that a necessary and sufficient condition for this system to have a nonzero solution is that its determinant be equal to 0.

$$\begin{vmatrix}
a_0 & & & & b_0 & & & \\
a_1 & a_0 & & & b_1 & b_0 & & \\
\vdots & a_1 & \vdots & & \vdots & b_1 & \vdots & \\
\vdots & \vdots & \vdots & a_0 & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & a_1 & b_n & \vdots & \vdots & b_0 \\
a_m & \vdots & \vdots & \vdots & & b_n & \vdots & b_i \\
 & a_m & \vdots & \vdots & & & \vdots & \vdots \\
 & & \vdots & \vdots & & & \vdots & \vdots \\
 & & & a_m & & & & b_n
\end{vmatrix} = 0$$

By transposing the matrix of this determinant we can summarize the foregoing in the following theorem.

Theorem 8.2.2. *Suppose D is a unique factorization domain (U.F.D.), and*

$$f(x) = a_0x^m + \cdots a_m \qquad a_0 \neq 0$$

$$g(x) = b_0x^n + \cdots b_n \qquad b_0 \neq 0$$

are polynomials over D. Then a necessary and sufficient condition for f and g to possess a nontrivial common factor is that the determinant be equal to 0.

$$\mathscr{R}(f,g) = 0$$

where

$$\mathscr{R}(f,g) = \begin{vmatrix} a_0 & a_1 & \dots & \dots & \dots & a_m & & & \\ & a_0 & a_1 & \dots & \dots & \dots & a_m & & \\ & & \dots & \dots & \dots & \dots & \dots & \dots & \\ & & & a_0 & a_1 & \dots & \dots & \dots & a_m \\ b_0 & b_1 & \dots & \dots & b_n & & & & \\ & b_0 & b_1 & \dots & \dots & b_n & & & \\ & & \dots & \dots & \dots & \dots & \dots & & \\ & & & & b_0 & b_1 & \dots & \dots & b_n \end{vmatrix}$$

Definition 8.2.3. *This determinant, $\mathscr{R}(f,g)$, is called the eliminant (or resultant) of f and g.*

Definition 8.2.4. *Suppose D is a U.F.D. Then the eliminant of $f \in D[x]$ and its derivative polynomial f', denoted by*

$$\mathscr{D}(f) \equiv \mathscr{R}(f,f')$$

is called the discriminant of f.

Corollary 8.2.5. *Suppose D is a unique factorization domain (U.F.D.), then a necessary and sufficient condition for $f \in D[x]$ to have multiple factors is that its disriminant be equal to 0, i.e. $\mathscr{D}(f) = 0$*

Theorem 8.2.6. *An irreducible plane algebraic curve C has at most finitely many singular points.*

Proof. Choose a coordinate system in $P^2\mathbb{C}$ such that C possesses an affine equation of the following form:

$$f(x,y) = y^n + a_1(x)y^{n-1} + \cdots + a_n(x) = 0,$$

where $a_j(x) \in \mathbb{C}[x]$ with deg $a_j(x) \leq j$ or $a_j(x) = 0$. This can be done in the following way. Let $g(x,y) = 0$ be the affine equation of C which is not necessarily in the above form. Make a suitable coordinate transformation,

$$x = x' + \lambda y'$$
$$y = y'.$$

Consider the coefficient $b(\lambda)$ of the term involving y'^n in $g(x'+\lambda y', y')$. Clearly it is a non-zero polynomial in λ and hence is 0 for only finitely many values of λ. We can choose λ such that $b(\lambda) \neq 0$. we write

$$f(x',y') = \frac{1}{b(\lambda)} g(x' + \lambda y', y')$$

and in the affine coordinate system (x', y'), the equation of C is $f(x',y') = 0$ which is of the required form.

Consider f as an element of $\mathbb{C}[x][y]$ and look at its discriminant (here $f_y = \partial f / \partial y$).

$$\mathscr{D}(f) \equiv \mathscr{R}(f, f_y)$$

$\mathscr{D}(f)$ is now an element in $\mathbb{C}[x]$. For clarity we write $\mathscr{D}(f)(x)$. Since f is irreducible we must have

$$\mathscr{D}(f)(x) \not\equiv 0$$

Hence it can have atmost finitely many roots. Let S denote the set of singular points of C. Obviously

$$S \cap \mathbb{C} \subset \{(x.y) \in \mathbb{C}^2 \mid f(x, y) = f_y(x, y) = 0\}$$

Consider the set

$$D = \{x \in \mathbb{C} \mid \mathscr{D}(f)(x) = 0\}$$

then D is a finite set. Moreover for each $x_0 \in \mathbb{C}$, there are only finitely many y such that $f(x_0, y) = 0$. This shows that $S \cap \mathbb{C}^2$ is a finite set. Moreover since C is an irreducible curve, C intersects the line at infinity at finitely L_∞ many points. Thus $S \cap L_\infty$ is finite. thus we have proven that an irreducible curve has atmost a finite number of singular points. □

Let us recall that an *analytic function element* is a pair, (Δ, f), which consists of an open disc $\Delta \subset \mathbb{C}$ and an analytic function f defined on this disc. Two analytic function elements (Δ_1, f_1) and (Δ_2, f_2) are said to be *direct analytic continuations* of each other if

$$\Delta_1 \cap \Delta_2 \neq \emptyset$$

and on $\Delta_1 \cap \Delta_2$ we have $f_1 \equiv f_2$. An *analytic continuation chain* is a collection of analytic function elements

$$(\Delta_1, f_1), (\Delta_2, f_2), \ldots, (\Delta_N, f_N)$$

in which any pair of successive analytic function elements are direct analytic continuations of each other. Suppose γ is a connected continuous curve (path) in $\mathbb{C}$, whose starting point and ending point are labelled as a and b, respectively, and suppose (Δ_0, f_0) is an analytic function element which satisfies $a \in \Delta_0$. Then we say that (Δ_0, f_0) can be *analytically continued along the path* γ, if there exists a partition of γ

$$\gamma = \bigcup_{j=0}^{N} \gamma_j$$

such that $\gamma_j \subset \Delta_j$ and an analytic continuation chain

$$(\Delta_0, f_0), (\Delta_1, f_1), (\Delta_2, f_2), \ldots, (\Delta_N, f_N)$$

. We state a famous result (without proof) on analytic continuations.

Theorem 8.2.7. ***(Riemann Monodromy Theorem)*** *Suppose $\Omega \subset \mathbb{C}$ is a simply connected open set. If an analytic function element, (Δ, f) can be analytically continued along any path inside Ω, then this analytic function element can be extended to be a single-valued holomorphic function defined on the whole of Ω.*

Let $C^* := C \setminus S$. We shall discuss the connectedness of C^* and C. We already know that C can have at most a finite number of singular points, and that C and L_∞, the line at infinity, intersect in a finite number of points. So the closure

$$\overline{C^* \cap \mathbb{C}^2} = C$$

The following result is a familiar fact from point set topology: if the set A is connected, and $A \subseteq B \subseteq \bar{A}$, then the set B is also connected, and in particular $\bar{A}$ is connected. Thus,

$$C^* \cap \mathbb{C}^2 \subseteq \; C^* \subseteq \; C = \overline{C^* \cap \mathbb{C}^2}$$

For simplicity, we shall temporarily use C^* and C to denote $C^* \cap \mathbb{C}^2$ and $C \cap \mathbb{C}^2$ in the following proof.

Suppsoe $C : f(x, y) = 0$. We can choose a coordinate system so that f as in Theorem 8.2.6. Consider the discriminant $\mathscr{D}(f)$ of f and the zero-set D. Let

$$\pi : C \to \mathbb{C}$$

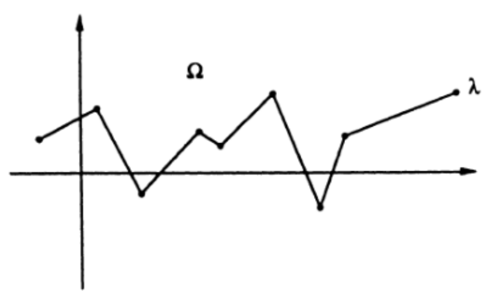
be the projection from into the x axis. We know that $\pi^{-1}(D)$ is a finite set. For $x \in \mathbb{C} \setminus D$, we have just n distinct points

$$(x, y_\nu(x)) \in C \setminus \pi^{-1}(D) \qquad (\nu = 1, ..., n)$$

such that

$$f(x, y_\nu(x)) = 0.$$

Moreover, for the points in $C \setminus \pi^{-1}(D)$, $f_y \neq 0$, and from the implicit function theorem, every $y_\nu(x)$ can be regarded as an analytic function element defined on a disc.
Let Λ be a simple broken line which connects the points (finitely many) in D and which goes to infinity. Cut the complex plane $\mathbb{C}$ along this broken line, and we obtain the simply connected region Ω as in the figure.



From the Riemann monodromy theorem, all n function elements $y_\nu(x)$ $(\nu = 1, ..., n)$, can be extended to be single-valued holomorphic functions defined over the whole of Ω, and we denote these extended functions still by $y_\nu(x) \quad (\nu = 1, ..., n)$. From the identity theorem of analytic functions, the extended $y_\nu(x)$ must still satisfy

$$f(x, y_\nu(x)) = 0.$$

Now continue $y_\nu(x) \;\; (1 \leq \nu \leq n)$ along a path γ which crosses $\Lambda \setminus D$. The extended function $y_\nu^*(x)$ must still satisfy the equation

$$f(x, y_\nu^*(x)) = 0$$

and must still be one of $y_1(x), ..., y_n(x)$. If the original

$$y_\nu(x) \neq y_{\nu'}(x)$$

then after extension we still have

$$y_\nu^*(x) \neq y_{\nu'}^*(x)$$

(otherwise we would get $y_\nu(x) = y_{\nu'}(x)$ for a continuation along the reverse path $-\gamma$). If there exists a path γ in $\mathbb{C} \setminus D$ such that $y_\nu(x)$ and $y_\mu(x)$ are mutually continuable along γ, we can then write

$$y_\mu(x) \sim y_\nu(x)$$

and it is easy to see that $\sim$ is an equivalence relation. Using the equivalence relation to divide $y_1(x), ..., y_n(x)$ into equivalence classes $E_1, E_2, \dots, E_l$ we shall prove that for every E_j we have

$$\prod_{y_\nu(x) \in E_j} (y - y_\nu(x)) \in \mathbb{C}[x, y]$$

and

$$f(x, y) = \prod_{j=i}^{l} \prod_{y_\nu(x) \in E_j} (y - y_\nu(x))$$

Whence, if $f(x, y)$ is irreducible, we can only have $l = 1$, i.e., $y_1(x), ..., y_n(x)$ all belong to one equivalence class and they are all mutually continuable along paths in $\mathbb{C} \setminus D$. That is to say, any two points and $(x_0, y_\nu(x_0))$ and $(x_1, y_\mu(x_1))$ in $C \setminus \pi^{-1}(D)$ can be connected by a path. This proves that $C \setminus \pi^{-1}(D)$ is connected. Thus the proof of the connectedness of C^* and C reduces to the proof of the following lemma.

Lemma 8.2.8. *(Same notation as in the preceding.) For any equivalence class E of the equivalence relation $\sim$ formed by $y_1(x), ..., y_n(x)$, we have*

$$\prod_{y_\nu(x) \in E} (y - y_\nu(x)) \in \mathbb{C}[x, y]$$

Proof. There is no harm in assuming $E = \{y_1(x), ..., y_m(x)\}$. Then,

$$\begin{aligned}\prod_{y_\nu(x) \in E} (y - y_\nu(x)) &= \prod_{\lambda=1}^{m} (y - y_\lambda(x)) \\ &= y^m + b_1(x) y^{m-1} + \cdots + b_m(x).\end{aligned}$$

where

$$\begin{aligned} b_1(x) &= -\sum_{\lambda=1}^{m} y_\lambda(x) \\ b_2(x) &= \sum_{1 \le \lambda < \mu \le m} y_\lambda(x) y_\mu(x) \\ \dots & \quad \dots \quad \dots \quad \dots \\ b_m(x) &= (-1)^m y_1(x) y_2(x) \cdots y_m(x). \end{aligned}$$

Since the continuation of any path in $\mathbb{C} \setminus D$ only leads to a permutation in E, each $b_j(x) \quad (j = 1, ..., m)$ being unchanged under such a permutation defines a single-valued holomorphic function on $\mathbb{C} \setminus D$.

By Rouche's theorem, if the coefficients of the polynomial

$$y^n + a_1 y^{n-1} + \cdots + a_n$$

satisfy

$$|a_j| \le M \qquad (j = 1, ..., n)$$

then every root of this polynomial must satisfy

$$|y_\nu| \leq 1 + M$$

Therefore every $b_\lambda(x)(\lambda = 1, ..., m)$ as defined above is bounded in a neighborhood of every point in D. By Riemann's extension theorem, each $b_\lambda(x)$ can be extended to be a holomorphic function on the whole of $\mathbb{C}$, and we denote the extended function still by $b_\lambda(x) \quad (\lambda = 1, ..., m)$. We shall now prove that every $b_\lambda(x)$ is in fact a polynomial. In order to do this, let us examine the $b_\lambda(x)$'s in a neighborhood of the point at infinity. We need only show that the point at infinity is a pole of each $b_\lambda(x)$. In the original polynomial

$$f(x, y) = y^n + a_i(x)y^{n-1} + \cdots + a_n(x)$$

we make a change of variables

$$\begin{aligned} x &= 1/x' \\ y &= y'/x'. \end{aligned}$$

to obtain

$$x'^n f\left(\frac{1}{x'}, \frac{y'}{x'}\right) = y'^n + \left(x' a_1 \left(\frac{1}{x'}\right)\right) y'^{n-1} + \cdots + x'^n a_n \left(\frac{1}{x'}\right)$$

Since we are working under the hypothesis that $f(x, y)$ satisfies the condition of Theorem 8.2.6 , we have

$$\deg a_\nu \leq \nu \quad \text{or} \quad a_\nu = 0 \quad (\nu = 1, \ldots, n)$$

So,

$$x'^\nu a_\nu \left(\frac{1}{x'}\right) \in \mathbb{C}[x']$$

and therefore

$$x'^n f\left(\frac{1}{x'}, \frac{y'}{x'}\right) = y'^n + \left(x' a_1 \left(\frac{1}{x'}\right)\right) y'^{n-1} + \cdots + x'^n a_n \left(\frac{1}{x'}\right) \in \mathbb{C}[x', y']$$

Fix x' and consider this polynomial as a polynomial in y'. Then $r \equiv r(x')$ is a root of this polynomial in $'$ if and only if $x'^n f(1/x', r/x') = 0$, if and only if $f(x', r/x') = 0$, if and only if $r/x' = y_\nu(x)$ for some $\nu \in 1, ..., n$, if and only if $r = x' y_\nu(1/x')$ for some $\nu \in 1, ..., n$. Hence in the set

$$\{x' \mid 1/x' \in \Omega \equiv \mathbb{C} \setminus \Lambda\}$$

the roots of the above polynomial in y' give rise to n holomorphic functions

$$y'_\nu(x') = x' y_\nu (1/x')$$

and m of these $\{y'_1(x'), \ldots, y'_m(x')\}$ get permuted among themselves when analytically continued along any path which avoids the set

$$\{x' \mid x' = 0 \quad \text{or} \quad 1/x' \in D\}$$

Now observe that for the same reason as above, each $y'_\nu(')$ is bounded in a neighborhood of $x' = 0$. Furthermore,

$$\begin{aligned}
x'b_1\left(\frac{1}{x'}\right) &= -x'\sum_{\lambda=1}^{m} y_\lambda\left(\frac{1}{x'}\right) = -\sum_{\lambda=1}^{m} y'_\lambda(x'),\\
x'2b_2\left(\frac{1}{x'}\right) &= x'^2 \sum_{1\le\lambda<\mu\le n} y_\lambda\left(\frac{1}{x'}\right) y_\mu\left(\frac{1}{x'}\right) = \sum_{1\le\lambda<\mu\le n} y'_\lambda(x')y'_\mu(x'),\\
\cdots \quad & \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots\\
x'^m b_m\left(\frac{1}{x'}\right) &= (-1)^m x'^m y_1\left(\frac{1}{x'}\right)\cdots y_m\left(\frac{1}{x'}\right) = (-1)^m y'_1(x')\cdots y'_m(x').
\end{aligned}$$

Hence $x'^\nu b_\nu(1/x'),\ \nu = 1, ..., m.$ are all bounded holomorphic functions in a neighborhood of $x' = 0$. This tells us that each $b_\lambda(1/x')$ has a pole at $x' = 0$ of multiplicity atmost λ, so that $b_\lambda(x)$ is a polynomial of degree at most λ. □

The preceding discussion has already proven that $C \setminus \pi^{-1}(D)$ is connected, and as remarked before the connectedness of $C^* = C \setminus S$ and C is then a direct consequence of this due to

$$C \setminus \pi^{-1}(D) \subseteq C^* \subseteq C = \overline{C \setminus \pi^{-1}(D)}$$

Theorem 8.2.9. *Suppose C is an irreducible plane algebraic curve. Then C and C^*, the set of smooth points of C, are both connected sets in $P^2\mathbb{C}$.*

Corollary 8.2.10. *C^* is a Riemann surface.*

8.3 Concept of Normalization

Definition 8.3.1. *Suppose C is an irreducible plane algebraic curve, and S is the set of its singular points. If there exists a compact Riemann surface $\tilde{C}$ and a holomorphic mapping*

$$\sigma : \tilde{C} \to P^2\mathbb{C}$$

such that

1. *$\sigma(\tilde{C}) = C$,*
2. *$\sigma^{-1}(S)$ is a finite set,*
3. *$\sigma : \tilde{C} \setminus \sigma^{-1}(S) \to C \setminus S$ is injective*

then we call $(\tilde{C}, \sigma)$ the normalization of C. When there is no danger of confusion, one would simply say that $\tilde{C}$ is the normalization of C.

We end this chapter with the statement of the following theorem (without proof).

Theorem 8.3.2. *The normalization of an irreducible plane algebraic curve C exists and is unique in the sense of isomorphism, i.e., if $(\tilde{C}, \sigma)$ and $(\tilde{C}', \sigma')$ are normalizations of C, then there exists an isomorphism (biholomorphic mapping),*

$$\tau : \tilde{C} \to \tilde{C}'$$

such that $\sigma = \sigma' \cdot \tau$

Chapter 9

Appendix I

9.1 Introduction to Manifolds

Definition 9.1.1. *Assume n is a positive is a positive integer. An n-dimensional manifold is a Hausdorff topological space such that each point has an open neighbourhood homeomorphic to the open unit disc U^n $(= \{x \in \mathbb{R}^n : |x| = 1\})$ in $\mathbb{R}^n$.*

For simplicity we will say "n-manifold".

Example 9.1.2. Euclidean n-space $\mathbb{R}^n$ is obviously an n-manifold. We can easily prove that the n-dimensional sphere

$$S^n = \{x \in \mathbb{R}^{n+1} \ : \ |x| < 1\}$$

is an n-manifold. For the point $(1, 0, \cdots, 0)$, the set $\{(x_1, x_2, \cdots, x_{n+1}) \in S^n : x_1 > 0\}$ is a neighbourhood with the required properties. As we see by taking orthogonal projection on the hyperplane defined by $x_1 = 0$ of $\mathbb{R}^{n+1}$. For any other point $x \in S^n$ there is a rotation which takes the point x to $(1, 0, \cdots, 0)$ and this rotation is a homeomorphism os S^n onto itself. Thus x also has the required kind of neighbourhood.

Example 9.1.3. If M^n is any n-manifold then it immediately follows that any open subset of M^n is also an n-manifold.

Connected n-manifolds for $n > 1$ are divided into two kinds: orientable and non-orientable. Consider the case $n = 2$. We can prescribe various orientations in $\mathbb{R}^2$ or more generally for a small region in the plane. For example we can consider the co-ordinate system to be right-handed or left-handed. Another way would be which direction of rotation in the plane about a point is to be considered positive. Roughly, orientability means if we take an orientable circle in the surface and move around it, no matter how, we end up with the same orientation. A typical example of a non-orientable surface is $M\ddot{o}bius\ strip$. We will give a more mathematical definition of orientability. But before that let us give a few definitions.

Definition 9.1.4. *A coordinate chart on a set X is a subset U $\subseteq$ X, together with a homeomorphism*

$$\varphi : U \to \varphi(U)$$

onto an open subset $\varphi(U)$ of $\mathbb{R}^n$.

Thus we can parametrize x in U by n coordinates $\varphi(x) = (x_1, x_2, \cdots, x_n)$. A transition map provides a way of comparing two charts. To make this comparison, we consider the composition of one chart with the inverse of the other.

Definition 9.1.5. *Suppose* $(U_\alpha, \varphi_\alpha)$ *and* (U_β, φ_β) *are two charts for a manifold X such that* $U_\alpha \cap U_\beta \neq \emptyset$*. The transition maps are defined by*

$$\varphi_\beta \circ \varphi_\alpha^{-1} : \varphi_\alpha(U_\alpha \cap U_\beta) \to \varphi_\beta(U_\alpha \cap U_\beta)$$

$$\varphi_\alpha \circ \varphi_\beta^{-1} : \varphi_\beta(U_\alpha \cap U_\beta) \to \varphi_\alpha(U_\alpha \cap U_\beta)$$

Definition 9.1.6. *An atlas for X is a colection of charts* $\{(U_\alpha, \varphi_\alpha)\}$ *such that* $\bigcup_\alpha U_\alpha = X$ *and the transition maps are homeomorphisms.*

The transition maps formalizes the notion of "patching together pieces of a space to make a manifold" the manifold produced also contains the data of how it has been patched together. However, different atlases (patchings) may produce "the same" manifold; a manifold does not come with a preferred atlas. And, thus, one defines a topological manifold to be a space as above with an equivalence class of atlases, where one defines equivalence of atlases below.

Two atlases $\mathcal{A}_1$ and $\mathcal{A}_2$ are equivalent if and only if their union $\mathcal{A}_1 \cup \mathcal{A}_2$ is an atlas.

Definition 9.1.7. *A differentiable manifold is a topological manifold equipped with an equivalence class of atlases whose transition maps are all differentiable.*

9.1.1 Orientability

We come back to defining orientability in mathematical terms. Let us consider a differentiable n-manifold M. Let P be a point on M. Then there is a neighbourhood N_P of P which is homeomorphic to the unit disc. Let us identify N_P with this unit disc $\{(x_1, x_2, \cdots, x_n) \in \mathbb{R}^n : |x_1|^2 + \cdots + |x_n|^2 < 1\}$.
Given another point P' on M, we likewise identify a neighbourhood $N_{P'}$ with the unit disc $\{(x'_1, x'_2, \cdots, x'_n) \in \mathbb{R}^n : |x'_1|^2 + \cdots + |x'_n|^2 < 1\}$.On $N_P \cap N_{P'}$ we can express $x'_1, x'_2, \cdots, x'_n$ as functions of $x_1, x_2, \cdots, x_n$ using transition maps. On a differentiable manifold this maps have continuous partial derivatives, hence we can talk about the Jacobian determinant $det\left(\frac{\partial x'_i}{\partial x_j}\right)_{1\leq i,j\leq n}$. Now orientability can be defined by requiring that for each pair of point P, P' on M, the value of the above determinant is positive on $N_P \cap N_{P'}$.

By changing $\mathbb{R}$ to $\mathbb{C}$ in the definition of a manifold, and requiring the transition maps to be holomorphic we get a differentiable complex manifold. By splitting the complex local coordinates into real and imaginary parts $x_i = u_i + \iota v_i$, M becomes a differentiable real manifold of dimension $2n$. In case of $n = 1$, Cauchy-Riemann equations gives the positivity of the Jacobian determinant. So that one dimensional complex manifolds are orientable as real manifolds. In fact,

A complex manifold of any dimension is orientable as a real manifold.

Sketch of the proof : Let us consider a complex n-manifold M. Like earlier we identify charts of M with unit disks in $\mathbb{C}^n$,
N_P with $\{(z_1, z_2, \cdots, z_n) \in \mathbb{C}^n : |z_1|^2 + \cdots + |z_n|^2 < 1\}$ and
$N_{P'}$ with $\{(Z_1, Z_2, \cdots, Z_n) \in \mathbb{C}^n : |Z_1|^2 + \cdots + |Z_n|^2 < 1\}$. So that the Jacobian is

$$\mathcal{J} = \left(\frac{\partial\, Z_k(z_1, \ldots, z_n)}{\partial\, z_l}\right)_{1\leq k,l\leq n} = (c_{lk})_{1\leq k,l\leq n} \in \mathrm{GL}(n, \mathbb{C})$$

Identifying $\mathbb{C}^n$ with $\mathbb{R}^{2n}$ by $(z_1, \ldots, z_n) \leftrightarrow (x_1, y_1, \ldots, x_n, y_n)$ where $z_k = x_k + \iota y_k$ and using Cauchy-Riemann equations we get

$$\begin{aligned}
\mathcal{J}_{\mathbb{R}} &= \begin{pmatrix} \frac{\partial\ X_k(x_1,y_1,\ldots,x_n,y_n)}{\partial\ x_l} & \frac{\partial\ X_k(x_1,y_1,\ldots,x_n,y_n)}{\partial\ y_l} \\ \frac{\partial\ Y_k(x_1,y_1,\ldots,x_n,y_n)}{\partial\ x_l} & \frac{\partial\ Y_k(x_1,y_1,\ldots,x_n,y_n)}{\partial\ y^l} \end{pmatrix}_{1\le k,l\le n} \\
&= \begin{pmatrix} \mathrm{Re}(c_{lk}) & -\mathrm{Im}(c_{lk}) \\ \mathrm{Im}(c_{lk}) & \mathrm{Re}(c_{lk}) \end{pmatrix}_{1\le k,l\le n} \in \mathrm{GL}(2n, \mathbb{R}),
\end{aligned}$$

We will calculate the determinant of these. Consider the $\mathbb{R}$-algebra homomorphism $\rho : M_n(\mathbb{C}) \to M_{2n}(\mathbb{R})$

$$(c_{lk})_{1\le k,l\le n} \mapsto \begin{pmatrix} \mathrm{Re}(c_{lk}) & -\mathrm{Im}(c_{lk}) \\ \mathrm{Im}(c_{lk}) & \mathrm{Re}(c_{lk}) \end{pmatrix}_{1\le k,l\le n}$$

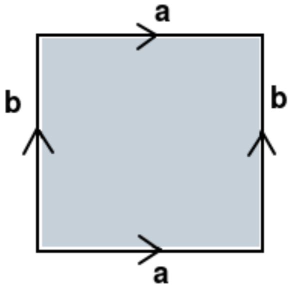
Since only finite dimensional spaces are involved, ρ is continuous. Also it is a homomorphism, we have $\det\ \rho(P^{-1}AP) = \det(\rho(P)^{-1}\rho(A)\rho(P)) = \det(\rho(A))$. Finally diagonalizable matrices are dense in $M_n(\mathbb{C})$, so that we can restrict our calculations to diagonalizable matrices. So,
$\det(\rho(A)) = \det\ \rho(P^{-1}AP) = \det\rho(\mathbf{diag}(c_1, \ldots, c_n))$

$$\begin{aligned}
&= \det\big(\rho(\mathrm{Diag}(c_1, \ldots, c_n))\big) \\
&= \det\ \mathrm{Diag}\left(\begin{pmatrix} \mathrm{Re}(c_1) & -\mathrm{Im}(c_1) \\ \mathrm{Im}(c_1) & \mathrm{Re}(c_1) \end{pmatrix}, \ldots, \begin{pmatrix} \mathrm{Re}(c_n) & -\mathrm{Im}(c_n) \\ \mathrm{Im}(c_n) & \mathrm{Re}(c_n) \end{pmatrix}\right) \\
&= \prod_{i=1}^{n} \det \begin{pmatrix} \mathrm{Re}(c_i) & -\mathrm{Im}(c_i) \\ \mathrm{Im}(c_i) & \mathrm{Re}(c_i) \end{pmatrix} \\
&= \prod_{i=1}^{n} |c_i|^2 \\
&= |\det\ \mathrm{Diag}(c_1, \ldots, c_n)|^2,
\end{aligned}$$

So that we conclude $\forall A \in M_n(\mathbb{C}),\ \det\rho(A) \ge 0$. In particular, as $\mathcal{J}_{\mathbb{R}} \in \mathrm{GL}(2n, \mathbb{R})$, $\det(\mathcal{J}_{\mathbb{R}}) > 0$. So M is orientable as a real manifold.

9.2 Compact surfaces and Classification Theorem

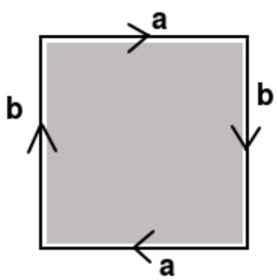
From now on we will restrict ourselves to real manifolds. A connected 2-manifold is called a *surface*.
Example: The simplest example of a surface is the 2-sphere S^2. Another example is a *torus*. A torus may be defined more precisely as: Let X denote the unit square in the plane $\mathbb{R}^2$:$\{(x, y) \in \mathbb{R}^2 : 0 \le x \le 1,\ 0 \le y \le 1\}$. Then a torus is any space homeomorphic to the quotient space of X obtained by identifying the opposite sides of the square according to the following rule : The points $(0, y)$ and $(1, y)$ are to be identified for $0 \le y \le 1$; and the points $(x, 0)$ and $(x, 1)$ are to be identified for $0 \le x \le 1$. It is convenient to indicate symbolically how such identifications are made. As in the figure, sides with the same labelled alphabet are to be identified such that the directions indicated by the arrows agree.



Example 9.2.1. Our next example of a compact surface is the real projective plane. We give a different definition here:

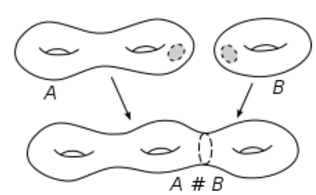
Definition 9.2.2. *The quotient space of the 2-sphere S^2 obtained by identifying every pair of diametrically opposite points is called a projective plane.*

Observe if we interpret homogeneous coordinates $[x_1, x_2, x_3]$ of a point in the projective plane (in our usual definition) as the ordinary Euclidean coordinates (x_1, x_2, x_3) of a point in $\mathbb{R}^3$, then (x_1, x_2, x_3) and (x'_1, x'_2, x'_3) represent the same point iff they lie on the same line passing though the origin. Each line passing through origin intersects the unit sphere S^2 in two diametrically opposite points. Hence is such a definition. Let $H = \{(x, y, z) \in S^2 : z \geq 0\}$ denote the closed upper hemisphere of S^2. Of each diametrically opposite pair of points in S^2, atleast one lies in H. If both lie in H, then they are on the equator.



Thus we could also define projective plane by the quotient space of H obtained by identifying diametrically opposite points in the equator (boundary of H). H is homeomorphic to the the closed unit disc $U^2 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\}$ and hence the quotient space obtained by identifying the diametrically opposite points on the boundary of U^2, gives the projective plane. Also we can replace U^2 by any space homemorphic to it, e.g. the unit square. Thus a projective plane is obtained by identifying the opposite sides of a square as shown in the figure below. One can easily see that this surface is non-orientable, infact it contains a subset homeomorphic to the $M\ddot{o}bius\ strip$.

9.2.1 Connected Sums



Let $S_1,\ S_2$ be two disjoint surfaces. Their ***connected sum***, denoted by $S_1 \# S_2$, is formed by cutting a small circular hole in each surface and gluing the surfaces together along the boundary of the hole. More precisely, we choose $D_1 \subset S_1$ and $D_2 \subset S_2$ to be two closed discs (i.e. homeomorphic to the closed unit disc in $\mathbb{R}^2$). Choose a homeomorphism $h : \partial D_1 \to \partial D_2$. Denote $S'_i = S_i - Int(D_i)$ for $i = 1, 2$. Then $S_1 \# S_2$ is the quotient space of $S'_1 \cup s'_2$ obtained by identifying the points x and $h(x)$ for all points x in ∂D_1 (the boundary of D_1).

Example 9.2.3. If S_2 be the two sphere then for any surface S_1, then $S_1 \# S_2$ is homeomorphic to S_1.

Example 9.2.4. If $S_1,\ S_2$ are both tori, then as in the figure, $S_1 \# S_2$ is the double tori.

From definition it is clear that there is no distinction between $S_1 \# S_2$ and $S_2 \# S_1$. Hence the operation of forming connected sums is commutative. Also it is not difficult to see that $S_1 \# (S_2 \# S_3)$ and $(S_1 \# S_2) \# S_3$ are homeomorphic. By example [9.2.3], the 2-sphere act as an identity element. However we may not have inverses. Thus the set of homeomorphism classes of compact surfaces form a *semigroup* under the operation of forming connected sums.

Let us now define what is known to be a "canonical form" for a connected sum of tori. Recall our description of a torus as a square with two sides identified. We try to obtain a similar description of the connected sum of two tori. Represent each of the tori T_1 and T_2 by two squares with opposite sides identified. Observe for each of the squares, all four vertices are identifed with a single point. To cut out a circular hole, (as we can do this any way we want,) we cut out the shaded regions as in figure in the next page. Label the boundaries c_1 and c_2 and they are to be identified as indicated by the arrows. We can also represent the complement of the holes by the pentagons shown in the figure. We now identify c_1 and c_2 which gives us the octagon in which sides are to be identified in pairs as indicated. Note that all the vertices of this octagon are to be identified to a single point. This octagon with the edges in pairs is our desired "canonical form" for the connected sum of two tori. By repeating this process using induction one can easily prove the connected sum of an n-tori is homeomorphic to the quotient space of a $4n$-gon whose edges are to be identified in pairs.

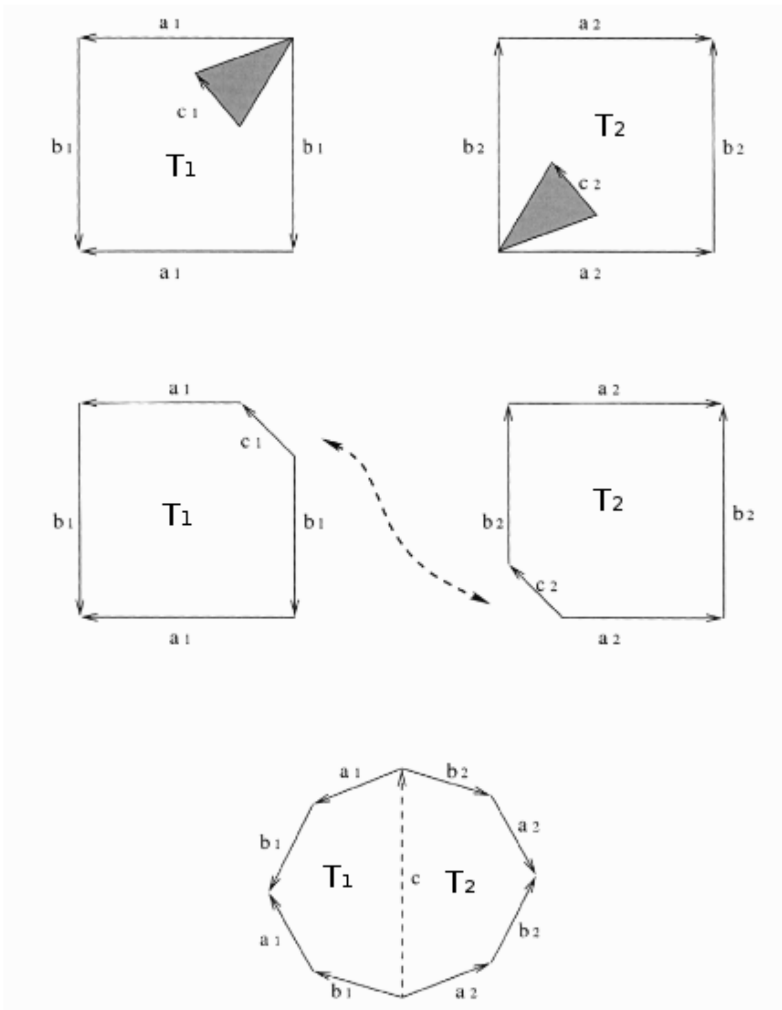


Figure I.3 : Gluing together a 2-tori

We now introduce a more convenient method of indicating more precisely which pair of edges are to be identified. Starting with a vertex we proceed along the boundary of the polygon recording the letters as follows : If the arrow on a side is in the *same* direction that we are going around the boundary, then we write the letter for that side with no exponent. If the arrow points on the *opposite* direction, then we write the letter for that side with a -1 exponent. So for the octagon in the above figure, begining with the top vertex we write

$$a_1 b_1 a_1^{-1} b_1^{-1} a_2 b_2 a_2^{-1} b_2^{-1}$$

Or as per our description of a torus as a square with opposite sides identified, one can write a torus as $aba^{-1}b^{-1}$. One can also think of a sphere according to thic scheme. Think of a sphere with a zipper on it, if the zipper is opened the purse can be flattened out. Hence it is the quotient space of a 2-gon with edges identified and can be written as aa^{-1}. The coonected sum of n-tori : $a_1 b_1 a_1^{-1} b_1^{-1} \dots a_n b_n a_n^{-1} b_n^{-1}$.

We end this chapter with the statement (without proof) of the major theorem which classifies all compact orientable surfaces.

9.3 Classification Theorem

Theorem 9.3.1. *Any compact, orientable surface is homeomorphic to a sphere or a connected sum of tori.*

Chapter 10

References

[1] Shreeream S. Abhyankar, *Algebraic Geometry for Scientists and Engineers*, AMS, First Indian edition (2011).

[2] Shreeram S. Abhyankar, *Historical Ramblings in Algebraic Geometry and Related Algebra*, *The American Mathematical Monthly*, Vol. 83, No.6, MAA.

[3] Joseph H. Silverman, John T. Tate, *Rational Points on Elliptic Curves*, Springer, Undergraduate Texts in Mathematics, Second edition.

[4] Lecture Notes on "*Introduction to Algebraic Geometry*", by Sudhir R. Ghorpade at *Science Special Lecture Series, University of Mysore*, March, 2007.

[5] Lecture Notes on "*Commutative Algebra*", by Sudhir R. Ghorpade at *Annual Foundation School-II, Bhaskaracharya Pratisthana, Pune*, June 2006.

[6] Henning Stichtenoth, *"Algebraic Function Fields and Codes"*, *Graduate text in Mathematics,* Springer.

[7] Sudhir R. Ghorpade, *"Discriminants in Algebra and Arithmetic"*, Bona Mathematica, Vol. 11.

[8] Phillip A. Griffiths, *"Introduction to Algebraic Curves"*, TRANSLATIONS OF MATHEMATICAL MONOGRAPHS, Vol 76, AMS.