The Riemann Roch Theorem
(for algebraic curves)

Weiqiong Zheng

Nov. 2017

A thesis submitted for the degree of Doctor of Philosophy
of the Australian National University
For someone or something or whatever
Declaration

The work in this thesis is my own except where otherwise stated.

Weiqiong Zheng
Acknowledgements

First, I want to thank my supervisor, Amnon Neeman, for the opportunity of doing research project with you. Also for providing suggestions and help for my honours year. I would also like to thank Joan Licata, for the kindly suggestions, understanding, and help during this year. Then I want to thank you to my classmates Kie Seng Nge, for the advise and help in both my study and life.

An enormous thank you to all of you.
Abstract

The Riemann-Roch theorem is a useful tool to calculate the dimension of the space of meromorphic functions with prescribed zeros and poles. There are several versions of the theorem such as the Riemann-Roch theorem for line bundles, for (algebraic) curves, for surfaces and for higher dimensions.

In this thesis, we will focus on the Riemann-Roch theorem for algebraic curves over an algebraically closed field, which is a very important result in complex analysis and algebraic geometry.

The study of the fields of rational functions on curves can be very useful in the proof. So we will recall some pre-knowledges in commutative algebra and some facts about affine varieties. Then talk about function fields, discrete valuation rings and Weil differentials to prove the theorem, using the methods of Andre Weil.
## Contents

Acknowledgements .......... vii
Abstract ..................... ix
Notation and terminology ... xvii

### 1 Algebraic Backgrounds  .......... 1

1.1 Rings and Ideals ............... 1

1.1.1 Definition: Rings, Integral Domains .......... 1

1.1.2 Proposition: .................. 1

1.1.3 Definition: Quotient Fields .......... 1

1.1.4 Definition: Kernel and Ideals .......... 1

1.1.5 Definition: Polynomial Rings .......... 2

1.1.6 Proposition: .................. 2

1.2 Local Rings .................. 2

1.2.1 Theorem: .................... 2

1.2.2 Definition: Local Rings and Residue Fields .......... 3

1.2.3 Proposition: .................. 3

1.2.4 Definition: Semi-local Rings .......... 3

1.3 Hilbert Basis Theorem ............ 3

1.3.1 Definition: Unit .......... 3

1.3.2 Definition: Irreducible(Prime) element .......... 3

1.3.3 Definition: Unique Factorization Domain .......... 4

1.3.4 Proposition: Gauss’s Lemma .......... 4

1.3.5 Definition: Finite Generated Ideals .......... 4

1.3.6 Definition: Noetherian Rings .......... 4

1.3.7 Theorem: Hilbert Basis Theorem .......... 5

1.3.8 Corollary: .................... 5

1.3.9 Application: .................. 6

1.4 Modules .................. 6

1.4.1 Definition: Modules .......... 6

1.4.2 Examples: Modules .......... 6

1.4.3 Definition: Submodules .......... 7
## CONTENTS

1.4.4 Example: Submodules ........................................... 7  
1.4.5 Definition: Finitely Generated Modules ...................... 7  
1.4.6 Definition: Module Homomorphisms .......................... 7  
1.4.7 Example: ....................................................... 8  
1.4.8 Proposition: .................................................... 8  
1.4.9 Definition: Direct Sum and Free Modules .................. 9  
1.4.10 Definition: Free Modules on a Set .......................... 9  
1.5 Localization of Rings ........................................... 9  
1.5.1 Motivation ...................................................... 9  
1.5.2 Definition: Multiplicatively Closed Subsets ............... 9  
1.5.3 Remark: ....................................................... 10  
1.5.4 Example: ....................................................... 10  
1.5.5 Definition: Rings of Fractions ............................... 10  
1.5.6 Theorem: Universal Property of the Ring of Fractions ...... 10  
1.5.7 Proposition: ................................................... 10  
1.5.8 Definition: Localization ..................................... 11  
1.5.9 Example: Localization ....................................... 11  
1.5.10 Proposition: Ideals in localizations ....................... 12  
1.5.11 Remarks: Prime Ideals in \( R_P \) ........................... 12  
1.5.12 Definition: Localization of Modules ...................... 12  
1.6 Dual Vector Space .............................................. 13  
1.6.1 Definition: Dual Space ..................................... 13  

2 Affine Varieties 15  
2.1 Affine Spaces and Algebraic Sets ............................... 15  
2.1.1 Definition: Affine spaces .................................. 15  
2.1.2 Definition: Algebraic Sets .................................. 15  
2.1.3 Examples: Algebraic Sets ................................... 15  
2.1.4 Proposition: .................................................. 16  
2.1.5 Definition: Zariski Topology ................................. 16  
2.1.6 Example: Zariski topology on affine spaces ............... 16  
2.2 Ideal of a Set ................................................... 17  
2.2.1 Definition: Radical ideal, radical ........................... 17  
2.2.2 Definition: Ideal of a subset ................................ 17  
2.2.3 Proposition: .................................................. 17  
2.2.4 Proposition: .................................................. 18  
2.3 Hilbert’s Nullstellensatz ..................................... 18  
2.3.1 Theorem: Weak Hilbert’s Nullstellensatz .................. 18  
2.3.2 Theorem: Hilbert’s Nullstellensatz ......................... 19  
2.3.3 Corollary: .................................................... 19  
2.3.4 Definition: Coordinate Rings .............................. 19  
2.4 Irreducibility and Dimensions ................................. 19  
2.4.1 Definition: Irreducible and connected spaces .......... 20
3 Function Field and Discrete Valuation Rings

3.1 Regular Local Rings
   3.1.1 Proposition: ........................................... 23
   3.1.2 Definition: Regular Local Ring ............................. 23

3.2 Function Fields and Valuation Rings
   3.2.1 Definition: Function field .................................... 24
   3.2.2 Definition: Valuation Ring ................................... 24
   3.2.3 Theorem: ................................................ 24
   3.2.4 Proposition: Properties of Valuation Rings ................. 26

3.3 Discrete Valuation Rings ....................................... 27
   3.3.1 Definition: discrete valuation ................................ 27
   3.3.2 Proposition: ............................................. 27
   3.3.3 Definition: Discrete Valuation Rings ......................... 27
   3.3.4 Lemma: ................................................... 28
   3.3.5 Example of Discrete Valuation Rings: ....................... 28
   3.3.6 Definition: uniformizing parameter .......................... 28
   3.3.7 Proposition: ............................................. 29
   3.3.8 Proposition: Equivalent conditions for discrete valuation rings . 29
   3.3.9 Proposition: ............................................. 30
   3.3.10 Definition: Dedekind Domains ................................ 31
   3.3.11 Proposition: ............................................. 31

3.4 Places ...................................................... 31
   3.4.1 Definition: Place ........................................... 31
   3.4.2 Theorem: ................................................ 31
   3.4.3 Lemma: ................................................... 33
   3.4.4 Theorem: ................................................ 34
   3.4.5 Definition: Zeros, poles and multiplicity .......................... 36

4 The Riemann-Roch Theorem ...................................... 37
   4.1 Divisors ..................................................... 37
   4.1.1 Definition: Divisor of a function field ........................ 37
   4.1.2 Definition: Degree of a divisor ................................ 37
   4.1.3 Example: Divisors ........................................... 37
   4.1.4 Definition: divisor of zeros and divisor of poles .............. 38
   4.1.5 Definition: Effective divisor ................................ 38
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.6</td>
<td>Corollary:</td>
<td>38</td>
</tr>
<tr>
<td>4.1.7</td>
<td>Definition: Equivalence relation on divisors</td>
<td>39</td>
</tr>
<tr>
<td>4.1.8</td>
<td>Proposition:</td>
<td>39</td>
</tr>
<tr>
<td>4.2</td>
<td>Properties of Divisors and $L(D)$</td>
<td>39</td>
</tr>
<tr>
<td>4.2.1</td>
<td>Theorem:</td>
<td>39</td>
</tr>
<tr>
<td>4.2.2</td>
<td>Definition: Partial Order on Divisors</td>
<td>40</td>
</tr>
<tr>
<td>4.3</td>
<td>The vector spaces $L(D)$</td>
<td>40</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Definition: $L(D)$</td>
<td>40</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Corollary:</td>
<td>40</td>
</tr>
<tr>
<td>4.3.3</td>
<td>Theorem:</td>
<td>40</td>
</tr>
<tr>
<td>4.3.4</td>
<td>Corollary:</td>
<td>41</td>
</tr>
<tr>
<td>4.3.5</td>
<td>Proposition:</td>
<td>42</td>
</tr>
<tr>
<td>4.4</td>
<td>The Adeles</td>
<td>42</td>
</tr>
<tr>
<td>4.4.1</td>
<td>Definition: Adele ring and Adele space</td>
<td>42</td>
</tr>
<tr>
<td>4.4.2</td>
<td>Proposition: Properties of Adele rings</td>
<td>43</td>
</tr>
<tr>
<td>4.4.3</td>
<td>Lemma:</td>
<td>43</td>
</tr>
<tr>
<td>4.4.4</td>
<td>Definition: $r(D)$</td>
<td>45</td>
</tr>
<tr>
<td>4.4.5</td>
<td>Lemma:</td>
<td>45</td>
</tr>
<tr>
<td>4.4.6</td>
<td>Theorem:</td>
<td>45</td>
</tr>
<tr>
<td>4.5</td>
<td>Genus and the Riemann’s theorem</td>
<td>47</td>
</tr>
<tr>
<td>4.5.1</td>
<td>Definition: genus</td>
<td>47</td>
</tr>
<tr>
<td>4.5.2</td>
<td>Theorem: Riemann’s Theorem</td>
<td>48</td>
</tr>
<tr>
<td>4.5.3</td>
<td>Corollary:</td>
<td>48</td>
</tr>
<tr>
<td>4.5.4</td>
<td>Corollary:</td>
<td>49</td>
</tr>
<tr>
<td>4.6</td>
<td>Weil Differentials</td>
<td>49</td>
</tr>
<tr>
<td>4.6.1</td>
<td>Motivation:</td>
<td>49</td>
</tr>
<tr>
<td>4.6.2</td>
<td>Definition: Weil Differential</td>
<td>51</td>
</tr>
<tr>
<td>4.6.3</td>
<td>Theorem:</td>
<td>51</td>
</tr>
<tr>
<td>4.6.4</td>
<td>Corollary:</td>
<td>51</td>
</tr>
<tr>
<td>4.6.5</td>
<td>Theorem:</td>
<td>52</td>
</tr>
<tr>
<td>4.6.6</td>
<td>Definition: div($\omega$)</td>
<td>52</td>
</tr>
<tr>
<td>4.6.7</td>
<td>Remark:</td>
<td>53</td>
</tr>
<tr>
<td>4.6.8</td>
<td>Lemma:</td>
<td>53</td>
</tr>
<tr>
<td>4.6.9</td>
<td>Lemma:</td>
<td>54</td>
</tr>
<tr>
<td>4.7</td>
<td>The space of Weil differentials</td>
<td>54</td>
</tr>
<tr>
<td>4.7.1</td>
<td>Theorem:</td>
<td>54</td>
</tr>
<tr>
<td>4.7.2</td>
<td>Corollary:</td>
<td>55</td>
</tr>
<tr>
<td>4.8</td>
<td>Riemann-Roch Theorem</td>
<td>56</td>
</tr>
<tr>
<td>4.8.1</td>
<td>Theorem: The Riemann-Roch Theorem</td>
<td>56</td>
</tr>
<tr>
<td>4.9</td>
<td>Applications of Riemann-Roch theorem</td>
<td>56</td>
</tr>
<tr>
<td>4.9.1</td>
<td>Corollary:</td>
<td>57</td>
</tr>
<tr>
<td>4.9.2</td>
<td>Proposition:</td>
<td>57</td>
</tr>
<tr>
<td>4.9.3</td>
<td>Theorem:</td>
<td>57</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>4.9.4</td>
<td>Remark: Other approaches towards the proof</td>
<td>59</td>
</tr>
<tr>
<td>4.9.5</td>
<td>Remark: Generalization of the theorem</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td>Bibliography</td>
<td>60</td>
</tr>
</tbody>
</table>
# Notation and terminology

Let \( v \) be a discrete valuation on a ring \( R \),

- \( R \) be a commutative ring with multiplicative identity,
- \( S \) be a subset of polynomials in \( k[x_1, \ldots, x_n] \).

## Notation

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( Z )</td>
<td>The ring of integers, rational numbers, real numbers, complex numbers.</td>
</tr>
<tr>
<td>( Q ), ( R ), ( C )</td>
<td>a commutative ring with identity element</td>
</tr>
<tr>
<td>( S^{-1}R )</td>
<td>the field of fractions of ( R ) (w.r.t. the set ( S ))</td>
</tr>
<tr>
<td>UFD</td>
<td>unique factorization domain</td>
</tr>
<tr>
<td>PID</td>
<td>principal ideal domain</td>
</tr>
<tr>
<td>( V(S) )</td>
<td>the set of common zeros of the polynomials in ( S )</td>
</tr>
<tr>
<td>( V^*, V^\vee ), ( \text{Hom}(V, F) )</td>
<td>the dual space of ( V )</td>
</tr>
<tr>
<td>( I(X) )</td>
<td>the ideal of a set ( X )</td>
</tr>
<tr>
<td>( (I)_{L[x_1, \ldots, x_n]} )</td>
<td>the ideal in ( L[x_1, \ldots, x_n] ) generated by ( I ).</td>
</tr>
<tr>
<td>( O_v )</td>
<td>the discrete valuation ring with respect to ( v )</td>
</tr>
<tr>
<td>( m_v )</td>
<td>the valuation ideal for ( v )</td>
</tr>
<tr>
<td>( R_p )</td>
<td>localization at ( p )</td>
</tr>
<tr>
<td>( \text{ord}_P(f) )</td>
<td>the valuation of ( f \in K ) at ( P )</td>
</tr>
<tr>
<td>(</td>
<td>\text{ord}_P(f)</td>
</tr>
<tr>
<td>( L(D) )</td>
<td>the dimension of the vector space ( L(D) )</td>
</tr>
<tr>
<td>( l(D) )</td>
<td>the vector space ( {0} \cup { f \in K^\times : \text{div}(f) + D \geq 0 } )</td>
</tr>
<tr>
<td>( \mathbb{A}_K )</td>
<td>the adele ring of a function field ( K )</td>
</tr>
<tr>
<td>Symbol</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>$A_K(D)$</td>
<td>the adele space for a divisor $D$</td>
</tr>
<tr>
<td>$\Omega_K$</td>
<td>the space of differentials of $K$</td>
</tr>
<tr>
<td>$\Omega_K(D)$</td>
<td>the space of differentials which vanishes on $A_K(D)$ for a fixed divisor $D$</td>
</tr>
<tr>
<td>$\mathcal{D}_K$</td>
<td>the group of divisors of a function field $K/F$</td>
</tr>
<tr>
<td>$\text{div}(f)$</td>
<td>the divisor of $f \in K^x$</td>
</tr>
</tbody>
</table>
Chapter 1

Algebraic Backgrounds

Let’s recall some knowledges from commutative algebra. This chapter contains a summary of some notations and facts about rings and modules.

1.1 Rings and Ideals

1.1.1 Definition: Rings, Integral Domains

By a ring we will always mean a commutative ring with a multiplicative identity element 1. A ring homomorphism \( f \) from a ring \( R \) to \( R' \) is a map that ‘preserves’ addition and multiplication, and sending the multiplicative identity in \( R \) to the multiplicative identity in \( R' \). A ring \( R \) is called an integral domain if \( R \) has no nonzero zero divisors, and \( R \neq \{0\} \). An integral domain \( R \) is a field if any element \( x \) in \( R \) has a multiplicative inverse.

1.1.2 Proposition:

Any ring homomorphism from a field \( F \) to a nonzero ring \( R \) is injective. [1][Proposition 1.2]

1.1.3 Definition: Quotient Fields

Any integral domain \( R \) has a quotient field \( K \), which is a field that contains \( R \) has a subring, and the elements in the field are of the form \( a/b \), with \( a, b \in R \).

1.1.4 Definition: Kernel and Ideals

A subset \( I \) of \( R \) is an ideal of \( R \) if it is an additive subgroup of \( R \) that preserves multiplication by elements of \( R \). From the view of ring homomorphisms, The kernel of a ring homomorphism \( \phi \) is the set \( \phi^{-1}(0) \) of elements mapped to zero, written as \( \text{Ker}(\phi) \).
• An ideal $P$ of $R$ is prime if $P \neq R$ and, if $a$ and $b$ are two elements of $R$ such that their product $ab$ is an element of $P$, then $a$ is in $P$ or $b$ is in $P$. Equivalently, $P$ is a prime ideal of $R$ if and only if the quotient ring $R/P$ is an integral domain.

• An ideal $I$ of $R$ is maximal if there are no other ideals contained between $I$ and $R$, and $I \neq R$. Equivalently, $I$ is a maximal ideal of $R$ if and only if the quotient ring $R/I$ is a field. Therefore it is clear that any maximal ideal is a prime ideal.

• An ideal $I$ of $R$ is principal if it is generated by one single element of $R$.

1.1.5 Definition: Polynomial Rings

For any ring $R$, let $R[x]$ be the ring of polynomials with coefficients in $R$. A polynomial is called monic if it has degree 1. A polynomial with integer coefficients is called primitive if the greatest common divisor of all its coefficients is 1.

1.1.6 Proposition:

Let $K$ be a field, $P = (a_1, \ldots, a_n) \in K^n$, $a_i \in K$ be an arbitrary point in $K^n$, then the ideal

$$m_P := (x_1 - a_1, \ldots, x_n - a_n) \subset K[x_1, \ldots, x_n]$$

in $K[x_1, \ldots, x_n]$ is a maximal ideal.

**Proof.**

From the construction of $m_P$ we have that every polynomial $f \in K[x_1, \ldots, x_n]$ is congruent to $f(a_1, \ldots, x_n)$ modulo $m_P$. It follows that $m_P$ is the kernel of the homomorphism

$$\phi : K[x_1, \ldots, x_n] \to K, \ f \mapsto f(a_1, \ldots, a_n),$$

so we must have

$$k[x_1, \ldots, x_n]/m_P \simeq K.$$

Thus the statement holds.

1.2 Local Rings

1.2.1 Theorem:

Every nonzero ring $R \neq 0$ has at least one maximal ideal.

The proof of the theorem is a standard application of Zorn’s lemma. [1][Theorem 1.3]
1.2.2 Definition: Local Rings and Residue Fields

There are some rings with exactly one maximal ideal, for example fields. A ring \( R \) with exactly one maximal ideal \( \mathfrak{m} \) is called a local ring. The field \( k = R/\mathfrak{m} \) is called the residue field of \( R \).

Next we will introduce criterion for local rings:

1.2.3 Proposition:

- Let \( R \) be a ring, \( \mathfrak{m} \neq (1) \) be an ideal of \( R \) and every \( x \in A - \mathfrak{m} \) is a unit in \( R \). Then \( R \) is a local ring and \( \mathfrak{m} \) is its unique maximal ideal.

- Let \( R \) be a ring, \( \mathfrak{m} \neq (1) \) be an ideal of \( R \), such that every element of \( 1 + \mathfrak{m} \) (i.e., every \( 1 + x \), where \( x \in \mathfrak{m} \)) is a unit in \( R \). Then \( R \) is a local ring.

Proof.

1. It is easy to show that every ideal \( \neq (1) \) consists of non-units, hence is contained in the maximal ideal \( \mathfrak{m} \). Hence \( \mathfrak{m} \) is the only maximal ideal of \( R \).

2. Let \( x \in R - \mathfrak{m} \). Since the ideal \( \mathfrak{m} \) is maximal, we know that the ideal generated by \( x \) and \( \mathfrak{m} \) is the whole ring \( (1) \). Therefore there exist \( y \in R \) and \( t \in \mathfrak{m} \) such that \( xy + t = 1 \); thus \( xy = 1 - t \) belongs to \( 1 + \mathfrak{m} \) and therefore is a unit. Then we can apply the first statement to get the result.

1.2.4 Definition: Semi-local Rings

A ring with only a finite number of maximal ideals is called semi-local.

1.3 Hilbert Basis Theorem

1.3.1 Definition: Unit

An element \( r \in R \) is a unit if it has a multiplicative inverse in \( R \).

1.3.2 Definition: Irreducible(Prime) element

A nonzero element \( r \in R \) is an irreducible element (also called prime element) if it is not unit, and for any factorization or \( r \) like \( r = xy \), where \( x, y \in R \), either \( x \) or \( y \) is a unit.
1.3.3 Definition: Unique Factorization Domain

An integral domain $R$ is called a unique factorization domain, written UFD, if every nonzero non-unit element in $R$ can be uniquely factorized as a product of irreducible elements (uniquely up to order and units), very similar to the fundamental theorem of arithmetic for the integers.

1.3.4 Proposition: Gauss’s Lemma

There are two results from Gauss that are related to polynomials with integer coefficients:

- The product of any two primitive polynomials is again primitive.
- If a non-constant polynomial with integer coefficients is irreducible over the integers, then it is also irreducible as a polynomial over the rationals.

[4][Section 5.4]

In particular, if $R$ is a UFD with quotient field $K$, then any irreducible element $f \in R[x]$ is still irreducible in $K[x]$. And if $f$ and $g$ are polynomials in $R[x]$ with no common factors in $R[x]$, then they also have no common factors in $K[x]$.

1.3.5 Definition: Finite Generated Ideals

Let $S$ be a set of elements in a ring $R$, $I$ be an ideal in $R$, $S$ is said to generate $I$ if $I = \{ \sum a_i s_i : s_i \in S, a_i \in R \}$, written $I = (S)$.

And an ideal $I$ is finitely generated if it is generated by a finite set $S$, in particular, if the generating set $S$ contains only one single element, then we say $I = (S)$ is a principal ideal.

1.3.6 Definition: Noetherian Rings

A ring $R$ is Noetherian if every ideal in $R$ is finitely generated.

Equivalently, $R$ is Noetherian if for any ascending chain of ideals in $R$

$$I \subset I_1 \subset \ldots I_k \subset I_{k+1} \subset \ldots$$

there is an integer $n \geq 1$ such that

$$I_n = I_{n+1} = \ldots$$

[1][Proposition 6.2]

Next we will introduce an important result called Hilbert Basis theorem, which is a fundamental result in the study of algebraic geometry since it
allows every algebraic set over a field to be described as the set of common zeros of finitely many polynomial equations.

### 1.3.7 Theorem: Hilbert Basis Theorem

If \( R \) is a Noetherian ring, then the polynomial ring \( R[x_1, \ldots, x_n] \) is a Noetherian ring.

**Proof.**

Since \( R[x_1, \ldots, x_n] \) is isomorphic to \( R[x_1, \ldots, x_{n-1}][X_n] \), the theorem will follow by induction if we can prove that \( R[x] \) is Noetherian whenever \( R \) is Noetherian. Let \( I \) be an ideal in \( R[x] \). We must find a finite set of generators for \( I \).

And recall that for any polynomial \( f \) where \( f = a_0 + a_1 X + \cdots + a_d X^d \in R[x] \), \( a_d \neq 0 \), we call \( a_d \) the leading coefficient of \( f \). Let \( J \) be the set of leading coefficients of all polynomials in \( I \). It is easy to check that \( J \) is an ideal in \( R \), so there are polynomials \( f_1, \ldots, f_r \in I \) whose leading coefficients generate \( J \). Take an integer \( N \) larger than the degree of each \( f_i \). For each \( m \leq N \), let \( J_m \) be the ideal in \( R \) consisting of all leading coefficients of all polynomials \( f \in I \) such that \( \deg(f) \leq m \). Let \( \{f_{mj}\} \) be a finite set of polynomials in \( I \) of degree \( \leq m \) whose leading coefficients generate \( J_m \). Let \( I' \) be the ideal generated by the \( f_i \)'s and all the \( f_{mj} \)'s. It suffices to show that \( I = I' \).

Suppose \( I' \) were smaller than \( I \); let \( g \) be an element of \( I \) of lowest degree that is not in \( I' \). If \( \deg(g) > N \), we can find polynomials \( h_i \) such that \( \sum h_if_i \) and \( g \) have the same leading term. But then \( \deg(g - \sum h_if_i) < \deg(g) \), so \( g - \sum h_if_i \in I' \), so \( g \in I' \). Similarly if \( \deg(g) = m \leq N \), we can lower the degree by subtracting off \( \sum h_jF_{mj} \) for some \( h_j \).

Then the theorem follows.

There is a useful corollary follows directly from the theorem:

### 1.3.8 Corollary:

Let \( k \) be a field, then \( k[x_1, \ldots, x_n] \) is Noetherian.
1.3.9 Application:

If $R$ is a commutative ring and $A$ is an $R$-algebra, then we say that $A$ is a finitely presented $R$-algebra if it is a quotient of a polynomial ring over $R$ in finitely many variables by a finitely generated ideal.

If $A$ is a finitely-generated $R$-algebra, then we know from the above definition that

$$A \simeq R[x_1, \ldots, x_n]/I$$

where $I$ is an ideal in $R[x_1, \ldots, x_n]$.

The Hilbert basis theorem implies that the ideal $I$ must be finitely generated, say,

$$I = (a_1, \ldots, a_m),$$

thus $A$ is finitely presented.

1.4 Modules

In linear algebra, one the most important structure is that of a vector space over a field. For commutative algebra, similarly, it is therefore useful to consider the generalization of this concept, i.e., to the case where the underlying space of scalars is a commutative ring $R$ instead of a field. In this section we will discuss about modules.

1.4.1 Definition: Modules

Let $R$ be a ring. An $R$-module is a commutative group $M$ (the group law on $M$ is written $+$; the identity of the group is 0, or $0_M$) together with a scalar multiplication, i.e., a mapping from $R \times M$ to $M$ (denote the image of $(a, m)$ by $a \cdot m$ or $am$) satisfying:

1. $(a + b)m = am + bm$ for $a, b \in R, m \in M$.
2. $a \cdot (m + n) = am + an$ for $a \in R, m, n \in M$.
3. $(ab) \cdot m = a \cdot (bm)$ for $a, b \in R, m \in M$.
4. $1_R \cdot m = m$ for $m \in M$, where $1_R$ is the multiplicative identity in $R$.

1.4.2 Examples: Modules

1. A $\mathbb{Z}$-module is a commutative group, where $(\pm a)m$ is $\pm (m + \cdots + m)$ ($a$ times of $m$) for $a \in \mathbb{Z}, a \geq 0$.
2. If $R$ is a field, an $R$-module can be viewed as a vector space over $R$. 
3. The multiplication in $R$ makes any ideal of $R$ into an $R$-module. If \( \varphi : R \to S \) is a ring homomorphism, we define \( r \cdot s \) for \( r \in R, s \in S \), by the equation \( r \cdot s = \varphi(r)s \), which makes $S$ into an $R$-module. In particular, if a ring $R$ is a subring of a ring $S$, then $S$ is an $R$-module.

1.4.3 Definition: Submodules

A subgroup $N$ of an $R$-module $M$ is called a submodule if $am \in N$ for all $a \in R$, $m \in N$; $N$ is then an $R$-module.

If $S$ is a set of elements of an $R$-module $M$, the submodule generated by $S$ is defined to be

\[
\left\{ \sum r_is_i | r_i \in R, s_i \in S \right\} ;
\]

it is the smallest submodule of $M$ that contains $S$. If $S = \{s_1, \ldots, s_r\}$ is finite, the submodule generated by $S$ is denoted by $\sum Rs_i$.

1.4.4 Example: Submodules

Let $R$ be a ring. If we consider $R$ itself to be an $R$-module, a submodule of $R$ is by definition the same as an ideal $I$ of $R$. Moreover, the quotient ring $R/I$ is then by definition an $R$-module again.

One thing worth mentioning is that in this case modules and vector spaces behave in a slightly different way: if $K$ is a field and we view $K$ itself as an one-dimensional $K$-vector space $K$, then it has no non-trivial subspaces.

1.4.5 Definition: Finitely Generated Modules

The module $M$ is said to be finitely generated if $M = \sum Rs_i$ for some $s_1, \ldots, s_r \in M$. Note that this concept agrees with the notions of finitely generated commutative groups and ideals, and with the notion of a finite-dimensional vector space if $R$ is a field.

1.4.6 Definition: Module Homomorphisms

Let $R$ be a ring, if $f : M \to N$ is an $R$-module homomorphism, similar to the definition in ring theory, the kernel of $f$ is the set

\[\text{Ker}(f) = x \in M : f(x) = 0\]

and clearly is a submodule of $M$.

The image of $f$ is the set

\[\text{Im}(f) = f(M)\]

and is a submodule of $N$. 
And sometimes it is useful to consider the cokernel of a module-homomorphism, where the cokernel of \( f \) is defined to be
\[
\text{Coker}(f) = N/\text{Im}(f)
\]
which is a quotient module of \( N \).

If \( M' \) is a submodule of \( M \) such that \( M' \subset \text{Ker}(f) \), then \( f \) gives rise to a homomorphism \( \bar{f} : M/M' \to N \), defined as follows: if \( \bar{x} \in M/M' \) is the image of \( x \in M \), then \( \bar{f}(\bar{x}) = f(x) \). The kernel of \( \bar{f} \) is \( \text{Ker}(f)/M' \).

The homomorphism \( \bar{f} \) is said to be induced by \( f \). In particular, taking \( M' = \text{Ker}(f) \), we have an isomorphism of \( R \)-modules
\[
M/\text{Ker}(f) \cong \text{Im}(f).
\]

1.4.7 Example:

(a): Let \( R \) be a ring. If we consider \( R \) itself as an \( R \)-module, a submodule of \( R \) is by definition the same as an ideal \( I \) of \( R \).

(b): The polynomial ring \( K[x_1, \ldots, x_n] \) over a field \( K \) is finitely generated as a \( K \)-algebra (by \( \{x_1, \ldots, x_n\} \)), but not finitely generated as a \( K \)-module, i.e. as a \( K \)-vector space (the monomials are linearly independent). So if we use the term ‘finitely generated’ we always have to make sure to specify whether we mean ‘finitely generated as an algebra’ or ‘finitely generated as a module’, as these are two different concepts.

1.4.8 Proposition:

1. If \( L \supset M \supset N \) are \( A \)-modules, then
\[
(L/N)/(M/N) \cong L/M.
\]

2. If \( M_1, M_2 \) are submodules of \( M \), then \( (M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2) \).

Proof.

1. Define \( \theta : L/N \to L/M \) by \( \theta(x+N) = x+M \). Then \( \theta \) is a well-defined \( A \)-module homomorphism of \( L/N \) onto \( L/M \), since
\[
x + N = y + N \Rightarrow x - y \in N \Rightarrow x - y \in M \Rightarrow x + M = y + M
\]
and its kernel is \( M/N \) since \( \text{Ker}(\theta) = \{x+N : x \in M\} = M/N \), hence (i).

2. The composite homomorphism \( M_2 \to M_1 + M_2 \to (M_1 + M_2)/M_1 \) is surjective, and its kernel is \( M_1 \cap M_2 \); hence (ii) by defining \( \theta : M_2 \to (M_1 + M_2)/M_1 \) : \( x \mapsto x + M_1 \).
1.4.9 Definition: Direct Sum and Free Modules

If \( M, N \) are \( R \)-modules, their direct sum \( M \oplus N \) is the set of all pairs \((x, y)\) with \( x \in M, y \in N \). This is an \( R \)-module if we define addition and scalar multiplication in the trivial way:

\[
(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)
\]

\[
a(x, y) = (ax, ay).
\]

Generally speaking, if \((M_i)_{i \in I}\) is any collection of \( R \)-modules, we can define their direct sum \( \bigoplus_{i \in I} M_i \), its elements are families \((x_i)_{i \in I}\) such that \( x_i \in M_i \) for each \( i \in I \) and almost all \( x_i \) are 0.

A free \( R \)-module is one which is isomorphic to an \( R \)-module of the form \( \bigoplus_{i \in I} M_i \), where each \( M_i \simeq R \).

1.4.10 Definition: Free Modules on a Set

Let \( R \) be a ring, \( X \) be any set, we could define

\[
M_X := \{ f : X \to R : f(x) = 0 \text{ for all but finitely many elements of } x \in X \}.
\]

Then \( M_X \) can be made into an \( R \)-module in a traditional way, [6][Section 2.11]. In this case, \( M_X \) is called the free \( R \)-module on the set \( X \). In particular, if \( R = \mathbb{Z} \), then a free \( \mathbb{Z} \)-module on a set \( X \) is called the free abelian group on \( X \).

1.5 Localization of Rings

1.5.1 Motivation

In this section we will discuss the rings of fractions and the localization of rings. Localization of rings is a powerful technique in commutative algebra that often allows us to reduce questions about rings and modules to a union of smaller ‘local’ problems.

Recall that for any integral domain \( R \), we could construct its quotient field which contains all the elements of the form \( a/b \) where \( a, b \in R \). The verification of the construction involves canceling, i.e. the fact that an integral domain \( R \) has no zero-divisor \( \neq 0 \). However, the concept of ‘fraction’ it can be generalized for all rings:

1.5.2 Definition: Multiplicatively Closed Subsets

Let \( R \) be a ring. A multiplicatively closed subset of \( R \) is a subset \( S \) of \( R \) such that \( 1 \in S \) and \( S \) is closed under multiplication.
And we will define a relation \( \equiv \) on \( R \times S \) by:

\[
(r, s) \equiv (r', s') \text{ if and only if } (rs' - r's)t = 0 \text{ for some } t \in S.
\]

Follow by the definition, it is not complicated to show that this relation is indeed an equivalence relation. \[\text{[Definition 6.1]}\]

We use \( r/s \) to denote the equivalence class of \( (r, s) \), and let \( S^{-1}R \) denote the set of all the equivalence classes. We could set up a ring structure on \( S^{-1}R \) by defining addition and multiplication in the trivial way, formally:

\[
(r/s) + (r'/s') = (rs' + r's)/(ss'), \quad \text{and} \quad (r/s)(r'/s') = (rr'/ss').
\]

1.5.3 Remark:

These definitions are independent of the choices of representatives elements \( (r, s) \) and \( (r', s') \).

1.5.4 Example:

(1): If \( R \) is an integral domain and \( S = R - \{0\} \), then \( S^{-1}R \) is in fact the field of fractions of \( R \).

(2): If \( S = \{1\} \), then \( S \) is a multiplicatively closed subset of \( R \), and it implies the isomorphism

\[ S^{-1}R \simeq R. \]

1.5.5 Definition: Rings of Fractions

The ring \( S^{-1}R \) is called the ring of fractions of \( R \) with respect to the set \( S \).

Then we would discuss some properties about the ring of fractions, first let us look at the homomorphisms:

1.5.6 Theorem: Universal Property of the Ring of Fractions

Let \( g : R \to R' \) be a ring homomorphism such that \( g(s) \) is a unit in \( R' \) for all \( s \in S \). Then, there exists a unique ring homomorphism \( \phi : S^{-1}R \to R' \) such that \( g = \phi \circ f \).

1.5.7 Proposition:

Let \( S \) be a multiplicatively closed subset of \( R \), the ring of fractions \( S^{-1}R \) and the homomorphism \( f : R \to S^{-1}R \) satisfy following properties:

1. \( s \in S \Rightarrow f(s) \) is a unit in \( S^{-1}R \);
2. Let \( r \in R, f(r) = 0 \Rightarrow rs = 0 \) for some \( s \in S \);
3. Every element of $S^{-1}R$ is of the form $f(r)f(s)^{-1}$ for some $r \in R$ and some $s \in S$.

In particular, these three conditions actually determine the ring $S^{-1}R$ up to isomorphism.

**1.5.8 Definition: Localization**

Let $\mathfrak{p}$ be a prime ideal of $R$. Then it is obvious that the subset $S = R - \mathfrak{p}$ is multiplicatively closed in $R$. In fact $R - \mathfrak{p}$ is multiplicatively closed if and only if $\mathfrak{p}$ is a prime ideal. Conventionally, we write $R_\mathfrak{p}$ for $S^{-1}R$ in this case.

The elements $r/s$ with $r \in \mathfrak{p}$ form an ideal $m$ in $R_\mathfrak{p}$. If $r'/s' \notin m$, then $r' \notin \mathfrak{p}$, $r'/s'$ is a unit in $R_\mathfrak{p}$ since $r' \in S$.

As a consequence, we could show that $R_\mathfrak{p}$ is a local ring. To see this, if $I$ is an ideal in $R_\mathfrak{p}$ such that $m$ does not contain $I$, then $I$ contains a unit and $I$ is the whole ring. Hence $m$ is the only maximal ideal in $R_\mathfrak{p}$.

The process of passing from $R$ to $R_\mathfrak{p}$ is called localization at $\mathfrak{p}$.

**1.5.9 Example: Localization**

1. Let $R = \mathbb{Z}$, $\mathfrak{p} = (p)$, where $p$ a prime number; in this case $R_\mathfrak{p}$ is the set of all rational numbers $m/n$ where $n$ is prime to $p$; if $f \in \mathbb{Z}$ and $f \neq 0$, then $R_f$ is the set of all rational numbers whose denominator is a $f^k$ for some integer $k$.

2. For a fixed element $a \in R$, let $S = \{a^n : n \in \mathbb{N}\}$. Then $S$ is clearly multiplicatively closed, and the corresponding localization $S^{-1}R$ is denoted by $R_a$, and we call $R_a$ the localization of $R$ at the element $a$.

3. Let $R = k[x_1, x_2, \ldots, x_n]$, where $k$ is a field, $R$ is the polynomial ring over $k$ with $n$ variables. Let $\mathfrak{p}$ be a prime ideal in $R$.

Then $R_\mathfrak{p}$ is the ring of all rational functions $f/g$, where $g \notin \mathfrak{p}$. If $V$ is the variety defined by the ideal $\mathfrak{p}$, that is to say the set of all $x = (x_1, x_2, \ldots, x_n) \in k^n$ such that $f(x) = 0$ whenever $f \in \mathfrak{p}$, then $R_\mathfrak{p}$ can be identified with the ring of all rational functions on $k^n$ which are defined at almost all points of $V$; it is the local ring of $k^n$ along the variety $V$.

After we have set up the definition and have seen some examples of localizations, let us now discuss their properties. We will start by relating ideals (especially prime ideals) in a localization $S^{-1}R$ to ideals in $R$. 
1.5.10 Proposition: Ideals in localizations

Let \( R \) be a ring. Let \( S \) be a multiplicatively closed subset of \( R \). In the following, we will consider contractions and extensions by the ring homomorphism

\[
\phi : R \to S^{-1}R.
\]

1. For any ideal \( I \) in \( R \), we have

\[
I^e = \frac{a}{s} : a \in I, s \in S.
\]

2. For any ideal \( I \) in \( S^{-1}R \), we have

\[
(I^e)^e = I.
\]

3. The contraction and extension by \( \phi \) provide a one-to-one correspondence between

\[
\{ \text{prime ideals in } S^{-1}R \} \overset{I \mapsto I^e}{\leftrightarrow} \{ \text{prime ideals } I \text{ in } R \text{ with } I \cap S = \emptyset \}
\]

[REF]

1.5.11 Remarks: Prime Ideals in \( R_P \)

In particular, a localization of a ring \( R \) at a prime ideal \( P \), i.e., with respect to the multiplicatively closed subset \( R_P \), gives a one-to-one correspondence by contraction and extension

\[
\{ \text{prime ideals in } R_P \} \overset{1:1}{\leftrightarrow} \{ \text{prime ideals } I \text{ in } R \text{ with } I \subset P \}
\]

We also have a one-to-one correspondence between

\[
\{ \text{prime ideals in } R/P \} \overset{1:1}{\leftrightarrow} \{ \text{prime ideals } I \text{ in } R \text{ with } I \text{ contains } P \}
\]

But generally, ideals do not behave such nicely; ideals in the quotient ring \( R/P \) still correspond to ideals in \( R \) containing \( P \), the similar statement for all ideals would not hold.

1.5.12 Definition: Localization of Modules

Let \( S \) be a multiplicatively closed subset of ring \( R \), and let \( M \) be an \( R \)-module, \( s, s' \in S, m, m' \in M \), then the relation

\[(m, s) \sim (m', s') \iff \text{there is an element } u \in S \text{ such that } u(s'm - sm') = 0.\]

is an equivalence relation on \( M \times S \), and we denote the equivalence class of \((m, s)\) by \( m/s \). And the set of all the equivalence classes is denoted by

\[S^{-1}M := \{ m/s : m \in M, s \in S \},\]

and is called the localization of \( M \) at \( S \).
1.6. DUAL VECTOR SPACE

We claim that $S^{-1}M$ is an $S^{-1}R$ - module. To see this, simply set up the addition and scalar multiplication in the trivial way, as in the definition of rings of fractions.

1.6 Dual Vector Space

The definitions of vector spaces, linear transformations are regarded as prerequisite here. [7][Section 4.1, Section 6.1]

1.6.1 Definition: Dual Space

Given any vector space $V$ over a field $F$, the (algebraic) dual space $V^*$, (sometimes also denoted by $V^*$), is defined as the set of all the linear transformations $f : V \rightarrow F$.

Since linear transformations are homomorphisms between vector spaces, the dual space can be denoted by Hom($V, F$).

The dual space itself becomes a vector space over $F$ when equipped with an addition and scalar multiplication are defined trivially. [7][Section 4.3] Elements of the algebraic dual space $V^*$ are called covectors.
Chapter 2

Affine Varieties

2.1 Affine Spaces and Algebraic Sets

Affine spaces and affine varieties provide us a framework for the study of geometry. In particular, it is possible to deal with points, curves, surfaces and other objects in a way that is independent of any specific choice of a coordinate system.

2.1.1 Definition: Affine spaces

Let \( k \) be any field, affine \( n \)-space over \( k \), denoted by \( \mathbb{A}^n(k) \), is the cartesian product of \( k \) with \( k \) itself for \( n \) times. The elements in \( \mathbb{A}^n(k) \) are called points.

In particular, \( \mathbb{A}^1(k) \) is called the affine line over \( k \), and \( \mathbb{A}^2(k) \) is called the affine plane over \( k \).

2.1.2 Definition: Algebraic Sets

An algebraic set \( X \subset \mathbb{A}^n(k) \) is the set of common zeroes of a collection of polynomials \( f_1, \ldots, f_n \) in \( k[x_1, \ldots, x_n] \). Let \( S \) be a subset of polynomials \( f_1, \ldots, f_n \) in \( k[x_1, \ldots, x_n] \), we define

\[
V(S) = \bigcap_{f \in S} V(f).
\]

And we usually write \( V(f_1, \ldots, f_n) \) instead of \( V(f_1, f_2, \ldots, f_n) \). A subset \( X \subset \mathbb{A}^n(k) \) is an affine algebraic set, or simply an algebraic set, if \( X = V(S) \) for some \( S \).

2.1.3 Examples: Algebraic Sets

- Affine \( n \)-space itself is an algebraic set: \( \mathbb{A}^n = V(0) \).
The empty set is an algebraic set: $\emptyset = V(1)$.

Any single point in $\mathbb{A}^n$ is an algebraic set:

$$(a_1, \ldots, a_n) = V(x_1?a_1, \ldots, x_n?a_n).$$

### 2.1.4 Proposition:

If $X = V(S)$ for some subset of polynomials $S$, the following statements hold:

1. If $I = (S)$ is the ideal generated by $S$, then $V(S) = V(I)$.
2. If $I \subset J$, then $V(J) \subset V(I)$.
3. $V(\cup \alpha I_\alpha) = V(\sum \alpha I_\alpha) = \cap V(I_\alpha)$.
4. $V(I \cap J) = V(I \cdot J) = V(I) \cup V(J)$.

Now let’s recall that, a topology on a set $X$ is a collection of subsets of $X$, which are called the open subsets of $X$, satisfying:

- The empty set $\emptyset$ and the whole space $X$ are open.
- The union of any family of open subsets of $X$ is also open.
- The intersection of any finitely many open subsets is also open.

And a topological space is thus defined to be a set $X$ together with a topology on $X$.

The closed subsets of a topological space is the complement set of any open subset of $X$, as a consequence, we can also define a topological structure on $X$ by specifying which sets are closed subsets.

### 2.1.5 Definition: Zariski Topology

Let us define a topology on $\mathbb{A}^n$ by defining the closed subsets to be the algebraic subsets. $U \subset \mathbb{A}^n$ is open if and only if the complement set $\mathbb{A}^n U = V(S)$ for some subset $S$ of polynomials in $k[x_1, \ldots, x_n]$.

And the conditions for topology hold. [3][Proposition 1.2]

### 2.1.6 Example: Zariski topology on affine spaces

(1): Consider $\mathbb{A}^1(k)$, we claim that the algebraic sets are finite sets, as well as all of $\mathbb{A}^1(k)$ and the empty set. Algebraic sets are zeroes of polynomials in some ideal. In this case we are considering ideals in $k[x]$, which is a PID, so those ideals all look like $(f)$ for some polynomial $f$. Our field is
algebraically closed, so write \( f = a(x - \alpha_1) \cdots (x - \alpha_n) \). So all the closed sets are of the form \( V(f) = \{ \alpha_1 \cdots \alpha_n \} \). (And, of course, for every finite set we can find a polynomial where those are the only roots, so every finite set is closed.)

(2) : Now consider \( \mathbb{A}^2(k) \). Obviously, we have \( \mathbb{A}^2(k) \) and \( \emptyset \) are algebraic sets. Also, we have things that are plane curves: \( V(f) \). However, not every ideal is generated by one polynomial: we also have the ideals \( V(f_1, f_2) \). Suppose \( f_1 \) is irreducible, and \( f_2 \) is not divisible by \( f_1 \). Then \( V(f_1, f_2) \) is a finite set. But every other set is some union of sets of the form \( V(f') \) or \( V(f, g) \).

### 2.2 Ideal of a Set

Next, we will describe the precise relation between algebraic sets in affine spaces and the ideals in the polynomial ring \( k[x_1, \ldots, x_n] \).

We have already introduced the operation \( V(\cdot) \) that takes an ideal (or any subset of polynomials in \( k[x_1, \ldots, x_n] \)) to an algebraic set in an affine space.

Here we will discuss an operation that does the opposite job.

#### 2.2.1 Definition: Radical ideal, radical

\[ \sqrt{I} = \{ f \in k[x_1, \ldots, x_n] : f^r \in I \} \]

is the radical of the ideal \( I \). A radical ideal is a set whose radical is itself.

#### 2.2.2 Definition: Ideal of a subset

If \( X \subset \mathbb{A}^n(k) \) is any subset, then we define that the polynomials vanish on \( X \) to be

\[ \mathcal{I}(X) = \{ f \in K[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ for any } (a_1, \ldots, a_n) \in X \}. \]

The following proposition shows some of the relations between ideals and algebraic sets:

#### 2.2.3 Proposition:

1. If \( X_1 \subset X_2 \) are subsets of \( \mathbb{A}^n(k) \), then \( \mathcal{I}(X_2) \subset \mathcal{I}(X_1) \).
2. For any two subsets \( X_1, X_2 \in \mathbb{A}^n \), we have

\[ \mathcal{I}(X_1 \cup X_2) = \mathcal{I}(X_1) \cup \mathcal{I}(X_2) \]

3. For any ideal \( I \in K[x_1, \ldots, x_n] \), \( \mathcal{I}(Z(I)) = \sqrt{I} \).
CHAPTER 2. AFFINE VARIETIES

[3][Proposition 1.2]
The following proposition shows that, algebraically, the set of zeros of
an ideal corresponds to a set of maximal ideals in the polynomial ring
\( K[x_1, \ldots, x_n] \).

2.2.4 Proposition:

Let \( k \) be an algebraically closed field, \( I \) be a set of polynomials in \( K[x_1, \ldots, x_n] \),
and \( \mathcal{M}_I \) be the collection of maximal ideals in \( K[x_1, \ldots, x_n] \) which contains
\( I \). Then the map

\[ f : V(I) \to \mathcal{M}_I \]

that maps \( f(a_1, \ldots, a_n) \) to \((x_1 - a_1, \ldots, x_n - a_n)\) is a bijection. [2][Theorem 1.7]

2.3 Hilbert’s Nullstellensatz

Given a field extension \( K \subset L \), and an ideal \( I \) in the polynomial ring
\( K[x_1, \ldots, x_n] \), conventionally we use \((I)_L[x_1, \ldots, x_n] \) to denote the ideal in
\( L[x_1, \ldots, x_n] \) generated by \( I \).

2.3.1 Theorem: Weak Hilbert’s Nullstellensatz

Let \( K \) be a field, and let \( I \) be a proper ideal of \( K[x_1, \ldots, x_n] \), then \( V(I) \neq \emptyset \).
Proof.

Let \( \bar{K} \) be the algebraic closure of \( K \). By the previous proposition , let \((\bar{I})\) denote \((I)_{\bar{K}[x_1, \ldots, x_n]} \), then \((\bar{I})\) is a proper ideal of
\( K[x_1, \ldots, x_n] \) which is a Noetherian ring. It follows that \((\bar{I})\) is
contained in a maximal ideal \( m \) of \( K[x_1, \ldots, x_n] \).

Now we can prove the Hilbert’s Nullstellensatz theorem, which establishes a
fundamental relationship between geometry and algebra, and is also called
the Theorem of Zeros.
2.3.2 Theorem: Hilbert’s Nullstellensatz

Let \( K \) be an algebraically closed field and let \( I \subset K[x_1, \ldots, x_n] \) be an ideal in a polynomial ring. Then

\[
I(V(I)) = \sqrt{I}.
\]

Proof.

We will use the weak Nullstellensatz to prove this. Let \( I \subset k[x_1, \ldots, x_n] \), which is a Noetherian ring, thus \( I \) is finitely generated, we can write \( I \) as

\[
I = (f_1, \ldots, f_k).
\]

Let \( J = (f_1, \ldots, f_k, x_{n+1}f - 1) \) be an ideal in \( k[x_1, \ldots, x_n] \), clearly \( V(J) = \emptyset \), and the weak Nullstellensatz implies that \( 1 \in J \), i.e., \( J = k[x_1, \ldots, x_n] \) the whole ring.

Thus there exists \( p_1, p_2, \ldots, p_{k+1} \in k[x_1, \ldots, x_n, x_{n+1}] \) such that

\[
1 = f_1p_1 + \ldots + f_kp_k + p_{K+1}(x_{n+1}f - 1).
\]

Now let \( x_{n+1} = 1/f \), substituting and clearing the denominators, we get the result

\[
f^r \equiv 0 \mod (f_1, \ldots, f_k).
\]

And one of the most well-known consequences of Hilbert’s Nullstellensatz is that we obtain an ideal-variety correspondence given by the following corollary:

2.3.3 Corollary:

There is a correspondence between algebraic subsets of \( \mathbb{A}^n \) and radical ideals.

2.3.4 Definition: Coordinate Rings

If \( X \subset \mathbb{A}^n \) is an affine algebraic set, i.e., an irreducible algebraic set in \( \mathbb{A}^n \), we define the coordinate ring of \( X \) by \( k[X] \), [REF],

\[
k[X] := k[x_1, \ldots, x_n]I(X).
\]

2.4 Irreducibility and Dimensions

Now we are going to discuss about the decomposition of algebraic sets.
2.4.1 Definition: Irreducible and connected spaces

Let $X$ be any topological space.

(a) We say that $X$ is reducible if it can be written as $X = X_1 \cup X_2$ where $X_1, X_2$ are proper closed subsets of $X$, and $X_1 \cap X_2 = \emptyset$. Otherwise $X$ is called irreducible.

(b) The space $X$ is called disconnected if $X$ can be written as $X = X_1 \cup X_2$ for proper closed subsets $X_1, X_2 \subset X$ and $X_1 \cap X_2 = \emptyset$. Otherwise $X$ is called connected.

Similarly, an algebraic set $V \subset \mathbb{A}^n$ is reducible if $V = V_1 \cup V_2$, where $V_1, V_2$ are proper algebraic subsets. Otherwise $V$ is called an irreducible algebraic set.

2.4.2 Proposition:

An algebraic set $V$ is irreducible if and only if the ideal of $V$ ($I(V)$) is a prime ideal.

Proof. If $I(V)$ is not prime, suppose $f_1f_2 \in I(V)$, $f_i \notin I(V)$. Then $V = (V \cap V(f_1)) \cup (V \cap V(f_2))$, and $V \cap V(f_1) \subset V$, so $V$ is reducible.

Conversely if $V = V_1 \cup V_2, V_i \subset V$, then $I(V_i) \supset I(V)$; let $f_i \notin I(V_i), f_i \notin I(V)$. Then $f_1f_2 \in I(V)$, so $I(V)$ is not prime. □

2.4.3 Examples: affine varieties.

(1): It is clear that $\mathbb{A}^1$ is an affine variety. In fact, so is every $\mathbb{A}^n$: use the fact that $\mathbb{A}^1 = V(0)$, and zero is prime in the polynomial ring.

(2): Linear varieties: let $l_1, \ldots, l_m$ be independent linear forms of $x_1, \ldots, x_m$. (These are linearly independent homogeneous polynomials of degree 1.) Let $x_1, \ldots, x_m \in k$

Then $V(l_1 - a_1, \ldots, l_m - a_m) \in \mathbb{A}^n$ is an affine variety, which we call a linear variety of dimension $n - m$. For example, if $l = ax + by$ then $V(l - c)$ is just the line $ax + by = c$.

2.4.4 Definition: Noetherian Space

A topological space $X$ is called Noetherian if every descending chain

$$X \supset X_1 \supset X_2 \supset \cdots$$

of closed subsets of $X$ is stationary.
2.4. IRREDUCIBILITY AND DIMENSIONS

By Hilbert’s Basis theorem, $k[x_1,\ldots,x_n]$ is a Noetherian ring for any field $k$.

2.4.5 Proposition:

Let $X$ be a Noetherian topological space, then $X$ can be written as a finite union

$$X = X_1 \cup X_2 \cup \cdots \cup X_r$$

of irreducible closed subsets $X_i$. If $X_i \subset X_j$ for all $i \neq j$, then the $X_i$ are unique (up to permutation).

And in this case, they are called the irreducible components of $X$. In particular, any algebraic set is a finite union of affine varieties in a unique way.

**Proof.**

First of all, to prove existence, we use proof by contradiction, suppose the statement is false, i.e. $X$ is reducible, hence $X = X_1 \cup X_2$, where $X_1 \cap X_2 = \emptyset$ and $X_1, X_2 \subsetneq X$.

Moreover, the statement of the proposition must be false for at least one of these two subsets, say $X_1$. Continuing this construction, one arrives at an infinite chain

$$X \supsetneq X_1 \supsetneq X'_1 \cdots$$

of proper closed subsets of $X$, which is a contradiction as $X$ is Noetherian.

To show uniqueness, assume that we have two decompositions

$$X = X_1 \cup \cdots \cup X_r = X'_1 \cup \cdots \cup X'_s.$$ 

Then $X_1 \subset \bigcup_i X'_i$, thus

$$X_1 = \bigcup_i (X_1 \cap X'_i)$$

, but $X_1$ is irreducible, so we can assume that $X_1 = X_1 \cap X'_1$, i.e. $X_1 \subset X'_1$.

For the same reason, we must have $X'_1 \subset X_i$ for some $i$. So $X_1 \subset X'_1 \subset X_i$ which means by assumption that $i = 1$. Therefore $X_1 = X'_1$ is contained in both decompositions.

Now let $Y = X \setminus X_1$, then

$$Y = X_2 \cup \cdots \cup X_r = X'_2 \cup \cdots \cup X'_s,$$

so proceeding by induction on $r$ we could obtain the uniqueness of the decomposition.

Thus our statement follows. 

$\square$
2.4.6 Definition: Krull Dimension

Let \( X \) be a (non-empty) irreducible topological space. The dimension of \( X \) is the biggest integer \( n \) such that there is a chain

\[
\emptyset \neq X_0 \subsetneq \cdots \subsetneq X_n = X
\]

of irreducible closed subsets of \( X \). If \( X \) is any Noetherian topological space, the dimension of \( X \) is defined to be the supremum of the dimensions of its irreducible components.

In particular, a space of dimension 1 is called a curve, a space of dimension 2 is called a surface.

The idea is that, if \( X \) is an irreducible topological space, then any closed proper subset of \( X \) must have dimension smaller than \( X \).

2.4.7 Example: Dimensions of Some topological spaces

The dimension of \( \mathbb{A}^1 \) is 1, as single points are the only irreducible closed subsets of \( \mathbb{A}^1 \) that are not equal to \( \mathbb{A}^1 \).

In fact, the dimension of \( \mathbb{A}^n \) is always \( n \), but this is a fact from commutative algebra that we will not prove at the moment. But we can at least see that the dimension of \( \mathbb{A}^n \) is not less than \( n \), because there are sequences of inclusions

\[
\mathbb{A}^0 \subsetneq \mathbb{A}^1 \subsetneq \cdots \subsetneq \mathbb{A}^n
\]

of linear subspaces of increasing dimension.

2.4.8 Theorem: Krull Intersection Theorem

Let \( R \) be a Noetherian ring, \( I \) is an ideal of \( R \), \( M \) is a finitely-generated \( R \)-module, and

\[
L = \bigcap_{n=1}^{\infty} I^n M,
\]

then \( I \cdot L = L \).
Chapter 3

Function Field and Discrete Valuation Rings

3.1 Regular Local Rings

Recall that a ring $R$ is a local ring if it has exactly one maximal ideal $m$.

3.1.1 Proposition:

Let $R$ be a local ring with its unique maximal ideal $m$, $m/m^2$ can be viewed as an $R/m$ - vector space. [2][Lemma 13.1]

Proof.

To see this, note that $m$ is an abelian group which contains $m^2$ as a normal subgroup. Thus for the quotient group $m/m^2$, the additive group operation is defined as

$$(m_1 + m^2) + (m_2 + m^2) = (m_1 + m_2) + m^2.$$

And it is closed under multiplication by $R$ since $m$ is an ideal. To see that $m/m^2$ has the structure of an $R/m$ - vector space.

- The scalars are the cosets $r + m$ in the field $R/m$, $r \in R$.
- The scalar multiplication is defined in the trivial way

$$(r + m)(m + m^2) = rm + m^2$$

$\square$

3.1.2 Definition: Regular Local Ring

Note that we write $\dim m/m^2$ as the dimension of $m/m^2$ when viewed as an $R/m$ - vector space. And $\dim R$ is the Krull dimension of the ring $R$. 

23
A Noetherian local ring \( R \) with its maximal ideal \( m \) is a regular local ring if
\[ \dim \frac{m}{m^2} = \dim R. \]

[2][Section 13.1]

We are particularly interested in regular local rings of dimension 1, which correspond to rings \( \mathcal{O}_P \) of regular functions at a smooth point \( P \) on a curve (a variety of dimension one).

### 3.2 Function Fields and Valuation Rings

#### 3.2.1 Definition: Function field

Let \( F \) be an algebraically closed field, a function field over \( F \) is a finitely generated extension \( K \) of \( F \) with transcendence degree 1, such that \( F \) is algebraically closed in \( K \).

#### 3.2.2 Definition: Valuation Ring

A subring \( R \) of a field \( K \) is a valuation ring of \( K \) if for every nonzero \( a \in K \) either \( a \) or \( a^{-1} \) belongs to \( R \).

#### 3.2.3 Theorem:

Let \( R \) be a subring of the field \( K \), and \( h : R \to F \) a ring homomorphism from \( R \) into an algebraically closed field \( F \). Then \( h \) has a maximal extension \((V,h)\). In other words, \( V \) is a subring of \( K \) containing \( R \), \( h \) is an extension of \( h \), and there is no extension to a strictly larger subring.

In addition, for any maximal extension, \( V \) is a valuation ring of \( K \).

**Proof.**

First we prove a claim about field extension to rings.

Claim: Let \( R \) be a subring of the field \( K \), and \( h : R \to F \) be a ring homomorphism from \( R \) into an algebraically closed field \( F \). If \( \alpha \) is a nonzero element of \( K \), then either \( h \) can be extended to a ring homomorphism \( \tilde{h} : R[\alpha] \to F \), or \( h \) can be extended to a ring homomorphism \( \tilde{h} : R[\alpha^{-1}] \to F \).

**Proof of the Claim:**

Without loss of generality, we may suppose that \( R \) is a local ring and \( L = h(R) \) is a subfield of \( F \).

Since that if we let \( P \) be the kernel of \( h \), \( P \) is a prime ideal, and we can extend \( h \) to \( g : R_P \to F \) via \( g(a/b) = h(a)/h(b) \), \( h(b) = 0 \).
The kernel of $g$ is $PR_P$, so by the first isomorphism theorem,
$$(R_P) \simeq R_P/PR_P$$
, a field (because $PR_P$ is a maximal ideal). Thus we can replace $(R, h)$ by $(R_P, g)$.

First, we extend $h$ to a homomorphism of polynomial rings.

If $f \in R[x]$ with $f(x) = \Sigma a_i x^i$, we take $h(f) = h(a_i) x^i \in L[x]$.

Let $I = \{ f \in R[x] : f(\alpha) = 0 \}$. Then $J = h(I)$ is an ideal of $L[x]$, which is principal. Let’s say $J = (j(x))$. If $j$ is non-constant, it must have a root $r$ in $F$ since $F$ is algebraically closed.

We can then extend $h$ to $\bar{h} : R[\alpha] \to F$ by $\bar{h}(\alpha) = r$, as desired. To show that $\bar{h}$ is well-defined, suppose $f \in I$, thus $f(\alpha) = 0$. Then $h(f) \in J$, hence $h(f)$ is a multiple of $j$, and therefore $h(f)(r) = 0$.

Then we suppose that $j$ is constant. If the constant $j$ is zero, then we may extend $h$ exactly as we described above, with $r$ be chosen arbitrary. We can assume that $j = 0$, and it follows that $1 \in J$. As a consequent, there exists $f \in I$ such that $h(f) = 1$.

This gives us
$$\Sigma_{i=0}^r a_i \alpha^i = 0, \quad a_i \in R.$$ 

And
$$\bar{a}_i = h(a_i) = 1 \text{ if } i = 0, \quad \bar{a}_i = h(a_i) = 0 \text{ if } i > 0.$$ 

Then we choose $t$ as small as possible. Using the same argument to deal with the $\alpha^{-1}$ case, assuming that $h$ has no extension to $R[\alpha^{-1}]$, we have
$$\Sigma_{i=0}^r b_i \alpha^{-i} = 0, \quad b_i \in R.$$ 

And
$$\bar{b}_i = h(b_i) = 1 \text{ if } i = 0, \quad \bar{b}_i = h(b_i) = 0 \text{ if } i > 0.$$ 

Take $s$ as small as possible, and assume (without loss of generality) that $t \geq s$.

Let $M$ denote the unique maximal ring of the local ring $R$. Since $h(b_0) = 1 = h(1)$, it follows that
$$b_0 - 1 \in ker(h) \subset M.$$ 

Since $M$ is maximal, $1 \notin M$, thus $b_0 \notin M$, $b_0$ is a unit. We then have
$$a^s + b_0^{-1} b_1 a^{s-1} + \cdots + b_0^{-1} b_s = 0,$$
by multiplying $b_0^{-1} a^s$ on the both sides. Finally, we multiply by $a_i$ and subtract the first result to contradict the minimality of $t$. Thus we have prove the claim.

Now let’s get back to the theorem itself, let $S$ be the set of all $(R_i, h_i)$, where $R_i$ is a subring of $K$ containing $R$ and $h_i$ is an
extension of \( h \) to \( R_i \).

We can define a partial order on the set \( S \) by \((R_i, h_i) \leq (R_j, h_j)\) if and only if \( R_i \) is a subring of \( R_j \) and the map that \( h_j \) restricted to \( R_i \) coincides with \( h_i \).

Using Zorn’s lemma, it is easy to prove that there is a maximal extension \((V, h)\).

If \( a \) is a nonzero element of \( K \), then by the above claim, \( h \) must have an extension to either \( V[\alpha] \) or \( V[\alpha^{-1}] \).

By the maximality of the extension \((V, h)\), either \( V[\alpha] = V \) or \( V[\alpha^{-1}] = V \).

Therefore \( \alpha \in V \) or \( \alpha^{-1} \in V \). □

### 3.2.4 Proposition: Properties of Valuation Rings

Let \( V \) be a valuation ring of the field \( K \), and the following statements hold:

1. The fraction field of \( V \) is \( K \).
2. Any subring of \( K \) containing \( V \) is a valuation ring of \( K \).
3. \( V \) is a local ring.
4. \( V \) is an integrally closed ring.
5. If \( I \) and \( J \) are ideals of \( V \), then either \( I \subseteq J \) or \( J \subseteq I \). i.e. The ideals of \( V \) are totally ordered by inclusion.

**Proof:**

1. The proof for the first statement follows directly from the fact that any nonzero element \( \alpha \) of \( K \) can be written as \( \alpha \) (i.e. \( \alpha /1 \)) or as \( 1/\alpha^{-1} \).
2. The proof for the second statement follows from the definition.
3. For the third statement, we will show that the set \( M \) of nonunits of \( V \) is an ideal. If \( a \) and \( b \) are nonzero nonunits, then either \( a/b \) or \( b/a \) belongs to \( V \). If \( a/b \in V \), then \( a + b = b(1 + a/b) \in M \) (because if \( b(1 + a/b) \) were a unit, then \( b \) would be a unit as well). Similarly, if \( b/a \in V \), then \( a + b \in M \). If \( r \in V \) and \( a \in M \), then \( ra \in M \), else a would be a unit. Thus \( M \) is an ideal.
4. To show that \( V \) is integrally closed. Let \( \alpha \) be any nonzero element of \( K \), such that \( \alpha \) is integral over \( V \). Then there is an equation of the form

\[
\alpha n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0
\]

with each \( c_i \) in \( V \). We now show that \( \alpha \in V \). If not, then \( \alpha^{-1} \in V \), and if we multiply the above equation of integral dependence by
3.3. **DISCRETE VALUATION RINGS**

\[ \alpha^{-(n-1)} \], we get
\[ \alpha = -c_{n-1} - c_{n-2}\alpha^{-1} - \cdots - c_0\alpha^{-(n-1)} \]
thus \( \alpha \in V \). Thus \( V \) is integrally closed.

5. Suppose that \( I \) is not contained in \( J \), and pick \( a \in I - J \) (hence \( a = 0 \)). If \( b \in J \), we must show that \( b \in I \). If \( b = 0 \) then we are finished, so assume \( b = 0 \). We have \( b/a \in V \) (else \( a/b \in V \), so \( a = (a/b)b \in J \), which leads to a contradiction). Therefore \( b = (b/a)a \in I \).

3.3 **Discrete Valuation Rings**

3.3.1 Definition: discrete valuation

A (discrete) valuation on a field \( K \) is a function \( v : K \rightarrow \mathbb{Z} \cup \{\infty\} \), such that

1. \( v(x) = \infty \) if and only if \( x = 0 \).
2. \( v(xy) = v(x) + v(y) \).
3. \( v(x + y) \geq \min(v(x), v(y)) \)

3.3.2 Proposition:

Let \( R \) be a commutative ring with identity element, then the followings are equivalent:

1. \( R \) is a local principal ideal domain, and not a field.
2. \( R \) is an integrally closed Noetherian local ring with Krull dimension one.
3. Let \( K \) be the field of fractions of \( R \). There is some discrete valuation \( v \) on \( K \), such that \( R = \{x \in K : v(x) \geq 0\} \).

[1][Proposition 9.2]

3.3.3 Definition: Discrete Valuation Rings

For any discrete valuation \( v \) on \( K \) there is a discrete valuation ring
\[ O_v := \{x \in K : v(x) \geq 0\} \]
with its unique maximal ideal
\[ m_v := \{x \in K : v(x) \geq 1\} \].
The residue field of a discrete valuation ring \( A \) with its unique maximal ideal \( m \) is the field \( A/m \).
3.3.4 Lemma:

The valuation ideal \( m_v \) is principal.

Proof.

Let \( t \) be an element of \( O_v \) such that \( v(t) = 1 \). If \( f \in O_v \), then \( v(tf) = 1 + v(f) \geq 0 \), thus \( tO_v \subset m_v \).

For any \( x \in m_v \), \( v(x) = k \geq 1 \) and \( v(x/t) = k - 1 \geq 1 \geq 0 \). So \( x/t \in O_v \), \( x = t(x/t) \in tO_v \).

\[ \square \]

3.3.5 Example of Discrete Valuation Rings:

a. The ring of integers, \( \mathbb{Z} \), is clearly a UFD (unique factorization domain), for any nonzero element \( n \), \( n \) could be written as a product of prime numbers, say

\[ n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \]

for some positive integer \( r \).

And for any prime number \( p \), we can define the valuation w.r.t \( p \) by

\[ \text{ord}_p(n) = e_i \text{ if } p = p_i. \]

and \( \text{ord}_p(n) = 0 \) otherwise.

We can also extend any such function to \( \mathbb{Q}^\times \) by defining \( \text{ord}_p(n/m) = \text{ord}_p(n) - \text{ord}_p(m) \).

To show that this is actually well-defined, if \( \frac{n_1}{m_1} = \frac{n_2}{m_2} \) for any nonzero, \( n_1, n_2, m_1, m_2 \in \mathbb{Z} \), then \( n_2m_1 = n_1m_2 \).

Then we have

\[ \text{ord}_p(n_2) + \text{ord}_p(m_1) = \text{ord}_p(n_1) + \text{ord}_p(m_2). \]

Thus

\[ \text{ord}_p(n_1/m_1) = \text{ord}_p(n_1) - \text{ord}_p(m_1) = \text{ord}_p(n_2) - \text{ord}_p(m_2) = \text{ord}_p(n_2/m_2). \]

b. For the \( p \)-adic valuation \( v_p : \mathbb{Q} \rightarrow \mathbb{Z} \cup \{ \infty \} \), we have the valuation ring

\[ \mathbb{Z}_{(p)} := \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, p \text{ is not a divisor of } b \right\}. \]

The maximal ideal of \( \mathbb{Z}_{(p)} \) is \( m = (p) \), which is the localization of the ring \( \mathbb{Z} \) at the prime ideal \( (p) \). The residue field in this case is

\[ \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p. \]

3.3.6 Definition: uniformizing parameter

Let \( V \) be a discrete valuation ring, then any element \( t \in V \) with \( v(t) = 1 \) is called a uniformizing parameter, sometimes also called the uniformizing generator.
3.3.7 Proposition:

Let $t$ be a uniforming parameter in the discrete valuation ring $V$. Then $t$ generates the maximal ideal $M$ of $V$, in particular, $M$ is principal. Conversely, if $t$ is any generator of $M$, then $t$ is a uniforming parameter.

Proof.

Since $M$ is the unique maximal ideal, $(t) \subset M$. If $a \in M$, then $v(a) \geq 1$, so

$$v(at^{-1}) = v(a) - v(t) \geq 1 - 1 = 0,$$

thus $at^{-1}$, and consequently $a \in (t)$.

Now suppose that $M = (s)$ for some $s \in V$. Since $t \in M$ we have $t = cs$ for some $c \in V$.

Thus

$$1 = v(t) = v(cs) = v(c) + v(s) \geq 0 + 1 = 1$$

which implies that $v(s) = 1$.

3.3.8 Proposition: Equivalent conditions for discrete valuation rings

Let $V$ be an integral domain. The followings are equivalent.

1. $V$ is a Noetherian valuation ring.
2. $V$ is local and is a principal ideal domain.
3. $V$ is Noetherian and local and its maximal ideal is generated by a single element.
4. $V$ is Noetherian, local of Krull dimension less than or equal to one, and integrally closed in its field of fractions.

Proof.

1. $(1) \iff (2)$: In a valuation ring every finitely generated ideal is principal, so $(1)$ implies $(2)$. And a local ring is a valuation ring if and only if every finitely generated ideal is principal, so $(2)$ implies $(1)$.

2. $(2) \iff (3)$: A principal ideal domain is always noetherian, so $(2)$ implies $(3)$. Then we want to show that $(3)$ implies $(2)$, suppose that $\pi$ generates the maximal ideal of $V$. Since $V$ is a noetherian ring, $\cap m^i = 0$. If $a \neq 0$, there is then an element $k$ such that $a \in m^k$ but $a$ is not in $m^{k+1}$, so $a = b\pi^k$ for some $b \notin m$. 

Thus $b$ is a unit, and $(a) = (\pi^k)$, let $v(a) := k$. If $I$ is any nonzero ideal of $V$, let $\gamma$ be the minimum of $\gamma(a)$ over all the nonzero elements $a \in I$. Then $I = (\pi^k)$, which is clearly a principal ideal.

3. (2) $\Rightarrow$ (4) : Since a principal ideal domain has dimension at most one and is integrally closed, (2) implies (4).

4. (4) $\Rightarrow$ (3) : Now it remains only to prove that (4) implies (3). If the maximal ideal $m$ of $V$ is the zero ideal, $V$ is a field. Suppose this is not the case. Since $m$ is finitely generated, Nakayama’s lemma implies that there is some element

$$\pi \in m \ m^2.$$ 

Then it suffices to prove that $m = (\pi)$. Since $V$ is integral, (0) is a prime ideal, and since $V$ has dimension at most one, (0) $\subset m$ is a maximal chain of primes.

Thus the dimension of $V$ is in fact 1, and since every prime ideal $P$ contains(0) and is contained in $m$, $V$ has exactly two prime ideals. Since $\pi \neq 0$, the quotient ring $V/(\pi)$ has only one prime ideal, which is $m/(\pi)$, and hence every element of $m/(\pi)$ is a nilpotent element. Since $m$ is finitely generated, it follows that $m^i \subset (\pi)$ for some $i$. It will suffice to prove that the smallest $i$ is 1.

We prove it by contradiction, suppose that $i \geq 2$. Then we choose the element $a$ to be in $m^{i-1}$. Then for any $x \in m$, $ax \in m^i$, and hence $ax = \pi x'$ for some $x' \in V$. Since $a \in m^{i+1}$ and $i \geq 2$, $a \in m$ and $ax \in m^2$.

Since $\pi \notin m^2$, $x'$ is not a unit, so $x' \notin m$. We have just proved that multiplication by the element $a/\pi$ of the fraction field $K$ of $V$ maps $m$ into $m$ itself. But $m$ is a finitely generated faithful $V$-module, and it follows from this that $a/\pi$ is integral over $V$. Since $V$ is integrally closed in $K$, it follows that $a/\pi \in V$, i.e. $a \in (\pi)$. Thus we have proved that $m^{i+1} \subset (\pi)$, contradicting the minimality of $i$.

Thus the statement follows.

3.3.9 Proposition:

let $R$ be a Noetherian domain of dimension one, then the following statements are equivalent:

1. $R$ is integrally closed.
2. Every prime ideal $P$ in $R$ is a prime power.
3. Every local ring $R_p$ for some $p \neq 0$ is a discrete valuation ring.

[1][Theorem 9.3]
3.4. PLACES

3.3.10 Definition: Dedekind Domains

A ring \( R \) satisfying any of the conditions in proposition 3.4.9 is called a Dedekind domain.

Then we have a useful result about Dedekind domains:

3.3.11 Proposition:

Let \( R \) be a Dedekind domain, every non-zero ideal in \( R \) has a unique factorization of prime ideals. [1][Corollary 9.4]

3.4 Places

3.4.1 Definition: Place

A place of a function field \( K \) over \( F \) is a discrete valuation \( v \) on \( K \) such that

\[ v(F^\times) = 0. \]

We often write a valuation on \( K \) such that \( v(F^\times) = 0 \) as \( P \), and the valuation of \( f \in K \) at \( P \) written as \( \text{ord}_P(f) \).

The following theorem describes all of the places of \( K \):

3.4.2 Theorem:

Let \( K \) be a function field and let \( x \in K - F \), the places of \( K \) which are non-negative on \( x \) are in one-to-one correspondence with the primes in \( R_x \), the integral closure of \( F[x] \) in \( K \). In particular, for a place \( P \) and its corresponding prime \( \mathfrak{p} \),

\[ (R_x)_\mathfrak{p} = O_P. \]

Proof.

Let \( P \) be a place such that \( \text{ord}_P(x) \geq 0 \), To show that \( R_x \subset O_P \)
, recall that \( x \in O_P, F[x] \subset O_P, \) and since \( O_P \) is a discrete valuation ring by its definition (thus it is integrally closed). Let’s look at the intersection \( \mathfrak{m}_P \cap R_x \), we want to show that it is a prime ideal of \( R_x \). Suppose it is is the zero set, then

\[ R_x - \{0\} \subset O_P - \mathfrak{m}_P = O_P^\times. \]

Then \( F(x) \) is a subset of \( O_P \), and so its integral closure, the integral closure of \( F(x) \) is however the algebraic closure of \( F(x) \), i.e. \( K \). This is not possible since if \( K \subset O_P \) then \( \text{ord}_P \) only has non-negative values then it is therefore not onto \( \mathbb{Z} \).
Thus we have shown that
\[ m_P \cap R_x \neq \{0\} \]
it is a prime ideal of \( R_x \).

Suppose we are given a prime ideal \( p \) in \( R_x \), by proposition 3.4.9
\( R_x \) is a Dedekind domain (since \( R_x \) is the integral closure of the
\( F[x] \)). For any nonzero \( y \in R_x \), \( yR_x \) can be factorized uniquely
into a product of prime ideals \( \prod q_i^{k_i} \), use this correspondence we
could define a function
\[ \text{ord}_q(y) := k_q. \]
For any nonzero element \( z \in R_x \), \( zR_x = \prod q_i^{l_i} \), then we have
\[ \text{ord}_q(yz) = k_q + l_q = \text{ord}_q(y) + \text{ord}_q(z). \]

Since \( 1/zR_x = \prod q_i^{-l_i} \), we want to extend the function on \( K^\times \)
using
\[ \text{ord}_q(y/z) = \text{ord}_q(y) - \text{ord}_q(z). \]
Thus we have a group homomorphism between \( K^\times \) and \( \mathbb{Z} \) for any
given prime \( p \), we want to show that it is surjective. We show this
by contradiction. For some prime \( p \), if there is no element \( t \in R_x \)
such that \( \text{ord}_p(t) = 1 \), then \( p = p^2 \) since
\[ p - p^2 = 0. \]
Thus \( p = p^2 = p^4 \) and so on by the definition of \( p^n \), thus
\[ p = \bigcap_{n>0} p^n. \]
Since \( R_x \) is a Dedekind domain, it is Noetherian, by the Krull
intersection theorem
\[ p = \bigcap_{n>0} p^n = (0) \]
thus not prime in \( R_x \). Thus the homomorphism is surjective.

Let \( y, z \) be elements in \( K^\times \),
\[ m := \min(\text{ord}_p(y), \text{ord}_p(z)). \]
If \( m \geq 0 \) then \( y, z \in p^m \), thus \( y + z \in p^m \), which implies \( \text{ord}_p(y + z) \geq m \). On the other hand, if \( m < 0 \), then let \( t \in p - p^2 \), we have
\[ \text{ord}_p(t^{-m}y + t^{-m}z) = -m + \text{ord}_p(y + z) \geq 0 \Rightarrow \text{ord}_p(y + z) \geq m \]
since \( t^{-m}y + t^{-m}z = t^{-m}(y + z) \).
Thus given any prime \( p \) we have a discrete valuation defined as
\( \text{ord}_p \) on \( K^\times \). Since \( F \) is a field, the only ideals of \( F \) is \( (0) \) and the
whole field, and since \( p \) is a proper ideal, \( 1 \notin p \), thus \( F \cap p = (0) \),
thus for any \( a \in F \), \( \text{ord}_p(a) = 0 \).

For any discrete valuation on a ring, by Definition 3.4.3, we have
the discrete valuation \( O_p \) for it. Since \( (R_x)_p \) is a local ring with
its unique maximal ideal \( p(R_x)_p \),
\[
R_x \cap p(R_x)_p = p.
\]
Now it suffices to show that \( O_p = (R_x)_p \).
The first direction is obvious, since \( p \subset O_p, (R_x - p) \subset O^\times_p \), which implies \( O_p \supset (R_x)_p \). To show the other inclusion, it suffices to show that
\[
O^\times_p \subset (R_x)_p,
\]
since that for any \( f \in O_p \), if \( t \in p - p^2 \), then \( f = t^{\text{ord}_p(f) (t^{-\text{ord}_p(f)} f)} \).
Since \( t \in R_x \) and \( \text{ord}_p(t^{-\text{ord}_p(f)} f) = 0 \).
To show that \( O^\times_p \subset (R_x)_p \), let \( f \in O^\times_p \). Since \( O_p \subset K \), and \( K \) is the fraction field of \( R_x \), there are \( y,z \in R_x - \{0\} \) with \( f = y/z \).
Since \( \text{ord}_p(y/z) = 0 \), we have \( \text{ord}_p(y) = \text{ord}_p(z) \). If we consider the fractional ideal \( f = (y)(z)^{-1} \), \( f = ab^{-1} \) where \( (a,b) = R_x \), and \( a,b \) are both coprime to \( p \). Suppose \( a \) can be factorized into prime ideals
\[
q_1^{r_1} q_2^{r_2} \cdots q_m^{r_m}.
\]
Take \( r \in R_x - p \), then there is some \( a \in R_x \) such that
\[
a \equiv r \mod p \quad \text{and} \quad a \equiv 0 \mod q_i^{r_i}
\]
by the Chinese Reminder theorem. Thus \( a \in a, (a) \subset a \), and \( (a) = ac \) where \( (c,p) = R_x \).
We have \( fb = a \) since \( (f) = ab^{-1} \), thus \( fbc = ac = (a) \). Then \( bc = (a/f), \) let \( a/f = b, \) since \( bc \subset R_x \) and both \( b \) and \( c \) are coprime to \( p \) as in the assumption ,then we have \( b \in R_x - p \).
Finally,
\[
f = ab^{-1} \in R_x(R_x - p)^{-1} = (R_x)_p,
\]
thus \( O^\times_p \subset (R_x)_p, (R_x)_p = O_p \).

We then prove a lemma that connect the field of constants, \( F \), with the valuation ring \( O_P \).

3.4.3 Lemma:

For any place \( P \), \( [O_P/m_P : F] \) is finite, and if \( F \) is an algebraically closed field,
\[
O_P/m_P \simeq F.
\]

Proof.

Since \( \text{ord}_P \) is trivial on \( F^\times, F^\times \subset O^\times_P \). In addition, \( F \to O_P/m_P \) since that any nontrivial ring homomorphism from a field to a ring is injective. Then we want to show that \( O_P/m_P \) is a finite
extension over $F$. Choose some $x \in K - F$, such that $\text{ord}_P(X) \geq 1$, the extension $K/F(x)$ is finite.

Now let $\{e_1, \ldots, e_m\}$ be the elements of $O_P$ whose residue classes modulo $m_P$ are linearly independent over $F$.

Claim: $m \leq [K : F(x)]$.

We prove the claim by contradiction, suppose that $m > [K : F(x)]$, there is a set of rational functions which are not all zero

$$\{f_1(x), \ldots, f_m(x)\} \subset F(x),$$

such that

$$f_1(x)e_1 + \ldots + f_m(x)e_m = 0.$$ 

$f_i(x)$ can be viewed as not all zero elements of $F[x] \subset O_P$ by cancelling the denominators, if non of the $f_i$ have a nonzero constant term, just divide both sides of the equation by $x$ until at least one of the $f_i$s has a nonzero constant term.

Next, let $c_i$ be the constant term of $f_i(x)$, since $\text{ord}_P(x) \geq 1$ by the assumption, all the $x$’s will vanish and we have

$$c_1e_1 + \ldots + c_m e_m = 0$$

when we reduce modulo $m_P$.

Which is a contradiction with the linear independence of the $e_i$’s over $F$, thus $m \leq [K : F(x)]$.

\[\square\]

3.4.4 Theorem:

For any element $x \in K - F$,

$$[K : F(x)] = \sum_P \max(\text{ord}_P(x), 0)[O_P/m_P : F].$$

Proof.

Let $x \in K - F$, $R_x$ be the integral closure of $F[x]$ in $K$, $R_x$ is a Dedekind domain.

Therefore $xR_x$ factors uniquely as

$$xR_x = \Pi_p p^{\text{ord}_p(x)}.$$ 

By the Chinese Remainder theorem,

$$R_x/xR_x = R_x/\Pi_p p^{\text{ord}_p(x)} \simeq \Pi_R/p^{\text{ord}_p(x)}.$$ 

Since we have that $R_x$ is the integral closure of $F[x]$ in $K$, which is a finite field extension, then it is a free $F[x]$ module of rank $[K : F(x)]$. For convenience, let $d = [K : F(x)]$. Now, let
Thus since from commutative algebra we know that \( \dim \) is a finite product.

The kernel of the map will be the set \( \ker R\to R = R_t \mod \mathfrak{m} \) and \( \ker R\to R = R_t \mod \mathfrak{m} \) is onto.

The kernel of the map will be the set \( K = \{ f \in R_x : f \equiv t^{-j}f \pmod{p^j} \} \).

Thus \( \Sigma_{j=1}^k \dim_F (p^{-j}p^j) = k \dim_F (R_x/P) \)

which implies that \( \Sigma_{P} \dim_F (R_x/P^{\text{ord}_p(x)}) = \Sigma_{P} \dim_F \text{ord}_p(x) \dim_F (R_x/P) \)

if the dimension of \( R_x/p \) over \( F \) is finite.

Now we should discuss the dimension of \( R_x/p \) over \( F \), Let \( \phi \) be the map from \( R_x \) to \( (R_x)_p/P(R_x)_p \), defined by \( \phi(f) = f \pmod{P(R_x)_p} \).

Since \( R_x \) is Dedekind, every prime ideal of \( R_x \) is a maximal ideal, and thus if \( z \in R_x - P \), there is some \( z' \in R_x \) such that \( zz' \equiv 1 \pmod{P} \).

Thus \( \phi \) is surjective since for any \( y \in R_x \), \( z \in R_x - P \), we can take \( f = yz' \).

Because \( f \equiv z \pmod{P} \), \( f \equiv y/z \pmod{p(R_x)_p} \), thus

\[ \Sigma_{P} \text{ord}_p(x) \dim_F (R_x/P) = \Sigma_{P} \text{ord}_p(x) \dim_F ((R_x)_p/P(R_x)_p). \]

For each prime \( P \), we have a unique valuation \( P \) such that \( \text{ord}_P(x) \geq 0 \)

and each valuation was given by a prime, also the localization of
\( R_x \) at \( p \) is the valuation ring \( O_P \), thus
\[
O_P/m_P = (R_x)_P/p(R_x)_P
\]
ard
\[
\sum_{\text{ord}_P(x) \dim_F((R_x)_P/P(R_x)_P) = \sum_{\text{ord}_P(x) \geq 0} \text{ord}_P(x) \dim_F(O_P/m_P)
\]
by the previous theorem.
We know from the previous lemma, for any \( P \)
\[
\dim_F(O_P/m_P) = [O_P/m_P : F]
\]
is finite, thus
\[
[K : F(x)] = \sum_{\text{ord}_P(x) \geq 0} \text{ord}_P(x) [O_P/m_P]).
\]
And the theorem follows.

\[\square\]

### 3.4.5 Definition: Zeros, poles and multiplicity

With respect to the notations in complex analysis, if \( \text{ord}_P(f) > 0 \) then \( f \) has a zero of order \( \text{ord}_P(f) \) at \( P \), if \( \text{ord}_P(f) < 0 \) then \( f \) has a pole of order \( \text{ord}_P(f) \).

The multiplicity of \( f \) at \( P \) is the absolute value \( |\text{ord}_P(f)| \).
Chapter 4

The Riemann-Roch Theorem

4.1 Divisors

Let us start by giving the definition of divisors.

4.1.1 Definition: Divisor of a function field

Let \( K/F \) be a function field, a divisor of \( K/F \) is of the form
\[
\Sigma P n_P P, \ n_P \in \mathbb{Z}
\]
where \( P \) is a place of \( K \).

The group of divisors of \( K/F \), denoted by \( \mathcal{D}_K \) is a free abelian group on the places of \( K \) (By Definition 1.4.10),
\[
\mathcal{D}_K = \bigoplus_P \mathbb{Z}P = \{ \Sigma_P n_P P : n_P = 0 \text{ for all but finitely many } P \}
\]
where \( n_P \in \mathbb{Z} \) and \( n_P = 0 \) for all but finitely many \( n_P \).

And the addition of divisors is defined component-wise:
\[
\Sigma_P n_P P + \Sigma_P m_P P = \Sigma_P (n_P + m_P)P.
\]

4.1.2 Definition: Degree of a divisor

The degree of a divisor is defined as
\[
\deg(\Sigma_P n_P P) = \Sigma_P n_P \in \mathbb{Z}.
\]

4.1.3 Example: Divisors

1. Particularly, for any function field \( K \), there is a zero divisor of \( K \) such that \( 0 = \Sigma_P n_P P \) where \( n_P = 0 \) for every \( P \).
2. For a counter example, consider a function field $K/F$, and $\Sigma P_n P$ such that $n_P = 1$ for all $P$. In this case, it is not a divisor since it has nonzero coefficients at an infinite number of places $P$.

4.1.4 Definition: divisor of zeros and divisor of poles

For any $f \in K^\times$, the divisor of $f$, denoted by $\text{div} f$, is defined by $\Sigma P \text{ord}_P(f) P$.

For any $f \in K$ we have:
\[
\text{div}(f) = \text{div}_0(f) - \text{div}_\infty(f)
\]
where the positive and negative parts are defined trivially as:
\[
\text{div}_0(f) = \Sigma P \max(\text{ord}_P(f), 0) P,
\]
\[
\text{div}_\infty(f) = \Sigma P \min(\text{ord}_P(f), 0).
\]

Where the $\text{div}_0(f)$ is called the divisor of zeroes of $f$ and $\text{div}_\infty(f)$ is called the divisor of poles of $f$.

4.1.5 Definition: Effective divisor

A divisor $\Sigma P_n P$ is called effective at $P$ if $n_P \geq 0$. And a divisor is called effective if it is effective at each $P$.

In particular, for all $x \in K - F$, $\text{div}_0(x)$ and $\text{div}_\infty(x)$ are effective by definition.

4.1.6 Corollary:

For any $x \in K - F$,
\[
\deg(\text{div}_0(x)) = \deg(\text{div}_\infty(x)) = [K : F(x)].
\]
Thus for any $x \in K - F$ there are as many zeros of $x$ as there are poles, when we count in multiplicities.

Proof.

First from Theorem 3.5.4 we have that
\[
\deg(\text{div}_0(x)) = [K : F(x)].
\]
Now if we replace $x$ with $1/x$, since $F(x) = F(1/x)$ and
\[
\text{div}_0(1/x) = \text{div}_\infty(x),
\]
thus $\deg(\text{div}_\infty(x)) = [K : F(x)]$, we get the results.

$\square$
4.2. Properties of Divisors and \( L(D) \)

4.1.7 Definition: Equivalence relation on divisors

Two divisors \( D_1 \) and \( D_2 \) are said to be linear equivalent if

\[ D_2 = D_1 + \text{div}(x) \]

for some \( x \in K \), in this case, we write \( D_1 \equiv D_2 \).

It follows easily from the definition that:

4.1.8 Proposition:

The relation \( \equiv \) on divisors is an equivalence relation.

4.2 Properties of Divisors and \( L(D) \)

4.2.1 Theorem:

For any divisor \( D_1, D_2 \in \mathcal{D}_K \), for any \( f, g \in K^\times \):

1. \( \text{deg}(D_1 + D_2) = \text{deg}(D_1) + \text{deg}(D_2) \).
2. \( \text{div}(fg) = \text{div}(f) + \text{div}(g) \).
3. \( \text{deg}(\text{div}(f)) = 0 \).
4. For any divisor \( D \), for any \( f \in K^\times \), \( \text{deg}(D + \text{div}(f)) = \text{deg}(D) \).
5. Let \( D_1, D_2 \) be nonzero divisors in \( \mathcal{D}_K \), then \( \text{div}(D_1) = \text{div}(D_2) \) if and only if \( D_1 = \lambda D_2 \) for some \( \lambda \in k \).

Proof.

1. The first statement follows from direct calculation.
2. For the second statement, recall that \( \text{ord}_P(\cdot) \) is a valuation on \( K \). Thus for any \( f, g \in K^\times \),

\[ \text{ord}_P(fg) = \text{ord}_P(f) + \text{ord}_P(g) \]

for all places \( P \).

Therefore \( \Sigma_P \text{ord}_P(fg) = \Sigma_P(\text{ord}_P(f) + \text{ord}_P(g)) \).
3. For the third statement, \( \text{deg}(\text{div}(a)) = \Sigma_P 0 = 0 \) since \( \text{div}(a) = 0 \) for any \( a \in F^\times \).
4. For the fourth statement, use the fact that \( \text{deg}(D + \text{div}(f)) = \text{deg}(D) + \text{deg}(\text{div}(f)) \) and \( \text{deg}(\text{div}(f)) = 0 \).
5. The last statement follows easily from the definition.
4.2.2 Definition: Partial Order on Divisors

Define the $\geq$ relation on divisors $D = \Sigma_P n_P P$ and $E = \Sigma_P m_P P$,

$$D \geq E \text{ if and only if } n_P \geq m_P \text{ for all } P.$$ 

The reflexivity, antisymmetry and transitivity follow directly from the definition.

4.3 The vector spaces $L(D)$

4.3.1 Definition: $L(D)$

First, let us define

$$L(D) := \{0\} \cup \{f \in K^\times : \text{div}(f) + D \geq 0\}.$$ 

Thus $L(D)$ can be viewed as an $F$-vector space, and the dimension of $L(D)$ is defined by

$$l(D) := \dim_F(L(D))$$

(when the dimension is finite). The definition of $L(D)$ is very important since the aim of the Riemann-Roch Theorem is to compute $l(D)$. Later in this chapter we will show that for any divisor $D$, $L(D)$ is actually a finite-dimensional over $F$.

4.3.2 Corollary:

For any divisor $D$ with $\dim_F(L(D)) < \infty$ and any element $f \in K$,

$$L(D + \text{div}(f)) = L(D).$$

Thus $l(D + \text{div}(f))$ is defined and equal to $l(D)$.

Proof.

If $L(D) = \{g \in K : \text{div}(g) + D \geq 0\}$ then

$$L(D + \text{div}(f)) = \{g \in K^\times : \text{div}(g) + \text{div}(f) + D \geq 0\} \cup \{0\}$$

$$= \{g \in K^\times : \text{div}(fg) + D \geq 0\} \cup \{0\}$$

$$= \{h \in K^\times : \text{div}(h) + D \geq 0\} \cup \{0\}$$

$$= L(D).$$

(4.2)

Proof.

4.3.3 Theorem:

For any divisor $D$ where $l(D)$ is defined,

$$l(D + P) \leq l(D) + 1$$
4.3. THE VECTOR SPACES $L(D)$

for all points $P$.

**Proof.**

Let $L(D)$ be some finite-dimensional vector space over $F$, where

$$D = n_P P + \sum_{Q \neq P} n_Q Q,$$

then for all $f \in L(D + P)$ we have $\text{ord}_P(f) \geq -n_P - 1$.

In particular, if $f \not\in L(D)$ then we have that, for some place $Q$,

$$\text{ord}_Q(f) + n_Q < 0.$$

Since $f \in L(D + P)$, this can only happen for $Q = P$, and

$$\text{ord}_Q(f) + n_P = -1.$$

Let $m = n_P + 1$, we have

$$\text{ord}_Q(f) = -n_P - 1 = -m.$$

For any $f \in L(D + P) - L(D)$, $f$ has order $-m$ at $P$, if such an $f$ does not exist, then $L(D + P) = L(D)$.

Let $f \in L(D + P)$ has exact order $-m$ at $P$, then consider some uniformizing parameter $t$ of $P$.

Since that $\text{ord}_P(f) = -m$ and $\text{ord}_P(t^m)$ we have that $t^m f \in O_P - m_P$.

Since $O_P/m_P \simeq F$, $t^m f \equiv a \mod P$ for some element $a \in F^\times$ and thus $t^m f = a + xt$ for some $x \in O_P$. Now if $g$ is some other element of $L(D + P)$ of exact order $-m$ at $P$, then we can likewise write $t^m g = b + yt$ for $b \in F$, and some $y \in O_P$.

Thus

$$f = at^{-m} + xt^{-m+1}, \quad g = bt^{-m} + yt^{-m+1}.$$

Thus

$$g - \frac{b}{a} f = (y - \frac{b}{a} x)t^{-m+1}.$$

We also have

$$\text{ord}_P(g - \frac{b}{a} f) = \text{ord}_P(y - \frac{b}{a} x) + \text{ord}_P(t^{-m+1}) \geq -m + 1 = -n_P.$$

Between any two nonzero elements of $L(D + P)/L(D)$ we have a linear independence. Thus $\dim_F L(D + P)/L(D) = 1$ so that

$$l(D + P) \leq 1 + l(D).$$

$$\square$$

4.3.4 Corollary:

For any divisor $D$ of $K$, if $l(D) \neq 0$, then $l(D) \leq \deg(D) + 1$.

**Proof.**

Claim: If $\deg(D) < 0$, then $l(D) = 0$.
We prove the claim by contradiction, suppose there is some nonzero \( g \in L(D) \), since \( g \in L(D) \), then

\[
\deg(\text{div}(g) + D) \geq 0
\]

by definition, since we have

\[
\deg(\text{div}(g) + D) = \deg(D) < 0.
\]

Thus such nonzero \( g \) doesn’t exist in \( L(D) \), thus \( \deg(D) < 0 \) implies that \( l(D) = 0 \).

Now suppose \( g(D) = 0 \), then for any point \( P \), \( \deg(\ D - P) = -1 \). And \( l(D) = l(D - P + P) \leq l(D - P) + 1 = 1 \) since \( l(D - P) = 0 \).

Suppose for any divisor \( D' \) with \( \deg(D') = n \geq 0 \) (by induction), \( l(D') \leq n + 1 \). Let \( D \) be an arbitrary divisor of degree \( n + 1 \), then \( l(D) = l(D - P + P) \leq L(D - P) + 1 \leq n + 1 + 1 = \deg(D) + 1 \).

4.3.5 Proposition:

For the zero divisor \( 0 \), we have

\[
l(0) = 1.
\]

Proof.

If \( D = 0 \) then \( L(D) \) is the set of functions that have no poles at all. By Theorem 3.5.4, for any \( f \in L(0) \) we have

\[
\deg \text{div}_{\infty} f = 0
\]

if and only if \( f \in k^{\times} \), so \( L(0) = k \), \( l(0) = 1 \).

4.4 The Adeles

4.4.1 Definition: Adele ring and Adele space

The adele ring \( \mathbb{A}_K \) of a function field \( K \) is the restricted direct product of \( K \) w.r.t. \( O_P \) indexed by the places \( P \) of \( K \).

The element of the adeles are of the form

\[
\Pi_P x_P
\]

which we denote by \( (x_P) \).

The diagonal embedding is the map \( x \mapsto (x, x, x, \ldots) \), which is in \( \mathbb{A}_K \) by Theorem 3.5.4.

For any divisor \( D = \sum_P n_P P \), the adele space \( \mathbb{A}_K(D) \) is the set of all adeles \( (x_P) \) where \( \text{ord}_P(x_P) + n_P \geq 0 \) or \( x_P = 0 \).
Since $n_P = 0$ for all but finitely many $P$, $\mathbb{A}_K(D) \subset \mathbb{A}_K$ for all $D$.

4.4.2 Proposition: Properties of Adele rings

Let $D_1 = \Sigma_P n_P P$, $D_2 = \Sigma_P m_P P$, the following statements hold:

1. If $D_1 \leq D_2$ then $A_K(D_1) \subset A_K(D_2)$.
2. Define $\min\{D_1, D_2\} := \Sigma_P \min\{n_P, m_P\} P$, then
   \[ A_K(\min\{D_1, D_2\}) = A_K(D_1) \cap A_K(D_2). \]
3. Define $\max\{D_1, D_2\} := \Sigma_P \max\{n_P, m_P\} P$, then
   \[ A_K(\max\{D_1, D_2\}) = A_K(D_1) + A_K(D_2). \]
4. Under the diagonal embedding, $K \cap A_K(D) = L(D)$.

Proof.

If $D_1 \leq D_2$ then by definition, $m_P \geq n_P$ for all $P$. If $(\phi_P) \in A_K(D_1)$ then $\phi_P \neq 0$,
\[
\text{ord}_P(\phi_P) + m_P \geq \text{ord}_P(\phi_P) + n_P \geq 0.
\]
Thus $A_K(\min\{D_1, D_2\}) \subset A_K(D_1) \cap A_K(D_2)$. If $(\phi_P) \in A_K(D_1)$ and $(\psi_P) \in A_K(D_2)$, then for any $P$ so that $\phi_P \neq 0$,
\[
\text{ord}_P(\phi_P) + n_P \geq 0 \text{ and } \text{ord}_P(\phi_P) + m_P \geq 0.
\]
Thus we have $\text{ord}_P(\phi_P) + \max\{n_P, m_P\} \geq 0$, therefore
\[
A_K(D_1) \cap A_K(D_2) = A_K(\min\{D_1, D_2\}).
\]
If $\phi_P \in A_K(D_1)$, $\psi_P \in A_K(D_2)$, then for the places $P$ where $\phi_P = -\psi_P$ there is nothing left for us to show. If for one of (or both) $\phi_P$, $\psi_P$ is nonzero, then we claim that if $\phi_P$ is zero and $\psi_P$ is nonzero, then
\[
\min\{\text{ord}_P(\phi_P), \text{ord}_P(\psi_P)\} = \text{ord}_P(\psi_P).
\]
Then $\text{ord}_P(\phi_P + \psi_P) \geq \min\{\text{ord}_P(\phi_P), \text{ord}_P(\psi_P)\}$ by the definition of a valuation. Thus for all places $P$,
\[
\text{ord}_P(\phi_P + \psi_P) + \max\{n_P, m_P\} \geq \min\{\text{ord}_P(\phi_P), \text{ord}_P(\psi_P)\} + \max\{n_P, m_P\}
\]
and
\[
\min\{\text{ord}_P(\phi_P), \text{ord}_P(\psi_P)\} + \max\{n_P, m_P\} \geq 0.
\]
The last statement follows by the definitions of $A_K(D)$ and $L(D)$.

4.4.3 Lemma :

For divisors $D_1$ and $D_2$, if $D_1 \leq D_2$, then
\[
\dim_F\left(\frac{A_K(D_2)}{A_K(D_1)}\right) = \deg(D_2) - \deg(D_1).
\]
Proof.

Prove by induction on deg\((D_2) - deg(D_1)\).

If deg\((D_2) = deg(D_1)\), then since \(D_1 \leq D_2\), we have \(D_1 = D_2\),
\(A_K(D_1) = A_K(D_2)\), and \(\frac{A_K(D_2)}{A_K(D_1)} = \{0\}\).

If deg\((D_2) - deg(D_1) = 1\), then \(D_2 = D_1 + P\) for some place \(P\) since \(D_1 \leq D_2\). If for any divisor \(D = \Sigma_P n_P P\) and any place \(P\), we can project from \(A_K(D_1 + P)\) to \(m_P^{-n_p-1}\).

And then we can reduce modulo \(m_P^{-n_p}\) giving the map \((x_Q) \mapsto x_P \mod m_P^{-n_p}\).

Since \((x_Q) \in A_K(D_1)\) implies that for any \(f \in m_P^{-n_p-1}, f \in \Pi_Q x_Q \in A_K(D_1 + P)\). Thus the map is surjective.

Consider the kernel of this map, if \((x_Q) \in A_K(D_1 + P)\) is in the kernel, then \(x_P \in m_P^{-n_p}\) so \(ord_P(x_P) = -n_P\) or \(x_P = 0\).

For \(Q \neq P\), since \((x_Q) \in A_K(D_1 + P)\) we have \(ord_Q(x_Q) \geq -n_Q\) and \((x_Q) \in A_K(D_1)\). Thus
\[A_K(D_1 + P)/A_K(D_1) \simeq m_P^{-n_p-1}/m^{-n_p}.
\]

Let \(t\) be a uniformizing parameter of \(P\), consider the map \(O_P \to m_P^k/m_P^{k+1}\) by sending \(f\) to \(ft^k \mod m_P^{k+1}\). The map is surjective with kernel \(m_P\). Therefore we have
\[m_P^k/m \simeq O_P/m_P.
\]

When \(deg(D_2) - deg(D_1) = 1\), the theorem then follows.

If for some \(n \geq 1\),
\[\dim_F(\frac{A_K(D_2)}{A_K(D_1)}) = deg(D_2) - deg(D_1)
\]
for any \(D_2 \geq D_1\). And \(n = deg(D_2) - deg(D_1)\), we then can find some divisor \(D_3\) such that
\[D_2 \geq D_3 \geq D_1\]
with the following two conditions hold
\[(1) \ deg(D_1) - deg(D_3) = 1.
(2) \ deg(D_3) - deg(D_1) = n. \quad (4.3)
\]

Since \(A_K(D_1) \subset A_K(D_3) \subset A_K(D_2)\),
\[\dim_F(\frac{A_K(D_2)}{A_K(D_1)}) = \dim_F(\frac{A_K(D_2)}{A_K(D_3)}) + \dim_F(\frac{A_K(D_3)}{A_K(D_1)})
= deg(D_2) - deg(D_3) + deg(D_3) - deg(D_1)
= deg(D_2) - deg(D_1).
\quad (4.4)
\]

\square
4.4. **Definition:** $r(D)$

For any divisor $D$, let $r(D) := \deg(D) - l(D)$.

4.4.5 **Lemma:**

If $f \in K^\times$ and $D_1, D_2$ are divisors on $K$, then for $r : \mathcal{D}_K \to \mathbb{Z}$

1. If $D_1 \leq D_2$, $r(D_1) \leq r(D_2)$.
2. For any $D$, $r(\text{div}(f) + D) = r(D)$.

**Proof.**

1. First we prove a claim.

   **Claim:** We can view $K$ diagonally in $F$, and
   
   $\dim_F \frac{A_K(D_2) + K}{A_K(D_1) + K} = (\deg(D_2) - l(D_2)) - (\deg(D_1) - l(D_1))$

   **Proof of the claim:**

   Since $A_K(D_2) \cap (A_K(D_1) + K)$ is the kernel of the map from $A_K(D_2) \to (A_K(D_1) + K) \to \frac{A_K(D_2) + K}{A_K(D_1) + K}$, and the map is onto.

   
   
   
   And we have
   
   $\dim_F \frac{A_K(D_2) + K}{A_K(D_1) + K} = \deg(D_2) - \deg(D_1) - \dim_F \frac{A_K(D_1) + L(D_2)}{A_K(D_1)}$
   
   since
   
   $\frac{A_K(D_2)}{A_K(D_1) + L(D_2)} = \frac{A_K(D_2)/A_K(D_1)}{(A_K(D_1) + L(D_2))/A_K(D_1)}$.

   Since $K \cap A_K(D_1) = L(D_1)$ and $L(D_2) \subset K$, thus $A_K(D_1) \cap L(D_2) \subset L(D_1)$. And $L(D_1) \subset L(D_2)$ since $D_2 \geq D_1$ thus we have $A_K(D_1) \cap L(D_2) = L(D_1)$.

   Thus
   
   $\frac{A_K(D_1) + L(D_2)}{A_K(D_1)} = \frac{L(D_2)}{L(D_1)}$.

   And the claim follows from the lemma such that
   
   $\dim_F \frac{L(D_2)}{L(D_1)} = l(D_2) - l(D_1)$.

2. The second statement is a consequence of the properties of divisors,

   $\deg(\text{div}(f) + D_1) = \deg(D_1)$ and $l(\text{div}(f) + D_1) = l(D_1)$.

   $\square$

4.4.6 **Theorem:**

For any function field $K/F$, $r(D)$ has an upper bound for any divisor $D$. 
Proof.

Take an arbitrary \( x \in K - F \). By Corollary 4.1.6, \( \deg(\text{div}_\infty(x)) = [K : F(x)] \), which we denote by \( n \).

We have that \( y \) is integral over \( O_P \). Since if we use \( R_x \) denote the integral closure of \( F[x] \) in \( K \), consider any \( y \in R_x \), if \( \text{ord}_P(x) \geq 0 \) then \( x \in O_P \), so \( F[x] \subset O_P \).

Since \( O_P \) is integrally closed in \( K \), \( \text{ord}_P(y) \geq 0 \).

Thus if \( \text{ord}_P(y) < 0 \) then \( \text{ord}_P(y) < 0 \), i.e. any pole of \( y \) will be a pole of \( x \).

Because the divisor of poles is effective for any \( f \in K^\times \), there is some \( k \in \mathbb{Z}^+ \) so that \( \text{div}_\infty(y) \leq k\text{div}_\infty(x) \) and \( k\text{div}_\infty(x) + \text{div}(y) \geq \text{div}_0(y) \geq 0 \).

For any element \( y \) of \( R_x \), \( y \in L(k\text{div}_\infty(x)) \) for some \( k > 0 \) depending on \( y \). We can find a basis \( \{y_1, \ldots, y_n\} \) since \( [K : F(x)] = n \), where each \( y_i \in R \). Thus \( y_i \in L(k_i\text{div}_\infty(x)) \) for some \( k_i \in \mathbb{Z}^+ \).

Take \( k = \max \{k_1, \ldots, k_n\} > 0 \), so each \( y_i \) will be inside \( L(k\text{div}_\infty(x)) \).

Since \( x \) is transcendental over \( F \), then for any \( m \geq k \), the elements \( \{x^iy^j : 1 \leq j \leq n, 0 \leq i \leq m - k\} \) are linear independent over \( F \) and are all in \( L(m\text{div}_\infty(x)) \). Thus \( L(m\text{div}_\infty(x)) \geq n(m - k + 1) \).

Recalling the notation \( r(D) = \deg(D) - l(D) \) and note that by Lemma 4.4.5, \( r(D_2) \geq r(D_1) \) when \( D_2 \geq D_1 \), we find that

\[
\begin{align*}
r(m\text{div}_\infty(x)) &= \deg(m\text{div}_\infty(x)) - l(m\text{div}_\infty(x)) \\
&\leq (mn) - (n(m - k + 1)) \quad (4.5) \\
&= nk - n.
\end{align*}
\]

By the claim in Lemma 4.4.5, we know that \( \{r(m\text{div}_\infty(x))\}_{m \in \mathbb{Z}} \) is an increasing sequence of integers, but by the above proof it is bounded and thus eventually constant. Let the constant to be \( g - 1 \) to ensure \( g \) is non negative. If \( m = 0 \) then \( m\text{div}_\infty(x) = 0 \) and \( r(0) = -1 \).

We want to prove that \( r(D) \leq g - 1 \) for all divisors \( D \). For a divisor \( D \), we want to break up the support of \( D \) into some parts where \( x \) has no poles, and where \( x \) has poles. We do this as follows:

\[
-D = D_1 + D_2
\quad \text{supp}(D_1) \cap \text{supp}(\text{div}_\infty(x)) = \emptyset \\
\text{supp}(D_2) \subset \text{supp}(\text{div}_\infty(x)).
\quad (4.6)
\]

Consider any place \( P \) where \( D_1 \) is not effective, since \( x \) doesn’t have a pole at \( P \), \( F[x] \subset O_P \). And \( F[x] \cap \mathfrak{m}_P \neq \{0\} \), thus \( F[x] \cap \mathfrak{m}_P \) is a prime ideal of \( F[x] \). Choose \( \pi_P(x) \) to be a nonzero irreducible element generating \( F[x] \cap \mathfrak{m}_P \), thus there is some in-
4.5. GENUS AND THE RIEemann’s theorem

For any function field $K/F$, the genus of $K$ is defined by
$$g := 1 + \max_D r(D),$$
i.e. $g$ is the least integer for which $\deg(D) - l(D) \leq g - 1$ holds.

Now we are able to prove an important result called Riemann’s Theorem, also called Riemann’s inequality. For any fixed compact connected Riemann surface $X$ of genus $g$. Riemann’s inequality gives a sufficient condition to construct meromorphic functions with prescribed singularities.
4.5.2 Theorem: Riemann’s Theorem

For any divisor $D$ of a function field $K/F$,

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

, where $g$ is the genus of $K$, and the equality holds for all divisors of sufficiently large degree.

Proof.

Since $r(D) := \deg(D) - l(D)$, and $r(D) \leq g - 1$ by the above theorem,

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

\[\square\]

Indeed, the Riemann’s theorem gives a sharp lower bound on $l(D)$.

4.5.3 Corollary:

There is some constant $c$ such that, if $D$ is a divisor, and $\deg(D) \geq c$, then

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

Proof.

Again, let $x \in K - F$, and $m$ is large enough so that

$$r(m \div^\infty(x)) = g - 1.$$ 

Then define $d := m[K : F(x)] + g$, if a divisor $D$ is such that $\deg(D) \geq c$ then

$$\deg(D - m \div^\infty(x)) = \deg(D) - \deg(m \div^\infty(x))$$

$$\geq (m[K : F(x)] + g) - m[K : F(x)] = g.$$ 

(4.7)

Thus by Theorem 4.5.2,

$$l(D - m \div^\infty) \geq \deg(D - m \div^\infty) - g + 1$$

$$\geq g - g + 1$$

(4.8)

$$= 1.$$ 

So $L(D - m \div^\infty(x)) \neq \{0\}$, pick any nonzero $y \in L(D - m \div^\infty(x))$, by definition, $\div(y) + D - m \div^\infty \geq 0$, i.e. $\div(y) + D \geq m \div^\infty(x)$. 

By Lemma 4.4.5,

$$r(D) = r(\div(y) + D) \geq r(m \div^\infty(x)) = g - 1.$$ 

But we already $l(D) \leq g - 1$, we must then have $r(D) = \deg(D) - l(D) = g - 1$. And thus the corollary follows. 

\[\square\]
If we combine the results of Theorem 4.3.3 and Theorem 4.4.6 we find that for a function field $K$ of genus $g$, and for any divisor $D$,
\[ \deg(D) + 1 - g \leq l(D) \leq \deg(D) + 1. \]

4.5.4 Corollary:

For any divisor $D$ such that $\deg(D) \geq c$, where $c$ is the constant from Corollary 4.5.3, we have
\[ A_K(D) + K = \mathbb{A}_K. \]

Proof.

By the claim in Lemma 4.4.5,
\[ \dim_F A_K(D_2) + K = r(D_2) - r(D_1) \]
for any divisors $D_2 \geq D_1$. By Corollary 4.5.3, $\deg(D) \geq c$ implies $r(D) = g - 1$. Thus if $\deg(D_2), \deg(D_1) \geq c$, then
\[ A_K(D_2) + K = A_K(D_1) + K. \]

For any divisor $D = \sum P n_P P$ with $\deg(D) \geq c$ and for any adele $(\phi_P)$, define
\[ E = \max(D, -\text{div}((\phi_P))). \]
Therefore $E \geq D$, $\deg(E) \geq \deg(D) \geq c$ thus $A_K(E) + K = A_K(D) + K$, we have that
\[ (\phi_P) \in A_K(\text{div}((\phi_P))) \subset A_K(E) \subset A_K(E) + K = A_K(D) + K. \]
If $\deg(D)$ is large enough, then any adele is in $A_K(D) + K$, $\mathbb{A}_K \subset A_K(D) + K$. And we have that $\mathbb{A}_K \supset A_K(D) + K$ since $A_K(D)$ and $K$ are both subsets of the adeles under the diagonal embedding. Thus $A_K(D) + K = \mathbb{A}_K$.

4.6 Weil Differentials

So far, we have a precise bound for $l(D)$ based on $\deg(D)$, then to calculate $l(D)$ precisely, we need to introduce another object called the Weil differentials.

4.6.1 Motivation:

Before we define a Weil differential, here is some motivation following [5][Chapter 6].
Recall that a Riemann surface $X$ is a connected complex manifold of complex dimension one. And in complex analysis, a meromorphic function on an open subset $U$ is a function that is holomorphic everywhere on $U$ except for a set of isolated points, which are so called poles of the function.

Let $X$ be a compact Riemann surface of genus $g$, and $M$ is the field of meromorphic functions on $X$ and $\Omega$ is the space of meromorphic differential forms on $X$.

Fix some $\omega \in \Omega$, a point $P \in X$, pick $t$ such that $t$ vanishes to order one at the point $P$. If we pick some derivation $d$ on $X$, there is $\omega = \sum_{k \in \mathbb{Z}} a_k t^k dt$.

Since $\omega$ is meromorphic, there is some least integer $N$ such that $a_k$ is nonzero at $P$. Let $N$ be the order of $\omega$ at $P$, $\text{ord}_P(\omega) = 0$ for all but finitely many $P$, thus we could define $\text{div}(\omega) = \sum_P \text{ord}_P(\omega) P$ as a divisor of the points of $X$. For a function $f \in M$, we could write $f = \sum_{j=-1}^{\infty} b_j t^j$ when look at $\phi$ locally. By integrating over a small simple closed path around the point $P$, the residue of $f \omega$ at $P$ is $\text{Res}_P (f \omega) = c_{-1} = \sum_{i,j=1} a_i b_j$.

Then we can define a map $\omega_P : M \rightarrow \mathbb{C}$ by defining $f \mapsto \text{Res}_P (f \omega)$.

Then by the Residue theorem [6][Section 8.1], we have $\sum_{P \in X} \text{Res}_P (\omega) = 0$ on $X$.

Then for all $f \in M$ we have $\sum_{P \in X} \omega_P (f) = 0$.

Let $H_P$ be the set of functions in $M$ which are holomorphic at $P$, let $A_X$ be the vector space over $\mathbb{C}$ inside $\Pi P M$ which satisfies $\phi = (\phi_P) \in A_X \implies \phi_P \in H_P$ for all but finitely many $P$.

For any divisor $D = \sum_P n_P P$, let $A_X(D)$ be defined by $A_X(D) = \{\phi \in A_X : \text{ord}_P(\phi_P) + n_P \geq 0 \text{ or } \phi_P = 0 \text{ for all } P\}$.

Then define a function $\hat{\omega} : A_X \rightarrow \mathbb{C}$ by $\hat{\omega}(\phi_P) := \sum_P \omega_P (\phi_P) = \sum_P \text{Res}_P (\phi_P \omega)$.

If $\phi_P \in H_P$, $\text{ord}_P(\omega) \geq 0$, then $\text{Res}_P (\phi_P \omega) = 0$, thus $\hat{\omega}(\phi_P)$ is defined by a finite sum, therefore the function $\hat{\omega}(\phi_P)$ is well-defined.

The function $\hat{\omega}(\phi_P)$ is also $\mathbb{C}$-linear since $\text{Res}$ is $\mathbb{C}$-linear.
4.6.2 Definition: Weil Differential

A Weil differential $\omega$ on a function field $K$ over an algebraically closed field $F$, is an $F$-linear map from $A_K$ to $F$ such that there is some divisor $D$ of $K$ where $\omega$ vanishes both on $K$ and on $A_K(D)$.

We denote the space of differentials on $K$ by $\Omega_K$ and the space of differential vanishes on $A_K(D)$ for some divisor $D$ denote by $\Omega_K(D)$.

4.6.3 Theorem:

For any divisor $D$, $\Omega_K(D)$ is finite dimensional over $F$,

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

**Proof.**

For all $a \in F$, $\omega \in \Omega_K$, $a\omega$ is also an $F$-linear map from $A_K$ to $F$, thus $\Omega_K$ and $\Omega_K(D)$ can be both viewed as $F$-vector spaces.

And since $\omega \in \Omega_K(D)$ if and only if when $\omega$ is from an $F$-linear map from $A_K/(A_K(D) + K)$ to $F$.

$$\Omega_K(D) = \text{Hom}_F(A_K/(A_K(D) + K) \to F).$$

(Recall the definition of dual vector space in Definition 1.6.1.)

Next, by Corollary 4.5.4 We have

$$\Omega_K(D) = (A_K/(A_K(D) + K))^*,$$

for any divisor $D$ for any divisor $E \geq D$ with large enough degree.

Then by the claim from Lemma 4.4.5, for any divisor $D' \geq D$,

$$\dim_F(A_K(D') + K/A_K(D) + K) = r(D') - r(D)$$

which is of finite dimension. Thus $\Omega_K(D)$ is finite-dimensional, and by duality

$$\dim_F(\Omega_K(D)) = \dim_F(A_K/(A_K(D) + K)).$$

Next, since $r(D') = g - 1$ and $A_K(D') + K = A_K$ for any divisor $D'$ with large enough degree,

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

Thus the results hold. \qed

4.6.4 Corollary:

The genus

$$g = \dim_F \Omega_K(D).$$
Proof.

By Theorem 4.6.2 above,

\[ l(0) = \deg(0) - g + 1 + \dim_F \Omega_K(D) \]

\[ 1 = 0 - g + 1 + \dim_F \Omega_K(D), \]

thus \( \dim_F \Omega_K(D) = g. \)

\[ \square \]

4.6.5 **Theorem:**

Let \( \omega \) be any nonzero differential, there exists a greatest divisor \( D \) such that, for any other divisor \( D' \), \( D' \leq D \) if and only if \( \omega \) vanishes on \( A_K(D') \).

**Proof.**

Let \( S_\omega \) be the set of divisors such that \( \omega \) vanishes on \( A_K(E) \). By Corollary 4.5.4,

\[ \deg(D') \geq c \Rightarrow A_K(D') + K = \mathbb{A}_K. \]

Or, equivalently,

\[ \mathbb{A}_K \neq A_K(E) + K \Rightarrow \deg(D') < c. \]

Next, there is some adele \( \phi \) on which \( \omega \) does not vanish since \( \omega \) is nonzero. Thus \( A_K(D') + K \) is not all of the adeles, so we have a bound on the degree of divisors in the set \( S_\omega \).

Now, let’s fix some divisor \( D \) of maximal degree in \( S_\omega \). To show that this divisor of maximal degree is unique, if we pick any other divisor, say \( E \) in \( S_\omega \), \( \omega \) vanishes on both \( A_K(E) \) and \( A_K(D) \) thus \( \omega \) will also vanishes on the union

\[ A_K(E) + A_K(D) = A_K(max(D, E)). \]

Thus \( max(D, E) \in S_\omega \). By the definition of \( max(D, E) \), \( \deg(max(D, E)) \geq \deg(D) \). Since \( D \) is of maximal degree in \( S_\omega \), we have that \( D = max(D, E) \), \( D \geq E \), thus the divisor in \( S_\omega \) which has maximal degree is indeed unique. And the statement of the theorem follows.

\[ \square \]

4.6.6 **Definition: div(\( \omega \)**

\( \text{div}(\omega) \) is defined as the divisor \( D \) of greatest degree such that \( \omega \) vanishes on \( A_K(D) \).
4.6.7 Remark:

By Theorem 4.6.5 above, for all $\phi \in A_K(\text{div} \omega)$, $\omega(\phi) = 0$, and if for all $\phi \in A_K(D')$ we have $\omega(\phi) = 0$, then

$$D' \leq \text{div}(\omega).$$

4.6.8 Lemma:

For any $\omega \in \Omega_K$, $\alpha \in K^\times$, we have

$$\text{div}(\alpha \omega) = \text{div}(\alpha) + \text{div}(\omega).$$

Proof.

Let $\phi \in L_K$, $D = \Sigma_P n_P P$, $\alpha \in K^\times$.

$$\alpha \phi \in A_K(D) \iff \text{ord}_P(\alpha \phi P) + n_P \geq 0 \text{ or } \phi P = 0 \text{ for all } P$$

$$\iff \text{ord}_P(\phi) + (\text{ord}_P(\alpha) + n_P) \geq 0 \text{ or } \phi P = 0 \text{ for all } P$$

$$\iff \phi \in A_K(\text{div}(\alpha) + D)$$

(4.10)

Thus if $\omega$ vanishes on $A_K(D)$, then $\alpha \omega$ vanishes on $A_K(\text{div}(\alpha) + D)$, and the reverse is also true, thus we have

$$\omega \in \Omega_K(D) \iff \alpha \omega \in \Omega_K(\text{div}(\alpha) + D).$$

Now, obviously

$$\omega \in \Omega_K(\text{div}(\omega)),$$

let $S_{\alpha \omega}$ be defined as in Theorem 4.6.4, thus

$$\text{div}(\alpha) + \text{div}(\omega) \in S_{\alpha \omega}.$$

Thus

$$\text{div}(\alpha \omega) \geq \text{div}(\alpha) + \text{div}(\omega).$$

By the relation

$$\omega \in \Omega_K(D) \iff \alpha \omega \in \Omega_K(\text{div}(\alpha) + \alpha \omega),$$

we know that $\alpha \omega \in \Omega_K(\text{div}(\alpha) + (\text{div}(\alpha \omega) - \text{div}(\alpha)))$ implies

$$\omega \in \Omega_K(\text{div}(\alpha \omega) - \text{div}(\alpha)).$$

Then by Definition,

$$\text{div}(\alpha \omega) \leq \text{div}(\alpha) + \text{div}(\omega).$$

since $\text{div}(\omega) \geq \text{div}(\alpha \omega) - \text{div}(\alpha)$, Combining with the previous result $\text{div}(\alpha \omega) \geq \text{div}(\alpha) + \text{div}(\omega)$, the statements hold.
4.6.9 Lemma:

Let $\omega \in \Omega_K$ be any nonzero differential, $D$ be any divisor, then

$$L(\text{div}(\omega) - D)\omega \subset \Omega_K(D).$$

Proof.

For any $\alpha \in K^{\times}$, we have

$$\alpha \in L(\text{div}(\omega) - D) \text{ if and only if } \text{div}(\alpha) + \text{div}(\omega) = \text{div}(\alpha \omega) \geq D.$$  

Therefore

$$A_K(\text{div}(\alpha \omega)) \supset A_K(D).$$

And $\alpha \omega$ vanishes on $\Omega_K(D)$ since it vanishes on $\Omega_K(\alpha \omega)$.

4.7 The space of Weil differentials

4.7.1 Theorem:

The space of Weil differentials is a one dimensional $K$-vector space.

Proof.

By Lemma 4.6.8, we have that if for two different differentials $\omega_1$, $\omega_2$ and any divisor $D$:

$$L(\text{div}(\omega_1) - D)\omega_1 \subset \Omega_K(D), L(\text{div}(\omega_2) - D)\omega_2 \subset \Omega_K(D).$$

And $\omega_1$, $\omega_2$ are linearly dependent over $K$ since if we have some nonzero element $x$ in the intersection and $x = \alpha \omega_1 = \beta \omega_2$ for some nonzero $\alpha$ and $\beta$ in $K$. We also have

$$L(\text{div}(\omega_1) - D)\omega_1 \subset \Omega_K(D), \text{ and } L(\text{div}(\omega_2) - D)\omega_2 \subset \Omega_K(D).$$

as $F$-subspaces.

Let’s suppose that

$$L(\text{div}(\omega_1) - D)\omega_1 \cap L(\text{div}(\omega_2) - D)\omega_2 = \{0\}.$$  

Then we have

$$\Omega_K(D) \supset L(\text{div}(\omega_1) - D)\omega_1 \bigoplus L(\text{div}(\omega_2) - D)\omega_2 = \{0\}.$$  

Then

$$\dim_F(\Omega_K(D)) \geq l(\text{div}(\omega_1) - D) + l(\text{div}(\omega_2) - D)$$

Choose some integer $n \geq 1$ and a place $P$, if we let $D = -np$.

By Theorem 4.6.2,

$$\dim_F(\Omega_K(D)) = \dim_F(\Omega_K(-np)) = l(-np) - \deg(-np) + g - 1.$$
4.7. THE SPACE OF WEIL DIFFERENTIALS

\( l(-np) = 0 \) since there are no nonzero functions which has a zero but has no poles. Thus by Theorem 4.4.6 we have that

\[ \dim_F(\Omega_{K}(-np)) = n + g - 1. \]

We have

\[ l(\text{div}(\omega_1) + np) \geq \deg(\text{div}(\omega_1)) + np - g + 1 = \deg(\text{div}(\omega_1))n - g + 1. \]

and

\[ l(\text{div}(\omega_2) + np) \geq \deg(\text{div}(\omega_2)) + np - g + 1 = \deg(\text{div}(\omega_2))n - g + 1. \]

Thus, if

\[ L(\text{div}(\omega_1) - D)\omega_1 \cap L(\text{div}(\omega_2) - D)\omega_2 = \{0\}. \]

And

\[ n + g - 1 \geq 2n - 2g + 2 + \deg(\text{div}(\omega_1)) + \deg(\text{div}(\omega_2)) \]

which implies that

\[ n \leq 3g - 3 - \deg(\text{div}(\omega_1)) - \deg(\text{div}(\omega_2)). \]

Clearly, this inequality will be false if we take \( n \) to be large enough.

Thus we have that if \( D = -np \),

\[ L(\text{div}(\omega_1) - D)\omega_1 \cap L(\text{div}(\omega_2) - D)\omega_2 \neq \{0\}. \]

Thus we have the result. Any two different differentials are linearly independent over \( K \). Therefore, the space of Weil differentials is a one dimensional \( K \) vector space.

\[ \square \]

4.7.2 Corollary:

For any differential \( \omega \in \Omega_{K}(D), \omega \neq 0, \)

\[ L(\text{div}(\omega) - D) \simeq \Omega_{K}(D) \]

as \( F \)-vector spaces.

Proof.

By Lemma 4.6.8, there is an injective map from \( L(\text{div}(\omega) - D) \) into \( \Omega_{K}(D) \) by mapping

\[ \alpha \mapsto \alpha \omega \]

(Since any ring homomorphism from a field (\( K \), in this case) is injective).

And since the space of Weil differentials is a one dimensional \( K \)-vector space as we just proved, any nonzero differential \( \omega' \) can be written as

\[ \omega = a \omega \]

for some \( a \in K^\times \).
We then want to prove that
\[ \text{div}(a) + \text{div}(\omega) = \text{div}(a\omega) \geq D \]
i.e. we would only need to show that \( a \in L(\text{div}(\omega) - D) \). Suppose on the contrary, \( a \notin L(\text{div}(\omega) - D) \), then
\[ \text{div}(a\omega) < D, \]
moreover,
\[ \deg(\text{div}(a\omega)) = \deg(\text{div}(a)) + \deg(\text{div}(\omega)) = \deg(\text{div}(\omega)) < \deg(D). \]
By Theorem 4.6.4, \( \text{div}(\omega) \geq D \) since \( \omega \in \Omega_K(D) \), thus \( \deg(\text{div}(\omega)) \geq \deg(D) \).
Therefore we have proved the claim, and the map \( \alpha \mapsto \alpha \omega \) is an isomorphism from \( L(\text{div}(\omega - D)) \) to \( \Omega_K(D) \).

\[ \square \]

## 4.8 Riemann-Roch Theorem

Finally we are able to prove the Riemann-Roch Theorem,

### 4.8.1 Theorem: The Riemann-Roch Theorem

For any divisor \( D \) and nonzero differential \( \omega \),
\[ l(D) = \deg(D) - g + 1 + l(\text{div}(\omega) - D) \]

**Proof.**

By Corollary 4.7.2, for any divisor \( D \) and nonzero differential \( \omega \), we have
\[ \dim_F \Omega_K(D) = l(\text{div}(\omega) - D). \]
Then by Theorem 4.6.2 we have
\[ l(D) = \deg(D) - g + 1 + \dim_F \Omega_K(D). \]
Thus
\[ l(D) = \deg(D) - g + 1 + l(\text{div}(\omega) - D) \]
as desired.

\[ \square \]

## 4.9 Applications of Riemann-Roch theorem

Recall that the Riemann-Roch theorem states that
\[ l(D) = \deg(D) - g + 1 + l(C - D) \]
where \( C \) is the divisor of any nonzero differential.
4.9. APPLICATIONS OF RIEMANN-ROCH THEOREM

4.9.1 Corollary:

For any divisors with \( \deg(D) \geq 2g - 1 \),
\[
  l(D) = \deg(D) - g + 1.
\]

**Proof.**

If \( \deg(D) \geq 2g - 1 \) then
\[
  \deg(\text{div}(\omega) - D) = 2g - 2 - \deg(D) < 0.
\]
But from Theorem 4.4.6 we know that
\[
  \deg(E) < 0
\]
implies that \( l(E) = 0 \) for any divisor \( E \).
Then since \( \deg(C) = 2g - 2 \) but \( l(C) = g \) and
\[
  g \neq 2g - 2 - g + 1 = g - 1
\]
we know that this inequality is sharp.

With this in mind, let’s look at the case when the genus zero:

4.9.2 Proposition:

If \( K \) has genus zero, then every divisor of degree zero is equal to the divisor of some \( x \in K^\times \).

**Proof.**

Let \( D = \Sigma P n_P P \) be a divisor of degree zero, then we can find \( x \in K^\times \) such that \( x \in L(D) \) since by Corollary 4.9.1, \( l(D) = 1 \).
To show that this \( x \) satisfies our condition, since
\[
  \deg(D) = \deg(\text{div}(x)) = 0
\]
and
\[
  0 = \Sigma P \ord_P(x) \geq \Sigma P - n_P = 0
\]
we have
\[
  \ord_P(x) = -n_P \text{ for all } P.
\]
Thus \( D = \text{div}(x^{-1}) \).

Then let’s look at the genus one case:

4.9.3 Theorem:

If a function field \( K/F \) has genus one, then \( K = F(x, y) \) with
\[
  y^2 + b_1 xy + b_2 y = x^3 + a_1 x^2 + a_2 x + a_3
\]
where $b_i, a_i \in F$, and not all of them are zero.

Proof:

Claim: $\{1, x, y, x^2, xy, y^2, x^3\}$ all lie in $L(6P)$.

To prove the claim, first note that by Corollary 4.9.1, if $K$ has genus one and $n > 0$, then for any place $P$, 

$$\ell(nP) = n - 1 + 1 = n.$$ 

Thus the space $L(P)$ only contains constants. Let’s look at the space $L(2P)$, it only consists of linear combinations of constants (since it is a one-dimensional vector space) and some $x \in K - F$ which has a pole only at $P$. Let $y$ be an element of $L(3P)$ which is linearly independent of $\{1, x\}$ over $F$, since $\ell(6P) = 6$ and there is some linear relation 

$$b_0y^2 + b_1xy + b_2y = a_0x^3 + a_1x^2 + a_2x + a_3,$$

where not all the $a_i, b_i$ are zero, then $\{1, x, y, x^2, xy, y^2, x^3\}$ all lie in $L(6P)$.

In fact, we have that the $a_i'$s are not all zero, and the $b_i'$s are not all zero. To show this, suppose that all the $a_i'$s are zero, then by the equation above we have that 

$$b_0y^2 + b_1xy + b_2y = 0.$$ 

By canceling $y$ on both sides we have 

$$b_0y + b_1x + b_2 = 0.$$ 

which is contradict with that $1, x$ and $y$ are linear independent. Using similar arguments we could show that not all the $b_i'$s are zero.

We could also show that $b_0, a_0 \neq 0$. Recall $\text{ord}_P(x) = -2$, $\text{ord}_P(y) = -3$, since we have just shown that not all of the $a_i'$s are zero, 

$$\text{ord}_P(a_0x^3 + a_1x^2 + a_2x + a_3) \in 2\mathbb{Z}.$$ 

Thus we also have 

$$\text{ord}_P(b_0y^2 + b_1xy + b_2y) \in 2\mathbb{Z}.$$ 

To show that $a_0 \neq 0$, we use proof by contradiction. Suppose $a_0 = 0$, then $\text{ord}_P(a_1x^2 + a_2x + a_3) \geq -4$, and $\text{ord}_P(b_0y^2 + b_1xy + b_2y) = \text{ord}_P(b_0y^2) = -6$, thus we have a contradiction here. And using similar arguments we could show that $b_0 \neq 0$.

Next we have 

$$\frac{b_0^3}{a_0^2}y^2 + \frac{b_1b_0^2}{a_0^2}xy + \frac{b_2b_0}{a_0}y = \frac{b_0^3}{a_0^2}x^3 + \frac{a_1b_0^2}{a_0^2}x^2 + \frac{a_1b_0}{a_0}x + a_3$$

by replace $x$ by $\frac{b_0x}{a_0}$, and also replace $y$ by $\frac{b_0y}{a_0}$. Then multiply
\[
\frac{a_0^2}{b_0^2} \quad \text{on both sides, we have}
\]
\[
y^2 + \frac{b_1}{b_0} xy + \frac{b_2 a_0}{b_0^2} y = x^3 + \frac{a_1}{b_0} x^2 + \frac{a_1 b_0}{b_0^2} x + \frac{a_3 a_0^2}{b_0^3},
\]
by renaming the constants in the above equation, we get
\[
y^2 + b_1 xy + b_2 y = x^3 + a_1 x^2 + a_2 x + a_3
\]
where \( b_i, a_i \in F \), and not all of them are zero.

It suffices to show that \( K = F(x, y) \), the inclusion \( K \supset F(x, y) \) is easy to follow. Since \( F(x, y) \neq F(x) \), we have \( [F(x, y) : F(x)] \geq 2 \), and
\[
\deg(\text{div}_{\infty}(x)) = [K : F(x)] = 2
\]
since \( x \in L(2P) - L(P) \). Thus \( [K : F(x, y)] = 1 \), our whole statement is shown.

\hfill \Box

4.9.4 Remark: Other approaches towards the proof

Here we learned function fields and Weil differentials to prove the Riemann-Roch theorem for algebraic curves over an algebraically closed field, this approach can also be generalized to all the perfect field. (Recall that a field \( k \) is perfect if every irreducible polynomial over \( k \) has distinct roots.)

There are some other ways to prove the Riemann-Roch theorem, one of them uses the Serre Duality, see [8][Page. 316].

4.9.5 Remark: Generalization of the theorem

The Riemann-Roch theorem can be generalized not only, to surfaces.

Even in higher dimensions, there is the so called the HirzebruchRiemannRoch theorem, named after Friedrich Hirzebruch, Bernhard Riemann, and Gustav Roch. The HirzebruchRiemannRoch theorem is the first generalization of the classical RiemannRoch theorem to all higher dimensions.

Later in the history of algebraic geometry, the GrothendieckRiemannRoch theorem is a generalisation of the HirzebruchRiemannRoch theorem.
Bibliography
Bibliography


