Master's Thesis

Algebraic Curves over Finite Fields

Carmen Rovi

LiTH - MAT - INT - A - - 2010 / 02 - - SE

Algebraic Curves over Finite Fields

MAI Mathematics, Linköping Universitet

Universidad Nacional de Educación a Distancia. Spain

Carmen Rovi

LiTH - MAT - INT - A - - 2010 / 02 - - SE

Master's Thesis: **30 ECTS**

Supervisor: **Milagros Izquierdo**,
MAI Mathematics, Linköping Universitet

Examiner: **Milagros Izquierdo**,
MAI Mathematics, Linköping Universitet

Linköping: **June 2010**

LINKÖPINGS UNIVERSITET

Avdelning, Institution
Division, Department

Matematiska Institutionen
581 83 LINKÖPING
SWEDEN

Datum
Date

June 2010

Language

☐ Svenska/Swedish
☒ Engelska/English
☐ _____

Rapporttyp
Report category

☐ Licentiatavhandling
☒ Examensarbete
☐ C-uppsats
☐ D-uppsats
☐ Övrig rapport
☐ _____

ISBN

ISRN
LiTH - MAT - INT - A - - 2010 / 02 - - SE

Serietitel och serienummer **ISSN**
Title of series, numbering 0348-2960

URL för elektronisk version

http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-56761

Titel
Title

Algebraic Curves over Finite Fields

Författare
Author

Carmen Rovi

Sammanfattning
Abstract

This thesis surveys the issue of finding rational points on algebraic curves over finite fields. Since Goppa's construction of algebraic geometric codes, there has been great interest in finding curves with many rational points. Here we explain the main tools for finding rational points on a curve over a finite field and provide the necessary background on ring and field theory. Four different articles are analyzed, the first of these articles gives a complete set of table showing the numbers of rational points for curves with genus up to 50. The other articles provide interesting constructions of covering curves: covers by the Hemitian curve, Kummer extensions and Artin-Schreier extensions. With these articles the great difficulty of finding explicit equations for curves with many rational points is overcome. With the method given by Arnaldo García in [6] we have been able to find examples that can be used to define the lower bounds for the corresponding entries in the tables given in http: //wins.uva.nl/˜geer, which to the time of writing this Thesis appear as "no information available". In fact, as the curves found are maximal, these entries no longer need a bound, they can be given by a unique entry, since the exact value of $N_q(g)$ is now known.
At the end of the thesis an outline of the construction of Goppa codes is given and the NXL and XNL codes are presented.

Nyckelord
Keyword

Nullstellensatz, variety, rational function, Function field, Weierstrass gap Theorem, Ramification, Hurwitz genus formula, Kummer and Artin-Schreier extensions, Hasse-Weil bound, Goppa codes.

Abstract

This thesis surveys the issue of finding rational points on algebraic curves over finite fields. Since Goppa's construction of algebraic geometric codes, there has been great interest in finding curves with many rational points. Here we explain the main tools for finding rational points on a curve over a finite field and provide the necessary background on ring and field theory. Four different articles are analyzed, the first of these articles gives a complete set of table showing the numbers of rational points for curves with genus up to 50. The other articles provide interesting constructions of covering curves: covers by the Hemitian curve, Kummer extensions and Artin-Schreier extensions. With these articles the great difficulty of finding explicit equations for curves with many rational points is overcome. With the method given by Arnaldo García in [6] we have been able to find examples that can be used to define the lower bounds for the corresponding entries in the tables given in http: //wins.uva.nl/˜geer, which to the time of writing this Thesis appear as "no information available". In fact, as the curves found are maximal, these entries no longer need a bound, they can be given by a unique entry, since the exact value of $N_q(g)$ is now known.

At the end of the thesis an outline of the construction of Goppa codes is given and the NXL and XNL codes are presented.

Keywords: Nullstellensatz, variety, rational function, Function field, Weierstrass gap Theorem, Ramification, Hurwitz genus formula, Kummer and Artin-Schreier extensions, Hasse-Weil bound, Goppa codes.

Acknowledgments

I would like to thank my supervisor Milagros Izquierdo for having introduced me to this fascinating and beautiful subject. Her enthusiasm, her wonderful explanations and guidance have given me a new view on what mathematics means. My deepest thanks to her.

I would also like to thank Jonas Karlsson for his interesting questions and for his very useful comments on my drafts of this thesis. Finally I would like to say that say that this work would not have been possible without the constant support of my sister and my parents.

Nomenclature

Symbols

$K[x, y]$	ring of polynomials in x and y.
$K(x)$	field of rational functions.
$\bar{K}$	algebraic closure of the field K.
F/K	field extension F of K.
$[F : K]$	degree of the field extension
$\mathbb{F}_q$	finite field of order q
$\mathbb{H}_p$	Hessian of the polynomial P.
$I_p(C, D)$	intersection number of curves C and D at the point p.
$R_{P,Q}(x, y)$	resultant with respect to z.
$\mathbb{P}^1$	projective line
$\mathbb{P}^2$	projective plane
$[x, y.z]$	homogeneous coordinates of a projective point.
F	function field
K	full constant field of F
F'	extension field of F
K'	full constant field of F'
K_P	residue class field of F at a place P
$K'_{P'}$	residue class field of F' at an extension place P'
$\mathcal{O}_P$	valuation ring
$P_{p(x)}$	place
$v_P(z)$	valuation of z at the place P.
$\mathbb{P}_F$	set of places of the function field F
D	divisor
$\mathcal{L}(D)$	Riemann-Roch space
$l(D)$	dimension of the Riemann-Roch space
κ	canonical divisor
$P'\|P$	P' is a place lying over P
$e(P'\|P)$	ramification index of F'/F at the place $P' \in F'$
$f(P'\|P)$	relative degree of P' over P
t_P	local parameter at a place P
$\mathcal{S}$	subset of places in $\mathbb{P}_F$
$\mathcal{T}$	over-set of $\mathcal{S}$
$\mathcal{O}_\mathcal{T}$	integral closure of $\mathcal{O}_\mathcal{S}$ in F'
$\mathcal{C}_\mathcal{T}$	complementary set of $\mathcal{O}_\mathcal{T}$
$d(P'\|P)$	different exponent of P' over P
Diff (F'/F)	global different divisor of F'/F

$\mathrm{Gal}(F'/F)$	Galois automorphism group
$c_P(F'/F)$	conductor exponent
$\mathrm{cond}(F'/F)$	conductor
$G_Z(F'/F)$	the decomposition group
$G_T(F'/F)$	the inertia group
$G_i(F'/F)$	the ith ramification group

List of Figures

Contents

Introduction

Historical Background

Algebraic curves have been widely studied throughout the history of mathematics. The ancient Greeks already worked with the concept of algebraic curves, although as they did not have the notation to write down equations, their approach was completely different from the modern approach to the subject.

The foundations for the modern approach to this field where laid by mathematicians like Fermat and Euler with their discoveries in classical number theory. Another crucial step was taken by Riemann in the 19th century by introducing the idea that more abstract spaces than the Euclidean space could be dealt with.

Around 1940, Hasse and Weil proved the formula for a bound of the number of rational places that may lie on a curve over a finite field $\mathbb{F}_q$. Nevertheless, the interest in finding curves with many rational points lay dormant until 1980, when Goppa found important applications of curves over finite fields to coding theory. Since then, the interest of many mathematicians has turned towards algebraic geometry over finite fields, and an intense research activity is undertaken in this subject.

Outline of the Chapters

Chapter 1: This chapter includes important concepts form ring theory and field theory that are crucial to the rest of the thesis. Important concepts such as splitting field, separable field extension and the Galois automorphisms group are explained.

Chapter 2: In this chapter we explain the concept of plane curves. We define the concepts of affine varieties, radical ideals and ideals of varieties leading to a formulation of the nullstellensatz theorem for planar curves ands to the definition of affine coordinate ring and polynomial maps. In the second part of this chapter we see how the concepts defined for affine geometry have their counterpart when explaining projective plane curves. the way two projective curves in $\mathbb{P}^2$ can intersect is also discussed and we state Bézout's theorem.

Chapter 3: Here we introduce the concept of function field of a curve and the concepts of place, valuations, valuation rings and rational points explaining the relationships between them.

Chapter 4: Building on chapter 3, this chapter introduces the concept of divisor, its dimension and the Riemann-Roch space. After explaining the genus of nonsingular curves and the genus of an algebraically closed function field,we state and proof the Riemann-Roch Theorem.

Chapter 5: Here we explain the concept of covering and explain the concept of ramification. A proof of the fundamental equality involving the relative degree and the ramification index is given. We introduce the Hurwitz genus formula which provides an important tool for finding the genus of the extensions function field F'. We also explain Kummer and Artin-Schreier extensions.

Chapter 6: This chapter surveys the importance of constructing curves with many rational points. Methods for finding explicit equations for Kummer covers and Artin-Schreier covers are given. Implementing the method given by Arnaldo García in [6] we have found new entries for the tables in http: //wins.uva.nl/~geer.

Chapter 1

Preliminaries

1.1 Rings

Let R be a set with two binary operations $+$, $\times$ then R is a ring if:

1. R is a commutative group under $+$ with identity 0.
2. R is associative under multiplication $(r \times s) \times t = r \times (s \times t)$.
3. R is distributive over addition $r \times (s+t) = r \times s + r \times t$ and $(s+t) \times r = s \times r + t \times r$.
4. There exists an element $1 \neq 0$ such that $1 \times r = r \times 1 = r$.

Example 1.1

The set of integers $\mathbb{Z}$ under addition and multiplication is a commutative ring.

□

Example 1.2

The set $\mathbb{Z}_n = \{0, \ldots, n-1\}$ under addition and multiplication modulo n is a commutative ring.

□

Ring homomorphism

Consider two rings R_1 and R_2, then a ring homomorphism is a mapping f from R_1 into R_2 such that,

1. $f(r+s) = f(r) + f(s)$
2. $f(xy) = f(x)f(y)$
3. $f(1) = 1$, that is, the identity is preserved.

Unit

A **unit** in a ring R is an element with multiplicative inverse, that is, an element r is a unit in R if there exists an element $s \in R$ such that $rs = 1$. s can also be written as r^{-1}.

Zero divisor

If r is a **zero divisor** in a ring R then there exists an $s \neq 0$ in R such that $rs = 0$.

Integral domain

A commutative ring R is an **integral domain** if for all $r, s \in R$, $rs = 0 \implies r = 0$ or $s = 0$. That is, an integral domain is a ring which does not contain any zero divisors.

Polynomial ring

For a commutative ring R, the ring of polynomials over R in the indeterminate x is the set of formal sums,

$$R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \mid a_i \in R, n \text{ is a nonnegative integer}\}$$

A polynomial ring $K[x, y]$ in two variables x and y consists of all finite sums of terms of the form $ax^i y^j$.

Example 1.3

The following are examples of polynomials in the ring $\mathbb{Z}[x, y]$.

$$P_1(x, y) = x^3 y + y^3 + x$$

$$P_2(x, y) = 2x^2 + 3y - 5xy^2$$

□

In general, a polynomial ring in n variables $x_1, \ldots, x_n$ consists of all finite sums of terms of the form $ax_1^{d_1} \times \ldots \times x_n^{d_n}$ and is denoted by $R[x_1, \ldots, x_n]$.

1.2 Ideals

Definition

An ideal of a ring is a subset $I \subset R$ satisfying:

1. $(I, +)$ is a subgroup of $(R, +)$
2. For all $x \in I, r \in R$ we have $x \times r \in I$ and $r \times x \in I$
3. $1 \in I \Leftrightarrow I = R$

Proper ideal

If $I \neq R$ then I is a proper ideal.

Prime ideal

If the product ab of two elements $a, b \in R$ is an element of the ideal I, then at least one of a and b is an element of P.

Maximal ideal

I is a proper ideal with the condition that it is not contained in larger ideal. Every maximal ideal is prime.

Example 1.4

Let $p(x) \in K[x]$ be an irreducible polynomial over K. The ideal $(p(x))$ is maximal in $K[x]$ and $K[x]/(p(x))$ is a field.

□

1.3 Noetherian Ring

R is a Noetherian ring if it satisfies these three equivalent properties

1. Every ideal of R is finitely generated.
2. Every ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ terminates, that is, there exists an integer N such that $I_N = I_{N+1}$
3. Every nonempty collection of ideals has a maximal element.

Example 1.5

The ring $K[x]$ of polynomials in X over the field K is Noetherian.

The same holds for $K[x_1, \cdots, x_n]$ for a finite number of x_n. But the polynomial ring $K[x_1, x_2, \cdots]$ in an infinite number of indeterminates x_i is not Noetherian since the sequence $(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \cdots$ is strictly increasing and does not terminate.

□

Example 1.6

The ring $\mathbb{Z}$ is Noetherian. Every ideal can be generated by one element and the chain $\cdots 8\mathbb{Z} \subseteq 4\mathbb{Z} \subseteq 2\mathbb{Z} \subseteq \mathbb{Z}$ terminates.

More generally, if $a = p_1^{r_1} \dots p_n^{r_n}$, where p_i is a prime with $i \in \{i, \dots, n\}$, the chain $a\mathbb{Z} \subseteq \dots \subseteq p_i\mathbb{Z}$ terminates.

□

1.4 Dedekind ring

A Dedekind ring is a commutative ring in which the following hold:

1. It is a Noetherian ring and an integral domain.
2. Every nonzero prime ideal is also a maximal ideal.

Example 1.7

Polynomial rings $K[x_1, \ldots, x_n]$ for a finite number of x_n, like $K[x, y]$ are Dedekind rings.

□

The **ideal class group** of a Dedeking domain D tells us how unique factorization fails. The order of the ideal class group is called the **class number**. If a ring is a unique factorization domain, then the class group is trivial.

1.5 Local ring

A commutative ring R is called a local ring if it has a unique maximal ideal.

The maximal ideal of a local ring in called a **place**.

For a point $p = (x_0, y_0)$, the local ring $\mathcal{O}_P$ at the point P is the ring of all rational functions defined at P; that is,

$$\mathcal{O}_P = \{f/g | f, g \in K[x, y], g(P) \neq 0\}$$

where f/g are rational functions defined at P.

We will show that O_p is a local ring in chapter 3.

1.6 Fields

Definition of Field

Let K have two binary operations $+$, $\times$, then K is a field if

1. K is an abelian group under $+$ with identity 0.
2. The nonzero elements of K form an abelian group under $\times$ with identity 1
3. Distributivity: $a \times (b + c) = a \times b + a \times c$

Example 1.8

The set $\mathbb{Z}_p$, where p is prime is a field.

$K(x)$ is the field of rational functions in the variable x over K. With $f(x)$ and $g(x)$ polynomials in $K[x]$, the elements of $K(x)$ are of the form $\frac{f(x)}{g(x)}$, where $g(x) \neq 0$.

□

Important Relationship between Rings, Ideals and Fields

Given any ring R and an ideal I, the quotient R/I is

1. An integral domain if and only if the ideal I is prime.
2. A field if and only if the ideal I is maximal.

Example 1.9

[The ideal (x) generated by x in $\mathbb{Z}[x]$ is prime but not maximal]

First we note that $\mathbb{Z}[x]/(x)$ is isomorphic to $\mathbb{Z}$. We know that $\mathbb{Z}$ is ring but not a field.

To show that the ideal (x) is prime we note that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ is an integral domain, since $\mathbb{Z}$ (and hence $\mathbb{Z}[x]/(x)$) has no zero divisors. Since $\mathbb{Z}[x]/(x)$ is an integral domain, we deduce that the ideal (x) is prime.

Since $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ is not a field then the ideal (x) cannot be maximal, since as we have stated above, if I is maximal that implies that the quotient R/I must be a field.

□

Characteristic of a field K

If we denote the identity of K as 1, the characteristic of K is the smallest positive integer p such that

$$p.1 = 0$$

If there exists no such p, then then characteristic is defined to be zero.

Example 1.10

1. The characteristic of $\mathbb{C}$, $\mathbb{R}$ or $\mathbb{Q}$ is 0.
2. The characteristic of $\mathbb{Z}_p$, $\mathbb{F}_p$ or $\mathbb{F}_{p^m}$ is p, where $\mathbb{F}_p$ and $\mathbb{F}_{p^m}$ are finite fields of order p and p^m.

□

Frobenius Automorphism

For a field K with characteristic p and $x, y \in K$ we have that,

$$(xy)^p = x^p y^p$$

and also

$$(x+y)^p = x^p + y^p$$

This second equation holds since

$$(x+y)^p = x^p + \begin{pmatrix} p \\ 1 \end{pmatrix} x^{p-1}y + \ldots + \begin{pmatrix} p \\ i \end{pmatrix} x^{p-i}y^i + \ldots + y^p$$

All the binomial coefficients for $i \in \{1, 2, \ldots, p-1\}$ are divisible by p, hence they can be written as 0 in a field of characteristic p, so we see that the equation

$$(x + y)^p = x^p + y^p$$

holds for fields with characteristic p.

1.6.1 Field Extensions

Let K be a subfield of the field F, then F/K is called a field extension. F can be seen as a vector space over K, so that the dimension, that is, the number of vectors in a basis of this vector space is the degree of the extension. This can be written as,

$$[F : K] = \text{degree of the field extension } F/K$$

Example 1.11

The field $\mathbb{C}$ is two-dimensional over $\mathbb{R}$, since $\{i, 1\}$ is a basis over $\mathbb{R}$ of $\mathbb{C}$. Thus, the degree of the extension $\mathbb{C}/\mathbb{R}$ is

$$[\mathbb{C} : \mathbb{R}] = 2$$

□

Algebraic or Transcendental

We can classify extensions as algebraic or transcendental.

If an element α is the root of some irreducible polynomial $p(x) \in K[x]$ (the polynomial ring over K), then α is said to be algebraic over K, otherwise α is said to be transcendental.

Example 1.12

$\sqrt{2}$ is algebraic over $\mathbb{Q}$ since it is the root of $x^2 - 2 = 0$.

$\sqrt{\pi}$ is algebraic over $\mathbb{R}$ since $x^2 - \pi = 0$ is a polynomial in $\mathbb{R}[x]$

$\sqrt{\pi}$ is **not** algebraic over $\mathbb{Q}$ since we cannot find a polynomial in $\mathbb{Q}[x]$ that has $\sqrt{\pi}$ as a root. Thus $\sqrt{\pi}$ is transcendental over $\mathbb{Q}$.

The field of rational functions in x over the field K, that is $K(x) = K[x, 1/x]$, is a transcendental field extension over K.

□

Algebraically Closed Field K

If every polynomial $p(x) \in K[x]$ contains a root in K, then K is algebraically closed.

Example 1.13

The field $\mathbb{C}$ is algebraically closed.

The field $\mathbb{Q}$ is not algebraically closed. As we explained in Example 1.12 there are polynomials in $\mathbb{Q}[x]$ that have roots not in $\mathbb{Q}$

□

Algebraic Closure of K, $\bar{K}$

For any field there exists a field $\bar{K}$, unique up to isomorphism, which is the smallest algebraically closed field containing K.

Given $p(x)$ a polynomial over K, $\bar{K}$ contains the zeros of $p(x)$.

Example 1.14

1. The field $\mathbb{C} = \mathbb{R}(x^2 + 1)$ is the algebraic closure of $\mathbb{R}$.
2. $\bar{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$.

□

Splitting Field

Let K be a field with algebraic closure $\bar{K}$. Then there exists a subfield F of $\bar{K}$ that is a field extension of K, such that any polynomial g over K is also a polynomial over F, so that the roots of the polynomial g are in F.

Given the field K we can construct the minimum field extension F such that the polynomial g splits over F. This minimum field extension is called a splitting field for the polynomial g over K.

Example 1.15

1. Let g be the polynomial in $\mathbb{Q}$ given by $x^2 - 2 = 0$.

   Then the splitting field for this polynomial over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$.

   Note that the polynomial also splits over bigger extensions like $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, but $\mathbb{Q}(\sqrt{2})$ is the splitting field since it is the minimum extension containing the roots of the polynomial.

2. Consider the polynomial $x^n - 1$ over $\mathbb{Q}$. The roots of this polynomial are the n^{th} roots of unity. Over $\mathbb{C}$, the equation $x^n = 1$ has n distinct solutions of the form

$$e^{2\pi ki/n} = \cos(2\pi k/n) + i\sin(2\pi k/n)$$

In the complex plane, the n^{th} roots of unity are represented as

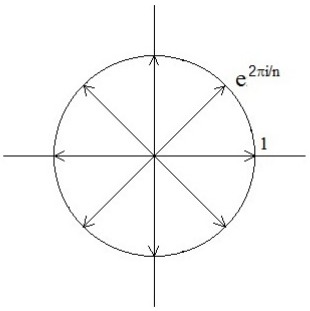

Figure 1.1: n-th roots of unity.

The n^{th} roots of unity form a group under multiplication. A generator of this group is called a primitive n^{th} root of unity. A possible choice for a primitive n^{th} root of unity that generates the other roots is $e^{2\pi i/n}$. Hence the splitting field for $x^n - 1$ over $\mathbb{Q}$ is $\mathbb{Q}(e^{2\pi i/n})$.

The field $\mathbb{Q}(e^{2\pi i/n})$ is called the *cyclotomic field* of n^{th} roots of unity.

3. The splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$ is the set of p^n roots of the polynomial,

$$\mathbb{F}_{p^n} = \{p^n \text{ roots of the polynomial } x^{p^n} - x\}$$

The field $\mathbb{F}_{p^n}$ is an extension of degree n of $\mathbb{F}_p$.

When $n = 1$, this polynomial becomes $x^p - x$ which is in fact the statement of Euler's Theorem. In this case the extension is of degree 1 and the extension field is $\mathbb{F}_p$ itself.

4. In this part of the example we are going to find the splitting field of the irreducible polynomial $x^3 + x^2 + 3$ over $\mathbb{Z}_{11}[x]$.

First we write α as a root of this polynomial, so we can write,

$$x^3 + x^2 + 3 = (x - \alpha)(x^2 + (1 + \alpha)x + (\alpha^2 + \alpha))$$

From $x^2 + (1 + \alpha)x + (\alpha^2 + \alpha) = 0$ we have to find the other two roots of the polynomial, so

$$x = \frac{-(1 + \alpha) \pm \sqrt{(1 + \alpha)^2 + 7(\alpha^2 + \alpha)}}{2}$$

$$= \frac{-(1 + \alpha) \pm \sqrt{1 + 9\alpha + 8\alpha^2}}{2} \tag{1.1}$$

Any element in the field $\mathbb{Z}_{11}[x]/(x^3+x^2+3)$ can be written as $a+b\alpha+c\alpha^2$ where $a,b,c \in \mathbb{Z}_{11}$, so it remains of check that $1+9\alpha+8\alpha^2$ has a square root in this field, to see if the three roots of x^3+x^2+3 split in $\mathbb{Z}_{11}[x]/(x^3+x^2+3)$. We will in fact find that this is not the splitting field of x^3+x^2+3 over $\mathbb{Z}_{11}[x]$, since if we write $1+9\alpha+8\alpha^2 = (a+b\alpha+c\alpha^2)^2$ and solve the resulting equations as polynomials in α, we find that there are no $a,b,c \in \mathbb{Z}_{11}$ satisfying these equations, and hence the roots of x^3+x^2+3 given by equation 1.1 do not split in $\mathbb{Z}_{11}[x]/(x^3+x^2+3)$.

The splitting field extension of x^3+x^2+3 over $\mathbb{Z}_{11}[x]$ is given by

$$\mathbb{Z}_{11}\left(\alpha, \sqrt{1+9\alpha+8\alpha^2}\right)/\mathbb{Z}_{11}$$

The degree of this extension is,

$$\left[\mathbb{Z}_{11}\left(\alpha, \sqrt{1+9\alpha+8\alpha^2}\right) : \mathbb{Z}_{11}\right] = 6$$

Hence the splitting field of x^3+x^2+3 over $\mathbb{Z}_{11}[x]$ has 11^6 elements.

□

Separable Field Extension

Consider F/K an algebraic field extension. An element $\alpha \in F$ is *separable* over K if its corresponding minimal polynomial in $K[x]$ is separable, that is, if all the roots of this polynomial are distinct. F/K is a separable field extension if all $\alpha \in F$ are separable over K.

Example 1.16

1. Consider $\mathbb{Q}(\sqrt{2})$, that is, an algebraic field extension of $\mathbb{Q}$.

   Here $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is separable over $\mathbb{Q}$ since the corresponding minimal polynomial in $\mathbb{Q}[x]$, $x^2-2=0$, can be factorized as $(x-\sqrt{2})(x+\sqrt{2})=0$ so that its roots are distinct.

2. The field extension $\mathbb{Q}(e^{2\pi i/k})/\mathbb{Q}$ discussed in Example 1.15 is separable.

3. The field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ given in Example 1.15 is separable, since the minimal polynomial $x^{p^n}-x$ has p^n distinct roots.

□

1.6.2 Galois Automorphism Group

An automorphism α of a field F is a map that provides an isomorphism $\alpha : F \to F$ of F onto itself.

The different automorphisms of F form a group under composition which we denote as $\mathrm{Aut}(F)$.

An automorphism $\alpha \in \mathrm{Aut}(F)$ is said to fix an element $x \in F$ if

$$\alpha(x) = x$$

If we consider the field extension F/K, then $\mathrm{Aut}(F/K)$ denotes the set of automorphisms $\alpha \in \mathrm{Aut}(F)$ such that α fixes all the elements in K.

$$\alpha(K) = K, \text{ for all } k \in K$$

Note that $\mathrm{Aut}(F/K)$ is also a group under composition, in fact it is a subgroup of $\mathrm{Aut}(F)$.

If F is the splitting field over K of the polynomial $g(x)$ then

$$|\mathrm{Aut}(F/K)| \leq [F : K]$$

If the polynomial $g(x)$ is separable then equality holds,

$$|\mathrm{Aut}(F/K)| = [F : K]$$

In this case we are dealing with a Galois extension, which means that F is a splitting field extension of K over the polynomial $g(x)$, and F is also a separable field extension.

The automorphism group $\mathrm{Aut}(F/K)$ is now called a Galois group $\mathrm{Gal}(F/K)$ since F/K is a Galois extension.

Example 1.17

The following is a straightforward example of the Galois group of a field extension.

$\mathbb{Q}(\sqrt{2}, \sqrt{5})$ is a Galois extension of $\mathbb{Q}$ since it is the splitting field of the minimal polynomial $(x^2 - 2)(x^2 - 5)$ and $\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}$ is a separable field extension.

The automorphism group of this extension is therefore a Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q})$.

The degree of the extension is

$$[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}] = 4$$

so the number of automorphisms is also 4, as discussed above,

$$|\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q})| = 4$$

The four automorphisms in the Galois automorphism group are completely determined by the action on $\sqrt{2}$ and $\sqrt{5}$, so labelling each of the automorphisms as ι, α, β and $\alpha\beta$ we have,

ι	α	β	$\alpha\beta$
$\sqrt{2} \to \sqrt{2}$	$\sqrt{2} \to -\sqrt{2}$	$\sqrt{2} \to \sqrt{2}$	$\sqrt{2} \to -\sqrt{2}$
$\sqrt{5} \to \sqrt{5}$	$\sqrt{5} \to \sqrt{5}$	$\sqrt{5} \to -\sqrt{5}$	$\sqrt{5} \to -\sqrt{5}$

Gal($\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}$) is isomorphic to the Klein 4-group.

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}) \cong V_4 \cong C_2 \times C_2$$

□

Example 1.18

1. Let $p(x) = x^{p-1} + x^{p-2} + \ldots + 1$ be an irreducible polynomail in $\mathbb{Q}$ then $F = \mathbb{Q}[x]/(p(x))$ is the splitting field over $p(x)$ in $\mathbb{Q}$, and $p(x)$ is a separable polynomial, so the extension $F/\mathbb{Q}$ is Galois. In this case the Galois group is isomorphic to the cyclic group of order $p-1$,

$$\mathrm{Gal}(F/\mathbb{Q}) \cong C_{p-1}$$

2. The extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ discussed in example 1.15 is also Galois. Its Galois group is cyclic of order n.

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong C_n$$

3. The splitting field found in part 4 of example 1.15 is also separable, so the extension,

$$\mathbb{Z}_{11}\left(\alpha, \sqrt{1+9\alpha+8\alpha^2}\right) \Big/ \mathbb{Z}_{11}$$

is a Galois extension.

The Galois automorphism group of this extension is of order 6 and is isomorphic to D_3,

$$\mathrm{Gal}\left(\mathbb{Z}_{11}\left(\alpha, \sqrt{1+9\alpha+8\alpha^2}\right) \Big/ \mathbb{Z}_{11}\right) \cong D_3$$

□

Chapter 2

Curves

In this chapter we have followed the approaches given by Kirwan [9], Reid [12] and Hirschfeld [8]. Examples 2.6, 2.7, 2.14 are exercises set by Reid [12], and examples 2.19, 2.20, 2.21 are exercises set by Silverman [13]. Examples 2.23 and 2.24 can be found in Hirschfeld [8].

Let K be an algebraically closed field, and $K[x, y]$ be the ring of polynomials in x and y. If p is a polynomial in this ring, the corresponding affine plane curve can be defined as follows,

$$C = \{(x, y) \in A_k^2 | p(x, y) = 0\}$$

Following Kirwan [9] the degree of the curve C is the degree of the polynomial, that is,

$$deg = max\{r + s : C_{r,s} \neq 0\}$$

where $p(x, y) = \sum_{r,s} C_{r,s} x^r y^s$.

Example 2.1

The degree of the curve defined by the polynomial $x^3y + x^2y + x$ is 4. □

A curve is homogeneous of degree d if the sum of the exponents in each term is always d.

Example 2.2

The curve defined by the polynomial $x^3y + x^2y^2 + xy^3$ is homogeneous of degree 4. □

Components

The irreducible factors of a polynomial defining an affine plane curve also define planar curves.

Example 2.3

Take the curve C defined by the polynomial $x^2 - y^2$. This can be written as the product of two irreducible factors $x - y$ and $x + y$. These factors are polynomials in $K[x, y]$ and they also define affine curves which are called the *components* of the curve C.

□

Multiplicity

If the polynomial of the curve C can be written as the product $f = f_1^{n_1} f_2^{n_2} \dots f_j^{n_j}$ where the f_i are irreducible, then the multiplicity of each f_i is given by the exponent n_i.

Example 2.4

Take the affine curve defined by the polynomial $f = x^2(2y+1)^3$. The component given by x has multiplicity 2 and the component given by $(2y+1)$ has multiplicity 3.

□

Singularity of curves

A singular point of a curve C defined by a polynomial $P(x, y) = 0$ is a point (a, b) such that,

$$\frac{\partial P}{\partial x}(a, b) = 0 = \frac{\partial P}{\partial y}(a, b)$$

If the curve has no singular points, it is said to be non-singular.

If a point (a, b) is non-singular, then the curve has one tangent at that point, which is given by

$$\frac{\partial P}{\partial x}(x - a) + \frac{\partial P}{\partial y}(y - b) = 0$$

Example 2.5

The curve defined by $y^2 = x^3 + x^2$ has a singularity at the origin.

$$\frac{\partial P}{\partial x} = 3x^2 + 2x \text{ evaluated at } (0, 0) \text{ gives } 0.$$

$$\frac{\partial P}{\partial y} = 2y \text{ evaluated at } (0, 0) \text{ gives } 0$$

so $(0, 0)$ is a singular point of this curve.

□

Singular points can have different multiplicities. A double point has multiplicity 2, a triple point has multiplicity 3, ...

2.1 Ideal of a Curve

2.1.1 Affine Variety

Let K be a field, $A = K[x_1, \ldots, x_n]$ a polynomial ring and $p = (a_1, \ldots, a_k)$ a point of the n-dimensional affine space over K.

Any element of A can be evaluated at p,

$$f(a_1, \ldots, a_n) = f(p)$$

An ideal J of the polynomial ring A can be generated by a finite number of polynomials. A **variety** $V(J)$ is the set of points that are zeros of the polynomials in the ideal J.

Example 2.6

Let $J = (x^2 + y^2 - 1, y - 1)$

To find the variety $V(J)$, we must make $y - 1 = 0$, that is, $y = 1$, and when substituting in the other generating polynomial, we find that x can only be 0.

Hence the variety $V(J) = \{(0, 1)\}$

The set of functions that become 0 at $p = (0, 1)$ is also an ideal: $I(V(J))$.

For J defined as above, we find that $J \subset I(V(J))$ (being the inclusion strict), since there exist many more polynomials than those in J that become 0 at $p = (0, 1)$.

For example, $x + y^2 - 1 \in I(V(J))$ but $\notin J$

□

Example 2.7

Consider $J = (xy, xz, yz) \subset K[x, y, z]$

The variety $V(J)$ can be found as follows:

$$J \ni z(xy) + y(xz) - x(yz) = xyz$$

but $x, y, z \notin J$, so J is not prime and therefore

$$V(J) = V(J, X) \cup V(J, Y) \cup V(J, Z)$$

The three components are the three coordinate axes. Like in the previous example, J is strictly included in $I(V(J))$. In this case $I(V(J)) = (x, y, z)$

□

2.1.2 Radical

To define the concept of radical we think of an ideal I of A generated by polynomials. The radical of I contains other polynomials that do not necessarily belong to I, but that can be lifted to a convenient power so that the result belongs to I.

Example 2.8

Let $I = (x^2, y^5)$

1. $x \in Rad(I)$ since $x^2 \in I$, although $x \notin I$
2. $x^5y^2 \in Rad(I)$ since $(x^5y^2)^{10} = x^{50}y^{20} \in I$ although $x^5y^2 \notin I$

□

More formally we define

$$Rad(I) = \{f \in A | f^n \in I \text{ for some } n \in \mathbb{Z}^+\}$$

In some cases we have that $I = Rad(I)$. That is, the ideal is the same as its radical.

Example 2.9

Every prime ideal is a radical ideal.

Suppose that there exists a prime ideal that is not radical. Then if it is not radical, it contains some element $f \notin I$ such that $f^n \in I$ for some $n \in \mathbb{Z}^+$.

By the definition of a prime ideal we know that if $f^n \in I$, then $f \in I$. So we reach a contradiction and hence we deduce that every prime ideal is a radical ideal.

□

2.1.3 Radical Ideals and the Ideals of Varieties

The ideal of a variety, $I(V(J))$ consists of all polynomials which vanish on some variety $V(J)$.

If J is an ideal in $K[x_1, \ldots, x_n]$ then we can find two different situations:

1. If K is an arbitrary field, then the ideal of the variety of J, $I(V(J))$, can be any ideal.
2. If K is an algebraically closed field, then the ideal $I(V(J))$ must be a radical ideal. That is, $I(V(J)) = Rad(J)$.

This second case is specially important to the Nullstellensatz Theorem.

2.2 Nullstellensatz for Planar Curves

Let P and Q be polynomials in $K[x, y]$, where K is an algebraically closed field.

The algebraic curves defined by these polynomials P and Q are given by the varieties $V(P)$ and $V(Q)$

Example 2.10

Let P be the polynomial x^2. then the algebraic curve defined by P is $x^2 = 0$, that is $V(P)$.

□

$V(P) = V(Q)$ if and only if the following equivalent conditions **(a)**, **(b)** and **(c)** hold:

Condition (a) P and Q have the same irreducible factors possibly occurring with different multiplicities.

Example 2.11

Consider P to be the polynomial $(y - x^2)^2(2y^2 - 3x^2)^3$ and Q the polynomial $(y - x^2)^3(2y^2 - 3x)^2$

P and Q have the same irreducible factors $(y-x^2)$ and $(2y^2-3x)$; although $(y - x^2)$ occurs with multiplicity 2 in P and with multiplicity 3 in Q; and $(2y^2 - 3x)$ occurs with multiplicity 3 in P and 2 in Q.

□

The ideal consisting of all polynomials which vanish on a variety V has the property that if some power of a polynomial belongs to an ideal, then the polynomial itself must belong to the ideal. So we have $I(V(P)) = I(V(Q))$

Condition (b)

$Rad((P)) = Rad((Q))$ since $P \in Rad((Q))$ and $Q \in Rad((P))$

Condition (c)

There exist positive integers m and n such that P divides Q^n and Q divides P^m

Example 2.12

Consider the same polynomials as in the previous example,

$P : (y - x^2)^2(2y^2 - 3x^2)^3$ and $Q : (y - x^2)^3(2y^2 - 3x)^2$

For these polynomials we can see that P divides Q^6 and Q divides P^6

□

We can see that **(a)**, **(b)** and **(c)** are equivalent if we recall the properties of radical ideals and ideals of varieties mentioned before.

The Nullstellensatz holds for K an algebraically closed field and, as we mentioned before

$$I(V(J)) = Rad(J)$$

for K algebraically closed.

Proof If $f \in Rad(J)$ this means by definition that there is some $n \in \mathbb{Z}^+$ such that $f^n \in J$.

Hence f^n vanishes on $V(J)$. Thus $f \in I(V(J))$ and hence $Rad(J) \subset I(V(J))$.

Conversely, suppose that $f \in I(V(J))$. Then f vanishes on $V(J)$. Then there exists an integer $n \in \mathbb{Z}^+$ such that $f^n \in J$, which means that $f \in Rad(J)$ since f is an arbitrary function $I(V(J)) \subset Rad(J)$

Hence, $I(V(J)) = Rad(J)$

2.3 Affine Coordinate Ring

To define the concept of coordinate ring, we must think of an affine algebraic set Y. Consider the ideal $I(Y)$ of Y. The coordinate ring of Y is the quotient ring $K[x_1, \ldots, x_n]/I(Y)$.

If Y is an affine variety (which we call V) in an algebraically closed field, then $I(V)$ is a radical ideal. As shown in example 2.9, every radical ideal is a prime ideal. Hence the quotient ring $K[x_1, \ldots, x_n]/I(Y)$ becomes and integral domain.

The coordinate ring of an affine algebraic set is a finite generated $K-algebra$. Conversely, any finitely generated $K-algebra$ which is a domain is the quotient of a polynomial ring by an ideal.

Example 2.13

The coordinate ring of the curve $C : y = x^2$ is given by $K[C] = K[x, y]/(y-x^2)$. The representatives of the cosets in the coordinate ring can be written as $g+(f)$, where $f(x, y) = y - x^2$, and $g + (f)$ are classes of polynomials in $K[x, y]$

□

2.3.1 Polynomial Maps

Let $V \subset A^n$, $W \subset A^m$ be varieties. A function $f : V \longrightarrow W$ is called a polynomial map if there are m polynomial in n variables $T_1, \ldots, T_m \in K[x_1, \ldots, x_m]$ such that,

$$f(a_1, \ldots, a_n) = (T_1(a_1, \ldots, a_n), \ldots, T(a_1, \ldots, a_n)) \text{ for all } (a_1, \ldots, a_n) \in V$$

Example 2.14

1. Let $C = (y^2 = x^3 + x^2) \subset A^2$; the familiar parametrization $\varphi : A^1 \longrightarrow C$ given by $(T^2 - 1, T^3 - T)$ is a polynomial map, but is not an isomorphism.

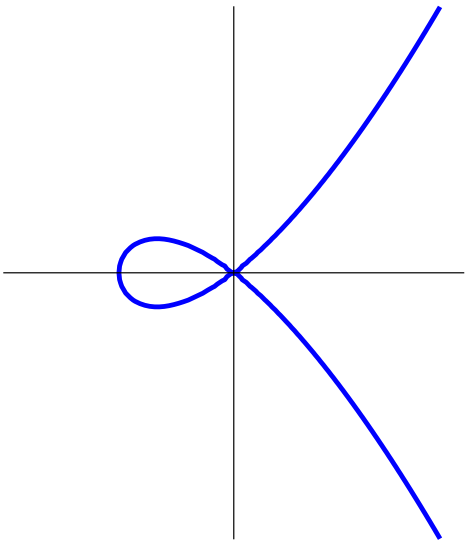

Figure 2.1: The nodal cubic

The nodal cubic crosses over itself at the origin $(0, 0)$, which is a singularity of this curve.

In this case, the homomorphism

$$\varphi* : K[C] = K[x, y]/(y^2 - x^3 - x^2) \longrightarrow K[T]$$

is given by $x \mapsto T^2 - 1, y \mapsto T^3 - T$.

The image of $\varphi*$ is the $K - algebra$ generated by $T^2 - 1$ and $T^3 - T$, that is $K[T^2 - 1, T^3 - T] \not\subseteq K[T]$ since $T^2 - 1,\ T^3 - T$ do not generate $K[T]$.

But we note that φ is not bijective, it is surjective since $\varphi(1) = \varphi(-1)$ and both these points map to the crossing point.

Hence we deduce that the polynomial map $\varphi : A^1 \longrightarrow C$ as defined above is **not** an isomorphism.

2. *Find out whether the restriction $\varphi' : A^1 \setminus \{1\} \longrightarrow C$ is an isomorphism.*

   Now that we have "taken away" one of the two points that prevented φ from being bijective, we find that $\varphi' : A^1 \setminus \{1\} \longrightarrow C$ is a bijective map.

   We can define an inverse map as follows,

   $\Psi : C \longrightarrow A^1 \setminus \{1\}$ given by

   $$\begin{cases} (x,y) \mapsto & 1 & \text{if } x = y = 0 \\ (x,y) \mapsto & y/x & \text{otherwise} \end{cases}$$

   And the homomorphism

   $$\varphi' * : K[C] \longrightarrow K[A^1 \setminus \{1\}]$$

   is an isomorphism so the polynomial map is an isomorphism.

□

2.4 Projective Plane Curves

The Projective Plane

Roughly speaking the projective plane $\mathbb{P}^2$ is obtained by adding points at infinity to the plane $\mathbb{R}^2$.

Any two lines in $\mathbb{R}^2$ intersect in a point except when they are parallel. In the projective plane, two parallel lines meet at a point at ∞ Thus the set of lines parallel to a given line L form an equivalence class $[L]$.

In this sense, the projective plane can be seen as the union of $\mathbb{R}^2$ with points at infinity, one point at infinity for each equivalence class $[L]$, i.e. each direction in $\mathbb{R}^2$.

Homogeneous Coordinates

If a triple $(x, y, z) \in \mathbb{R}^3 - \{0\}$ corresponds to a point $p \in \mathbb{P}^2$, we say that $[x, y, z]$ are homogeneous coordinates of the point p. The representation of homogeneous coordinates is not unique, so that $[x, y, z]$ and $[\lambda x, \lambda y, \lambda z] = \lambda[x, y, z]$ where $\lambda \in \mathbb{R} - \{0\}$, represent the same homogeneous coordinates. This means that the different representations of the homogeneous coordinates all lie on the same line through the origin in $\mathbb{R}^3$.

In the following figure we can see the representation of a point p. This point p is represented by the whole line, except at the origin.

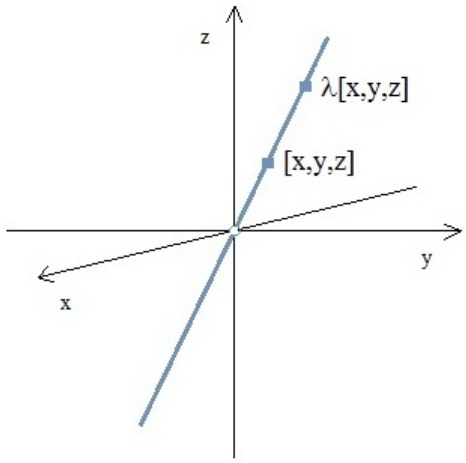

Figure 2.2: Homogeneous coordinates

Projective Plane Curves

Affine and projective curves are closely related. A projective curve can be obtained from an affine curve by adding points at infinity, so that the projective curve consists of the affine points and the points at infinity.

If we consider the algebraically closed field K, then for any homogeneous polynomial $F \in [x, y]$ of degree d, the projective plane curve of affine equation $F(x, y) = 0$ is given by,

$$\widetilde{C} = \{[x, y, z] \in \mathbb{P}^2 \mid z^d p(\frac{x}{z}, \frac{y}{z}) = 0\}$$

$$= \{[x, y, z] \in \mathbb{P}^2 \mid P(x, y, z) = 0\}$$

where P is an homogeneous polynomial associated to the polynomial p so that $P(x, y, z) = z^d p(\frac{x}{z}, \frac{y}{z})$

Example 2.15

Following the discussion above, the equation of an affine plane curve can be written as the equation for a projective curve by completing the degree of each term with z factors.

Consider the affine equation for the Klein quartic

$$x^3y + y^3 + x = 0$$

If we want to express this curve in projective coordinates we write x/z for x and y/z for y and multiply by z^4, since the affine curve is of degree 4.

Hence

$$z^4\left[\left(\frac{x}{z}\right)^3\left(\frac{y}{z}\right)+\left(\frac{y}{z}\right)^3+\left(\frac{x}{z}\right)\right]=0$$

that is,

$$x^3y+y^3z+xz^3=0$$

Similarly we can transform other equations of affine curves into equations for projective curves.

Equation of the affine curve		Equation of the projective curve
$x^2y^2+x^2y+x+y=0$	$\longrightarrow$	$x^2y^2+x^2yz+xz^3+yz^3=0$
$x^3+xy+y=0$	$\longrightarrow$	$x^3+xyz+yz^2=0$
$x^2y^2+y^2+y-x^2-x=0$	$\longrightarrow$	$x^2y^2+y^2z^2+yz^3-x^2z^2-xz^3=0$

As we will explain later, a projective curve must be defined as a rational function.

If we consider that last of the equations in this example, we can express it as polynomial over the field of rational function as follows,

$$\left(\frac{x}{z}\right)^2\left(\frac{y}{z}\right)^2+\left(\frac{y}{z}\right)^2+\left(\frac{y}{z}\right)-\left(\frac{x}{z}\right)^2-\left(\frac{x}{z}\right)=0$$

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

writing $\frac{x}{z}$ as x and $\frac{y}{z}$ as y we obtain the polynomial over the field of rational function

$$y^2+y=\frac{x(x+1)}{x^2+1}$$

□

Example 2.16

A line in $\mathbb{P}^2$ is a projective line $\mathbb{P}^1$. The projective line $\mathbb{P}^1$ is a line with a point at infinity.

An affine line equation is $Ax+By+C=0$. When changing to projective coordinates, z provides the point at infinity, so that a projective line has equation $Ax+By+Cz=0$.

Two projective lines always meet at exactly one point. If these two lines are not parallel, they meet just as affine lines do, at one point in $\mathbb{R}^2$. If the two projective lines are parallel, they also meet at one point, the point at infinity.

□

When defining affine plane curves we explained the concepts of degree, components, irreducibility and multiplicity.

For projective curves, these concepts follow directly form affine curves.

2.4.1 Projective Coordinate Ring

In this section we closely follow Fulton[4] and Reid[12].

Here we will explain how the concepts of variety, ideals of varieties, affine coordinate ring and polynomial maps can be carried over to projective geometry.

A **projective variety** in $\mathbb{P}^2$ is an irreducible algebraic set in $\mathbb{P}^2$ such that if S is a set of polynomials in $k[x, y]$ then the corresponding projective variety is the set of zeros of each polynomial in S.

$$V(S) = \{[x, y, z] \in \mathbb{P}^2 \mid [x, y, z] \text{ is a zero of each } f \in S\}$$

Like in affine geometry, this set of zeros generate an ideal $I(V(S))$. this ideal is prime if and only is V is irreducible. From the definition of projective variety we deduce that the ideal $I(V)$ is prime.

The **homogeneous or projective coordinate ring** is the quotient ring $K[x, y]/I(V)$. Since $I(V)$ is prime, this quotient defines an integral domain.

Example 2.17

The homogeneous coordinate ring of the projective line $\mathbb{P}^1$ is $K(x)$. The projective line is obtained by adding to the affine line $\mathbb{A}^1$ a point at infinity, so we need to consider functions of the field of rational functions $k(x)$ with x as a transcendental element.

Hence the homogeneous or projective coordinate ring of $\mathbb{P}^1$ is obtained via the quotient ring,

$$k[x, y]/\left(\frac{1}{x} - y\right) = k\left[x, 1/x\right] = k(x)$$

□

The transcendental element x in the example above is frequently denoted by t and called a **local parameter**.

Example 2.18

Consider the homomorphism

$$\varphi : K[x, y, z]/(y^2 z - x^3) \to K(t)$$

the local parameter is given by

$$t = \frac{y}{x}$$

□

2.4.2 Rational and Regular Functions

Let $V \subset \mathbb{P}^2$ be an irreducible algebraic set and $I(V)$ its ideal in $K[x, y, z]$.

A rational function $h : V \to K$ is a function of the form

$$h = \frac{f}{g}$$

where f and g are homogeneous polynomials of the same degree d. The rational function is well defined when $g \neq 0$.

It is important to note that the value of $\frac{f}{g}$ is independent of the choice of homogeneous coordinates,

$$\frac{f(\lambda x)}{g(\lambda x)} = \frac{\lambda^d f(x)}{\lambda^d g(x)} = \frac{f(x)}{g(x)}, \text{ for} \lambda \neq 0$$

Two functions $\frac{f_1}{g_1}$ and $\frac{f_2}{g_2}$ belong to the same equivalence class if and only if

$$g_1 f_2 - f_1 g_2 \in I(V)$$

A function h is regular at a point P if there exists an expression $h = \frac{f}{g}$ that is a well-defined rational function, that is, f and g are homogeneous polynomials of the same degree and $g(P) \neq 0$. The domain of definition of h, written as $dom(h)$, is the set of points P such that h is regular at P.

Note that a function $f \in K[x, y]$ is not a function on $\mathbb{P}^2$. Regular functions cannot be defined in $\mathbb{P}^2$ in terms of polynomials. Contrary to rational functions as defined above, a polynomial will be constant on equivalence classes if and only if it is homogeneous of degree 0, which means that it is a constant. Hence to define a projective curve we will need rational functions as we have explained in example 2.15.

The corresponding concept of a polynomial map between affine varieties when dealing with projective varieties is the concept of rational map.

A rational map between projective varieties $h : V \longrightarrow \mathbb{P}^2$ is defined by

$$P \mapsto [h_0(P), h_1(P), h_2(P)]$$

A rational map is regular at $P \in V$ if there exist $h = (h_0, h_2, h_2)$ such that each of the functions h_0, h_1 and h_2 are regular at P. Also, all the functions h_0, h_1 and h_2 cannot be 0 simultaneously.

Example 2.19

The rational map $h : \mathbb{P}^2 \to \mathbb{P}^2$ defined by $h = [x^2, xy, z^2]$ is regular everywhere except at $[0, 1, 0]$ where $x^2 = xy = z^2 = 0$

□

Definition A rational map that is regular everywhere is a morphism.

Example 2.20

Consider the curve V given by $y^2z = x^3 + z^3$ and the rational map as given in the previous example, $h = [x^2, xy, z^2]$.

As we will show, this rational map is regular everywhere so it is a morphism $h : V \to \mathbb{P}^2$.

h is clearly regular except at $[0, 1, 0]$. Using $x^3 = y^2z - z^3$ we have,

$$\begin{aligned} h &= [x^2, xy, z^2] \\ &= [x^2x^3, xyx^3, z^2x^3] \\ &= [x^2(y^2z - z^3), xy(y^2z - z^3), z^2x^3] \\ &= [x^2y^2z - x^2z^3, xy^3z - xyz^3, z^2x^3] \\ &= [xy^2 - xz^2, y^3 - yz^2, zx^2] \end{aligned}$$

Thus we have

$$h([0, 1, 0]) = [0, 1, 0]$$

so h is regular at every point of V.

□

Example 2.21

Consider the curve V given by $y^2z = x^3$. We first show that the map

$$\phi : \mathbb{P}^1 \to V$$

$$\phi = [S^2T, S^3, T^3]$$

is a morphism.

Writing $x = S^2T$, $y = S^3$ and $z = T^3$ we obtain

$$\frac{x}{z} = \left(\frac{S}{T}\right)^2 \text{ and } \frac{y}{z} = \left(\frac{S}{T}\right)^3$$

From these equations we deduce that $y^2z = x^3$ and hence ϕ is a morphism.

Now we want to find a rational map $\psi : V \to \mathbb{P}^1$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity map wherever they are defined.

The map given by

$$\psi : V \to \mathbb{P}^1$$

$$\psi = [y, x]$$

is a projection of the curve V onto the projective line $\mathbb{P}^1$. ψ is a rational map but not a morphism, but it is not defined at $[0, 0, 1]$, which is a singular point.

We now compute $\phi \circ \psi$ and $\psi \circ \phi$.

$$\phi \circ \psi : V \to V$$

$$[x, y, z] \overset{\psi}{\mapsto} [y, x] \overset{\phi}{\mapsto} [y^2x, y^3, x^3] = [y^2x, y^3, y^2z] = [x, y, z]$$

where $x^3 = y^2z$, $\phi \circ \psi$ is not defined at $[0, 0, 1]$ since this is a singular point of the variety $V : x^3 = y^2z$.

$$\phi \circ \psi : \mathbb{P}^1 \to \mathbb{P}^1$$

$$[S, T] \overset{\psi}{\mapsto} [S^2T, S^3, T^3] \overset{\phi}{\mapsto} [S^3, S^2T] = [S, T]$$

so $\psi \circ \phi = [S^3, S^2T] = [S, T]$ when $S \neq 0$.

□

A rational map is birational if it has a rational inverse.

2.4.3 Intersection Number

The way two projective curves C and D in $\mathbb{P}^2$ can intersect is stated by Bézout's theorem.

When considering projective geometry we have that:

- C and D always intersect in at least one point.
- if C and D have no common components. Then, they intersect in at most nm points, where n is the degree of C and m is the degree of D.
- C and D meet in exactly nm points if every point $C \cap D$ is a nonsingular point of C and D and the tangent lines of C and D at these points are distinct. The intersection multiplicity or intersection number of a point p can be written as $I_p(C, D)$, using the notation given by Kirwan [9].

These cases can be derived from Bézout's theorem which we can state as follows,

Bézout's Theorem

If C and D are two projective curves of degrees n and m in P^2 which have no common component then they have precisely nm points of intersection counting multiplicities, that is

$$\sum_{p \in C \cap D} I_p(C, D) = nm$$

From this statement of the theorem we can see that the concept of intersection number or intersection multiplicity is crucial to Bézout's theorem.

Value of Intersection Number

We show a chart that will guide us through the process of identifying the intersection number.

Does p belong to $C \cap D$?	$\xrightarrow{NO}$	$I_p(C,D) = 0$
YES $\downarrow$		
Does p lie on a common component of C and D?	$\xrightarrow{YES}$	$I_p(C,D) = \infty$
NO $\downarrow$		
Is p a nonsingular point of both C and D and tangent lines at p are distinct?	$\xrightarrow{YES}$	$I_p(C,D) = 1$
NO $\downarrow$		
$I_p(C,D) > 1$		

A useful tool for finding the intersection points of two curves and the multiplicity of these intersection points is provided by the concept of **resultant**.

Resultant

To see how the resultant can be found we are going to explain it through an example.

Example 2.22

Consider the curves C and D given by the nonconstant homogeneous polynomials,

$$P(x,y,z) = z^2 - x^2 - y^2$$
$$Q(x,y,z) = -z^3 - y^3 + x^2z + y^2z + yz^2$$

We want to find the resultant with respect to z which we write as $R_{P,Q}(x,y)$. First we note that P has degree 2 and Q has degree 3, and we find that,

$$P(x,y,z) = (-x^2 - y^2)z^0 + (0)z^1 + (1)z^2$$
$$Q(x,y,z) = (-y^3)z^0 + (x^2 + y^2)z^1 + (y)z^2 + (-1)z^3$$

We can display these coefficients of z in a $(3+2) \times (3+2)$ matrix as follows. The resultant is given by the determinant of this matrix:

$$R_{P,Q}(x,y) = det \begin{pmatrix} -x^2-y^2 & 0 & 1 & 0 & 0 \\ 0 & -x^2-y^2 & 0 & 1 & 0 \\ 0 & 0 & -x^2-y^2 & 0 & 1 \\ -y^3 & x^2+y^2 & y & -1 & 0 \\ 0 & -y^3 & x^2+y^2 & y & -1 \end{pmatrix} = x^4y^2$$

The polynomials $P(x,y,z)$ and $Q(x,y,z)$ have a nonconstant common factor if and only if $R_{P,Q}(x,y) = 0$.

So we write $x^4y^2 = 0$ and check the possible solutions.

- If $\mathbf{x} = \mathbf{0}$ then $-x^2 - y^2 + z^2 = 0$ becomes $z^2 = y^2$ and $y^3 + (x^2+y^2)z + yz^2 - z^3 = 0$ becomes $-y^3 + y^2z + yz^2 - z^3 = (z-y)(y^2-z^2) = 0$

  These two equations hold for $[0,1,-1]$ and $[0,1,1]$ which have multiplicity 4, as x has fourth power in the resultant.

- If $\mathbf{y} = \mathbf{0}$ then $-x^2 - y^2 + z^2 = 0$ becomes $z^2 = x^2$ and $y^3 + (x^2+y^2)z + yz^2 - z^3 = 0$ becomes $-x^2z - z^3 = z(x^2-z^2) = 0$

  These two equations hold for $[1,0,1]$ and $[1,0,-1]$ which have multiplicity 2, since y is squared in the resultant.

□

2.4.4 The Hessian Curve

The Hessian $\mathcal{H}_P$ of the polynomial P is the polynomial defined by,

$$\mathcal{H}_P(x,y,z) = det \begin{pmatrix} P_{xx} & P_{xy} & P_{xz} \\ P_{yx} & P_{yy} & P_{yz} \\ P_{zx} & P_{zy} & P_{zz} \end{pmatrix}$$

For a polynomial P of degree d, the second partial derivatives have degree $d-2$, so that the Hessian $\mathcal{H}_p$ has degree $3(d-2)$.

The points (a,b,c) for which the Hessian becomes 0 are points of inflection (flex) of the projective curve C defined by $P(x,y,z)$

- If $C = \{[x,y,z] \in \mathbb{P}_2 : P(x,y,z) = 0\}$ is an irreducible projective curve of degree d, then every point of C is a point of inflection if and only if $d = 1$.
- If $d \geq 2$ the C has at most $3d(d-2)$ points of inflection.
- If $d \geq 3$ then C has at least one point of inflection.

Example 2.23

The Hermitian curve has vanishing Hessian.

Let $K = \bar{\mathbb{F}}_q$ be the algebraic closure of the finite field $\mathbb{F}_q$ of cardinality $q = p^t$, where p is prime.

Then Hermitian curves are defined by,

$$F(x, y, z) = x^{q+1} + y^{q+1} + z^{q+1}$$

If we calculate the Hessian of this curve we have,

$$\frac{\partial F}{\partial x} = (q+1)x^q \quad \text{and} \quad \frac{\partial^2 P}{\partial^2 x} = (q+1)qx^{q-1}$$

Now as q is a factor of $(q+1)qx^{q-1}$, we have that in $\mathbb{F}_q, (q+1)qx^{q-1} = 0$. So that,

$$\frac{\partial^2 F}{\partial^2 x} = 0$$

Similarly for y and z we also obtain,

$$\frac{\partial^2 F}{\partial^2 y} = 0 \quad \text{and} \quad \frac{\partial^2 F}{\partial^2 z} = 0$$

All the mixed partial derivatives which we find in the other entries of the determinant of the Hessian are 0.

So we find that the Hessian of the Hermitian curve is

$$\mathcal{H}_P(x, y, z) = det \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 0$$

As we said before, the points (a, b, c) for which the Hessian becomes 0 are points of inflection.

For one Hermitian curve, the Hessian is 0 at all points, so that all points of the Hermitian curve are inflection points, whenever $p \neq 2$

□

Example 2.24

Consider the Fermat curves defined over $K = \bar{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$ where $q = p^t$ are given by

$$\mathbb{F}(x, y, z) = x^n + y^n + z^n, \quad \text{where } n \text{ is not divisible by } p$$

For this curve we have the Hessian

$$\mathcal{H}_P(x, y, z) = det \begin{pmatrix} n(n-1)x^{n-2} & 0 & 0 \\ 0 & n(n-1)y^{n-2} & 0 \\ 0 & 0 & n(n-1)z^{n-2} \end{pmatrix}$$
$$= n^3(n-1)^3 x^{n-2} y^{n-2} z^{n-2}$$

So in the Fermat curve all points are inflection points when

1. If $p = 2, n \equiv 1 \pmod{2^2}$
2. If $p \neq 2, n \equiv 1 \pmod{p}$

□

Chapter 3

Function Field of a Curve

In this chapter we introduce some of the basic definitions and results of the theory of function fields: places, valuations, valuation rings, rational points. These concepts will lead us to the statement of the Riemann-Roch Theorem in the next chapter.

3.1 The Function Field

Let F be an extension field of K, and let x be an element $x \in F$ which is transcendental over K. Then F is an algebraic function field if F is a finite algebraic extension of $K(x)$.

Thus F can be written as $K(x)[y]$, where y is algebraic over $K(x)$ and x (as we have already stated) is transcendental over K.

Example 3.1

In this example we are going to consider the curve given by $y^2 + y = \frac{x(x+1)}{x^2+1}$ over the field K. This function relates polynomial in y with a rational function in x.

First consider a function $f \in K(x)$. We know that $K(x)$ is the field of rational functions of x, so we write,

$$f = \frac{x(x+1)}{x^2+1}$$

On the other hand, we can write the polynomial $y^2 + y - f = 0$ so that y is a root of this polynomial of degree 2 in $K(x)[y]$. Hence y is algebraic over $K(x)$.

□

Function Field of a Curve

Let K be an algebraic number field, and let p be an irreducible polynomial over $K(x)$. The function field F is an extension of $K(x)$ over the polynomial p.

This polynomial defines a curve,

$$C : p(x, y) = 0$$

A rational function in F of the form $\frac{rp}{g}$, that is, with p dividing the polynomial in the numerator, but not the polynomial in the denominator, is said to be zero.

Now we consider any rational function $\frac{s}{t}$. The set of all rational functions that differ by zero from a given $\frac{s}{t}$, consists of the rational functions of the form,

$$\frac{s}{t} - \frac{rp}{g}$$

as we shall show, $\{\frac{s}{t} - \frac{rp}{g}\}$ is a field. This field is called the function field of the curve $C, K(C)$.

The class $[s/t]$ of functions that differ by zero from s/t form a place, P.

Example 3.2

The function field for the curve in example 3.1 is given by

$$F = K(x, t)$$

where t is a root of $y^2 + y - f = 0$ and $f = \frac{x(x+1)}{x^2+1}$.

Here the degree of the extension of the function field of this curve over $K(x)$ is 2

$$[F : K(x)] = 2$$

□

3.2 Places and Valuations

As explained above, a function field F is an extension of the field K. When each element $z \in F$ that is algebraic over K, belongs to K, then K is called the full constant field of F. We now define the concept of valuation ring. We denote a valuation ring as $\mathcal{O}$.

A valuation ring of the function field F satisfies the following properties

1. $K \subseteq \mathcal{O} \subseteq F$

2. For every non-zero element z of F, either $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$

The most straightforward case of a function field is the rational function field, where $F = K(x)$. So we first define the concepts of places and valuations for $F = K(x)$.

The Rational Function Field

In the case of a rational function field $K(x)$ we can define a valuation ring corresponding to an irreducible monic polynomial $p(x) \in K[x]$ as follows,

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

If we consider another polynomial, say $q(x)$, instead of $p(x)$, this gives rise to a different valuation ring of the rational function field $K(x) : \mathcal{O}_{q(x)}$.

With this definition of $\mathcal{O}_{p(x)}$, the units in this valuation ring are given by those elements which satisfy not only $p(x) \nmid g(x)$, but also $p(x) \nmid f(x)$. Hence the the elements that are not units satisfy $p(x) \nmid g(x)$ and $p(x) \mid f(x)$.

From this, we deduce the definition of a place P. The maximal ideal of a valuation ring is a **place**.

Thus the maximal ideal of $\mathcal{O}_{p(x)}$ as defined above is given by

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

The maximal ideal of a valuation ring, i.e., a place, is unique. Conversely, each place P determines its corresponding valuation ring uniquely.

We will denote the set of places of F as $\mathbb{P}_F$.

The polynomial $p(x)$ is a generator element for the place $P_{p(x)}$, which means that $P_{p(x)} = p(x)\mathcal{O}_{p(x)}$. Then any element $z \in F$ can be written as

$$z = p(x)^n \left(\frac{f(x)}{g(x)} \right)$$

where $n \in \mathbb{Z}$ and $\frac{f(x)}{g(x)}$ is a unit of the valuation ring $\mathcal{O}$, that is, $p(x) \nmid g(x)$ and $p(x) \nmid f(x)$.

We now define the concept of *zero place* and *pole place*.

Let $z_1 = \frac{h_1(x)}{g_1(x)} = \frac{(p(x))^2 f_1(x)}{g_1(x)}$, where $p(x) \nmid f_1(x)$ and $p(x) \nmid g_1(x)$, then the zeros of the polynomial $p(x)$ are also zeros of the function z_1. $\frac{f_1(x)}{g_1(x)}$ is a unit of the valuation ring $\mathcal{O}_{p(x)}$. So in this case the place $P_{p(x)}$ is a zero of z_1.

We now take a different function $z_2 \in F$, and we define $z_2 = \frac{f_2(x)}{s_2(x)} = \frac{f_2(x)}{(p(x))^3 g_2(x)}$, where $p(x) \nmid f_2(x)$ and $p(x) \nmid g_2(x)$. The zeros of $p(x)$ create poles for z_2. In this case, the place $P_{p(x)}$ is called a pole of z_2

We now define the infinite place of the rational function field $K(x)$ as,

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x],\ \deg f(x) < \deg g(x) \right\}$$

The valuation ring determined by this place is

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

The label chosen for the infinity place depends on the generating element x of $K(x)$, since if we choose $K(x) = K(1/x)$, then the infinite place is the place P_0 with respect to x.

Valuation Ring and Local Ring

We now return to the more general consideration of function fields F.

The concept of **local ring** was defined in the preliminary chapter. A local ring has only one maximal ideal, so to show that a valuation ring $\mathcal{O}$ is a local ring, we must show that a valuation ring has only one maximal ideal, which we call P.

P is a proper ideal of $\mathcal{O}$, so it cannot contain a unit. We denote the set of units in $\mathcal{O}$ by $\mathcal{O}^* = \{z \in \mathcal{O} \mid \exists w, wz = 1\}$.

So, if $x \in P$ and $z \in \mathcal{O}$, then xz is not a unit since this would mean that $x \in \mathcal{O}^*$. Thus, the set consisting of all elements in the valuation ring except the units in the ring is the unique maximal ideal P. That is, $P = \mathcal{O}/\mathcal{O}^*$.

Note that $z \in P$ if and only if $z^{-1} \notin \mathcal{O}$.

Valuation

A discrete valuation of a field F/K is a function $v : F \to \mathbb{Z} \cup \{\infty\}$ such that for all $x, y \in F$ we have

1. $\nu(x) = \infty \iff x = 0$
2. $\nu(xy) = v(x) + u(y)$ for all $x, y \in F$
3. $\nu(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in F$
4. $\nu(a) = 0$ for all $a \in K \setminus \{0\}$

Example 3.3

Given a prime number d, any non-zero rational number c can be written in the form,

$$c = d^k \frac{m}{n}$$

with k, m, n integers and n positive such that $d \nmid mn$.

Here the integer k, that indicates how often d divides c, is uniquely determined by c. Then $\nu(c) = k$ defines a normalized valuation of $\mathbb{Q}$, namely the "$d-adic$ valuation of $\mathbb{Q}$".

□

Relationship between Places and Valuations

To a place P we can associate a valuation function $\nu_P : F \to \mathbb{Z} \cup \{\infty\}$.

A **local parameter** is an element $t \in F$ such that $\nu_P(t) = 1$.

A local parameter acts as a generating element of the place P, so that if $\mathcal{O}$ is a valuation ring of F and P is the maximal ideal of that ring then $P = t\mathcal{O}$.

In this sense, if $P = t\mathcal{O}$, then each $z \in F/\{0\}$ can be uniquely represented as

$$z = t^n u$$

where u is a unit of the valuation ring $\mathcal{O}$, and n is some $n \in \mathbb{Z}$. The valuation of z at the place P is given by $\nu_P(z) = n$.

When considering the case of the rational function field $K(x)$, we defined the concepts of zero and pole places. For any function field F, this concepts can defined in a similar way.

Example 3.4

$\mathbf{v_P(z) > 0}$: Suppose $z_1 = t^2 u_1$, where $u_1 \in \mathcal{O}^*$. Then $\nu_P(z_1) = 2 > 0$ and P is a zero of z_1.

$\mathbf{v_P(z) < 0}$: We now consider $z_2 = t^{-3} u_2$, with $u_2 \in \mathcal{O}^*$. Here $\nu_P(z_2) = -3 < 0$, so that P is a pole of z_2.

$\mathbf{v_P(z) = 0}$: Let $z_3 = t^0 u_3$. Again $u_3 \in \mathcal{O}^*$, but this time we note that $z_3 = u_3$ so we deduce that when $\nu_P(z) = 0$, then z_3 is itself a unit of $\mathcal{O}$.

□

Following the discussion above, we define the valuation ring corresponding to a place P in F as

$$\mathcal{O}_P = \{z \in F \ : \ \nu_P(z) \geq 0\}$$

The set of units in this ring is given by

$$\mathcal{O}_P^* = \{z \in F \ : \ \nu_P(z) = 0\}$$

and as we explained before, the place P is the unique maximal ideal of $\mathcal{O}_P$, and consists of all the elements in $\mathcal{O}_P$ except for the units, so that,

$$P = \{z \in F \ : \ \nu_P(z) > 0\}$$

In the theory of function fields, the concept of a place P can be made to coincide with the notion of a point $P = (a, b)$ on the curve C, where $a, b \in K$ and $p(a, b) = 0$.

We know that the function fields of the curve $F = K(C)$ is the field of quotients of the coordinate ring $K[x, y]/(p)$, so that an element $z \in F$ can be written as $z = \frac{A(x,y)}{B(x,y)}$ where $A, B \in K[x, y]$. So we can associate the following rings to the points $P = (a, b)$,

$$\mathcal{O}_P = \{z \in F \mid z = \frac{A(x, y)}{B(x, y)}, B(a, b) = 0\}$$

$$P_P = \{z \in F \mid z = \frac{A(x, y)}{B(x, y)}, A(a, b) = 0\}$$

which are precisely the valuation ring and its corresponding place P.

Degree of a Place

The **degree of a place** of a function field F is defined by the degree of the extension of the residue class field $\mathcal{O}_P/P_P = K_P$ over the field K.

$$\deg P = [K_P : K] \leq [F : K(x)]$$

The residue class field is the quotient field of the valuation ring $\mathcal{O}_P$ and a place of this valuation ring, P_P. The valuation ring $\mathcal{O}_P$ is the ring of integers of the residue class field K_P.

If we now consider the places $P_1, \ldots, P_r$ to be zero place of an element z of the function field F, then,

$$\sum_{i=1}^{r} \nu_P(z) \deg P_i \leq [F : K(x)]$$

When K is algebraically closed and is the full constant field of F, we obtain the equality

$$\sum_{i=1}^{r} \nu_P(z) \deg P_i = [F : K(x)]$$

A place of degree 1 is called a *rational place*.

Example 3.5

In $\mathbb{P}^2$, the points of the curve given by $y^2 + y = f(x)$ are either rational points or points of degree 2. This can be deduced from the definition of degree of a place given above and the fact that for this curve $[F : K(x)] = 2$, as we stated in example 3.2.

□

An issue of crucial importance to coding theory is to know the number of rational places, that is of places of degree 1, for a curve with polynomial $p(x, y)$ and function field of the curve F, where F is a finite extension of $K(x)$.

In algebraic-geometric codes it is desirable to work with curves with many rational points. We will explain some methods for counting the number of rational places of a given function field in Chapter 6.

Example 3.6

In this example we are going to find some places of the Hermitian curve with function field $\overline{\mathbb{F}}_9[x, y]$.

The affine equation for this curve is given by,

$$y^3 + y = x^4$$

The corresponding equation of the projective curve is given by

$$y^3z + yz^3 = x^4$$

We can see that there is a unique place at infinity given by $P_\infty = [0, 1, 0]$, which is a rational place.

For each pair $(a, b) \in \mathbb{F}_9 \times \mathbb{F}_9$ such that $b^3 + b = a^4$, there is a place $P_{(a,b)}$ of degree 1. Thus another rational place of the Hermitian curve is given by $P_{(2,1)} = [2, 1, 1]$.

In general a Hermitian curve over $\mathbb{F}_{q^2}$ will have $q^3 + 1$ rational places.

As we will explain in Chapter 6, Hermitian curves are maximal, which means that they attain the maximum possible number of rational places, given g and q.

We have found some rational places, that is, places of degree 1, for a Hermitian curve over $\mathbb{F}_9$. Now we are going to find places of degree 2. To do this we need to find an extension of degree 2 over $\mathbb{F}_9$.

So we write $\mathbb{F}_{81} = \mathbb{F}_9[x]/(x^{9^2} - x)$, so that

$$[\mathbb{F}_{81} : \mathbb{F}_9[x]] = 2$$

Writing α for a root of $x^{9^2} - x$ in $\mathbb{F}_{81}$ we find that a place of degree 2 for the Hermitian curve is

$$P_{(\alpha,2)} = \{[\alpha, 2, 1]\}$$

The residue class field at this place is given by

$$\mathcal{O}_P/P_P = K_P = K[\alpha]$$

□

Chapter 4

The Riemann-Roch Theorem

4.1 Divisors

Definition of Divisor

The places of a function field F generate a free abelian group formally. This group is called the divisor group of F, $Div(F)$. The elements in this group $Div(F)$ are divisors of F.

A divisor D is a formal sum of places,

$$D = \sum n_P P,$$

where n_P is an integer and $n_P \neq 0$ only for a finite number of P.

The *zero element* of the group of divisors $Div(F)$ is given when $n_P = 0$ for all P, that is,

$$0 = \sum n_P P \text{ if } n_P = 0$$

Different divisors can be added coefficientwise, so that

$$\text{If } D = \sum n_P P \text{ and } D' = \sum n'_P P \text{ then } D + D' = \sum (n_P + n'_P) P$$

Support of a Divisor D

The support of a divisor D is the set of Places P with nonzero coefficient n_P in the formal sum defined above.

That is,

$$suppD = \{P \mid n_P \neq 0\}$$

This coefficient n_P is in fact $\nu_P(D)$, which is the valuation of the divisor D at the place P. In this case the support of a divisor D is the set:

$$suppD = \{P \mid \nu_P(D) \neq 0\}$$

where $D = \sum_{P \in suppD} \nu_P(D) P$

Degree of a Divisor

The degree of a Divisor D is defined as

$$\deg D = \sum \nu_P(D) \deg P$$

where $\deg P$ is the degree of the Place P as defined y section 3.2.

From the definitions of $\deg(P)$and $\nu_P(D)$ we can follow directly that $\deg D$ is always an integer.

A divisor with $\deg D = 2g - 2$, where g is the genus of the curve, is called a *canonical divisor*. We will refer to the canonical divisor as κ, using the same notation as given in Kirwan [9].

Example 4.1

In Example 3.6 we found some places of the Hermitian curve $y^3 + y = x^4$ over $\mathbb{F}_9$.

According to the given definition of a divisor we can write a divisor for this curve as follows,

$$D = 15P_\infty - 4P_{(2,1)} + 7P_{(\alpha,2)}$$

The support of this divisor is $\{P_\infty, P_{(2,1)}, P_{(\alpha,2)}\}$.

We know from example 3.6 that P_∞ and $P_{(2,1)}$ are rational places, so they have degree 1, and $P_{(\alpha,2)}$ is a place of degree 2.

So the degree of our divisor D is

$$\deg D = 15(1) - 4(1) + 7(2) = 25$$

□

Effective Divisor

A divisor D is called effective or positive if $D \geq 0$, which means that $n_P \geq 0$ for all places of a curve.

A non effective divisor is also called a virtual divisor.

Types of Divisors

Let $z = \frac{h}{g}$ be a function in the function field F.

When defining the relationship between places and valuations, we explained that the place P is called a zero of z if $\nu_P(z) > 0$ and a pole of z if $\nu_P(z) < 0$.

We now introduce the concepts of *zero divisor*, *pole divisor* and *principal divisor*.

Denoting $D_0(z)$ the set of zero places and $D_\infty(z)$ the set of pole places we define:

1. The zero divisor of z as

$$(z)_0 = \sum_{P \in D_0(z)} \nu_P(z) P$$

2. The pole divisor of z as

$$(z)_\infty = \sum_{P \in D_\infty(z)} (-\nu_P(z)) P$$

3. The principal divisor of z as

$$(z) = (z)_0 - (z)_\infty$$

All principal divisors have degree zero, and $\deg(z)_0 = \deg(z)_\infty = [F : K(x)]$

Example 4.2

For the Hermitian curve in Example 2.23,

$$f = y^3 + y - x^4$$

we found that the unique pole place of this curve is $P_\infty = [0, 1, 0]$.
Hence the pole divisor of f is

$$(f)_\infty = P_\infty$$

□

4.1.1 The Dimension of a Divisor

For a divisor $D \in Div(F)$, the Riemann-Roch space associated to D is given by,

$$\mathcal{L}(D) = \{z \in F \mid (z) + D \geq 0\} \cup \{0\} \tag{4.1}$$

The Riemann-Roch space $\mathcal{L}(D)$ is a vector space over F.

The following properties hold for $\mathcal{L}(D)$:

1. If $D' > D \Longrightarrow \mathcal{L}(D)$ is a subspace of $\mathcal{L}(D')$
2. If $D = 0 \Longrightarrow \mathcal{L}(D) = F$
3. If $\deg D < 0 \Longrightarrow \mathcal{L}(D) = \{0\}$

An important issue concerning the Riemann-Roch Theorem is the dimension of a divisor. For a divisor $D \in Div(F)$ we denote the dimension by,

$$\ell(D) = dim\mathcal{L}(D)$$

where $\ell(D)$ is an integer.

For a divisor D, the value of $\ell(D)$ is given in the following table.

Value of $\ell(D)$	Condition
0	$\deg D < 0$
0	$D \neq 0$ and $\deg D = 0$
1	$D = 0$
$g-1$	D is a non-canonical divisor
g	$\deg D = 2g-2$
$\deg D - g + 1$	$\deg D > 2g-2$

in this table, g denotes the genus of the function field, which we explain in the following section.

Example 4.3

Consider the divisor D found in Example 4.1

$$D = 15P_\infty - 4P_{(2,1)} + 7P_{(\alpha,2)}$$

The degree of this divisor was found to be

$$\deg D = 25$$

The genus of the Hermitian curve $y^3 + y = x^4$ is,

$$g = \frac{1}{2}(4-1)(4-2) = 3$$

As $\deg D = 25 \geq 2g - 2 = 4$ we deduce that the dimension of this divisor is

$$\ell(D) = \deg D - g + 1 = 23$$

□

4.2 Genus

In Chapter 2 we have defined the concept of singularity of a curve.

The genus of a curve can be found for both singular and non-singular curves. Nevertheless we will only define the genus for non-singular curves, which will be relevant for the statement of the Riemann-Roch Theorem in the next section.

Topologically, a non-singular projective curve in $\mathbb{P}^2$ can be viewed as a surface isomorphic to a sphere with g handles. The number g of handles is the genus of the curve. If $f(x, y)$ is a polynomial of degree d, then the genus of the corresponding non-singular projective plane curve is related to the degree d of the curve by the degree-genus or Plücker formula,

$$g = \frac{1}{2}(d-1)(d-2)$$

Example 4.4

An elliptic curve has an equation of the form

$$y^2 = f(x)$$

where $f(x)$ is a cubic polynomial with no repeated roots. For an elliptic curve the degree is $d = 3$ so the genus is

$$g = \frac{1}{2}(3-1)(3-2) = 1$$

□

Example 4.5

Consider the Hermitian curves as given in example 2.23,

$$F(x, y, z) = x^{q+1} + y^{q+1} + z^{q+1}$$

First we note that this curve is non-singular since,

$$\frac{\partial F}{\partial x} = (q+1)x^q, \quad \frac{\partial F}{\partial y} = (q+1)y^q, \quad \frac{\partial F}{\partial z} = (q+1)z^q$$

There does not exist any point $[a, b, c] \in \mathbb{P}^2$ such that

$$\frac{\partial F}{\partial x}[a, b, c] = \frac{\partial F}{\partial y}[a, b, c] = \frac{\partial F}{\partial z}[a, b, c] = 0$$

so Hermitian curves are non-singular.
Hence we deduce that the genus of a Hermitian curve is given by,

$$g = \frac{1}{2}((q+1)-1)((q+1)-2) = \frac{1}{2}q(q-1)$$

□

Example 4.6

The Klein quartic curve,

$$x^3y + y^3z + z^3x = 0$$

is non-singular and has genus

$$g = \frac{1}{2}(4-1)(4-2) = 3$$

□

The genus of a curve is closely related to the genus of the function field of that curve. Specifically, the genus of an irreducible algebraic curve is the genus of its function field F, where F is algebraically closed.

The Genus of a Function Field

The genus of the function field is defined by,

$$g = \max\{\deg D - \ell(D) + 1 \mid D \in Div(F)\}$$

The genus g is a non-negative integer. We know that for $D \leq D'$, the following inequality holds:

$$\deg D - \ell(D) \leq \deg D' - \ell(D')$$

so the smallest value for the expression,

$$\deg D - \ell(D) + 1$$

is given by $D = 0$. That is,

$$\deg(0) - \ell(0) + 1 = 0 - 1 + 1 = 0$$

Hence $g \geq 0$.

Riemann's Inequality provides an upper bound for the genus of the curve depending on the degree of the extensions of F over $K(x)$ and $K(y)$. Suppose that $F = K(x, y)$. If F has genus g, then

$$g \leq ([F : K(x)] - 1)([F : K(y)] - 1)$$

This bound is accurate and in most cases it cannot be improved.

With the Riemann-Roch Theorem we will give a different characterization of the genus, relating it implicitly to the concepts of degree and dimension of divisors.

4.3 Statement of the Riemann-Roch Theorem

In this section we present the statement of the Riemann-Roch Theorem as given in Kirwan [9].

If D is any divisor on a non-singular projective curve C of genus g in $\mathbb{P}^2$ and κ is a canonical divisor on C, then

$$\ell(D) - \ell(\kappa - D) = \deg(D) + 1 - g$$

Proof We have already stated above that the degree of the canonical divisor κ is given by

$$\deg \kappa = 2g - 2$$

If D is any divisor on C then we have the following inequality, which is also known as Riemann's Theorem

$$\ell(D) - \ell(\kappa - D) \geq \deg D + 1 - g \tag{4.2}$$

writing $\kappa - D$ instead of D in the inequality above we obtain

$$\ell(\kappa - D) - \ell(D) \geq \deg(\kappa - D) + 1 - g \tag{4.3}$$

First we are going to prove inequality 4.2.
Let A be a divisor of degree d on a curve C also of degree d, so

$$\deg(\kappa - mA) = \deg(\kappa) - m \deg A = \deg(\kappa) - md$$

for a large enough m,

$$\deg(\kappa) - md < 0$$

and hence,

$$\deg(\kappa - mA) < 0$$

This implies that

$$\ell(\kappa - mA) = 0$$

We have stated in section 4.2 that the genus of the function field of a curve satisfies

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

for any divisor D.
Rearranging, we write

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

Consequently for the divisor A and m as defined above,

$$\ell(mA) - \ell(\kappa - mA) \geq \deg(mA) - g + 1$$

For any divisor D and any $m_0 > 0$ there exists $m \geq m_0$ and places of the curve C, $P_1 \ldots, P_n$ such that the divisor mA belongs to the same equivalence class as $D + P_1 + \ldots + P_n$

$$mA \sim D + P_1 + \ldots + P_n$$

Any two linearly equivalent divisor on C have the same degree g_0

$$\deg(mA) = \deg(D + P_1 + \ldots + P_n) = \deg D + n$$

Hence

$$\ell(mA) - \ell(\kappa - mA) \geq \deg D + n - g + 1$$

so

$$\ell(mA) - \ell(\kappa - mA) - n \geq \deg D - g + 1$$

As $mA \sim D + P_1 + \ldots + P_n$, we can write this inequality as

$$\ell(D + P_1 + \ldots + P_n) - \ell(\kappa - D - P_1 - \ldots - P_n) - n \geq \deg D - g + 1 \quad (4.4)$$

It now remains to show that

$$\ell(D) - \ell(\kappa - D) \geq \ell(D + P_1 + \ldots + P_n) - \ell(\kappa - D - P_1 - \ldots - P_n) - n \quad (4.5)$$

$\mathcal{L}(D)$ is a subspace of $\mathcal{L}(D + P_1 + \ldots + P_n)$ of codimension at most n so,

$$0 \leq \ell(D) - \ell(D + P_1 + \ldots + P_n) \leq n$$

similarly

$$0 \leq \ell(\kappa - D) - \ell(\kappa - D - P_1 - \ldots - P_n) \leq n$$

It holds that,

$$0 \leq \ell(D) - \ell(D + P_1 + \ldots + P_n) - \ell(\kappa - D) + \ell(\kappa - D - P_1 - \ldots - P_n) \leq n$$

Rearraging we obtain inequality 4.5 and substituting in 4.4 gives,

$$\ell(D) - \ell(\kappa - D) \geq \deg D - g + 1$$

which is inequality 4.2 at the beginning of the proof.

From inequality 4.3 at the beginning of the proof

$$\ell(\alpha - D) - \ell(D) \geq \deg(\kappa - D) - g + 1$$

we have that

$$\deg(\kappa - D) = \deg \kappa - \deg D = 2g - 2 - \deg D$$

substituting in inequality 4.3 we obtain,

$$\ell(\kappa - D) - \ell(D) \geq 2g - 2 - \deg D - g + 1 = -\deg D + g - 1$$

Multiplying both sides of the inequality by -1, we have

$$\ell(D) - \ell(\kappa - D) \leq \deg D - g + 1 \quad (4.6)$$

combining inequalities 4.2 and 4.6 we obtain,

$$\ell(D) - \ell(\kappa - D) = \deg D - g + 1$$

and we obtain the result of the Riemann-Roch Theorem.

4.4 Some Consequences of the Riemann-Roch Theorem

As a consequence of the Riemann-Roch Theorem we can now explain the significance of a **gap number** of a place P, and state the Weierstrass gap theorem.

Gap Number

Let $P \in \mathbb{P}_F$. A **pole number** of P is an integer $n \geq 0$ if there exists an element $z \in F$ such that the pole divisor is $(z)_\infty = nP$. Otherwise, n is calls a **gap number** of P.

Weierstrass Gap Theorem

Consider the function field F with genus $g > 0$, and let P be a rational place of F. Then there are exactly g gap numbers $i_1, \ldots i_g$ of P which satisfy

$$i_1 = 1 \text{ and } i_1 < \ldots < i_g \leq 2g - 1$$

Proof First we show that 1 is a gap number. We show this by contradiction. Suppose that 1 is a pole number. The pole numbers form an additive semigroup, so if 1 is a pole number, then every $n \in \mathbb{N}$ is a pole number. But this means that there do not exist any gap numbers, so we arrive at a contradiction. Thus, as 1 cannot be a pole number, then it must be a gap number, $i_1 = 1$.

Each gap number i satisfies $i \leq 2g - 1$ for all $n \geq 2g$, there exist an element $z \in F$ with $(z)_\infty = nP$, that is each $n \geq 2g$ is a pole number.

i is a gap number of P if and only if

$$\mathcal{L}\left((i-1)P\right) = \mathcal{L}(iP)$$

we also note that $\ell(iP) \leq \ell((i-1)P) + 1$

So if we consider the ascending chain of Riemann-Roch spaces,

$$\mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq (2P) \subseteq \ldots \subseteq \mathcal{L}((2g-1)P)$$

where $\ell(0) = 1$ and $\ell((2g-1)P = g$.

then for $g - 1$ integers strict inclusion holds and we find pole numbers and for the remaining g integers, equality holds and we find gap numbers.

Chapter 5

Coverings

In topology a covering map $p : A \longrightarrow B$ is defined as a continuous surjective mapping. A open set $U \subset B$ is covered by p if $p^{-1}(U)$ can be written as the union of disjoint open sets $V_n \subset A$, and $p : V_n \longrightarrow U$ is an isomorphism.

Example 5.1

The map $p : \mathbb{C} \longrightarrow S^1 \times S^1$ is a covering of the torus by the complex place.

Any point $z \in \mathbb{C}$ can be represented as a point in the parallelogram

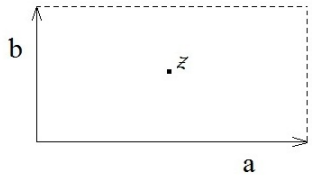

Figure 5.1: Complex plane

since $z = ta + sb$, where t, s are under two successive identifications α and β of opposite sides of the parallelogram

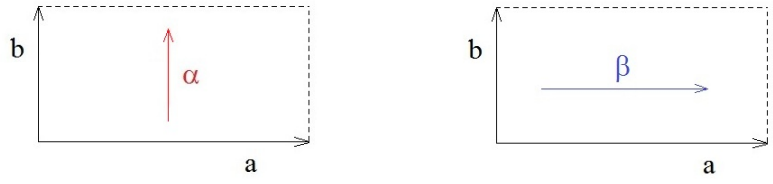

Figure 5.2: Edge identifications

we obtain the quotient topology of the torus, and each point $z \in \mathbb{C}$ has been mapped to a point on $S^1 \times S^1$

□

Example 5.2

The map $p : \mathbb{R} \longrightarrow S^1$ given by the equation

$$p(x) = (\cos 2\pi x, \sin 2\pi x)$$

is a covering map.

One can picture p as a function that wraps the real line $\mathbb{R}$ around the circle S^1, and in the process maps each interval $[n, n+1]$ onto S^1.

Consider the subset $U \subset S^1$ consisting of those point having positive first coordinate. The set $p^{-1}(U)$ consists of those points x for which $\cos 2\pi x$ is positive; that is, it is the union of intervals

$$V_n = \left(n - \frac{1}{4}, n + \frac{1}{4}\right)$$

for all $n \in \mathbb{Z}$

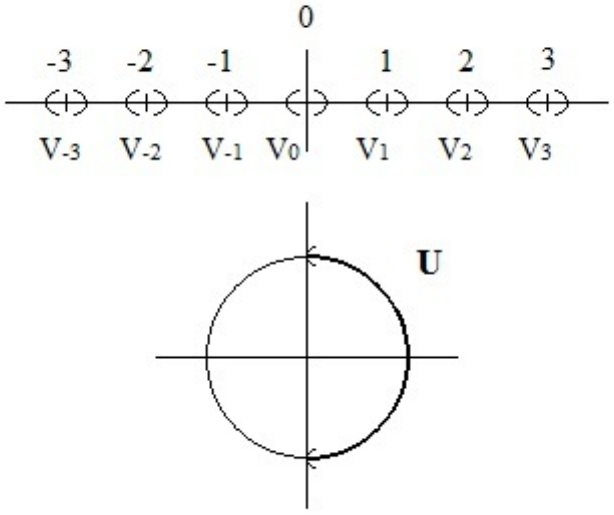

Figure 5.3: Covering of S^1.

□

If C is an algebraic curve with function field F' and X is another algebraic curve with function field F, then C is a covering of X if we can define a morphism $p : C \longrightarrow X$ between the curves C and X. This corresponds to a morphism $F' \longrightarrow F$ between function fields, where F' is an extension of F.

The degree of the covering is given by the degree of the field extension from the function field of the covered curve X to the function field of C, that is if $[F' : F] = n$, then the degree of the covering of X by C is also n.

Example 5.3

Consider the projective line $\mathbb{P}^1$. The function field of $\mathbb{P}^1$ is given by $K(x)$ as we have shown in example 2.17

If we consider the curve,

$$(x^4 + y^4 - x^2 - y^2)^2 = 2x^2y^2 \tag{5.1}$$

We have that the function field of this curve is an extension of degree eight of $K(x)$. Hence,

$$[F : K(x)] = 8$$

If we now consider the covering of the projective line $\mathbb{P}^1$ by the curve given by equation 5.1 we see that it is of degree 8, since the degree of the covering coincides with the degree of the field extension $F/K(x)$.

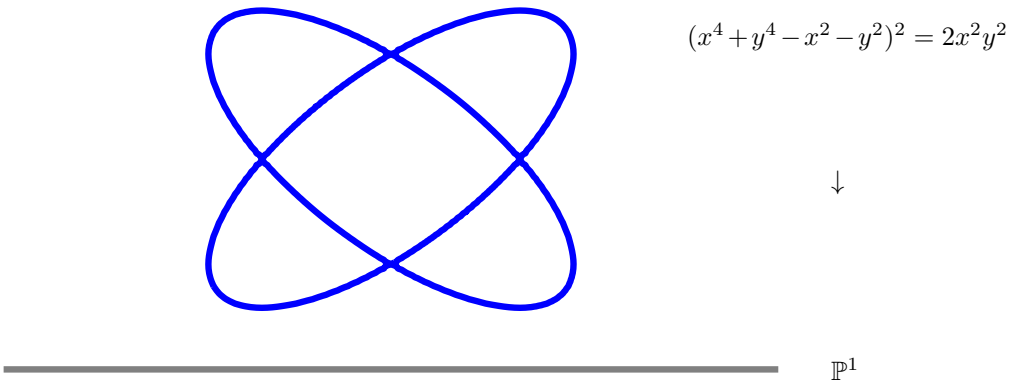

Figure 5.4: Ramified Covering of $\mathbb{P}^1$

The preimage $p^{-1}(x)$ of a point x is called the fiber of that point. As we can see in the figure, the fibers of some points in $\mathbb{P}^1$ are ramified places.

□

In chapter 6 we will present the method given by Van der Geer and Van der Vlugt in [17] to construct curves with many rational points as covers of $\mathbb{P}^1$. We will also present other methods of constructing covering curves with many rational points given in [15].

5.1 Ramification

In the last two examples we have seen how the coverings ramify over some places. In this section we are going to explain in more detail what is meant by ramification.

Consider again a covering of X by C, where F and F' are the corresponding function fields of these algebraic curves.

If P is a place in F, then there is at least one place P' in F' lying over P. To denote that a place P' lies over P we write $P'|P$. P' is also called and extension place of P.

Let $\mathcal{O}_P \subseteq F$ and $\mathcal{O}_{P'} \subseteq F'$ denote the valuation rings in F and F' corresponding to the places P and P' respectively, where P' is an extension place of P.

Then,

$$P'|P \Longrightarrow \mathcal{O}_P \subseteq \mathcal{O}_{P'}$$

Moreover, if $P'|P$ then

$$P = P' \cap F \text{ and } \mathcal{O}_P = \mathcal{O}_{P'} \cap F$$

According to this definition, the place P is also called the **restriction of** P' **to** F .

There is always a finite number of places P' in F' lying over places P in F, and each place P' is an extension place of exactly one place P, namely $P = P' \cap F$.

The function field F' is an extension of F, but both fields are also extensions of their full constant fields K' and K respectively.

The residue class fields of the places P' and P will be denoted as $K'_{P'}$ and K_P. Since F'/F is a field extension, $K'_{P'}/K_P$ is also a field extension. The degree of the extension $K'_{P'}/K_P$ is called the **relative degree** of the place P' over P, and is denoted by $f(P'|P)$ or $f_{P'}(F'/F)$.

$$f_{P'}(F'/F) = [K'_{P'} : K_P]$$

following the discussion above, we can consider the field extensions F'/F, F/K and F'/K. For these extensions the following relation holds,

$$f_{P'}(F'/K) = f_{P'}(F'/F) f_P(F/K)$$

If we aim to find rational points on the cover curve with function field F', then the value of $f(P'|P)$ is of great significance.

If P is a rational place in F and P' is an extension place of P in F', then P' is also a rational place if $f(P'|P) = 1$

Ramification Index

The ramification index of an extension place P' over a place P is denoted by $e(P'|P)$ or $e_{P'}(F'/F)$.

When counting valuations we have that the **ramification index** $e(P'/P)$ is given by the positive integer a such that,

$$\nu_{P'}(t_{P'}) = a.\nu_P(t_P)$$

where $t_P \in F$ is a local parameter at the place P.

Note that the value of a is independent of the choice of the parameter t.

The field extension F'/F is said to be unramified at P' if $e(P'|P) = 1$ and ramified when $e(P'|P) > 1$.

When F'/F is ramified at P', this ramification can be of different types.

The field extension F/F' is totally ramified at P' if,

$$e(P'|P) = [F' : F]$$

Note that when this sort of ramification occurs, there is only one P' in the extension field F' that lies over P in F. A place P' can also be tamely as wildly ramified in F'/F. To define this concept, we first recall that the function field F is already itself an extension of a field K.

P' is tamely ramifed in F'/F if $e(P'|P) > 1$ and $e(P'|P)$ is not divisible by the characteristic of K. When $e(P'|P)$ is divisible by the characteristic of K, then P' is said to be wildly ramified in F'/F.

The Fundamental Equality

The ramification index $e(P'|P)$ and the relative degree of P' over P, $f(P'|P)$ are related by

$$\sum_{i=1}^{n} e(P'_i|P) f(P'_i|P) = [F' : F]$$

where $P'_1, \ldots, P'_n$ are all the places of F' lying over P.

Proof. $[F' : K(t)] = [F' : K'(t)][K'(t) : K(t)]$

$$\begin{aligned}
&= \left(\textstyle\sum_{i=1}^{n} v_{P'}(t_{P'_i} \deg P'_i)\right)[K' : K] \\
&= \textstyle\sum_{i=1}^{n} v_P(t_P) e(P'_i|P)[K'_{P'_i} : K'][K' : K] \\
&= r \textstyle\sum_{i=1}^{n} e(P'_i|P)[K'_{P'_i} : K'][K' : K] \\
&= r \textstyle\sum_{i=1}^{n} e(P'_i|P)[K'_{P'_i} : K_P][K_P : K] \\
&= r.\deg P. \textstyle\sum_{i=1}^{n} e(P'_i|P) f(P'_i|P)
\end{aligned}$$

Now we can write another expression for $[F' : K(t)]$ using the tower law,

$$[F' : K(t)] = [F' : F][F : K(t)] = [F' : F].r.\deg P$$

combining the two expressions for $[F' : K(t)]$ we have

$$r.\deg P \sum_{i=1}^{n} e(P'_i|P) f(P'_i|P) = [F' : F].r.\deg P$$

Hence,

$$\sum_{i=1}^{n} e(P'_i|P) f(P'_i|P) = [F' : F]$$

which is the fundamental equality.

The fundamental equality provides an important algorithm for calculating the value of $f(P'_i|P)$. Once we know the value of the ramification index and the degree of the extension, it is straightforward to calculate $f(P'|P)$.

This is particularly important since if $f(P'|P) = 1$, then we know that the degree of a place P' lying over P is the same as the degree of P itself. As a consequence, if P is a rational place, that is a place of degree 1, then if the relative degree is $f(P'|P) = 1$ we will know that P' is also a rational place, i.e., $\deg P' = 1$.

The most interesting cases for which the relative degree $f(P'|P) = 1$ are when P splits completely so that there are $[F' : F] = n$ places P' over P with $e(P'|P) = f(P'|P) = 1$, or when P is totally ramified, so that $e(P'|P) = n = [F'|F]$ and $f(P'|P) = 1$.

Example 5.4

In the following figure we show some place P' lying over places P_i

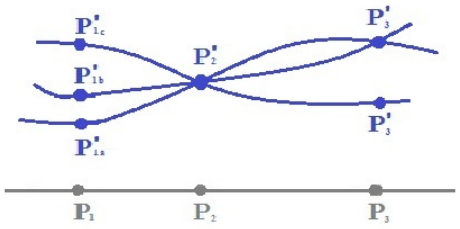

Figure 5.5: Covering.

Place P_1 is covered by the three places of C, P'_{1a}, P'_{1b}, P'_{1c}. These places are unramified in F'/F.

$e(P'_{1a}|P) = e(P'_{1b}|P) = e(P'_{1c}|P) = 1$ and $f(P'_{1a}|P) = f(P'_{1b}|P) = f(P'_{1c}|P) = 1$ so

$$\sum_{i=1}^{n} e(P'_i|P) f(P'_i|P) = 1 + 1 + 1 = 3$$

Place P_2' is totally ramified, since only P_2' lies over P_2. So $e(P_2'|P_2) = [F' : F]$=3 and $f(P_2'|P_2) = 1$.

Thus,

$$\sum_{i=1}^{n} e(P_i'|P) f(P_i'|P) = 3 \times 1 = 3$$

Place P_{3a}' is ramified but not totally ramified. Here $e(P_{3a}'|P_3) = 2$ and $f(P_{3a}'|P_3) = 1$, and $e(P_{3b}'|P_3) = 1$ and $f(P_{3b}'|P_3) = 1$ so,

$$\sum_{i=1}^{n} e(P_i'|P) f(P_i'|P) = 2 \times 1 + 1 \times 1 = 3$$

□

Corollary: Let F'/K' be a finite extension of F/K, and consider the place P in F and places $'$ in f' lying over P:

1. The number of places P' lying over P is always less than or equal to the degree of the extension $[F' : F]$.
2. P splits completely in F'/F if and only if $e(P'|P) = f(P'|P) = 1$ for all places P' lying over P.

5.1.1 Ramification when F'/F is a Galois Extension

Here we denote by F'/F a finite Galois extension, i.e., F'/F is a separable field extension and F' is the splitting field for the polynomial f over F.

P' is a place of F' lying over a place P of F. We will also call P' an extension of P. Gal(F'/F) is the Galois automorphism group of F'/F as defined in Chapter 1.

Let P_1' and P_2' be extensions of a place P of F. Then there exists a Galois automorphism $\alpha \in$ Gal(F'/F) such that,

$$P_2' = \alpha(P_1')$$

If F'/F is Galois, then the ramification index of the extensions $P_1', \ldots, P_i'$ of a place P is the same for all $P_1', \ldots, P_i'$. That is,

$$e(P_1'|P) = e(P_2'|P) = \ldots = e(P_i'|P)$$

This can be deduced from the definition of ramification index given above, and the fact that for $\alpha \in$ Gal (F'/F)

$$v_{P_j'}(t) = v_{\alpha(P_j')}(\alpha(t)) = v_{P_k'}(t)$$

with $e(P_1'|P) = e(P_2'|P) = \ldots = e(P_i'|P)$, the fundamental equality explained above becomes,

$$\sum_{i=1}^{n} e(P_i'|P)f(P_i'|P) = e(P'|P)(f(P_1'|P) + f(P_2'|P) + \ldots + f(P_i'|P))$$

if $[F' : F] = q$, with q a prime, then

$$e(P'|P)\,(f(P_1'|P) + f(P_2'|P) + \ldots + f(P_i'|P)) = q$$

so that if $e(P'|P) = q$ then $i = 1$ and $f(P'|P) = 1$. So that for each rational place P, the extension place P' is also a rational point.

Example 5.5

A finite Galois covering of the projective line is given by the curve C over $\mathbb{F}_9$ defined by the equation,

$$y^2 = \frac{x^9 + x^3}{x^3 + 2x}$$

The extension is Galois and its Galois automorphism group is isomorphic to C_2

As we have explained in example 5.3 the degree of the covering coincides with the degree of the field extension, so the curve given by $y^2 - f$ where $f = \frac{x^9+x^3}{x^3+2x}$ is a covering of degree 2 of the projective line.

As we are dealing with a covering of degree 2, we have three different possible cases:

1. $e(P'|P) = 2$ and $f(P'|P) = 1$

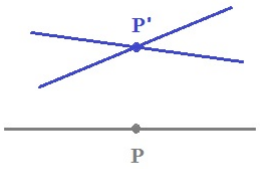

Figure 5.6: Ramified point

2. $e(P'|P) = 1$ and $f(P'|P) = 2$

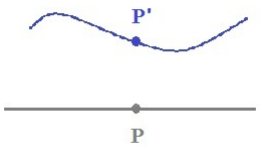

Figure 5.7: Unramified extension with relative degree $f(P'|P) = 2$

3. $e(P_1'|P) = e(P_2'|P) = 1$ and $f(P_1'|P) = f(P_2'|P) = 1$

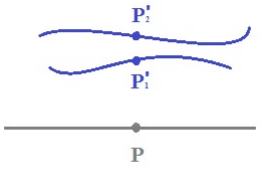

Figure 5.8: Unramified covering. The place P splits completely in the extension.

Note that for the particular covering given in this example, the second of the possible combinations is not possible.

The cover curve found in this example has at least 16 rational points.

□

Example 5.6

Consider the Hermitian curve C_H

$$y^3 + y = x^4$$

This curve defines a covering of degree 3 of the projective line. Let $z \in F$ be an element of the function field of C_H, then the curve given by C

$$z^2 = \frac{x^9 + x^3}{x^3 + 2x}$$

is a covering of degree 2 of the Hermitian curve C_H.

C and C_H form a tower of coverings over the projective line $\mathbb{P}^1$.

$$\begin{array}{ccc} C & \longrightarrow & C_H \\ & \searrow & \downarrow \\ & & \mathbb{P}^1 \end{array}$$

□

To find coverings of curves, the **Eisenstein's Irreducibility Criterion** is particularly useful.

Consider the function $f(x) \in F[x]$ where F/K is a function field and

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \text{ where } a_n = 1 \text{ and } a_1 \in F$$

such a polynomial is called an Eisenstein polynomial at a place P of F if

$$v_P(a_0) = 1 \text{ and } v_P(a_i) \geq 1 \text{ for } i = 1, \ldots, n-1$$

If $f(x)$ is an Eisenstein polynomial at some place P of F, then $f(x)$ is irreducible in $F[x]$.

If $F' = F(\alpha)$ where α is a root of $f(x)$, then there is a unique place $P' \in \mathbb{F}_{\mathbb{F}'}$ lying over P, so that $e(P'|P) = [F' : F]$ and the place P' is totally ramified.

The **Hilbert Class Field** F of an algebraic number field K is the maximally abelian unramified extension of K. By abelian extension we refer to a Galois extension whose Galois group is abelian. $\mathrm{Gal}(F/K)$ is the ideal class group of the ring of integers of K.

5.2 Hurwitz Genus Formula

In this section we are going to explain the Hurwitz genus formula following the approach given by Niederreiter and Xing [11] and Stichtenoth [14].

The Hurwitz genus formula gives a useful characterization of the genus of the extension field F'. This field F' is a separable extension of the function field F. We denote this extension by F'/F. Recall from the definition of the function field F at the beginning of Chapter 3 that F is itself an extension of K. Similarly, F' can also be viewed as a field extension of its full constant field, which we write as K'. By the full constant field K' we refer to a field which is algebraically closed in F', so that each element of F' that is algebraic over K' belongs to K'.

For the statement of the Hurwitz genus formula it is important to note that K' is a separable field extension of K.

Before we state Hurwitz genus formula, we first introduce the concepts of norm and trace map for a finite separable extension F'/F and the concept of the *different* of F'/F.

Norm and Trace

In a finite field extension F'/F of degree $n = [F' : F]$, F' can be seen as a vector space over F. If $\{u_1, \ldots, u_n$ is a basis of F'/F and $v \in F'$ then

$$v.u_i = \sum_{j=1}^{n} a_{ij} u_j \text{ where } a_{ij} \in F \text{ and } v \in F'$$

The norm of v with respect to F'/F is

$$N_{F'/F}(v) = \det(a_{ij})$$

The trace of v with respect of F'/F is,

$$\mathrm{Tr}_{F'/F}(v) = \sum_{i=1}^{n} a_{ii}$$

Example 5.7

In this example we are going to consider the field extension $\mathbb{C}/\mathbb{R}$. A basis for this extension is $\{1, i\}$ we find the norm and trace of $v = x + iy \in \mathbb{C}$ with respect to $\mathbb{C}/\mathbb{R}$.

First we have that $u_1 = 1$ and $u_2 = i$ so,

$$(x+iy).1 = \begin{bmatrix} a_{11} & a_{12} \end{bmatrix} \begin{bmatrix} 1 \\ i \end{bmatrix} = a_{11} + ia_{12}$$

from this we deduce that $a_{11} = x$ and $a_{12} = y$.

Now,

$$(x+iy).i = \begin{bmatrix} a_{11} & a_{12} \end{bmatrix} \begin{bmatrix} 1 \\ i \end{bmatrix} = a_{21} + ia_{22}$$

so we obtain the equation

$$ix - y = a_{21} + ia_{22}$$

so we deduce that $a_{21} = -y$ and $a_{22} = x$.

Therefore

$$N_{\mathbb{C}/\mathbb{R}}(x+iy) = \det \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = x^2 + y^2$$

$$\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(x+iy) = a_{11} + a_{22} = 2x$$

□

The following properties hold for the norm and trace of elements $v, w \in F'$ and $a \in F$ where $[F' : F] = n$:

1. $N_{F'/F}(a) = a^n$
2. $N_{F'/F}(v) = 0 \iff v = 0$
3. $N_{F'/F}(v.w) = N_{F'/F}(v).N_{F'/F}(w)$
4. $\mathrm{Tr}_{F'/F}(a) = n.a$
5. $\mathrm{Tr}_{F'/F}(v+w) = \mathrm{Tr}_{F'/F}(v) + \mathrm{Tr}_{F'/F}(w)$
6. $\mathrm{Tr}_{F'/F}(a.v) = a.\mathrm{Tr}_{F'/F}(v)$

In addition to these properties, if F'/F is a Galois extension with Galois automorphism group Gal $(F'/F) = \{\alpha_1, \ldots, \alpha_n\}$, then

$$N_{F'/F}(v) = \prod_{i=1}^{n} \alpha_i(v)$$

$$\mathrm{Tr}_{F'/F}(v) = \sum_{i=1}^{n} \alpha_i(v)$$

Example 5.8

In Chapter 1 we explained that the field $\mathbb{F}_{p^n}$ is an extension of degree n of $\mathbb{F}_p$, and that $\mathbb{F}_{p^n}$ is the splitting field of the separable polynomial $x^{p^n} - x$. We also noted that the Galois group of this extension is cyclic of order n:

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong C_n$$

so if we take $\alpha_1 \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ to be a generating element of the group such that

$$\langle \alpha_1 \rangle \cong C_n$$

Then the Frobenius automorphism

$$\begin{array}{rccc} \alpha_1 : & \mathbb{F}_{p^n} & \to & \mathbb{F}_{p^n} \\ & v & \mapsto & v^p \end{array}$$

where v is a root of the polynomial $x^{p^n} - x$.

Now consider another element of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, $\alpha_2 = \alpha_1.\alpha_1$.
Here we obtain

$$\alpha_2(v) = \alpha_1\left(\alpha_1(v)\right) = \alpha_1\left(v^p\right) = v^{p^2}$$

Similarly for α_{n-1}, we can argue in the same way and obtain

$$\alpha_{n-1}(v) = v^{p^{n-1}}$$

As the group is cyclic, α_n represents the identity so that

$$\alpha_n(v) = v$$

Hence by the formulas given above for Norm and Trace when the extension is Galois, we deduce that

$$\begin{aligned} N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(v) &= \alpha_1(v).\alpha_2(v)\ldots\alpha_{n-1}(v).\alpha_n(v) \\ &= v^p.v^{p^2}\ldots v^{p^{n-1}}.v \\ &= v^{1+p+p^2+\ldots+p^{n-1}} \\ &= v^{\frac{p^n-1}{p-1}} \end{aligned}$$

$$\begin{aligned} \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(v) &= \alpha_1(v) + \alpha_2(v) + \ldots + \alpha_{n-1}(v) + \alpha_n(v) \\ &= v + v^p + v^{p^2} + \ldots + v^{p^{n-1}} \end{aligned}$$

□

The Different of F'/F

Let $\mathcal{S}$ be a set of places P such that $\mathcal{S} \subset \mathbb{P}_F$. The set of extension places P' of $P \in \mathcal{S}$ is called the over-set of $\mathcal{S}$ and will be denoted by $\mathcal{T}$. The *integral closure* of $\mathcal{O}_\mathcal{S}$ in F' is,

$$\mathcal{O}_\mathcal{T} = \{z \in F' : v_{P'}(z) \geq 0 \text{ for all } P' \in \mathcal{T}\}$$

The complementary set of $\mathcal{O}_\mathcal{T}$ is similarly,

$$\mathcal{C}_\mathcal{T} = \{z \in F' \mid \mathrm{Tr}_{F'/F}(z.\mathcal{O}_\mathcal{T}) \subseteq \mathcal{O}_\mathcal{S}\}$$

$\mathcal{C}_\mathcal{T}^{-1}$ is an integral ideal of $\mathcal{O}_\mathcal{T}$.
The **different** of $\mathcal{O}_\mathcal{T}$ with respect to $\mathcal{O}_\mathcal{S}$ is given by

$$\mathcal{D}_\mathcal{S}(F'/F) = \mathcal{C}_\mathcal{T}^{-1}$$

we can also write $\mathcal{D}_\mathcal{S}(F'/F)$ as $\mathcal{D}_P(F'/F)$ if P is the only element in $\mathcal{S}$.
The different exponent of P' over P is defined by

$$d(P'|P) = v_P(\mathcal{D}_P(F'/F))$$

$d(P'|P) \geq 0$ and $d(P'|P) = 0$ for all but finitely many places P' of F'.
The different exponent $d(P'|P)$ and the ramification index $e(P'|P)$ are closely related,

1. $d(P'|P) \geq e(P'|P) - 1$
2. $d(P'|P) = e(P'|P) - 1$ if and only is $e(P'|P)$ is relatively prime to the characteristic of K.

The **global different divisor** of F'/F which we denote by $\mathrm{Diff}(F'/F)$ is a positive divisor of F'. This divisor is defined by

$$\mathrm{Diff}(F'/F) = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P)P' \tag{5.2}$$

The Hurwitz Genus Formula

In the statement of this formula we follow the same notation as in the discussion above, where F/K is an algebraic function field with genus g, F/F' is a finite separable extension and K' is the full constant field of F'. Finally we denote the genus of F' by g'. Thus the Hurwitz genus formula is given by,

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg \mathrm{Diff}(F'/F) \tag{5.3}$$

Note that if all places of F' are unramified in F'/F then as we have stated above, $d(P'|P) = 0$ and consequently $\mathrm{Diff}(F'|F) = 0$, so that the Hurwitz genus formula becomes simplified.

If K is algebraically closed and is the full constant field of F', then the Hurwitz genus formula becomes,

$$2g' - 2 = [F' : F](2g - 2) + \deg \mathrm{Diff}(F'/F) \tag{5.4}$$

5.3 Ramification Groups and Conductors

Here we consider a Galois extension F'/F, where F' and F are algebraic function field. We denote the Galois automorphism group of this extension by $\mathrm{Gal}(F'/F)$.

Let P' be a place of F' lying over a place P in F. For every integer $i \geq -1$ we define the i**th ramification group** by,

$$G_i(P'|P) = \{\alpha \in \mathrm{Gal}(F'/F) : v_{P'}(\alpha(z) - z) \geq i + 1 \text{ for all } z \in \mathcal{O}_{P'}\}$$

when $i = -1$, $G_{-1}(P'|P)$ is called the **decomposition group** which is also denoted by $G_Z(P'|P)$.

Similarly, when $i = 0$, $G_0(P'|P)$ is called the **inertia group** and is also denoted by $G_T(P'|P)$

The decomposition group of P' over P is defined by

$$G_Z(P'|P) = \{\alpha \in \mathrm{Gal}(F'/F) : \alpha(P') = P'\}$$

the inertia group of P' over P is given by

$$G_T(P'|P) = \{\alpha \in \mathrm{Gal}(F'/F) : v_{P'}(\alpha(z) - z) \geq 1 \text{ for all } z \in \mathcal{O}_{P'}\}$$

From this definitions we can see that both $G_Z(P'|P)$ and $G_T(P'|P)$ are subgroups of the Galois automorphism group. Furthermore,

$$G_T(P'|P) \subseteq G_Z(P'|P)$$

As a consequence of these definitions, the decomposition group and the inertia group of the place $\alpha(P')$, where $\alpha \in \mathrm{Gal}(F'/F)$ is given by,

$$G_Z(\alpha(P')|P) = \alpha G_Z(P'|P)\alpha^{-1}$$

$$G_T(\alpha(P')|P) = \alpha G_T(P'|P)\alpha^{-1}$$

From the definitions of $e(P'|P)$ and $f(P'|P)$, the decomposition group $G_Z(P'|P)$ has order $e(P'|P).f(P'|P)$. The inertia group $G_T(P'|P)$ has order $e(P'|P)$ and is a normal subgroup of $G_Z(P'|P)$.

The ramification groups form a descending chain,

$$G_{-1}(P'|P) \supseteq G_0(P'|P) \supseteq G_1(P'|P) \supseteq \ldots \supseteq G_i(P'|P) \supseteq G_{i+1}(P'|P) \supseteq \ldots$$

For sufficiently large k, $G_k(P'|P)$ consists of the identity, i.e $|G_k(P'|P)| = 1$

We will refer to the least integer k such that $|G_k(P'|P)| = 1$ as $a_P(F'/F)$.

The Conductor

Let $a_P(F'/F)$ be the least integer K such that $|G_k(P'|P)| = 1$ as defined before, $d_P(F'/f)$ the different exponent and $e_P(F'/F)$ the ramification index, then we define the **conductor exponent** as,

$$c_P(F'/F) = \frac{d_P(F'/F) + a_P(F'/F)}{e_P(F'/F)} \tag{5.5}$$

$c_P(F'/F) = 0$ if and only if P is unramified in F'/F.

$c_P(F'/F) = 1$ if and only if P is tamely ramified in F'/F.

By the definition above, we know that $c_P(F'/F) \geq 0$.

the **conductor** of F'/F is the positive divisor of F given by

$$\mathrm{Cond}(F'/F) = \sum_{P \in \mathbb{P}_F} c_P(F'/F)P$$

The support of this divisor is finite and it consists of exactly all places P of F that are ramified in F'/F. This is a consequence of the fact that P is unramified in F'/F if and only if $c_P(F'/F) = 0$. So unramified places contribute 0 to the sum above, and hence do not belong to the support of the conductor of F'/F.

5.4 Kummer and Artin-Schreier Extensions

We will work with tow kinds of coverings of curves: cyclic and dihedral. In this section we consider two types of cyclic covering.

Let F'/F be a separable extension with F' the splitting field for the minimal polynomial f over F. Then F'/F is said to be a Galois extension. If the Galois group $\mathrm{Gal}(F'/F)$ is cyclic, then we refer to F'/F as a cyclic extension.

Two interesting types of cyclic extension are Kummer extensions and Artin-Schreier extensions.

Although Kummer and Artin-Schreier extensions can be found for any function field F/K, here we are going to follow the definitions given in Niederreiter and Xing [11] and we are going to consider the global function field $F/\mathbb{F}_q$ and $E = F(y)$ a cyclic extension fo F of degree n.

Kummer Extension

Consider $F/\mathbb{F}_q$ and let $n > 1$ be an integer that divides $q - 1$. Suppose that $f \in F$ is an element that satisfies

$$f \neq g^d \text{ for all } g \in F \text{ where } d > 1 \text{ is an integer dividing } n$$

For y a root of the polynomial $T^n - f$ we obtain the extension $E = F(y)$. E is cyclic extension of F and $[E : F] = n$.

The element $f \in F$ satisfying the condition given above is said to be nth *Kummer nondegenerate*. If f is nth Kummer degerenate then $f = g^d$ for some $d|n$ and $d > 1$.

For any place P' in E lying over P in $F/\mathbb{F}_q$, the ramification index satisfies,

$$e(P'|P) = \frac{n}{\gcd(v_P(f), n)}$$

where f is nth Kummer nondegenerate.

We denote the genus of a Kummer extension E of $F/\mathbb{F}_q$ by g', and the genus of $F/\mathbb{F}_q$ by g. The genera of E and $F/\mathbb{F}_q$ are related by the following equality,

$$g' = 1 + n(g-1) + \frac{1}{2}\sum_{P\in\mathbb{P}_F}(n - \gcd(v_p(f), n))\deg P \tag{5.6}$$

where P is a place in F.

Note that the formula above achieves this form since the full constant field of E and F is $\mathbb{F}_q$ for both fields. Had we considered an extension F' of F with full constant fields K' and K respectively, the formula relating the genera of F' and F, where F' is a Kummer extension of F is given by,

$$g' = 1 + \frac{1}{[K':K]}(n(g-1) + \frac{1}{2}\sum_{P\in\mathbb{P}_F}(n - \gcd(v_P(f), n))\deg P)$$

Example 5.9

The curve

$$y^8 = \frac{x^9 + x^3}{x^3 + 2x} \text{ over } \mathbb{F}_9$$

represents a Kummer cover over the projective line $\mathbb{P}^1$.

It is straightforward to see that $\frac{x^9+x^3}{x^3+2x}$ is Kummer nondegenerate.

□

Artin-Schreier Extension

Here we consider again a function field $F/\mathbb{F}_{q=p^m}$ and $E = F(y)$ a cyclic extension of the field F.

Consider an element $f \in F/\mathbb{F}_q$ such that

$$f \neq g^p - g \text{ for all } g \in F$$

For y a root of the polynomial $T^P - T - f$, we obtain the extension $E = F(y)$. E is a cyclic extension of F and $[E : F] = p$.

The element $f \neq g^p - g$ as given above is Artin-Schreier nondegenerate. If f is Artin-Schreier degenerate, then there exits a $g \in F$ such that $f = g^p - g$.

For f a nondegenerate element, and $P \in \mathbb{P}_F$, we define the integer m_P,

$$m_P = \begin{cases} -1 & \text{if } v_P(f - (z^p - z)) \geq 0 \text{ for some } z \in F \\ m & \text{if } v_P(f - (z^p - z)) = -m < 0 \text{ and } m \text{ is coprime to } p \text{ for some } z \in F \end{cases}$$

In the first case, $m_P = -1$, P is unramified in E/F.

In the second case, $m_P = m$, P is totally ramified in E/F.

We denote the genus of an Artin-Schreier extension E of $F/\mathbb{F}_q$ by g' and the genus of $F/\mathbb{F}_q$ by g, then

$$g' = pg + \frac{p-1}{2}(-2 + \sum_{P \in \mathbb{P}_F} ((m_P + 1) \deg P) \tag{5.7}$$

where P is a place of F.

5.5 The Hasse-Weil Upper Bound

The number of places of degree one, that is, of rational places of a function field of a curve over $\mathbb{F}_q$ is finite and can be estimated by the Hasse-Weil bound and other bounds like the serre Bound, the Ihara bound, the Oesterlé bound and the Vlăduţ-Drindfeld Bound.

The Hasse-Weil Bound gives a good estimate for small genera with respect to q. When the genus grows larger, the Hasse-Weil bound fails to give a good estimate of the number of rational places.

Despite this, the Hasse-Weil bound is very important in the application of algebraic function fields to coding theory.

The Hasse-Weil bound is given by the inequality

$$N_q(g) \leq q + 1 + [2g\sqrt{q}]$$

where $N_q(g)$ is the maximal number of rational places of a curve over $\mathbb{F}_q$ with genus g.

When a curve attains the Hasse-Weil upper bound, it is said to be maximal, since it has the maximum possible number of rational points. As noted before, an example of maximal curve is the Hermitian curve, which attains the number of rational points given by the Hasse-Weil upper bound for a given genus g.

One of the aims of research in this field is to construct curves over finite fields attain or come close to attaining the Hasse-Weil bound for a given genus.

Chapter 6

Some Constructions and Applications

6.1 Tables of Curves with many Points

In their article "Tables of Curves with Many Points", Gerhard van der Geer and Marcel van der Vlugt present several tables giving the best bounds for the number of rational points on curves over finite fields of genera up to 50.

This article begins with a discussion of the different bounds given by several authors for the number of rational points of a curve over a finite field. The bounds given in the tables are the best bounds given by the following

Hasse-Weil Bound: $N_q(g) \leq q + 1 + [2g\sqrt{q}]$

Ihara: $N_q(g) \leq q + 1 + \left[\left(\sqrt{(8q+1)g^2 + 4(q^2-q)/g} - g\right)/2\right]$

Serre: $N_q(g) \leq q + 1 + g[2\sqrt{q}]$

Oesterlé: The Oesterlé upper bound is constructed following Serre's idea, but using methods from linear programming.

Once that the difference bounds have been introduced, the article goes further to explain the different methods to construct curves with many rational points explicitly, As these curves have many rational points, the value of $N_q(g)$ will come closer to the estimate given by the best upper bounds explained above.

The different methods for constructing curves have been developed by Serre, Schoof, Lauter, Niederreiter and Xing, Auer, Stichtenoch, Shabat, and Van der Geer and van der Vlugt.

We quote here the classification of methods given by van der Geer and van der Vlugt in [16]. These methods are among other:

I Methods from general class field theory

II Fibre products of Artin-Schreier curves

III Towers of curves with many points

IV Miscellaneous methods such as

1. formulas for $N_q(1)$ and $N_q(2)$
2. explicit curves, e.g. Hermitian curves, Klein's quartic, Artin-Schreier curves, Kummer extensions or curves obtained by computer search
3. elliptic modular curves $X(n)$ associated to the full congruence subgroups $\Gamma(n)$
4. quotients of curves with many points

Interpreting the Tables

The tables are constructed for curves over finite fields $\mathbb{F}_q$ where $q = 2^m$ with $1 \leq m \leq 7$, and $q = 3^m$ with $1 \leq m \leq 4$. The genera of the curves under consideration is $g \leq 50$.

The entries of the table give the value of $N_q(g)$, that is, the number of rational places of the corresponding curve.

When the entry consists of a unique number, it represents the exact value for $N_q(g)$.

Here we produce an example which shows how some entries in the tables can be obtained.

Example 6.1

A Hermitian curve is maximal so we know that it has the maximum number of rational points. Therefore $N_q(g)$ attains its maximum possible number and it produces a unique entry in the tables.

If we consider the entry for genus 3 and q=9 in the table for p=3, we see that it reads 28. A curve for which this number of rational points is attained is the Hermitian

$$y^3 + y = x^4$$

which is a curve over $\mathbb{F}_q$ with genus $g = \frac{1}{2}q(q-1) = 3$ and 28 rational points.

Another entry which can be obtained by a Hermitian curve is the entry for $g = 36$ and $\mathbb{F}_{81}$ in the table for $p = 3$. Here $N_q(g) = 730$, which is in fact the number of rational places of the Hermitian curve

$$y^9 + y = x^{10}$$

□

Some entries are given as ranges since the exact value for $N_q(g)$ is not known. In this case the smaller number means that there exist curves for the corresponding $\mathbb{F}_q$ and genus g with at least that number of rational points, and the bigger number is given by the best upper bound for $N_q(g)$.

Finally there are some missing entries in the tables. The reason given by van der Geer and van der Vlugt for these missing entries is that if for a given $\mathbb{F}_q$ and a genus g, a curve is known to have at least a number a of rational points, but the upper bounds of rational points are much bigger, then the curve is discarded.

Such a curve cannot be considered to have many rational points since the upper bound tells us that it could have many more rational points.

The paper [16] was published in 1999. Since then, some new entries have been found for these tables. Regularly updated tables can be found at

http: //wins.uva.nl/~geer

6.2 Curves over Finite Fields Attaining the Hasse-Weil Upper Bound

In the previous section we have seen how the maximum number of rational points can be calculated for some genera g of curves over finite fields. In his article "Curves over Finite Fields Attaining the Hasse-Weil Upper Bound", Arnaldo García looks upon this same issue from another point of view. He concentrates upon maximal curves and considers the determination of the possible genera of these curves. A. García also goes further to determine explicit equations for maximal curves; i.e. curves which attain the Hasse-Weil upper bound. These curves have similar equations to that of the Hermitian curve, but the exponent of x is now given by divisors of the original exponent in the Hermitian curve.

The Hermitian curve,

$$y^q + y = x^{q+1} \text{ over } \mathbb{F}_{q^2}(x, y)$$

is a maximal curve, and it also has the biggest possible genus. As shown in example 4.5, the genus of this curve is given by

$$g = \frac{1}{2}q(q-1)$$

As stated by Arnaldo García in this article, there is no known example of a maximal curve which cannot be covered by the Hermitian curve. But it is not yet known whether all maximal curves are in fact covered by Hermitian curves.

The Hermitian curve $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$ is the unique maximal curve with genus $g = \frac{1}{2}g(g-1)$, which is the maximum possible genus according to the Hasse-Weil upper bound.

Serre has shown that a curve over $\mathbb{F}_{q^2}$ covered by a maximal curve also over $\mathbb{F}_{q^2}$ is itself maximal. (A. García [6])

The curve over $\mathbb{F}_{q^2}$

$$y^q + y = x^m, \text{ where } m \text{ is a divisor of } (q+1)$$

is covered by the Hermitian curve $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$. So $y^q + y = x^m$ with $m|(q+1)$ is maximal. Nevertheless, this curve does not have maximum genus.

The genus of this curve is given by

$$g = \frac{1}{2}(m-1)(q-1)$$

If q is odd then $(q-1)$ is even and then $\frac{1}{2}(q-1)$ is an integer. As m is a divisor of $q+1$, m attains its largest value when $m=(q+1)/2$, so the largest genus of a curve of the form $y^q+y=x^m$ is,

$$g=\frac{1}{2}\left(\frac{q-1}{2}-1\right)=\frac{1}{4}(q-1)^2$$

This is the second largest possible genus for a maximal curve in $\mathbb{F}_{q^2}$.

Example 6.2

The curve $y^3+y=x^2$ is covered by the hermitian curve $y^3+y=x^4$.

$y^3+y=x^2$ is a maximal curve and using the Hasse-Weil bound we find that it has 16 rational places.

Looking back at the tables presented by van der Geer and van der Vlugt in [16] we can see that in the table for $p=3$, for $g=1$ and $q=3^2$, the entry is 16. A possible curve for that entry is therefore $y^3+y=x^2$.

□

With this method we can find the following examples. These examples can be used to define the lower bounds for the corresponding entries in the tables given in http: //wins.uva.nl/~geer, which to the time of writing this Thesis appear as "no information available". In fact, as the curves found are maximal, these entries no longer need a bound, they can be given by a unique entry, since the exact value of $N_q(g)$ is now known. As the curves are maximal, they attain the Hasse-Weil upper bound , which using the notation in [6] is given by

$$\#X(\mathbb{F}_{q^2})=q^2+1+2gq$$

Example 6.3

The curve $y^{25}+y=x^2$ over $\mathbb{F}_{25^2}$ has genus

$$g=\frac{1}{2}(2-1)(25-1)=12$$

and we can define

$$N_{5^4}(12)=1226$$

□

Example 6.4

The curve $y^7+y=x^4$ over $\mathbb{F}_{7^2}$ has genus

$$g=\frac{1}{2}(4-1)(7-1)=9$$

and we can define

$$N_{7^2}(9)=176$$

□

Example 6.5

The curve $y^{49} + y = x^2$ over $\mathbb{F}_{49^2}$ has genus

$$g = \frac{1}{2}(2-1)(49-1) = 24$$

and we can define

$$N_{49^2}(9) = 4754$$

□

Example 6.6

The curve $y^{11} + y = x^2$ over $\mathbb{F}_{11^2}$ has genus

$$g = \frac{1}{2}(2-1)(11-1) = 5$$

and we can define

$$N_{11^2}(9) = 232$$

□

Example 6.7

The curve $y^{11} + y = x^3$ over $\mathbb{F}_{11^2}$ has genus

$$g = \frac{1}{2}(3-1)(11-1) = 10$$

and we can define

$$N_{11^2}(9) = 342$$

□

Example 6.8

The curve $y^{11} + y = x^4$ over $\mathbb{F}_{11^2}$ has genus

$$g = \frac{1}{2}(4-1)(11-1) = 15$$

and we can define

$$N_{11^2}(9) = 452$$

□

6.3 Kummer Covers with many Rational Points

In this section we present the method given by van der Geer and van der Vlugt to construct curves over finite fields which are Kummer covers of $\mathbb{P}^1$. This method is one of the methods quoted by van der Geer and van der Vlugt in [16] for constructing explicit equations of curves with many points.

Here we are going to explain how this construction can be done by following one of the examples in [17], and by applying the method to construct new examples.

Broadly speaking, the method is based in splitting a polynomial $g = f_1 + f_2$ appropriately so that if we construct a rational function $f(x)$ using f_1 and f_2, this function $f(x)$ is Kummer nondegenerate and then the equation

$$y^{q-1} = f(x)$$

is a Kummer cover of the projective line $\mathbb{P}^1$.

As we are looking for covers with many rational points, $f(x)$ must satisfy some conditions.

1. With the first condition, the authors make sure that $f(x)$ is not a Kummer nondegenerate element.
2. The second condition "$f(x) = 1$ on a substantial subset $\mathbb{P}$ of $\mathbb{P}^1(\mathbb{F}_q)$" provides for a large number of rational places on the cover curve C.
3. With the third condition, the genus of C is kept within bounds.

Starting with a polynomial $R(x)$ in $\mathbb{F}_q[x]$,

$$R(x) = \sum_{i=0}^{r} a_i x^{p^i}$$

$$= x + a_1 x^p + a_2 x^{p^2} + a_3 x^{p^3} + a_4 x^{p^4}$$

Here we have set $r = 4$.

Now we want to split $R(x)$ into two parts $R_1(x)$ and $R_2(x)$ so that

$$R(x) = R_1(x) + R_2(x)$$

To do this van der Geer and van der Vlugt set

$$R_1(x) = \sum_{i=s}^{r} b_i x^{p^i} \text{ and } R_2(x) = \sum_{i=0}^{t} c_i x^{p^i}$$

where $0 < s < r$ and $t \leq s$.

We have set $r = 4$ above, so we can choose $s = 3$, then $R_1(x)$ becomes,

$$R_1(x) = b_3 x^{p^3} + b_4 x^{p^4}$$

That is, $R_1(x)$ consists of the part of the polynomial $R(x)$ with the p^3 and p^4 powers of x.

To construct $R_2(x)$, van der Geer and van der Vlugt set $t \leq s$. As we have set $s = 3$ we can choose $t \leq 3$, say $t = 3$. Then $R(x)$ can be written as,

$$R_2(x) = x + c_1 x^p + c_2 x^{p^2} + c_3 x^{p^3}$$

Now we note that $R_2(x)$ represents the part of the polynomial $R(x)$ with the p^0, p^1, p^2 and p^3 powers of x.

We also note that the coefficients in $R_1(x)$ of x^{p^3} is b_3 and the coefficient of x^{p^3} in $R_2(x)$ is c_3. As the sum $R_1(x) + R_2(x) = R(x)$ we deduce that

$$b_3 + c_3 \equiv a_3 \pmod{p}$$

The article works through an example of a construction of polynomials $R_1(x)$ and $R_2(x)$ starting with the polynomial $R(x) = x^{16} + x$. In this example, $r = 4$, $p = 2$ and the polynomial $R(x)$ is constructed over $\mathbb{F}_{16}[x]$. s is set as $s = 1$, as as $t \leq s$, we have $t = 1$.

With these conditions $R_1(x)$ and $R_2(x)$ are given by,

$$R_1(x) = \sum_{i=s=1}^{r=4} b_i x^{2^i} = b_1 x^2 + b_2 x^4 + b_3 x^8 + b_4 x^{16}$$

$$R_2(x) = \sum_{i=0}^{t=1} c_i x^{2^i} = c_0 x + c_1 x^2$$

In the example the authors choose to make some of the coefficients equal to 0 so that,

$$R_1(x) = x^2 + x^{16}$$

$$R_2(x) = x + x^2$$

adding up these two polynomial we obtain

$$R(x) = R_1(x) + R_2(x) = x^{16} + 2x^2 + x = x^{16} + x,$$

since $R(x) \in \mathbb{F}_2[x]$.

Now that the two polynomial $R_1(x)$ and $R_2(x)$ have been found, it is straightforward to construct the Kummer cover as stated at the beginning of this section.

$$y^{15} = \frac{x^{16} + x}{x^2 + x}$$

Now we are going to construct a similar example according to the method in the article.

Example 6.9

This time we are going to consider $R(x) = x + x^9$ in $\mathbb{F}_9[x]$. Here we have $p = 3$ and $r = 2$. Like in the first example given by van der Geer and van der Vlugt we set $s = t = 1$.

As before we write $R_1(x)$ and $R_2(x)$ as,

$$R_1(x) = \sum_{i=s=1}^{r=2} b_i x^{3^i} = b_1 x^3 + b_2 x^9$$

$$R_2(x) = \sum_{i=0}^{t=1} c_i x^{3^i} = c_0 x + c_1 x^3$$

we now choose convenient coefficients b_1, b_2, c_0 and c_1 and write

$$R_1(x) = x^3 + x^9 \text{ and } R_2(x) = x + 2x^3$$

The rational function we are looking for is given by

$$f(x) = -\frac{R_1(x)}{R_2(x)}$$

$$= \frac{x^3 + x^9}{x + 2x^3}$$

$$= \frac{x^9 + x^3}{x^3 + 2x}$$

Hence the curve C given by

$$y^8 = \frac{x^9 + x^3}{x^3 + 2x}$$

is a Kummer cover of the projective line $\mathbb{P}^1$.

A formula for the genus of such a Kummer cover C of $\mathbb{P}^1$ is given by,

$$g = \{(p^{r-s} + p^t - \delta - 1)(q-2) - \delta p^{\gcd(m,s)} - p^{\gcd(m,r-t)} + 2\delta + 2\}/2 \quad (6.1)$$

where δ is the number of common solution of $R_1(x)$ and $R_2(x)$.

Hence the genus of the curve found in this example is given by

$$g = \{(3^1 + 3^1 - 1 - 1)(9-2) - 3 - 3 + 2 + 2\}/2 = 13$$

The number of rational points on the cover curve is given by,

$$\mathbb{F} \subset (\mathbb{F}_q) \geq (p^r - \delta)(q-1) \quad (6.2)$$

So we know that the Kummer cover found is this example,

$$y^8 = \frac{x^9 + x^3}{x^3 + 2x}$$

has at least $(3^2 - 1)(9 - 1) = 64$ rational points.

□

In the tables in [16] we can see that in the table for $p = 3$, the entry for $g = 13$ and $q = 9$ reads 60-66. The source for this entry is the article [16] by van der Geer and van der Vlugt.

We now find that using this method for constructing Kummer covers provides us with a new lower bound for this entry, namely 64. In the updated tables that can be found online at http://wins.uva.nl/~ geer, van der Geer gives a new gound for $g = 13$ and $q = 9$. The new bound is 64-65. The reference article given for the lower bound 64 is in fact "Kummer covers with many rational points" [17].

Subspaces of Codimension 1

In this part of the article a subspace of $\mathbb{F}_{q=p^m}$ is considered, namely the $(m-1)$-dimensional subspace defined by

$$L = \{x \in \mathbb{F}_q : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} = 0\}, \text{ where } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) = x^{p^{m-1}} + \ldots + x^p + x$$

The polynomial $R(x) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) = \sum_{i=0}^{m-1} x^{p^i}$.

By a transformation $x \mapsto ax$ on $\mathbb{F}_q$ with $a \in \mathbb{F}_q^*$, any codimension 1 space can be transformed into the subspace L above.

A slightly different method is given at this point to split the polynomial $R(x)$ into the two polynomials $R_1(x)$ and $R_2(x)$: $R_1(x) = \sum_{i=s}^{m-1} x^{p^i}$ and $R_2(x) = \sum_{i=0}^{s-1} x^{p^i}$.

As before the curve is then given by

$$y^{q-1} = -\frac{R_1(x)}{R_2(x)}$$

Using the formulas for the genus and number of rational points given by 6.1 and 6.2, the article gives a proof and defined the genus and number of rational points by the following proposition that we quote here:

For $m \geq 3$ and $0 < x < m - 1$ such that $\gcd(m, s) = 1$ the curve C_m given by

$$y^{q-1} = -(x^{p^{m-1-s}} + \ldots + x)^{p^s}/(x^{p^{s-1}} + \ldots + x)$$

has genus

$$g(C_m) = \{(p^{m-1-s} + p^{s-1} - 2)(q - 2) - 2p + 4\}/2$$

and

$$\#C_m(F_q) = \begin{cases} (p^{m-1}-1)(q-1) & \text{if } pm \text{ odd and } p \nmid (s(m-s) \\ (p^{m-1}-1)(q-1) \quad +(p-1) & \text{if } pm \text{ odd and } p \mid s(m-s) \\ (p^{m-1}-1)(q-1) \quad +2(p-1) & \text{if } pm \text{ even and } p \nmid s(m-s) \\ (p^{m-1}-1)(q-1) \quad +3(p-1) & \text{if } pm \text{ even and } p|s(m-s) \end{cases}$$

According to this method the article gives several example. We now produce two new examples using this method.

Example 6.10

In this example we will consider as a subspace of $\mathbb{F}_{81}$, the 3 dimensional subspace

$$L = \{x \in \mathbb{F}_{81} : \mathrm{Tr}_{\mathbb{F}_{81}/\mathbb{F}_3}(x) = 0\}, \text{ where } \mathrm{Tr}_{\mathbb{F}_{81}/\mathbb{F}_3}(x) = x^{3^3} + x^{3^2} + x^3 + x$$

$$= x^{27} + x^9 + x^3 + x$$

So we have chosen $p = 3$, $m = 4$. Now we have $R(x) = x^{27} + x^9 + x^3 + x$. To split this polynomial in $R_1(x)$ and $R_2(x)$, we choose $s = 2$, so we obtain

$R_1(x) = \sum_{i=2}^{3} x^{p^i} = x^{3^2} + x^{3^3} = x^9 + x^{27}$

$R_2(x) = \sum_{i=0}^{1} x^{p^i} = x^{3^0} + x^{3^1} = x + x^3$

so we find the curve C_4 over $\mathbb{F}_{81}$ given by

$$y^{80} = -\frac{x^{27} + x^9}{x^3 + x}$$

We now find the genus and the rational points on this curve using the formulas given by the article.

$g(C_4) = \{(3^{4-1-2} + 3^{2-1})(81-2) - 2 \times 3 + 4\}/2$

$= \{(3+3-2)(79)-6+4\}/2$

$= 157$

$p_m = 3 \times 4 = 12$ is even and $s(m-s) = 2(4-2) = 4$ so $p = 3$ does not divide $s(m-s) = 4$, so the number of rational points is given by

$\#C_4(\mathbb{F}_{81}) = (p^{m-1}-1)(q-1) + 2(p-1)$

$= (3^3-1)(80) + 2(2) = 2084$

The Hasse-Weil upper bound for genus $g = 157$ and $q = 81$ is 2908.

□

6.4 Constructing Curves over Finite Fields with Many Points by Solving Linear Equations

In this section we present another method for constructing curves with many rational points. This time the method is based in the use of Artin-Schreier extensions.

Choosing a base curve C with many rational points, several curves C_{f_i} are constructed by using Artin-Schreier extensions. These are extensions of the function field $K(C)$ such that $K(C_{f_i}) = K(C)(z)$, where $z^p - z = f_i$.

The functions f_i are Artin-Schreier non-degenerate.

From the set of rational points of the base curve C, a preferably large subset $\mathcal{P}$ is chosen. Using places that are not in $\mathcal{P}$, a divisor is defined. That is, the support of the divisor D is disjoint from the set $\mathcal{P}$.

A covering C_F of the curve C is then constructed as a normalized product of C_f curves.

The most interesting feature about this construction of a covering C_F is that the places in C_F that lie over the places in $\mathcal{P}$ of C , are completely split. With this we will obtain in C_F many rational places. In fact, the degree of the extension of the function field of C_F over the function field of F will also tell us how many rational points lie over rational points in our selected subset of rational places of C, $\mathcal{P}$. It is therefore understandable that we want $\mathcal{P}$ to be a large set. As we have explained above, C_F is obtained from the normalized product of Artin-Schreier extensions C_{f_i}.

In their article, van der Geer and van der Vlugt impose certain conditions on the functions f_i that will later lead to the desired result.

The first condition is as follows,

$$F \cap \{g^p - g \ : \ g \in K(C)\} = \{0\}$$

with this condition, they assure that the functions f_i are indeed Artin-Schreier nondegenerate.

The second condition that f_i must satisfy is

$$\mathrm{Tr}_{q/p}(f(P)) = 0 \text{ for all } P \in \mathcal{P}$$

with this condition we know that all the places $P \in \mathcal{P}$ will be completely split in the extension.

In the article van der Geer and van der Vlugt give several similar examples of the construction of appropriate Artin-Schreier extensions which give rise to covering curves C_F.

Here we analyze example 3. In this example the elliptic curve defined by $y^2 + y = x^3$ over $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ is considered. This is a Hermitian curve and it attains the maximum possible number of rational points, in this case $\#C(\mathbb{F}_4) = 9$. The authors choose to leave 8 of this rational points belonging to $\mathcal{P}$ (the set of rational places that will split completely in the extension). The remaining place is $P_\infty = [0, 1, 0]$ is used to define the divisor D with support disjoint from $\mathcal{P}$, so $D = 11P_\infty$.

Van der Geer and van der Vlugt produce a table showing suitable elements f_i which are Artin-Schreier nondegenerate and which are then closed to construct the curves C_{f_i} $(i = 1, \ldots, 5)$. As we explained before, these functions must satisfy

$$\mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(f_i(P)) = 0, \text{ where } P \in \mathcal{P} \tag{6.3}$$

to achieve that the places lying over $P \in \mathcal{P}$ split completely in the cover curve C_F.

That this is satisfied can be seen in the following example.

Example 6.11

First we find that $P = [1, 0, 1]$ is a rational point of the curve defined by $y^2 + y = x^3$ so $[1, 0, 1] \in \mathcal{P}$ and we check that the condition given by 6.3 is satisfied:

$$\mathrm{Tr}(f_1([1, 0, 1])) = \mathrm{Tr}_{4/2}(1) = 1^2 + 1 = 0$$

$$\mathrm{Tr}(f_2([1, 0, 1])) = \mathrm{Tr}_{4/2}(\alpha) = (\alpha)^2 + \alpha = 0$$

$$\mathrm{Tr}(f_3([1, 0, 1])) = \mathrm{Tr}_{4/2}(0) = 0^2 + 0 = 0$$

$$\mathrm{Tr}(f_4([1, 0, 1])) = \mathrm{Tr}_{4/2}(1) = 1^2 + 1 = 0$$

$$\mathrm{Tr}(f_5([1, 0, 1])) = \mathrm{Tr}_{4/2}(\alpha) = \alpha^2 + \alpha = 0$$

It can be checked that for the 7 remaining rational points in $\mathcal{P}$, the condition 6.3 is satisfied. Hence we know that all these places split in the cover curve C_F.

□

The genus of each of the curve C_{f_i} can be found using the formula for the genus of an Artin-Schreier extension given by equation 5.7 when explaining artin-Schreier extensions in chapter 5.

The number of rational points $\#C_{f_i}(\mathbb{F}_4)$ is given by the formula

$$\#C_f(\mathbb{F}_q) = p(n - \delta) + \varepsilon_f$$

given in the article.

In example 3 of the article, $p = 2$. n is the number of places in $\mathcal{P}$, so $n = 8$. $\delta = \#(supp(D) \cap \mathcal{P})$ so $\delta = 0$, and ε_f is the number of rational points of C_f lying over points in $supp(D)$. In this case the support of D only consists of P_∞, so $\varepsilon_f = 1$.

Thus,

$$\#C_{f_i}(\mathbb{F}_4) = 2(8-0)+1 = 17$$

which is in fact the number calculated in the table in this example given in the article.

To end their example, van der Geer and van der Vlugt consider normalized products of combinations of different C_{f_i} $(i = 1, \ldots, 5)$, which produce different cover curves C_F. They calculate the genera of these C_F and their numbers of rational points.

The genus of these cover curves C_F is obtained by using the formula given in the article,

$$g(C_F) = g(C) + \sum_{f \in \mathbb{P}(F)} (g(C_f) - g(C))$$

For their first calculation they obtain the best possible number of rational points for that genus g and q. With this new method, van der Geer and van der Vlugt expect to find new entries and improvements to the tables in [16] although to the time of publishing this article, the calculations had not yet been made.

6.5 Applications to Coding Theory

Error-correcting codes have many technical applications which are part of our everyday life.

Codes present the information as a very long sequence of symbols. These symbols belong the a finite set called the alphabet of the code. The information encoded by these symbols is sent over a noisy-channel, but when they are received there is some probability that some of the symbols have been changed over the way. For this reason, some redundant symbols are sent giving us the opportunity to find out which symbols have been changed in their journey through the noisy-channel.

Here we will consider a code C over the alphabet $\mathbb{F}_q$, where $\mathbb{F}_q$ is the finite field with q elements. The elements of C will be called **codewords**. A codeword in C is given by $a = (a_1, \ldots, a_n)$ where each $a_i \in \mathbb{F}_q$. Thus the code C is formed by a set of codewords $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$, $c = (c_1, \ldots, c_n) \ldots$ which constitute a nonzero linear subspace of the vector space $\mathbb{F}_q^n$.

For a linear code $C \subseteq \mathbb{F}_q^n$ over $\mathbb{F}_q$, n is the **length** of the code. The number of codewords in C, that is, the dimensions of the linear subspace of $\mathbb{F}_q^n$ which constitutes C is denoted by $dim(C) = k$.

A code over $\mathbb{F}_q$ with length n and dimension k is called a $[n, k]$ code over $\mathbb{F}_q$. Note that $1 \leq k \leq n$.

The **Hamming weight** of a codeword $a \in \mathbb{F}_q^n$ is given by the number of nonzero coordinates of a.

The **minimum distance** for a linear code C over $\mathbb{F}_q$ is the smallest weight of any codeword in C.

A code with length n, dimension k and minimum distance d is called a linear $\{n, k, d\}$ code over $\mathbb{F}_q$.

6.5.1 Goppa Codes

In the period from 1977 to 1982, Goppa found important applications of algebraic curves over finite fields with many rational points to coding theory. Goppa codes are also called algebraic-geometry codes of AG codes.

The key idea for the construction of Goppa codes is to associate a code to a set of places $P_1, \ldots, P_n \in \mathbb{P}_F$ (where F is an algebraic field) by evaluating a set of rational functions on these places P_i.

More precisely, we consider the functions field $F/\mathbb{F}_q$ of a curve with genus g. We also consider a number n of rational places $P_1, \ldots, P_n$ of F with $n > g$.

Now let G be a divisor of F with support disjoint from the set of place $P_1, \ldots, P_n$.

In chapter 4, with equation 4.1, we defined the Riemann-Roch space of a divisor as,

$$\mathcal{L}(G) = \{z \in F \mid (z) + G \geq 0\} \cup \{0\}$$

we now note that for $z \in \mathcal{L}(G)$ it holds that $v_{P_i}(z) \geq 0$, $i = 1, \ldots, n$ since $suppG \cap \{P_1, \ldots, P_n\} = \emptyset$.

Hence we can define a linear map $\gamma : \mathcal{L}(G) \to \mathbb{F}_q^n$ by,

$$\gamma(z) = (z(P_1), \ldots, z(P_n)) \text{ for all } z \in \mathcal{L}(G)$$

$z(P_i)$ represent an element of the residue class field of P_i, K_{P_i}. As P_i is a rational place, then $\deg P_i = 1$. As we are considering the function field $F/\mathbb{F}_q$, we deduce that with $\deg P_i = 1$, $K_{P_i} = \mathbb{F}_q$.

From this we deduce that $z(P_i) \in \mathbb{F}_q$.

The image of the linear map $\gamma : \mathcal{L}(G) \to \mathbb{F}_q^n$ defined above is a linear subspace of $\mathbb{F}_q^n$. This sequence constitutes the code $C(P_1, \ldots, P_n; G)$.

Thus, for the code $C(P_1, \ldots, P_n; G)$, the codewords are

$$(z_1(P_1), \ldots, z_1(P_n)), (z_2(P_1), \ldots, z_2(P_n)), \ldots, (z_k(P_1), \ldots, z_k(P_n))$$

where $z_1, z_2, \ldots, z_k \in \mathcal{L}(G)$.

The alphabet for this code are the different $z(P_i) \in \mathbb{F}_q$.

The number of codewords, i.e., the dimension of the code $C(P_1, \ldots, P_n; G)$ is given by the number of functions $z_1, z_2, \ldots, z_k \in \mathcal{L}(G)$, which is k. k is by definition the dimension of the Riemann-Roch space $\mathcal{L}(G)$,

$$k = dim\mathcal{L}(G) = \ell(G)$$

It is straightforward to see that the length of the code is given by n since we are considering n rational places $P_1, \ldots, P_n$.

The minimum distance d of the code $C(P_1, \ldots, P_n; G)$ is given by

$$d \geq n - \deg(G)$$

If the weight of one of the codewords $\gamma(z)$ is d, then $z(P_i)$ becomes zero for $n - d$ places P_i. So $(z) + G - P_{i_1} - \ldots - P_{i(n-d)} \geq 0$.

Recalling that the degree of all principal divisors is zero, we can compute the degree of $(z) + G - P_{i_1} - \ldots P_{i(n-d)}$,

$$\deg G - (n-d) \geq 0$$

which shows that the minimum distance of the code $C(P_1, \ldots, P_n; G)$ is given by

$$d \geq n - \deg(G)$$

with this we have defined the Goppa code $C(P_1, \ldots, P_n; G)$ which is a linear $[n, k, d]$ code over $\mathbb{F}_q$.

For the implementation of such a code, we need to produce a generator matrix. Following the instructions above, if $\{z_1, \ldots, z_k\}$ is a basis of $, (G)$ over $\mathbb{F}_q$ then a generator matrix for the code $C(P_1, \ldots, P_n; G)$ is given by the $k \times n$ matrix,

$$\begin{pmatrix} z_1(P_1) & z_1(P_2) & \ldots & z_1(P_n) \\ z_2(P_1) & z_2(P_2) & \ldots & z_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ z_k(P_1) & z_k(P_2) & \ldots & z_k(P_n) \end{pmatrix}$$

Thus, constructing a generator matrix becomes a question of finding bases of the Riemann-Roch space $\mathcal{L}(G)$.

It also becomes clear why the construction of Goppa codes has spurred the interest in constructing curves over finite fields with many rational points.

6.5.2 NXL Codes and XNL Codes

As we have explained, Goppa codes are constructed using the rational places of a given function field.

Niederreiter, Xing and Lam go a step further by devising two new constructions of codes: the NXL codes and the XLN codes.

NXL Codes

In the construction of NXL codes, Niederreiter, Xing and Lam use not only rational places, i.e., places of degree one, but also places of higher degree.

For the construction of NXL codes two divisors G_1 and G_2 of F are defined such that $G_1 \leq G_2$.

The Riemann-Roch space $\mathcal{L}(G_1)$ is a linear subspace of $\mathcal{L}(G_2)$.

The length of the code is given

$$n = \ell(G_2) = dim\mathcal{L}(G_2)$$

The alphabet is given by elements of $\mathcal{L}(G_1)$ and the number of codewords is

$$K = \ell(G_1) = dim\mathcal{L}(G_1)$$

XNL Codes

The construction of XNL codes has been introduced by Xing, Niederreiter and Lam. These codes constitute an important generalization of Goppa's construction.

Like the NXL codes, XNL codes use places of arbitrary degree and not only rational places.

The fundamental idea in the construction of XNL codes is that the data used are obtained not only from the function field, but also from short linear codes as inputs, which then result in a longer linear code.

Open Questions

From Goppa's construction of the Goppa codes, there has been great interest in finding curves with many rational places, i.e., places of degree 1. Now that Niederreiter, Xing and Lam have constructed the NXL and XNL codes, which use places of higher degree, a similar interest could arise for finding curves with places of higher degree. A wide field of research could be opened by finding new methods that provide us with such curves.

Another interesting field of research is given by the question of how geometric properties can be used to decode Goppa codes.

Bibliography

[1] M. F. Atiyah and I. G. MacDonald *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Massachusetts, 1969.

[2] D. Cox, J. Little and D. O'Shea *An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer-Verlag, New York-Berlin-Heidelberg, 2007.

[3] D. S. Dummit and R. M. Foote *Abstract Algebra*, Prentice Hall, 1991

[4] W. Fulton *Algebraic Curves*, Benjamin, New York, 1969.

[5] J. A. Gallian *Contemporary Abstract Algebra*, Fourth Edition. Houghton Mifflin, Boston 1998. Goppa

[6] A. García *Curves over Finite Fields Attaining the Hasse-Weil Upper Bound*, Progress in Mathematical Physics, Birkhäuser-Verlag, Basel, v. 202, p. 199-205, 2001

[7] R. Hartshorne *Algebraic Geometry*, Springer-Verlag, New York, 1977

[8] J. W. P. Hirschfeld, G. Korchmáros and F. Torres *Algebraic Curves over a Finite Field*, Princeton Series in Applied Mathematics, ——, 2008

[9] F. Kirwan *Complex Algebraic Curves*, Cambridge Univ. Press, Cambridge, 1992

[10] C. Moreno *Algebraic Curves over Finite Fields*, Cambridge Tracts in Mathematics **97**, Cambridge Univ. Press, Cambridge, 1991

[11] H. Niederreiter, C.P. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, London Mathematical Society Lecture Note series **285**, Cambridge Univ. Press, Cambridge, 2001.

[12] M. Reid, *Undergraduate Algebraic Geometry*, Cambridge Univ. Press, Cambridge, 1988.

[13] J. H. Silverman *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

[14] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993

[15] G. van der Geer and M. van der Vlugt, *Constructing curves over finite fields with many points by solving linear equations*, Applications of Curves over Finite Fields (M.D. Fried, ed.), Contemporary Math., Vol. 245, pp. 41-47, American Math. Society, Providence, RI,1999.

[16] G. van der Geer and M. van der Vlugt, *Tables of curves with many points*, Math. Comp. 69, 797-810 (2000)

[17] G. van der Geer and M. van der Vlugt, *Kummer covers with many points*, Finite Fields Appl. 6, 327-341 (2000)

[18] H. van Lint and G. van der Geer, *Introduction to coding theory and algebraic geometry*, Birkhäuser, Basel, Boston, Berlin, 1988

[19] J. L. Walker, *Codes and Curves*, AMS in the IAS/Park City Mathematical Subseries of the Student Mathematical Series. 200

LINKÖPING UNIVERSITY
ELECTRONIC PRESS

LINKÖPINGS UNIVERSITET

Copyright

The publishers will keep this document online on the Internet - or its possible replacement - for a period of 25 years from the date of publication barring exceptional circumstances. The online availability of the document implies a permanent permission for anyone to read, to download, to print out single copies for your own use and to use it unchanged for any non-commercial research and educational purpose. Subsequent transfers of copyright cannot revoke this permission. All other uses of the document are conditional on the consent of the copyright owner. The publisher has taken technical and administrative measures to assure authenticity, security and accessibility. According to intellectual property law the author has the right to be mentioned when his/her work is accessed as described above and to be protected against infringement. For additional information about the Linköping University Electronic Press and its procedures for publication and for assurance of document integrity, please refer to its WWW home page: http://www.ep.liu.se/

Upphovsrätt

Detta dokument hålls tillgängligt på Internet - eller dess framtida ersättare - under 25 år från publiceringsdatum under förutsättning att inga extraordin"ara omständigheter uppstår. Tillgång till dokumentet innebär tillstånd för var och en att läsa, ladda ner, skriva ut enstaka kopior för enskilt bruk och att använda det oförändrat för ickekommersiell forskning och för undervisning. överföring av upphovsrätten vid en senare tidpunkt kan inte upphäva detta tillstånd. All annan användning av dokumentet kräver upphovsmannens medgivande. För att garantera äktheten, säkerheten och tillgängligheten finns det lösningar av teknisk och administrativ art. Upphovsmannens ideella rätt innefattar rätt att bli nämnd som upphovsman i den omfattning som god sed kräver vid användning av dokumentet påovan beskrivna sätt samt skydd mot att dokumentet ändras eller presenteras i sådan form eller i sådant sammanhang som är kränkande för upphovsmannens litterära eller konstnärliga anseende eller egenart. För ytterligare information om Linköping University Electronic Press se förlagets hemsida http://www.ep.liu.se/

© 2010, Carmen Rovi