Riemann Hypothesis for function fields

Nivedita
Chennai Mathematical Institute

May-June 2009

Contents

Abstract

This report (a summary of the work done in Ecole Normale Superieure under the guidance of Professor Olivier Wittenberg) presents Enrico Bombieri's proof of the Riemann Hypothesis for function fields.

The first section is devoted to introducing the notions of Picard group, divisors et al, the second section derives the analogues of the various well known properties of the Riemann-zeta function and the third section contains the actual proof which largely relies on the clever use of the Riemann-Roch theorem, a proof of which is included in the appendix. The Serre bound, an improvement of the Weil bound with the latter being equivalent to the Riemann Hypothesis, is also presented at the end.

Chapter 1

Preliminaries

1.1 Function fields

K is said to be a *function field* in one variable over F if it is a finitely generated field extension of transcendence degree 1 over F (ie) $\exists x \in K$ such that $[K : F(x)]$ is finite.

If F is algebraically closed in K, then F is called the *constant field* of K. This situation is useful because it implies that for any $y \in K \setminus F$, $[K : F(y)]$ is again finite. To see this, note that as F is the constant field of K, y is transcendental over F and since it is a one degree transcendental extension, y is algebraic over $F(x)$. This gives us that $g(x, y) = 0$ for some $g \in F[X, Y]$ but $g \notin F[Y]$. Thus x is algebraic over $F(y)$ which implies $[F(x, y) : F(y)] < \infty$. We know $[K : F(x, y)] \leq [K : F(x)] < \infty$ which proves that $[K : F(y)] < \infty$.

This condition is not asking for much because E (denoting the algebraic closure of F in K) is a finite extension of F ($[E : F] = [E(x) : F(x)] \leq [K : F(x)] < \infty$) and so in most cases we can replace F by E to get a function field K with the base field as its constant field.

It turns out that we can always choose a $w \in K$ where $K/F(w)$ is a separable finite extension if F is a perfect field of characteristic $p > 0$.

A proof would proceed as follows : K is finitely generated over F, say $K = F(x, x_1, \ldots, x_r)$. As the degree of transcendence of K/F is 1, x_1 is algebraic over $F(x)$. Thus let $g(t, u)$ be an irreducible polynomial in $F[t, u]$ which satisfies $g(x, x_1) = 0$. If only p^{th} powers of t, u occur in g, then as F is perfect of characteristic p, g is not irreducible in $F[t, u]$. So, say t doesn't occur as a p^{th} power somewhere. This implies that x is separable over $F(x_1)$ as it is a root of $h = g(t, x_1)$, a separable polynomial in $F(x_1)[t]$. And as x is separable over $F(x_1)$, it is also separable over $F(x_1, x_2, \ldots, x_n)$. The number of generators of $F(x_1, x_2, \ldots x_n)$ is lesser and one can induct on the number of generators.

A function field field in one variable over a finite constant field is called a *global function field.*

Hereforth K will refer to a global function field over F, the field of q elements with characteristic $p > 0$. K as described above can also be realized as the function field of a smooth projective curve C defined over base field F and from now on we switch back and forth between the language of function fields and curves as and when is neccesary, though overall most of the proofs are in terms of finitely generated function fields. The interested reader is invited to read the chapter entitled *Language of curves* given in the appendix where we give a brief introduction to projective curves and the correspondences between curves and function fields.

1.2 The zeta function

The Riemann-zeta function, named after the german mathematician Bernhard Riemann, as is well known is defined to be

$$\zeta(s) := \sum_{n \in \mathbb{N}} \frac{1}{n^s}$$

Here $\mathbb{N}$ refers to the set of strictly positive natural numbers, which can be realized as the set of all non-negative combinations of primes under multiplication by using the fundamental theorem of arithmetic. We would now like to analogously define Riemann-zeta function for K which invokes the need to introduce the concept of a *prime of* K.

1.2.1 Primes and Divisors

A *prime of* K refers to a pair (R, P) where R is a discrete valuation ring (which is nothing but a principal ideal domain with unique maximal ideal) with maximal ideal P such that the quotient field of R is K. This fits in with our usual notion of a prime of $\mathbb{Z}$ as one can check that indeed the only discrete valuation rings with fraction field $\mathbb{Q}$ are $R_p = \{\frac{a}{b} | \operatorname{GCD}(a,b) = 1, p \not| b\}$ (where $P \cap \mathbb{Z} = p\mathbb{Z}$) for all primes p.

It turns out that $F \subseteq R$ because any for $f \in F$, we have $f^q = f$. And hence $qv(f) = v(f)$ where v refers to the valuation[1] given by P on K which implies that $v(f) = 0$ and hence it belongs to R.

We generally drop the R when referring to the prime and denote it by P instead.

Let S_K denote the set of all primes P of K.

To each prime , we assign a *degree* which is defined to be the degree of the field extension $\frac{R}{P}/F$ (ie) $[\frac{R}{P} : F]$. The following proposition shows that this is indeed a finite number.

Proposition 1.1. *Degree of P, a prime of K is finite. In fact,*

$$\left[\frac{R}{P} : F\right] \leq [K : F(y)],$$

for any $y \neq 0 \in P$.

Proof. As remarked in the previous section,

$$[K : F(y)] < \infty \forall y \notin F,$$

and $P \cap F = (0)$. Pick any m F-linearly independent elements of $\frac{R}{P}$, say $u_1 + P, u_2 + P, \ldots, u_m + P$. We will show that $u_1, u_2 \ldots, u_m$ are $F(y)$ linearly independent, which will prove the proposition.

If they are not, let $f_1 u_1 + \ldots + f_m u_m = 0$ for $f_i \in F[y]$. Without loss of generality one may assume that y doesn't divide f_i for some i (Divide through out by a power of y if originally $y|f_i$ for all i). As $y \in P$ and y doesn't divide f_i, we get a non trivial relation for $u_1 + P, \ldots, u_m + P$ over F which is a contradiction.

□

The free abelian group generated by primes of K is called the *divisor group* which we shall denote by $\mathcal{D}_K$. This is the exact analogue of the positive rationals $\mathbb{Q}^*_+$.

[1] Refer to the chapter on discrete valuation rings in the appendix.

A divisor $D = \sum_{P \in S_K} n(P)P$ is termed *effective* (or $D \geq 0$) if $n(P) \geq 0$ for all primes P. We can hence define a partial order on $\mathcal{D}_K$ as

$$D_1 \geq D_2 \iff D_1 - D_2 \geq 0$$

The *degree* of a divisor D can be defined by naturally extending the defintion of the degree of primes as

$$D = \sum_P n(P)P \implies \deg(D) = \sum_P n(P)\deg(P).$$

To each effective divisor, we assign what is called a *norm* as follows :

$$ND = q^{\deg(D)} \text{ where } |F| = q$$

Note that norm is multiplicative (ie) $N(A+B) = N(A)N(B)$.And finally, we define the zeta function for K to be

$$\zeta_K(s) := \sum_{A \geq 0} \frac{1}{(NA)^s}$$

where A runs over all effective divisors of K.

Using the fact that $\mathcal{D}_K$ is the free abelian group generated primes of K, we can write down a formal expression of an eulerian product for ζ_K as

$$\begin{aligned}
\zeta_K(s) &= \sum_{A \geq 0} \frac{1}{(NA)^s} \\
&= \prod_{P \in S_K} \left(1 + \frac{1}{(NP)^s} + \frac{1}{(NP)^{2s}} + \dots\right) \\
&= \prod_{P \in S_K} \frac{1}{1 - (NP)^{-s}}
\end{aligned}$$

which matches with the eulerian product for the usual Riemann-zeta function.

1.2.2 The Picard Group

Any prime P of K gives a valuation on K as follows:

$$\operatorname{ord}_P(r) = \max\{n | r \in P^n\} \text{ for } r \in R,$$

which can be extended to all of K naturally.

If $\operatorname{ord}_P(a) > 0$, then a is said to have a *zero* at P and if $ord_P(a) < 0$, a is said to have a pole at P.

Now, to every element of K^*, we associate a divisor of K using the map below.

$$\operatorname{div} : K^* \to \mathcal{D}_K, a \rightsquigarrow \sum_{P \in S_K} \operatorname{ord}_P(a)P.$$

We denote $\operatorname{div}(a)$ by (a). The image of the div map is called $\mathcal{P}_K$ which refers to the group of *principal divisors*. It is apriori not clear that div is well-defined and hence we state the proposition below and give an outline of a proof.

Proposition 1.2.

- *Any $a \in K^*$ has only finitely many zeroes and poles.*
- $(a) = 0$ *iff* $a \in F^*$.
- *Any non constant a has atleast one zero and one pole.*
- *Degree of (a) = 0. In fact* $\deg((a)_0) = \deg((a)_\infty) = [K : F(a)]$ *where*

$$\begin{aligned} (a) &= (a)_0 - (a)_\infty \textit{ with} \\ (a)_0 &= \sum_{\operatorname{ord}_P(a)>0} \operatorname{ord}_P(a)P \textit{ and} \\ (a)_\infty &= -\sum_{\operatorname{ord}_P(a)<0} \operatorname{ord}_P(a)P. \end{aligned}$$

Proof. If $a \in F^*$, then it is clear that $(a) = 0$. If not, then $K/F(a)$ is a finite extension of degree n, say. Let U denote the integral closure of $F[a]$ in K. Then

U is a dedekind domain (Knapp, Basic Algebra gives a proof). Hence factorize the ideal Ua as

$$Ua = P_1^{e_1} P_2^{e_2} \dots P_k^{e_k}.$$

e_is are called the ramification indices of P_is.The localizations of R at the prime ideals P_i , denoted by $\mathcal{O}_{P_i}$ yield all the primes of K at which a has a zero. In fact $\mathrm{ord}_{P_i}(a) = e_i$. Poles of a correspond to zeroes of $\frac{1}{a}$ and hence we are done.

$(\mathcal{O}_{P_i}, P_i)$ lies above (X, Y) where X is the localization of $F[a]$ with respect to the multiplicatively closed set $F[a] \setminus (a)$ and Y its unique maximal ideal.

To see that $[K : F(a)] = \deg((a)_0) = \deg((a)_\infty)$, note that we are working over a finite field F which is therefore perfect. Then by a well known theorem in algebraic number theory, we have

$$n = \sum_{i=1}^{k} e_i f_i,$$

where $f_i = \left[\frac{\mathcal{O}_{P_i}}{P_i} : \frac{X}{Y}\right]$, the relative degree of P_i over the prime of $F(a)$ it lies above. However Y has degree 1 and so all is well.

□

We introduce an equivalence relation $\sim$ where

$$A \sim B \iff \exists a \in K^* \text{ such that } A - B = (a).$$

The *Picard group* denoted by Cl_K is $\frac{\mathcal{D}_K}{\mathcal{P}_K}$. Note that if $A \sim B$, then degrees of A and B are the same.

1.2.3 Riemann-Roch

With each divisor D, there exists an associated F vector-space

$$L(D) = \{k \in K^* | (k) + D \geq 0\} \cup (0)$$

We prove below, a little lemma, to show that it is indeed finite dimensional, whose dimension denoted $l(D)$ will be immensely useful later on. Before that, we would like to remark that if A and B are two equivalent divisors, (ie) $A = B + (h)$ for some $h \in K^*$, then $L(A) \cong L(B)$ by the isomorphism $k \rightsquigarrow kh$ and hence $l(A) = l(B)$ (if it is finite). Thus one can talk about $l(C)$ for $C \in Cl_K$.

Lemma 1.3. *$L(D)$ is a finite dimensional F-vector space.*

Proof. If $l(D) > 0$, there exists an $f \in K^*$ such that $D + (f) \geq 0$ and we have found an effective divisor equivalent to D. By the remark made above, $L(D + (f)) \cong L(D)$.

Hence without loss of generality, we can assume that $D \geq 0$. We will induct on the number of primes (counting multiplicities) n in the prime support of D, (ie) if $D = \sum_{P \in S_K} n(P)P$, then $n = \sum_{P \in S_K} n(P)$. For the base case $n = 0$, the divisor $D = 0$ and therefore $L(D) = F$ which has dimension 1.

Now let $D = A + P$, where $A \geq 0$ and P is a prime of K. By induction, assume $l(A)$ is finite. Fix an f in $L(A+P) \setminus L(A)$. Note that it has to be non-zero. Given any $g \in L(A + P)$, $\mathrm{ord}_P\left(\frac{g}{f}\right) \geq 0$ and hence is in $\mathcal{O}_P$.

Let us construct an F-linear map $\psi : L(D) \to \frac{\mathcal{O}_P}{P}$ which sends

$$g \rightsquigarrow \frac{g}{f} + P.$$

Since $\frac{\mathcal{O}_P}{P}$ is a finite dimensional F-vector space (dimension is the degree of P), it is enough to check that $\mathrm{kernel}(\psi)$ is finite dimensional.

It turns out that the kernel is $L(A)$. (It is easy to see that if g lies in the kernel, $\frac{g}{f} \in P$ and hence $g \in L(A)$) and hence by our induction hypothesis, we are done.

□

The following is an useful lemma which tells us that $L(D)$ of any divisor D with a negative degree is the zero vector space.

Lemma 1.4. *Let A be a divisor. If $\deg(A) \leq 0$ and $A \neq (a)$ for any $a \in K^*$, then $l(A) = 0$. If $A = (a)$, then $l(A) = 1$.*

Proof. If $A = (a)$, then by above remark, $L(A) \cong L(0)$. If $k \in L(0)$, then k has no poles. Therefore $k \in F$. And if $k \in F$, then clearly, $k \in L(0)$. Thus $L(0) = F$ and has dimension 1.

If $\deg(A) < 0$, and if $x \in L(A)$, by definition of $L(A)$, $(x) + A \geq 0$ which gives us a contradiction that

$$\deg((x) + A) = \deg((x)) + \deg(A) = \deg(A) \geq 0.$$

If $\deg(A) = 0$, and if $x \in L(A)$, by definition of $L(A)$, $(x) + A \geq 0$. Thus, let $(x) + A = \sum a(P)P$ where $a(P) \geq 0$ for all P. Now

$$\sum a(P)\deg(P) = \deg((x) + A) = \deg(A) = 0$$

which implies that $a(P) = 0$ for all P. Thus $A = (\frac{1}{x})$.

□

Bombieri's proof of the Riemann Hypothesis for function fields essentially hinges on the crucial use of the Riemann-Roch theorem, independently an important tool in complex analysis and algebraic geometry whose statement we give below and the proof in the appendix.

Theorem 1.5 (Riemann-Roch)**.** *Given K, there exists an integer $g \geq 0$ and a class C of the Picard group Cl_K such that for any divisor D and any $X \in C$, we have*

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

g is called the ***genus*** *of K and C, the* ***canonical class*** *of K.*

Corollary 1.6. *Some immediate and oft used corollaries are*

- $l(C) = g$.
- $\deg(C) = 2g - 2$.
- $\deg(D) > 2g - 2 \implies l(D) = \deg(D) - g + 1$.
- *If* $\deg(D) = 2g - 2$ *and $D \notin C$, then $l(D) = g - 1$.*

Proof.

- Take $D = 0$.
- Take $D = X$ for any $X \in C$.
- For any $X \in C$, $\deg(X - D) < 0$ and thus by lemma 1.4, $l(C - D) = 0$. Now apply Riemann-Roch.
- Similar reasoning as above. Only note that $X - D \neq (a)$ for any $a \notin K^*$

□

1.3 Notation

Here we fix the notations we will use in the remaining chapters.

- F denotes the finite field of $q = p^a$ elements where p is a prime.
- $\overline{F}$ is a fixed algebraic closure of F.
- F_n is the n^{th} degree extension of F which therefore sits inside $\overline{F}$.
- K is a function field in one variable over F with F as its constant field. (ie) K is a finitely generated one degree transcendental extension of F where F is algebraically closed in K.
- $\overline{K}$ denotes the compositum of fields K and $\overline{F}$, (ie) $\overline{K} = K\overline{F}$.
- K_n denotes the compositum of K and F_n which sits inside $\overline{K}$, (ie) $K_n = KF_n$.
- S_K is the set of all primes of K
- $\mathcal{D}_K$ refers to the divisor group of K
- Cl_K is the Picard group of K.
- Generally D refers to a divisor and P would mean a prime of K unless otherwise specified.

- Given a divisor D

$$L(D) = \{k \in K^* | (k) + D \geq 0\} \cup \{0\}$$

- $l(D) = \dim_F(l(D))$
- ord_P refers to the valuation on K given by a prime $(\mathcal{O}_P, P)$.
- g would in general mean the genus of K unless otherwise mentioned.

Chapter 2

The zeta function

The first question to ask is whether the various properties which hold good for ζ are true for ζ_K as well. In this chapter, we investigate the radius of convergence for ζ_K and find a rational expression which gives rise to an analytic continuation and find a functional equation satisfied by it.

$$\zeta_K(s) = \sum_{A \geq 0 \in \mathcal{D}_K} (NA)^{-s}.$$

Let us introduce some notation now

- a_n is the number of primes of K which have degree n.
- b_n is the number of effective divisors of degree n.

$$\begin{aligned} \zeta_K(s) &= \sum_{A \geq 0} (NA)^{-s} \\ &= \sum_{A \geq 0} q^{-\deg(A)s} \\ &= \sum_{n=0}^{\infty} b_n q^{-ns} \end{aligned}$$

Thus to get an estimate for the radius of convergence, we would like to bound b_n. Apriori, it is not even clear whether the b_ns so defined are finite quantities or not and hence we prove the following proposition:

Proposition 2.1. *Number of effective divisors of K of degree n is finite and hence number of primes of K of degree n is also finite.*

Proof. If L is an extension of some field T and (R, P) and (S, Q) are primes of L and T respectively, then (R, P) is said to lie *above* (S, Q) if $R \cap T = S$ and $P \cap T = Q$. And equivalently, (S, Q) is said to lie below (R, P).

As shown in 1.1, there exists an $x \in K$ such that $K/F(x)$ is a finite separable extension. If an effective divisor $D = \sum_P n(P)P$ has degree n, then clearly $n(P) \leq n$ for all primes P. Also if (S, Q) is the prime of $F(x)$ which lies below (R, P), then as

$$\deg(P) = \left[\frac{R}{P} : F\right] = \left[\frac{R}{P} : \frac{S}{Q}\right]\left[\frac{S}{Q} : F\right] \geq \deg(Q),$$

$\deg(Q)$ is also bounded above by n.

The idea now is to show that there are only finitely many primes in $F(x)$ of a given degree, that over a given prime of $F(x)$ there lies only finitely many primes of K and that every prime of K does indeed lie above a prime of $F(x)$. Showing these concludes the proof of this proposition.

Claim: There are only finitely many primes of $F(x)$ of degree n.

If (R, P) is a prime of $F(x)$, either $x \in R$ or $x \notin R$.

Consider the case when $x \in R$. This implies $F[x] \subseteq R$ as $F \subseteq R$. Therefore $P \cap F[x]$ is a non-zero prime ideal (nonzero because $P \neq (0)$ and hence there exists $\frac{r}{s} \in P$ where $r \neq 0, s \in F[x]$ and hence $s\frac{r}{s} = r \in P \cap F[x]$). Since $F[x]$ is a principal ideal domain, $P \cap F[x] = (f)$ where $f \in F[x]$ is a monic irreducible polynomial.

As one would expect, the localisation of $F[x]$ at the set $F[x] \setminus (f)$ (the localized ring, we shall temporarily call X) is R.

To see that, if possible take an element $\frac{r}{s} \in X$ where $r, s \in F[x]$ and $s \notin (f)$ such that $\frac{r}{s} \notin R$. As R is a DVR, this implies $\frac{s}{r} \in R$ and in fact is in P. As $r \in F[x] \subseteq R$, $r\frac{s}{r} = s \in P \cap F[x] = (f)$, a contradiction to the choice of s. This shows that $X \subseteq R$.

To prove the other inclusion, if possible take an element $\frac{r}{s} \in R$ which is not there in X where $r, s \in F[x]$ and are coprime to each other (Note that one can do this as fraction field of X and R are both $F(x)$ and $F[x]$ is a unique factorisation domain.) As X is a DVR, this would imply $\frac{s}{r}$ is in X and in fact in its maximal ideal. Thus s is also in the maximal ideal of X and hence $f|s$. Since $P \cap F[x] = (f)$, $s \in P$ also and thus $\frac{r}{s}s = r \in P \cap F[x] = (f)$ which gives us that $f|r$, a contradiction to the coprime nature of r and s.

The degree of X is $\left[\frac{F[X]}{(f)} : F\right]$ which is just the degree of the polynomial f.

For the second case, when $x \notin R$, we have $\frac{1}{x} \in R$ as it is a DVR. One can now use the automorphism $x \rightsquigarrow \frac{1}{x}$ of $F(x)$ to reduce to the case of a DVR R containing x. Anyway, finally we find that $F\frac{1}{x}]$ localised at the set $F[\frac{1}{x}] \setminus (\frac{1}{x})$ is the DVR R. And hence degree of $(R, P) = 1$. This prime is referred to as the *prime at infinity*.

Since there are only finitely many polynomials of degree n in $F[x]$ we are done proving the claim.

Claim: If L *is a finite separable extension of* T*, and* (S, Q) *is a prime of* T*, there are only finitely many primes of* L *which lie above it.*

Let U denote the integral closure of S in L. It is a well-known fact that U is a dedekind domain with fraction field L (Knapp, Basic Algebra). Let I denote the ideal generated by Q in U. Since U is a dedekind domain, let us factorize I into maximal ideals.

$$I = M_1^{k_1} M_2^{k_2} \dots M_r^{k_r}.$$

It turns out that the only maximal ideals of U are $M_1, M_2, \dots, M_r$. To see this, if M is any other maximal ideal of U, then $M \cap S$ is a non-zero prime ideal of S. (To see that it is non-zero, note that any $m \neq 0 \in M$ is integral over S and hence $m^t + s_{t-1}m^{t-1} + \dots + s_0 = 0$ with $s_0 \neq 0 \in S$ and hence $s_0 \in M \cap S$). The only non-zero prime ideal of a discrete valuation ring is its maximal ideal and hence $M \cap S = Q$ which would mean $I \subseteq M$ and hence $M = M_i$ for some $i \leq r$.

Let (R, P) be a prime of L which lies above (S, Q). As R is a discrete valuation ring with fraction field L, it is integrally closed in L. And R contains S which implies that it contains U also.

$P \cap U$ is a non-zero prime ideal of U. (For if $U \cap P$ is the zero ideal, it means that any $u \neq 0 \in U$ is a unit in R. The fraction field of U is L and hence $R = L$ which is not possible as R is a discrete valuation ring). Hence it is equal to M_i for some i.

We check that U_{M_i} (which is the ring U localised with respect to the set $U \setminus M_i$) is the DVR (R, P).

A check: If $\frac{r}{s} \in U_{M_i}$ where $r, s \in U$ and $s \notin M_i$ such that $\frac{r}{s} \notin R$, then because R is a DVR, $\frac{s}{r} \in R$ and in fact is in P. Thus $r\frac{s}{r} = s \in P$ which implies that $s \in P \cap U = M_i$, a contradiction to the choice of s. Thus $U_{M_i} \subseteq R$.

To prove the other inclusion, if $r \in R$ and $r \notin U_{M_i}$, then $\frac{1}{r} \in U_{M_i}$ as the latter is a DVR and in fact it belongs to the maximal ideal of U_{M_i}. Thus $\frac{1}{r} = \frac{s}{t}$ where $s \in M_i, t \in U \setminus M_i$. As $U \cap P = M_i$, $s \in P$ and hence $rs = \frac{t}{s}s = t \in P$ which implies $t \in P \cap U = M_i$, a contradiction.

And to conclude, U_{M_i}, the localisation of U with respect to $U \setminus M_i$ is a discrete valuation ring for any i as U is a dedekind domain and M_i is one of its maximal ideals.

If (R, P) is a prime of K, then it is a routine but weary check to see that $(R \cap F(x), P \cap F(x))$ is a prime of $F(x)$ which lies below it and hence we leave it to the conscientious reader to verify it.

□

To get a bound on b_n, we first estimate how many effective divisors are there in a given equivalence class of divisors and then count the number of equivalence classes of a given degree

Proposition 2.2. *Number of effective divisors in an equivalence class of divisors $\tilde{A}$ is $\frac{q^{l(\tilde{A})}-1}{q-1}$.*

Proof. Without loss of generality, choose a representative A of $\tilde{A}$ such that $A \not\geq 0$ (Choose an arbitrary representative B of the class and pick a prime P which does not lie in the support of B and set $A = B + (\frac{1}{f})$ where $f \in K^*$ has a zero at P).

Now $l(\tilde{A}) = 0$ if and only if there are no effective divisors in $\tilde{A}$. For if $l(A) > 0$, there exists an $f \in K^*$ such that $A + (f) \geq 0$ and hence you have found an equivalent effective divisor. And if there exists an effective divisor D equivalent to A, then $D = A + (f)$ where $f \in K^*$ as $A \not\geq 0$ and thus $f \in L(A)$. Hence $l(A) > 0$ and the proposition holds for $l(\tilde{A}) = 0$.

If it is not zero, then let us define a map ψ as follows :

$$\psi : L(A) \setminus \{0\} \rightarrow \text{ Effective divisors of } \tilde{A}$$

which sends $f \rightsquigarrow A + (f)$. ψ is well-defined and surjective. If $\psi(f) = \psi(h)$, then $A + (f) = A + (h)$ and hence $\frac{f}{h} \in F^*$. And conversely, $\psi(x) = \psi(xf)$ when $f \in F^*$.

Number of elements in the domain of ψ would be $q^{l(A)} - 1$ and each element in the range has a preimage set of cardinality $q - 1$ which gives us the required result.

□

Let the number of divisor classes of degree 0 be called h_K. This is called the *class number* of K.

Proposition 2.3. *Number of divisor classes of degree n is either 0 or h_K.*

Proof. Construct the deg map which assigns to each equivalence class of divisors, its degree

$$\deg : Cl_K \to \mathbb{Z},$$

and let the image of deg be $\delta\mathbb{Z}$. Note that $\delta \neq 0$ as $\deg(\tilde{P})$ for any equivalence class containing a prime P of K has degree atleast 1.

If $n \notin \delta\mathbb{Z}$, then number of divisor classes of degree n = 0. If n is a multiple of δ and $n \geq g$ where g is the genus of K, then by Corollary 1.6 of the Riemann-Roch theorem, for any divisor D of degree n

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

Thus each divisor class of degree n has an effective divisor representative (Pick $f \in K^* \cap L(D)$ and look at $D + (f)$) and hence number of divisor classes of degree n is atmost number of effective divisors of degree n which by proposition 2.1 is finite. Thus number of divisor classes of degree n for large enough n is finite.

Pick an $N \geq g$ and let $\mathcal{A} = \{A_1, A_2, \ldots, A_h\}$ be the set of all divisor classes of degree N where h is the number of effective divisor classes of degree N. For any other $n \in \delta\mathbb{Z}$, let $\mathcal{B} = \{B_\alpha\}_{\alpha \in I}$ for some index set I be the set of all divisor classes of degree n. Fix a B in $\mathcal{B}$.

Consider the set $X = \{B - B_\alpha + A_1\}_{\alpha \in I}$. Clearly any element of X is a divisor class of degree N and no two divisor classes in it are equivalent. Hence X is a subset of $\mathcal{A}$ which tells us that I is a finite set of cardinality atmost h. Similarly we can prove $h \leq |I|$. Thus for any $n \in \delta\mathbb{Z}$, number of divisor classes of degree n is a constant and as $0 \in \delta\mathbb{Z}$, the constant is nothing but h_K, the class number.

□

2.0.1 Convergence of the zeta function

Using the above propositions, we can, for large enough n (namely for any $n \geq 2g-1$), give an exact expression for b_n (!) as follows :

$$b_n = \begin{cases} h_K \frac{q^{n-g+1}-1}{q-1} & \text{if } n \in \delta\mathbb{Z}; \\ 0 & \text{else.} \end{cases} \tag{2.1}$$

This is because $n \geq 2g-1$ implies that $l(D) = \deg(D) - g + 1$ by Corollary 1.6 of the Riemann-Roch theorem where $\deg(D) = n$.

Since $\zeta_K(s) = \sum_{n=0}^{\infty} b_n q^{-ns}$, one can see that ζ_K converges absolutely for all s where $Re(s) > 1$.

Let us now examine the convergence of the euler product. $Re(s) > 1$.

$$\begin{aligned} \zeta_K(s) &= \prod_{P \in S_K} \frac{1}{1-(NP)^{-s}} \\ &= \prod_{n=1}^{\infty} (1-q^{-ns})^{-a_n} \end{aligned}$$

where recall that a_n is the number of primes of K of degree n. We now prove a little lemma concerning the convergence of infinite products.

Lemma 2.4. *If $x_1, x_2 \ldots, x_n, \ldots$ are complex numbers then $\prod_{n=1}^{\infty}(1-x_n)$ converges to a non-zero value if $\sum_{n=1}^{\infty} |x_n|$ converges.*

Proof. As $\sum |x_n|$ converges, for large enough n, $|x_n| < \frac{1}{2}$ and

$$\begin{aligned}|\log(1-x_n)| &= |x_n + \frac{{x_n}^2}{2} + \ldots| \\ &\leq |x_n| + \frac{|x_n|^2}{2} + \ldots \\ &\leq \frac{|x_n|}{1-|x_n|} \\ &\leq 2|x_n|.\end{aligned}$$

Thus $\sum_{n=1}^{\infty} |\log(1-x_n)|$ converges and hence the infinite product also converges (to the exponential of $\sum \log(1-x_n)$) to a non-zero value.

□

Thus for the euler product to converge for any s with $Re(s) > 1$, we would want the following to converge :

$$\sum_{n=1}^{\infty} a_n |q^{-ns}|$$

However $0 \leq a_n \leq b_n$ for any n and $\sum_{n=0}^{\infty} b_n q^{-ns}$ converges absolutely for $Re(s) > 1$ and hence we are through. In fact, the lemma shows that ζ_K has no zeroes in the region $Re(s) > 1$.

2.0.2 A rational expression for zeta

$$\zeta_K(s) = \sum_{n=0}^{\infty} b_n q^{-ns}.$$

By a change of variable, namely $u = q^{-s}$, we get

$$\zeta_K(s) = Z_K(u) = \sum_{n=0}^{\infty} b_n u^n.$$

Hereafter we shall interchangably use ζ_K and Z_K as and when is convenient.

It is a well known fact that there exists an analytic continuation of the Riemann-zeta function to all points of $\mathbb{C}$ except at $s = 1$ where it has a pole. The situation for ζ_K is even better as there exists a rational function which analytically extends it to the whole of the complex plane. We prove this in a series of steps during the course of which we shall also prove *Schmidt's* theorem which says that there exists a divisor of every degree.

Lemma 2.5. *K denotes (as usual) a global function field over F, a finite field of order q and characteristic p. Let $\delta\mathbb{Z}$ be the image of the map* $\deg : Cl_K \to \mathbb{Z}$ *which assigns to each divisor class, its degree. Then there exists a polynomial $L_K[u] \in \mathbb{Z}[u]$ with $L_K(0) = 1$ such that*

$$\zeta_K(s) = \frac{L_K(q^{-s})}{(1 - q^{-\delta s})(1 - q^{\delta(1-s)})}.$$

This holds for all s with $Re(s) > 1$. The right hand side provides an analytic continuation to the whole of the complex plane and the poles of ζ_K are simple.

Proof.

$$Z_K(u) = \sum_{n=0}^{\infty} b_n u^n.$$

Pick $N \in \mathbb{N}$ such that $N\delta \geq 2g - 1$ and $(N-1)\delta < 2g - 1$. So

$$Z_K(u) = \sum_{i=0}^{N-1} b_{i\delta} u^{i\delta} + \sum_{i=N}^{\infty} b_{i\delta} u^{i\delta}.$$

Let $p(u) = \sum_{i=0}^{N-1} b_{i\delta} u^{i\delta}$. We have already shown that $b_n = \frac{(h_K)(q^{n-g+1}-1)}{q-1}$ for any $n \geq 2g - 1$ which is divisible by δ. Thus

$$\begin{aligned} Z_K(u) &= p(u) + \frac{h_K}{q-1} \sum_{i=N}^{\infty} (q^{i\delta - g+1} - 1) u^{i\delta} \\ &= p(u) + \frac{h_K}{q-1} \left(\frac{q^{N\delta - g+1} u^{N\delta}}{1 - (qu)^\delta} - \frac{u^{N\delta}}{1 - u^\delta} \right) \\ &= p(u) + \frac{h_K}{q-1} \left(\frac{r(u)}{(1 - (qu)^\delta)(1 - u^\delta)} \right) \end{aligned}$$

for some $r(u) \in \mathbb{Z}[u]$ and one can check that $q-1$ divides $r(u)$. Thus there exists $L_K(u) \in \mathbb{Z}[u]$ such that

$$Z_K(u) = \frac{L_K(u)}{(1-u^\delta)(1-(qu)^\delta)}.$$

From the rational expression , it is clear that the poles of Z_K are simple. We note that $u = 1$ and $u = \frac{1}{q}$ are indeed poles because $L_K(1), L_K(\frac{1}{q})$ can be verified to be non-zero.

Also $L_K(0) = Z_K(0) = 1$.

□

It turns out that $\delta = 1$ and to prove it, we need to consider field extensions of F and the compositum of K with them. Let F_n denote the n-th degree field extension of F and $K_n = KF_n$. In terms of curves, if one extends the base field to F_n and considers curve C to be defined over F_n, then the function field of C so got is K_n.

One can construct the corresponding zeta function to be

$$\zeta_{K_n}(s) = \sum_{i=0}^{\infty} b_i(K_n)\,(q^n)^{(-is)}.$$

where $b_i(K_n)$ refers to the number of effective divisors of K_n of degree i. Similarly we can define the corresponding Z_{K_n} and L_{K_n} where

$$Z_{K_n}(u') = \frac{L_{K_n}(u')}{(1-u'^{\delta'})(1-(q^n u')^{\delta'})},$$

where $\delta'\mathbb{Z}$ is the image of the degree map $\deg : Cl_{K_n} \to \mathbb{Z}$. The crucial observation is that the poles of Z_{K_n} are again simple and $u' = 1, u' = \frac{1}{q^n}$ are both simple poles.

Z_K and Z_{K_n} are related quite naturally as follows

$$Z_{K_n}(u^n) = \prod_{\{z\in\mathbb{C}|z^n=1\}} Z_K(zu). \tag{2.2}$$

For a proof, we refer the reader to look at Rosen's book *Number theory in function fields*.

Now we are in a position to prove that δ is indeed 1.

Theorem 2.6 (Schmidt)**.** *There exists a divisor of K of degree 1.*

Proof.

$$\begin{aligned} Z_{K_n}(u^n) &= \prod_{\{z|z^n=1\}} Z_K(zu) \\ &= \prod_{\{z|z^n=1\}} \frac{L_K(zu)}{(1-(zu)^\delta)(1-(qzu)^\delta)} \end{aligned}$$

If we take $n = \delta$, then z runs over the δ-th roots of unity and hence

$$Z_{K_\delta}(u^\delta) = \frac{\prod_{\{z|z^\delta=1\}} L_K(zu)}{(1-u^\delta)^\delta(1-(qu)^\delta)^\delta}.$$

As $z^\delta = 1$, it follows from the expression of L_K that $L_K(zu) = L_K(u)$ and hence $L_K(z) \neq 0$ for any z such that $z^\delta = 1$. Therefore $u = 1$ is a simple pole of $Z_{K_\delta}(u^\delta)$. However the above expression implies that it is a pole of order δ which tells us that $\delta = 1$. □

Thus we have

$$Z_K(u) = \frac{L_K(u)}{(1-u)(1-qu)} \text{ where } L_K(u) \in \mathbb{Z}[u]. \tag{2.3}$$

2.0.3 The functional equation

Define $\xi(s) = q^{(g-1)s}\zeta_K(s)$ where g is the genus of K.

Lemma 2.7.

$$\xi(s) = \xi(1-s).$$

Proof. Let us convert the function equation in terms of $u = q^{-s}$. Note that

$$\zeta_K(s) = \sum_{n=0}^{\infty} b_n q^{-ns} = \sum_{n=0}^{\infty} b_n u^n = Z_K(u).$$

Thus

$$\zeta_K(1-s) = \sum_{n=0}^{\infty} b_n q^{-n+ns} = \sum_{n=0}^{\infty} b_n \left(\frac{1}{qu}\right)^n = Z_K\left(\frac{1}{qu}\right).$$

Thus the functional equation needed to be proved translates to

$$u^{1-g} Z_K(u) = \left(\frac{1}{qu}\right)^{1-g} Z_K\left(\frac{1}{qu}.\right)$$

Set $B(u) = (q-1)u^{1-g} Z_K(u)$. So what we need to show is that $B(u) = B\left(\frac{1}{qu}\right)$.

So let us actually expand out $B(u)$. Let

$$Cl_K^+ := \{\tilde{A} \in Cl_K | \deg(\tilde{A}) \geq 0\},$$

$$Cl_K^i := \{\tilde{A} \in Cl_K | 0 \leq \deg(\tilde{A}) \leq i\}.$$

$$\begin{aligned}
B(u) &= (q-1)u^{1-g}Z_K(u) \\
&= (q-1)u^{1-g}\left(\sum_{\tilde{A}\in Cl_K^+}\frac{q^{l(\tilde{A})}-1}{q-1}u^{\deg(\tilde{A})}\right) \\
&= u^{1-g}\left(\sum_{\tilde{A}\in Cl_K^+} q^{l(\tilde{A})}u^{\deg(\tilde{A})} - \sum_{\tilde{A}\in Cl_K^+} u^{\deg(\tilde{A})}\right) \\
&= u^{1-g}\left(\sum_{\tilde{A}\in Cl_K^{2g-2}} q^{l(\tilde{A})}u^{\deg(\tilde{A})} + \sum_{\{\tilde{A}|\,\deg(\tilde{A})\geq 2g-1\}} q^{l(\tilde{A})}u^{\deg(\tilde{A})} - \sum_{\tilde{A}\in Cl_K^+} u^{\deg\tilde{A}}\right) \\
&= \sum_{\tilde{A}\in Cl_K^{2g-2}} q^{l(\tilde{A})}u^{\deg(\tilde{A})-g+1} + h_k\left(\sum_{n=2g-1}^{\infty} q^{n-g+1}u^{n+1-g} - \sum_{n=0}^{\infty} u^{n+1-g}\right) \text{ (Using (2.1) and 2.6)} \\
&= \sum_{\tilde{A}\in Cl_K^{2g-2}} q^{l(\tilde{A})}u^{\deg(\tilde{A})-g+1} + h_K\left(\frac{q^g u^g}{1-qu} - \frac{u^{1-g}}{1-u}\right).
\end{aligned}$$

Let

$$R(u) := \sum_{\tilde{A}\in Cl_K^{2g-2}} q^{l(\tilde{A})}u^{\deg(\tilde{A})-g+1},$$

$$S(u) := h_K\left(\frac{q^g u^g}{1-qu} - \frac{u^{1-g}}{1-u}\right).$$

It is a trivial check to see that $S(u) = S\left(\frac{1}{qu}\right)$. Now ,

$$\begin{aligned}
R\left(\frac{1}{qu}\right) &= \sum_{\tilde{A}\in Cl_K^{2g-2}} q^{l(\tilde{A})}\left(\frac{1}{qu}\right)^{\deg(\tilde{A})-g+1} \\
&= \sum_{\tilde{A}\in Cl_K^{2g-2}} q^{l(\tilde{A})-\deg(\tilde{A})+g-1}u^{g-1-\deg(\tilde{A})}
\end{aligned}$$

We now define a map ψ on Cl_K^{2g-2} which sends $\tilde{A} \to \tilde{C} - \tilde{A}$ where $\tilde{C}$ is the canonical divisor class of K.

Note that by Corollary 1.6 of the Riemann-Roch theorem, $\deg(\tilde{C}) = 2g-2$ and hence ψ is well-defined. In fact it is clear that ψ is a bijection.

Using the facts that $\deg(\tilde{C}-\tilde{A}) = 2g-2-\deg(\tilde{A})$ and that $l(\tilde{C}-\tilde{A}) = l(\tilde{A}) - \deg(\tilde{A}) + g - 1$ which are derived from the Riemann-Roch theorem, we conclude as follows:

$$\begin{aligned} R(u) &= \sum_{\tilde{A}\in Cl_K^{2g-2}} q^{l(\tilde{A})} u^{\deg(\tilde{A})-g+1} \\ &= \sum_{\tilde{A}\in Cl_K^{2g-2}} q^{l(\tilde{C}-\tilde{A})} u^{\deg(\tilde{C}-\tilde{A})-g+1}, (\psi \text{ is a bijection}) \\ &= \sum_{\tilde{A}\in Cl_K^{2g-2}} q^{l(\tilde{A})-\deg(\tilde{A})+g-1} u^{g-1-\deg(\tilde{A})}. \end{aligned}$$

□

The functional equation translates to

$$L_K\left(\frac{1}{qu}\right) = q^{-g}u^{-2g}L_K(u). \tag{2.4}$$

The above equation tells us the degree of L_K ! We know that $L_K(0) = 1$. So let

$$L_K(u) = 1 + r_1 u + \ldots + r_k u^k \text{ where } r_1, r_2 \ldots, r_k \in \mathbb{Z}.$$

The functional equation implies that

$$\begin{aligned} 1 + \frac{r_1}{qu} + \ldots + \frac{r_k}{q^k u^k} &= u^{-2g}q^{-g}\left(1 + r_1 u + \ldots + r_k u^k\right) \\ &= \frac{1}{u^{2g}q^g} + \frac{r_1}{u^{2g-1}q^g} + \ldots + \frac{r_k}{u^{2g-k}q^g} \end{aligned}$$

Hence $k = 2g$ and $r_k = q^g$.

We summarize everything in the following theorem.

Theorem 2.8. *There exists a polynomial $L_K[u] \in \mathbb{Z}[u]$ of degree $2g$ where g is the genus of K with $L_K(0) = 1$ and the coefficient of u^{2g} in L_k equal to q^g such that*

$$\zeta_K(s) = \frac{L_K(q^{-s})}{(1 - q^{-s})(1 - q^{(1-s)})}.$$

This holds for all s with $Re(s) > 1$. The right hand side provides an analytic continuation to the whole of the complex plane and the only poles of ζ_K are at $s = 0, 1$ which are simple.

ζ_K satisfies a functional equation as described above.

2.0.4 A corollary of the functional equation

Since L_K is a polynomial of degree $2g$ with $L_K(0) = 1$, let

$$L_K(u) = \prod_{i=1}^{2g} (1 - \alpha_i u)$$

be the factorization of L_K in $\mathbb{C}[u]$. Thus the zeroes of L_K form the set $\{\frac{1}{\alpha_i} | 1 \leq i \leq 2g\}$.

The functional equation (2.4) implies that $L_K\left(\frac{\alpha_i}{q}\right) = 0$ and hence $\frac{q}{\alpha_i} = \alpha_j$ for some j.

Thus $\alpha_i \rightsquigarrow \frac{q}{\alpha_i}$ is a permutation of the α_is. This fact shall be used crucially in the proof of the Riemann Hypothesis.

Chapter 3

Riemann Hypothesis for function fields

Theorem 3.1 (Riemann Hypothesis for function fields)**.** *The zeroes of $\zeta_K(s)$ lie on the line $Re(s) = \frac{1}{2}$.*

First conjectured in 1924 by E.Artin for hyper-elliptic function fields, a proof for the case $g = 1$ was given by Hasse in 1934. Later, in the early 1940s, A.Weil came up with two different proofs which required some heavy machinery of algebraic geometry.

However S.A.Stepanov found a proof in the 1960s, albeit in special cases, which largely used just the Riemann-Roch. In this section, we present Bombieri's proof which used Stepanov's ideas to prove the result for the general case.

$u = q^{-s}$ gives $Z_K(u) = \zeta_K(s)$. Recall the rational expression for Z_K,

$$Z_K(u) = \frac{L_K(u)}{(1-u)(1-qu)}.$$

Using the fact that

$$L_K(u) = \prod_{i=1}^{2g} (1 - \alpha_i u) \, ,$$

and that the only simple poles are at $u = 1, \frac{1}{q}$, the zeroes of Z_K are just $\{\alpha_1, \alpha_2, \dots, \alpha_{2g}\}$.

Thus the Riemann hypothesis reduces to proving

$$|\alpha_i| = \sqrt{q} \forall i \leq 2g.$$

Equation (2.2) gives

$$\begin{aligned} Z_{K_m}(u^m) &= \prod_{\{z|z^m=1\}} Z_K(zu) \\ \implies \frac{L_{K_m}(u^m)}{(1-u^m)(1-q^m u^m)} &= \prod_{\{z|z^m=1\}} \frac{L_K(zu)}{(1-zu)(1-qzu)} \end{aligned}$$

Using the fact that $\prod_{\{z|z^m=1\}}(1-zt) = 1-t^n$ for any t, we have

$$L_{K_m}(u^m) = \prod_{i=1}^{2g}(1-\alpha_i^m u^m) \tag{3.1}$$

The zeroes of Z_{K_m} for the function field K_m over F_m correspond to $\frac{1}{\alpha_i^m}$ for all $i \leq 2g$. Thus if the Riemann Hypothesis holds for K_m, this would mean $|\alpha_i^m| = q^{\frac{m}{2}}$ which implies $|\alpha_i| = \sqrt{q}$ and thus Riemann hypothesis holds for K. We record these observations below in the form of a lemma.

Lemma 3.2. *If for some $m \in \mathbb{N}$, the Riemann Hypothesis holds for K_m, then the Riemann Hypothesis holds for our given function field K over F.*

3.1 The Weil bound

The euler product form for Z_K,

$$Z_K(u) = \prod_{d=1}^{\infty}(1-u^d)^{-a_d},$$

gives us another expression for Z_K as follows:

$$\begin{aligned}\log Z_K(u) &= \sum_{d=1}^{\infty} -a_d \log(1-u^d) \\ &= \sum_{d=1}^{\infty} a_d \left(u^d + \frac{u^{2d}}{2} + \dots\right) \\ &= \sum_{d=1}^{\infty} \frac{N_d(K)}{d} u^d,\end{aligned}$$

where $N_m(K) = \sum_{d|m} da_d$. Thus

$$Z_K(u) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m(K)}{m} u^m\right).$$

The quantity $N_m(K)$ so defined turns out to be equal to $N_1(K_m)$ (the number of rational points in the corresponding curve when the base field is extended to F_m)! (For $m = 1$ it is clear)

This remarkable fact we prove below by actually giving an expression in terms of α_is for the two quantities which has an important bearing in the proof of the Riemann Hypothesis for function fields.

Lemma 3.3.

$$N_m(K) = q^m + 1 - \left(\sum_{i=1}^{2g} \alpha_i^m\right)$$

Proof.

$$Z_K(u) = \frac{\prod_{i=1}^{2g}(1-\alpha_i u)}{(1-u)(1-qu)} = \exp\left(\sum_{m=1}^{\infty} \frac{N_m(K)}{m} u^m\right)$$

Taking the logarithmic derivative for both the expressions, we end up with

$$-\left(\sum_{i=1}^{2g} \frac{\alpha_i}{1-\alpha_i u}\right) + \frac{1}{1-u} + \frac{q}{1-qu} = \sum_{m=1}^{\infty} N_m(K) u^{m-1}.$$

Multiplying by u on both sides and expanding, we get

$$-\left(\sum_{i=1}^{2g}\sum_{m=1}^{\infty}(\alpha_i u)^m\right)+\sum_{m=1}^{\infty}u^m+\sum_{m=1}^{\infty}(qu)^m=\sum_{m=1}^{\infty}N_m(K)u^m.$$

Equating the coefficients of u^m gives us the neccesary equation.

□

Lemma 3.4.

$$N_1(K_m)=q^m+1-\left(\sum_{i=1}^{2g}\alpha_i^m\right).$$

Proof. This time, we consider the two expressions for the zeta function of the function field $K_m = KF_m$ over the base field F_m, which is the degree m extension of the field F.

$$\begin{aligned} Z_{K_m}(u') &= \frac{L_{K_m}(u')}{(1-u')(1-q^m u')} \\ &= \frac{\prod_{i=1}^{2g}(1-\alpha_i^m u')}{(1-u')(1-q^m u')} \text{ (By equation (3.1))} \end{aligned}$$

and

$$Z_K(u')=\sum_{k=0}^{\infty}b_k(K_m)u'^k.$$

Taking logarithmic derivative for both the expressions and evaluating at 0, we get

$$-\left(\sum_{i=1}^{2g}\alpha_i^m\right)+1+q^m=\frac{Z'_{K_m}(0)}{Z_{K_m}(0)}=\frac{b_1(K_m)}{b_0(K_m)}.$$

$b_0(K_m)$ is the number of effective divisors of K_m of degree 0 and hence is equal to 1. $b_1(K_m) = a_1(K_m) = N_1(K_m)$ and we are done.

□

Note the implications of the above lemma when combined with the Riemann Hypothesis. The latter tells us that $|\alpha_i| = \sqrt{q}$ which therefore gives us what is known as the *Weil bound* on the number of rational points of the smooth projective curve whose function field is K, which we state below

Theorem 3.5 (Weil bound)**.**

$$|N_1(K) - q - 1| \leq \sum_{i=1}^{2g} |\alpha_i| = 2g\sqrt{q}.$$

3.2 Bombieri's proof

Recall the expression for $N_m(K)$ (refer to lemma 3.3)

$$N_m(K) = q^m + 1 - \left(\sum_{i=1}^{2g} \alpha_i^m \right),$$

and construct the following series

$$\sum_{m=1}^{\infty} \left(N_m(K) - q^m - 1\right) u^m = -\sum_{i=1}^{2g} \sum_{m=1}^{\infty} (\alpha_i u)^m$$

The radius of convergence of the series on the right side is the minimum of the set $\{\frac{1}{|\alpha_i|}\}_{i=1}^{2g}$. If we can show that there exist constants A, B such that $N_m(K) = Aq^{\frac{m}{2}} + B + q^m$, then the radius of convergence of the series on the left is atleast $\frac{1}{\sqrt{q}}$.

This would mean that for all $i \leq 2g$, $\frac{1}{|\alpha_i|} \geq \frac{1}{\sqrt{q}}$. Using the fact that $\alpha_i \rightsquigarrow \frac{q}{\alpha_i}$ is a permutation of the α_is, we get

$$\frac{|\alpha_i|}{q} \geq \frac{1}{\sqrt{q}}$$

and hence $\sqrt{q} \leq |\alpha_i| \leq \sqrt{q}$ for all i which induces equality and concludes the proof of the Riemann Hypothesis !.

So all we are left to do is to show that $N_m(K) = q^m + O(q^{m/2})$ for all m.

Note that by $X(u) = O(f(u))$, we mean that there exist constants A, B such that $|X(u)| < A + Bf(u)$. Since we have proved that $N_1(K_m) = N_m(K)$ in the section on Weil bound, we need to prove that the number of rational points in K_m for any m is $O(q^{\frac{m}{2}}) + q^m$.

In the next few sections, we find an upper bound and lower bound for $N_1(K)$ by imposing certain conditions on K/F (we will see that if they hold for K/F, they will hold for K_m/F_m for any m) and finally find a constant field extension K_n/F_n which satisfies these conditions. Having proved the Riemann Hypothesis for K_n/F_n, we conclude using Lemma 3.2(which tells us that if the Riemann Hypothesis holds for any constant field extension K_n/F_n, then the result will also hold for K/F).

3.2.1 Curves

In the following sections, we will switch to using the language of curves and we again invite the reader to go through the chapter *Language of curves* given in the appendix before going ahead. However below, we briefly summarize a few ideas that we need for proving Bombieri's lemma.

F is the finite field of order q and characteristic p. $\overline{F}$ denotes the algebraic closure of F and π, its frobenius automorphism which sends $x \rightsquigarrow x^q$.

Let $\mathbb{P}^N = \mathbb{P}^N(\overline{F})$ be the projective space of $\overline{F}$. The set of F-rational points of $\mathbb{P}^N(\overline{F})$ defined to be

$$\mathbb{P}^N(F) := \{[a_0, a_1, \ldots, a_N] \in \mathbb{P}^N(\overline{F}) | a_i \in F \forall i \leq N\}$$

is exactly the set of points fixed by the automorphism ϕ of $\mathbb{P}^N(\overline{F})$ which sends

$$[\beta_0, \beta_1, \ldots, \beta_N] \rightsquigarrow [\beta_0^q, \beta_1^q, \ldots, \beta_N^q].$$

Let $C = C(\overline{F})$ be a smooth projective curve defined over F. Note that ϕ maps $C(\overline{F})$ to itself and the rational points of C denoted $C(F)$ (which is the set $C \cap \mathbb{P}^N(F)$) are the fixed points of ϕ in $C(\overline{F})$.

Define $I(C)$ to be the ideal generated in $\overline{F}[x_0, x_1, \ldots x_N]$ by the homogeneous polynomials with coefficients in F which vanish on C.

K consists of all rational functions $\frac{f}{g}$ such that

- f and g are homogeneous polynomials of the same degree in $F[x_0, x_1, \ldots, x_N]$.
- $g \notin I(C)$
- Two functions $\frac{f}{g}$ and $\frac{f'}{g'}$ are identified if $fg' - f'g \in I(C)$.

Likewise any element of $\overline{K}$ looks like $\frac{\bar{f}}{\bar{g}}$ where $\bar{f}, \bar{g}$ are homogeneous polynomials of the same degree, this time in $\overline{F}[x_0, x_1, \ldots, x_N]$ such that $\bar{g}$ does not vanish entirely on C with a similar identification process.

Given a point α of C, we can associate a prime of K with it as follows:

$$\mathcal{O}_\alpha = \left(\frac{f}{g} \in K | g(\alpha) \neq 0 \right),$$

where its maximal ideal denoted by P_α is

$$P_\alpha = \left\{ \frac{f}{g} : \frac{f}{g} \in \mathcal{O}_\alpha, f(\alpha) = 0 \right\}.$$

There is a natural action of the Galois group of $\overline{F}$ over F on C. It turns out that $(\mathcal{O}_\alpha, P_\alpha) = (\mathcal{O}_\beta, P_\beta)$ if and only if there exists $\sigma \in \operatorname{Gal}\left(\overline{F}/F\right)$ such that $\sigma(\alpha) = \beta$. Thus Galois orbits of C are in one to one correspondence with primes of K. It is also a fact that $\deg(P_\alpha) = |\{\sigma(\alpha) | \sigma \in \operatorname{Gal}\left(\overline{F}/F\right)\}|$, the cardinality of the Galois orbit of α. Hence as F rational points of C are fixed points of the Galois group action, they correspond exactly to primes of degree 1 of K.

3.2.2 An upper bound for $N_1(K)$

Theorem 3.6 (Bombieri). *Let g be the genus of C where the following assumptions hold*

- $q = |F|$ *is an even power of* p, *say* $q = p^{2b}$ *for some* $b \in \mathbb{N}$.
- $(g+1)^4 < q$

Then $N_1(K) \leq q + 1 + (2g+1)\sqrt{q}$.

Idea of the proof : We find a function f with a zero at almost all rational points but very few poles (that too, of small order). So for some small s,

$$(a_1 + O(1)) \leq \deg((f)_0) = \deg((f)_\infty) \leq s.$$

If we can construct a map ψ which sends $h \circ \phi \rightsquigarrow h$ for $h \circ \phi$ in the domain of ψ and if $h \circ \phi$ is in the kernel of ψ, then $h \circ \phi(\beta) = h(\beta) = 0$ for any rational point β where h is defined.

A good place to look for functions with very few poles (that too of low order) is

$$L(mP_\alpha) = \{k \in K^* | (k) + mP_\alpha \geq 0\},$$

for some rational point α. The detailed proof is given below.

Proof. If the number of rational points of $C = 0$, then there is nothing to prove as $N_1(K)$ is exactly the number of rational points in C. If not, let α be a rational point of C and $(\mathcal{O}_\alpha, P_\alpha)$, the corresponding prime of K.

For every positive integer m, define an F vector space,

$$R_m := L(mP_\alpha) = \{f \in K^* | (f) + mP_\alpha \geq 0\} \cup \{0\}.$$

As shown in Lemma 1.3, it is finite dimensional. Also note that $R_m \subseteq R_n \forall m \leq n$.

Since the base field has characteristic p,

$$R_m^{p^e} := \{f^{p^e} | f \in R_m\},$$

for any positive integer e, is also an F vector space and is a subspace of R_{mp^e}. To see this,

$$\begin{aligned} f \in R_m &\implies (f) + mP_\alpha \geq 0 \\ &\implies p^e(f) + mp^eP_\alpha \geq 0 \\ &\implies (f^{p^e}) + mp^eP_\alpha \geq 0 \\ &\implies f^{p^e} \in R_{mp^e}. \end{aligned}$$

Note that the dimension of $R_m^{p^e}$ is equal to the dimension of R_m as an F vector space (for the map from R_m to $R_m^{p^e}$ given by $f \rightsquigarrow f^{p^e}$ is bijective).

We define yet another F vector space

$$R_m \circ \phi := \{f \circ \phi | f \in R_m\}.$$

This sits inside R_{mq} as a subspace. To see this, pick any element $f = \frac{H}{G} \in R_m$ where H, G are homogeneous polynomials in $F[x_0, \dots, x_N]$ and using the fact that $a = a^q$ for any $a \in F$, observe that $f \circ \phi = f^q$.

The above observation also shows that $R_m \cong_F R_m \circ \phi$ by the isomorphism $f \rightsquigarrow f \circ \phi = f^q$, which one can easily check is bijective.

Finally if A, B are subspaces of a vector space R_s for any s, by AB we mean the subspace generated by the set $\{ab | a \in A, b \in B\}$. Observe that $R_mR_n \subseteq R_{m+n}$.

We would like to define a map $\psi : R_l^{p^e}(R_m \circ \phi) \to R_l^{p^e}R_m$, where the integers l, e, m will be determined later. Note that the domain sits inside R_{lp^e+mq} and so for any f in it, $\deg(f)_\infty \leq lp^e + mq$. A naive but natural definiton for ψ would be to send $g^{p^e}(f_i \circ \phi) \rightsquigarrow g^{p^e}f_i$ but this may apriori not be well-defined. So we set up an isomorphism between $R_l^{p^e} \otimes_F (R_m \circ \phi)$ and $R_l^{p^e}(R_m \circ \phi)$ as explained in the following lemma to prove that it is indeed well-defined.

Lemma 3.7. *$R_l^{p^e} \otimes_F (R_m \circ \phi) \cong_F R_l^{p^e}(R_m \circ \phi)$ if $lp^e < q$.*

Proof. First we would like to find a suitable basis for R_m. Note that $\dim R_0 = 1$ as $R_0 = F$.

Claim : $\dim R_{t+1} \leq \dim R_t + 1$ *for any* t

If f and g are elements of R_{t+1} with poles of order $t+1$ at α, then $\mathrm{ord}_{P_\alpha}(\frac{f}{g}) = 0$ (ie) $\frac{f}{g} \in \mathcal{O}_{P_\alpha}$. As P_α is a rational prime, $\left[\frac{\mathcal{O}_{P_\alpha}}{P_\alpha} : F\right] = 1$ and thus

$$\mathrm{ord}_{P_\alpha}\left(\frac{f}{g}-\gamma\right) \geq 1 \text{ for some } \gamma \in F.$$

And hence,

$$\mathrm{ord}_{P_\alpha}\left(g\left(\frac{f}{g}-\gamma\right)\right) \geq -t,$$

which implies $f - \gamma g \in R_t$, as at all other primes, $f - \gamma g$ has no pole because $f, g \in R_{t+1}$. Thus we can find a basis $\{f_1, f_2, \ldots, f_t\}$ for R_m where $\mathrm{ord}_{P_\alpha}(f_i) < \mathrm{ord}_{P_\alpha}(f_{i+1})$ for all $i < t$ and dimension of $R_m = t \leq m + 1$.

So any element of $R_l^{p^e} \otimes (R_m \circ \phi)$ can be written in the form

$$\sum_{i=1}^{t} g_i^{p^e} \otimes (f_i \circ \phi),$$

where g_i are elements of R_l.

The natural map is

$$\sum_{i=1}^{t} g_i^{p^e} \otimes (f_i \circ \phi) \rightsquigarrow \sum_{i=1}^{t} g_i^{p^e}(f_i \circ \phi)$$

which is clearly surjective. If the kernel is non-zero, then we have a relation $\sum_{i=1}^{t} g_i^{p^e}(f_i \circ \phi) = 0$ for some g_is $\in R_l$, not all zero. Choose r to be the smallest integer such that $g_r \neq 0$. Then we have

$$g_r^{p^e}(f_r \circ \phi) = -\sum_{i=r+1}^{t} g_i^{p^e}(f_i \circ \phi) \tag{3.2}$$

Since $f_i \circ \phi = f_i^q$, we have

$$\mathrm{ord}_{P_\alpha}(f_i \circ \phi) = q\,\mathrm{ord}_{P_\alpha}(f_i).$$

Thus taking order with respect to P_α on both sides of 3.2 and noting that $g_i \in R_l$,

$$\begin{aligned}
&p^e \operatorname{ord}_{P_\alpha}(g_r) + q \operatorname{ord}_{P_\alpha}(f_r) \\
&\geq \min_{r+1 \leq i \leq t} \operatorname{ord}_{P_\alpha}(g_i^{p^e}(f_i \circ \phi)) \\
&\geq -lp^e + q \operatorname{ord}_{P_\alpha}(f_{r+1})
\end{aligned}$$

Thus,

$$\begin{aligned}
p^e \operatorname{ord}_{P_\alpha}(g_r) &\geq q(\operatorname{ord}_{P_\alpha}(f_{r+1}) - \operatorname{ord}_{P_\alpha}(f_r)) - lp^e \\
&\geq q - lp^e \text{ (as } \operatorname{ord} f_{t+1} > \operatorname{ord} f_t) \\
&> 0 \text{ (by assumption).}
\end{aligned}$$

Thus g_r has a zero at P_α but as it belongs to R_r, it has no poles at any other prime, so $g_r \in F$ and is equal to 0, which is a contradiction to the assumption that r is the least integer for which is g_r is nonzero.

Thus the natural homomorphism is also injective, which makes it an isomorphism. □

Thus, our naive definition of the map $\psi : R_l^{p^e}(R_m \circ \phi) \to R_l^{p^e} R_m$ works by sending

$$\sum g_i^{p^e}(f_i \circ \phi) \rightsquigarrow \sum g_i^{p^e} f_i.$$

Supposing that the kernel of ψ is non-zero, then choose a nonzero element of the kernel, say

$$f = \sum_{i=1}^{t} g_i^{p^e}(f_i \circ \phi).$$

Note that f_i s are functions well defined on all rational points except maybe α as $f_i \in R_m$ for all $i \leq t$.So for any rational point $\beta \neq \alpha$,

$$\begin{aligned}f(\beta) &= \sum_{i=1}^{t} g_i^{p^e}(\beta)(f_i \circ \phi(\beta)) \\ &= \sum_{i=1}^{t} g_i^{p^e}(\beta) f_i(\beta) \text{ (as } \beta \text{ is a rational point)} \\ &= \psi(f)(\beta) \\ &= 0.\end{aligned}$$

So f has a zero at all the rational points except maybe at α.

Note that $f_i \circ \phi = f_i^q$. So if $q > p^e$, then f is a p^e power and hence f has a zero of order at least p^e at all rational points except maybe α and therefore we have

$$\deg(f)_0 \geq (N_1(K) - 1)p^e$$

As already observed,

$$f \in R_l^{p^e}(R_m \circ \phi) \subseteq R_{lp^e + mq},$$

and thus $\deg(f)_\infty \leq lp^e + mq$. Equating $\deg(f)_0$ and $\deg(f)_\infty$, we get

$$N_1(K) \leq 1 + l + \frac{mq}{p^e} \tag{3.3}$$

The Riemann-Roch theorem helps us ensure that the kernel is indeed non-zero by giving us a handle on the dimensions of the domain and image of ψ.

$$\psi : R_l^{p^e}(R_m \circ \phi) \to R_l^{p^e} R_m.$$

Using the Riemann inequality, we have

$$\begin{aligned}\dim_F R_l &\geq l - g + 1 \\ \dim_F R_m &\geq m - g + 1.\end{aligned}$$

Thus, we can lower bound the dimension of the domain as follows:

$$\begin{aligned}\dim_F\left(R_l^{p^e}(R_m \circ \phi)\right) &= \dim_F\left(R_l^{p^e} \otimes (R_m \circ \phi)\right)\\ &= \dim_F\left(R_l^{p^e}\right) \times \dim_F\left(R_m \circ \phi\right)\\ &= \dim_F(R_l) \times \dim_F(R_m)\\ &\geq (l-g+1)(m-g+1).\end{aligned}$$

If $l, m \geq g$, then $lp^e + m \geq 2g - 1$, and thus using Corollary 1.6, we have

$$\dim_F R_{lp^e+m} = lp^e + m - g + 1,$$

and therefore, the dimension of the image can be bounded as

$$\begin{aligned}\dim_F(\text{image}(\psi)) &\leq \dim_F(R_l^{p^e} R_m)\\ &\leq \dim_F(R_{lp^e+m})\\ &= lp^e + m - g + 1.\end{aligned}$$

Hence our kernel is lower bounded as follows:

$$\dim_F \text{kernel}(\psi) \geq (l-g+1)(m-g+1) - (lp^e + m - g + 1),$$

and to make sure our kernel is nonzero, we just have to choose e, l, m suitably so that the expression on the right hand side is positive. We have also made various assumptions about integers e, l, m on the way which have to be satisfied to complete the proof of the theorem. These are enumerated below.

1. $lp^e < q$
2. $l, m \geq g$
3. $(l-g+1)(m-g+1) > lp^e + m - g + 1$ which on simplification yields $(l-g)(m+1-g) > lp^e$
4. $q > p^e$.

Recall that $q = p^{2b}$. Put $e = b$, and $m = p^b + 2g$. Now substituting these values in the third condition, we find that we need $(l - g)(p^b + 1 + g) > lp^b$ which translates to

$$l > \frac{g(p^b + g + 1)}{g + 1} = \frac{gp^b}{g + 1} + g.$$

Thus, put $l = \left[\frac{gp^b}{g+1}\right] + g + 1$. Note that we also need to satisfy the first condition, so l should not be too big. These values of e, m, l satisfy the last three conditions.

$$\begin{aligned}\left(\frac{gp^b}{g+1} + g + 1\right)(g + 1) &= gp^b + (g + 1)^2\\ &< gp^b + p^b \text{ (because } (g + 1)^4 < q = p^{2b})\\ &= (g + 1)p^b.\end{aligned}$$

Hence

$$\begin{aligned}\frac{gp^b}{g+1} + g + 1 < p^b&\\ &\implies l < p^b\\ &\implies lp^e = lp^b < p^{2b} = q.\end{aligned}$$

and the first condition is also fulfilled.

Substituting these values into Equation 3.3 and using $l < p^b$, we get

$$\begin{aligned}N_1(K) &\le 1 + p^b + \frac{(p^b + 2g)p^{2b}}{p^b}\\ &= 1 + \sqrt{q} + q + 2g\sqrt{q}\\ &= q + 1 + (2g + 1)(\sqrt{q})\end{aligned}$$

□

3.2.3 A lower bound for $N_1(K)$

This method will involve consideration of Galois extensions of K and we give below, a few important definitions whose usage will prove crucial later on.

- Let K/F be a function field with constant field F and L, a finite field extension of K. If F is algebraically closed in L, then L is said to be a *geometric* extension of K/F.
- If S is a field extension of T and L is the smallest algebraic extension of S which is Galois over T, then L is called the *Galois closure* of S/T.

From now on until theorem 3.10, let L be a finite Galois extension of K with $G = \mathrm{Gal}\,(L/K)$ such that it is geometric over K/F. We introduce the following notations:

- $\overline{K} = K\overline{F}$ as denoted earlier.
- $\overline{L} = L\overline{F}$.

Since L is geometric over K/F, the Galois group of $\overline{L}/\overline{K}$, $\mathrm{Gal}\left(\overline{L}/\overline{K}\right)$, can be identified with $G = \mathrm{Gal}\,(L/K)$.

We now concern ourselves with certain sets of primes of the various fields which are described below.

1. S is the set of rational primes (ie) primes of degree 1 of K.
2. T is the set of all primes of $\overline{K}$ which lie above a rational prime of K.
3. $\tilde{T}$ refers to the set of all primes of $\overline{L}$ which lies above any one of the primes in T.

Recall that the points of the smooth projective curve C are in one to one correspondence with the primes of $\overline{K}$ and every prime of $\overline{K}$ lies above a prime of K. Also recall that the Galois orbits of C correspond to primes of K and in particular, rational primes of K are in one to one correspondence with the F rational points of C. Using all this, we conclude that $|T| = N_1(K)$.

Another way to characterise rational primes of $\overline{K}$ is by examining the action of the Frobenius map π (which sends $x \in \overline{F}$ to x^q) on them. Any element of $\overline{K}$ is of the form $\frac{f}{g}$ where $f, g \in \overline{F}[x_0, x_1, \ldots, x_N]$ are homogeneous polynomials of the same degree such that g does not vanish completely on C. Note that the Galois group of $\overline{F}$ over F acts naturally on $\overline{K}$, for instance we give below how $\sigma \in \mathrm{Gal}\left(\overline{F}/F\right)$ acts on $f = \sum b_a x_0^{a_0} x_1^{a_1} \ldots x_N^{a_N}$.

$$\sum b_a x_0^{a_0} x_1^{a_1} \ldots x_N^{a_N} \rightsquigarrow \sigma(b_a) x_0^{a_0} x_1^{a_1} \ldots x_N^{a_N}.$$

It is easy to see that $\pi P_\alpha = P_{\phi(\alpha)}$. And as F-rational points of C are nothing but fixed points of ϕ, $\pi P = P$ characterises the elements of T.

In the following discussion, we use some very useful propositions from algebraic number theory. First, fix a P in T and denote the set of all primes in $\tilde{T}$ which lie above P as $\tilde{T}_P$. More specifically, let

$$\tilde{T}_P = \{(\mathcal{O}_i, \mathfrak{P}_i)\}_{i=1}^r$$

be the primes of $\overline{L}$ which lie above P. It turns out that the Galois group $G = \mathrm{Gal}\left(\overline{L}/\overline{K}\right)$ acts transitively[1] on $\tilde{T}_P$. We have already seen that $\pi P = P$ if and only if $P \in T$. Hence $\pi \mathfrak{P}_i = \mathfrak{P}_j$ for some $j \leq r$. And due to the transitive action of the Galois group, there exists a $\sigma \in G$ such that $\pi \mathfrak{P}_i = \sigma \mathfrak{P}_i$.

Now look at the ideal generated by P in $\mathcal{O}_i$. Since the latter is a discrete valuation ring with maximal ideal $\mathfrak{P}_i$, we have

$$P\mathcal{O}_i = \mathfrak{P}_i^{e_i}.$$

e_i is said to be the *ramification index* of $\mathfrak{P}_i$. Due to the transitive action of the Galois group on $\tilde{T}_P$, $\exists \sigma' \in G$ such that $\sigma'(\mathfrak{P}_i) = \mathfrak{P}_j$ for any $i, j \leq r$ and hence the integers $e_i = e_j$ for all i, j. Let us denote the common value by e.

We can assign another integer f_i to each prime $\mathfrak{P}_i$ as follows:

$$f_i = \left[\frac{\mathcal{O}_i}{\mathfrak{P}_i} : \frac{\mathcal{O}_P}{P}\right]$$

.

[1] Given any two elements x, y of the set on which the group is acting, there exists a $\sigma \in G$ such that $\sigma x = y$.

However $\frac{\mathcal{O}_i}{\mathfrak{P}_i}$ is an algebraic extension of $\overline{F}$, an already algebraically closed field and hence $f_i = 1$ for any $i \leq r$.

By using the well known fact from number theory that $\sum_{i=1}^{r} e_i f_i = n$ where n is the degree of the extension $\overline{L}/\overline{K}$ and the cardinality of the Galois group, since it is a Galois extension, we get

$$re = n = |G|.$$

If $e = 1$, the primes $\mathfrak{P}_i$ are called *unramified*[2] and we find that $|\tilde{T}_P| = |G|$. Hence given any unramified $\mathfrak{P}_i$, there exists a unique $\sigma \in G$ such that $\pi\mathfrak{P}_i = \sigma\mathfrak{P}_i$.

The map η

Let $\tilde{T}^*$ denote the set of unramified primes in $\tilde{T}$. We are now in a position to define a map η as follows:

$$\eta : \tilde{T}^* \to G \text{ such that } \eta\left(\mathfrak{P}_i\right) = \sigma,$$

where $\sigma\mathfrak{P}_i = \pi\mathfrak{P}_i$.

And now we introduce the notation $N_1\left(\sigma, \overline{L}/\overline{K}\right)$ for any $\sigma \in G$ as

$$N_1\left(\sigma, \overline{L}/\overline{K}\right) := |\eta^{-1}\left(\sigma\right)|.$$

It is clear that $\tilde{T}^* = \bigcup_{\sigma \in G} \eta^{-1}\left(\sigma\right)$ and hence

$$|\tilde{T}^*| = \sum_{\sigma \in G} N_1\left(\sigma, \overline{L}/\overline{K}\right).$$

However, we have also proved that number of primes which lie above an unramified prime in T is $n = |G|$ and thus $|\tilde{T}^*| = |G|\left(N_1(K) + O(1)\right)$ where the $O(1)$ term is for the ramified[3] primes of $\overline{K}$. Equating the two expressions for $|\tilde{T}^*|$, we get the following very useful equality which we mark for later use.

[2] We sometimes also call P to be unramified

[3] primes which are not unramified

$$\sum_{\sigma\in G} N_1\left(\sigma, \overline{L}/\overline{K}\right) = |G|\left(N_1(K) + O(1)\right). \tag{3.4}$$

The proof of the upper-bound for $N_1(K)$ with very little modification yields us the following upper-bound for $N_1\left(\sigma, \overline{L}/\overline{K}\right)$.

Proposition 3.8. *Suppose that $q = |F|$ is an even power of the characteristic p and that $(\tilde{g}+1)^4 < q$ where $\tilde{g}$ is the genus of $\overline{L}$, then for any $\sigma \in G = \mathrm{Gal}\left(\overline{L}/\overline{K}\right)$,*

$$N_1\left(\sigma, \overline{L}/\overline{K}\right) \leq q + 1 + (2\tilde{g}+1)\sqrt{q}.$$

The above proposition subjected to very simple manipulations gives us a lower bound for $N_1\left(\sigma, \overline{L}/\overline{K}\right)$ as we see below.

Proposition 3.9. *For all $\sigma \in G = \mathrm{Gal}\left(\overline{L}/\overline{K}\right)$,*

$$q + 1 + \left(N_1(K) - q - 1\right)|G| + O\left(\sqrt{q}\right) \leq N_1\left(\sigma, \overline{L}/\overline{K}\right).$$

Proof. By proposition 3.8,

$$X(\sigma) = q + 1 + (2\tilde{g}+1)\sqrt{q} - N_1\left(\sigma, \overline{L}/\overline{K}\right) \geq 0.$$

Summing over all elements of G and using equation 3.4, we have

$$0 \leq X(\sigma) \leq \sum_{\sigma\in G} X(\sigma) = |G|\left(q + 1 + (2\tilde{g}+1)\sqrt{q} - N_1(K) + O(1)\right).$$

Expanding this inequality out by substituting for $X(\sigma)$, we get

$$q+1+(2\tilde{g}+1)\sqrt{q} - N_1\left(\sigma, \overline{L}/\overline{K}\right) \leq |G|\left(q + 1 + (2\tilde{g}+1)\sqrt{q} - N_1(K) - O(1)\right),$$

which on rearranging gives us the required equation.

□

And finally we are ready to give a lower bound for $N_1(K)$.

Theorem 3.10. *Let K/F be a function field of genus g over a finite field F with q elements with characteristic p. Suppose q is an even power of p. Suppose further that $\exists x \in K$ such that $K/F(x)$ is separable and that the Galois closure , L, of $K/F(x)$ is a geometric extension of $F(x)$. Finally assume that $(g+1)^4 < q$. Then,*

$N_1(K) \geq q + O(\sqrt{q})$.

Proof. Let $G = \mathrm{Gal}\left(\overline{L}/\overline{F}(x)\right)$ and $H = \mathrm{Gal}\left(\overline{L}/\overline{K}\right)$. Thus $H \subseteq G$.

Applying our previous proposition 3.9 to the extension $\overline{L}/\overline{F}(x)$, we get

$$q + 1 + |G|\left(N_1(F(x)) - q - 1\right) + O(\sqrt{q}) \leq N_1\left(\sigma, \overline{L}/\overline{F}(x)\right) \forall \sigma \in G.$$

However we have already proved in proposition 2.1 that all primes of degree 1 of $F(x)$ except one are in one to one correspondence with the monic irreducible polynomials of degree 1 in $F(x)$, which are q in number. (The remaining prime is the prime at infinity). Thus $N_1(F(x)) = q + 1$ and hence,

$$q + O(\sqrt{q}) \leq N_1\left(\sigma, \overline{L}/\overline{F}(x)\right).$$

Summing the above equation over all $\tau \in H$, we get

$$|H|\left(q + O(\sqrt{q})\right) \leq \sum_{\tau \in H} N_1\left(\tau, \overline{L}/\overline{F}(x)\right).$$

Claim: $N_1\left(\tau, \overline{L}/\overline{F}(x)\right) = N_1\left(\tau, \overline{L}/\overline{K}\right)$ for any $\tau \in H$.

Assuming this claim, we are but a step away from concluding as follows:

$$\begin{aligned} |H|\left(q + O(\sqrt{q})\right) &\leq \sum_{\tau \in H} N_1\left(\tau, \overline{L}/\overline{F}(x)\right) \\ &= \sum_{\tau \in H} N_1\left(\tau, \overline{L}/\overline{K}\right) \\ &= |H|\left(N_1(K) + O(1)\right) \text{ (Using 3.4)} \end{aligned}$$

Cancelling $|H|$ from both sides, we get our lower bound.

The proof of the claim follows easily from the definition of $N_1\left(\tau, \overline{L}/\overline{K}\right)$. Let $\mathfrak{P}$ be a prime of $\overline{L}$ which lies above a rational prime P of $\overline{F}(x)$ such that $\pi\mathfrak{P} = \tau\mathfrak{P}$ for some $\tau \in H$. Let Q be the prime of $\overline{K}$ lying under $\mathfrak{P}$. Then $\pi Q = \tau Q$. However as $\tau \in H$, it fixes elements of $\overline{K}$ and thus $\tau Q = Q$, which implies that $\pi Q = Q$ which shows that Q is a rational prime of $\overline{K}$. The other direction is clear.

□

We remark that if K/F satisfies the conditions explained previously so that $N_1(K) = q + O(\sqrt{q})$, then the constant field extensions K_m/F_m for any m satisfies the same conditions thus bounding $N_1(K_m)$ as,

$$N_1(K_m) = q^m + O(q^{\frac{m}{2}}).$$

3.2.4 The right constant field extension

We need to find an $n \in \mathbb{N}$ such that the function field K_n/F_n (where F_n is the n^{th} degree extension of F and $K_n = KF_n$) satisfies the following properties:

1. $|F_n| = q^n$ is an even power of p, so we will look for an even n.
2. $(g+1)^4 < q^n$ where g is the genus of K_n/F_n.
3. There exists an $x \in K_n$ such that $K_n/F_n(x)$ is a separable extension and if L is the Galois closure of $K_n/F_n(x)$, then L is geometric over $F_n(x)$.

Note that the genus of K/F is the same as genus of K_n/F_n for any n. (In terms of curves, the genus of curve C remains the same even if we enlarge the base field.) Thus choose an r such that $q^{2r} > (g+1)^4$ where g is the genus of K/F.

Consider the function field K_{2r}/F_{2r}. As shown in section 1, we can find an $x \in K_{2r}$ such that $K_{2r}/F_{2r}(x)$ is a finite separable field extension. Let L be the Galois closure of $K_{2r}/F_{2r}(x)$ with E denoting the algebraic closure of F_{2r} in L.

$$\begin{tikzcd}
E \arrow[r, hook] \arrow[d, dash] & L \arrow[d, dash] \\
F_{2r} \arrow[r, hook] & F_{2r}(x)
\end{tikzcd}$$

$$[E : F_{2r}] \leq [E(x) : F_{2r}(x)] \leq [L : F_{2r}(x)] < \infty.$$

Hence E is a finite extension of F_{2r} and is therefore equal to F_n for some n where $2r|n$. Note that n is forced to be even and $(g+1)^4 < q^{2r} \leq q^n$. Thus K_n/F_n satisfies the first two conditions. Since $K_{2r}/F_{2r}(x)$ is a separable extension, so is $K_n/F_n(x)$. Also as L is the Galois closure of $K_{2r}/F_{2r}(x)$ and $E = F_n \subseteq L$, it is also the Galois closure of $K_n/F_n(x)$ and by construction $F_n = E$ is algebraically closed in L.

And we have proved the Riemann Hypothesis for K_n/F_n ! Use lemma 3.2 to conclude the proof for K/F.

Chapter 4

Serre bound

Recall the Weil bound (Theorem 3.5)

$$|N_1(K) - q - 1| \leq \sum_{i=1}^{2g} |\alpha_i| = 2g\sqrt{q}.$$

A slight improvement can be obtained by noticing that $N_1(K)-q-1$ is an integer and therefore

$$|N_1(K) - q - 1| \leq [2g\sqrt{q}]$$

where $[x]$ refers to the greatest integer less than or equal to x. The following theorem due to Serre gives an improvement of the Weil bound.

Theorem 4.1 (Serre bound)**.**

$$|N_1(K) - q - 1| \leq g[2\sqrt{q}]$$

Proof. Recall that

$$L_K(u) = \prod_{i=1}^{2g}(1 - \alpha_i u)$$

Hence

$$\begin{aligned} u^{2g} L_K\left(\frac{1}{u}\right) &= u^{2g} \prod_{i=1}^{2g} \left(1 - \frac{\alpha_i}{u}\right) \\ &= \prod_{i=1}^{2g} (u - \alpha_i) \end{aligned}$$

However $L_K(u) \in \mathbb{Z}[u]$ with $L_K(0) = 1$, so let it be $1 + r_1 u + \ldots + r_{2g} u^{2g}$. Therefore

$$\begin{aligned} u^{2g} L_K\left(\frac{1}{u}\right) &= u^{2g} \left(1 + \frac{r_1}{u} + \ldots + \frac{r_{2g}}{u^{2g}}\right) \\ &= u^{2g} + r_1 u^{2g-1} + \ldots + r_{2g} \in \mathbb{Z}[u]. \end{aligned}$$

Hence α_is are all algebraic integers.

The Riemann Hypothesis tells us that $|\alpha_i| = \sqrt{q}$ for all i. Hence $\alpha_i \overline{\alpha}_i = q$. We have already shown that the function equation for L_K gives us a permutation of $\alpha_1, \alpha_2, \ldots, \alpha_{2g}$ by

$$\alpha_i \rightsquigarrow \frac{q}{\alpha_i}.$$

Therefore $\overline{\alpha}_i = \frac{q}{\alpha_i}$ is actually α_j for some j. Thus we can pair up the α_is and relabel them as follows :

$$\{(\alpha_1, \overline{\alpha}_1), (\alpha_2, \overline{\alpha}_2), \ldots, (\alpha_g, \overline{\alpha}_g)\}$$

Now for all $i \leq 2g$, set

$$\begin{aligned} \gamma_i &= \alpha_i + \overline{\alpha}_i + [2\sqrt{q}] + 1 \\ \delta_i &= -\alpha_i - \overline{\alpha}_i + [2\sqrt{q}] + 1. \end{aligned}$$

$|\alpha_i| = \sqrt{q}$ implies that γ_i, δ_i are all strictly positive real numbers. Note that they being combinations of algebraic integers are themselves algebraic integers. Set

$$\gamma = \prod_{i=1}^{g} \gamma_i \text{ and } \delta = \prod_{i=1}^{g} \delta_i$$

which are also algebraic integers. Now any embedding σ of $\mathbb{Q}\left(\alpha_1, \overline{\alpha}_1, \alpha_2, \dots, \alpha_g, \overline{\alpha}_g\right)$ in $\mathbb{C}$ has to send α_i to some α_j or $\overline{\alpha}_j$ because they are roots of the polynomial $u^{2g} L_K\left(\frac{1}{u}\right)$ which has integer coefficients. Now

$$\begin{aligned} \sigma(\overline{\alpha}_i) &= \sigma\left(\frac{q}{\alpha_i}\right) \\ &= \frac{\sigma(q)}{\sigma(\alpha_i)} \\ &= \frac{q}{\sigma(\alpha_i)} \\ &= \overline{\sigma(\alpha_i)} \end{aligned}$$

Thus σ permutes $\{\gamma_i\}_{i \leq g}$ and also $\{\delta_i\}_{i \leq g}$. And therefore for any embedding σ,

$$\sigma(\gamma) = \gamma \text{ and } \sigma(\delta) = \delta.$$

This shows that $\gamma, \delta \in \mathbb{Q}$. However they are also algebraic integers and therefore they must actually lie in $\mathbb{Z}$ as $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$. Note that they are also strictly positive and hence ≥ 1.

Let us now apply the arithmetic-geometric mean to γ_is.

$$\begin{aligned} \frac{\sum_{i=1}^{g} \gamma_i}{g} &\geq \sqrt[g]{\gamma} \geq 1 \\ &\implies \sum_{i=1}^{g} \alpha_i + \overline{\alpha}_i + g[2\sqrt{q}] + g \geq g \\ &\implies -N_1(K) + q + 1 + g[2\sqrt{q}] \geq 0 \end{aligned}$$

Applying it to δ_is gives us $N_1(K) - q - 1 + g[2\sqrt{q}] \geq 0$ and combining both these gives us the improved Serre bound.

□

Appendices

Appendix A

Discrete valuation rings

Discrete valuation rings keep popping up innumerably often during the study of curves and for the convenience of the amateur algebraist (like the author), we devote this appendix for defining a *DVR* (as it shall be called henceforth) and proving its basic properties.

Theorem A.1. *Let R be a domain but not a field. The following are equivalent:*

1. *R is noetherian, local with principal maximal ideal M.*
2. *$\exists t \in R$, an irreducible element of R, such that any $r \neq 0 \in R$ can be uniquely expressed as $u_r t^{n_r}$ where u_r is a unit of R and $n_r \in \mathbb{N} \cup \{0\}$.*

And any ring R which satisfies the above properties is called a DVR.

Proof. To show that the first condition implies the second, pick t to be a principal generator of the maximal ideal M. If $pq = t$, then as M is maximal and hence prime, either $p \in M$ or $q \in M$, say p. Thus $p = rt$ as $M = (t)$. Therefore $t = pq = rtq$ which gives us that $t(1 - rq) = 0$ and because R is a domain and $M = (t) \neq 0$, q is a unit and hence t is irreducible.

If $r = ut^n = vt^m$ for u, v units of R with $n \geq m$ say, then $\frac{v}{u} = t^{n-m}$ and as the expression on the left hand side of the equation is a unit, it means that $n = m$ and hence expression in such a form is unique.

To show the existence of such an expression in this form, pick $0 \neq r \in R$. If r is a unit, $r = rt^0$. If not, then $r \in M = (t)$, therefore $r = r_1 t$. If r_1 is a unit, then done, else $r_1 = r_2t$ and $r = r_2t^2$ and so on with $r_m = r_{m+1}t$ and $r = r_mt^m$ if r_m is not a unit and $r_m \neq 0$. If none of the r_is are units, we get an ascending chain

$$(r_1) \subseteq (r_2) \ldots \subseteq (r_m) \subseteq \ldots$$

which should terminate because of noetherianess of the ring R. If $(r_n) = (r_{n+1})$, then $r_{n+1} = r_nx = r_{n+1}tx$, which implies that t is a unit, a contradiction.

For showing the other direction of equivalence, given any nonzero ideal I, pick N to be the minimum of the set $S = \{n_\alpha | u_\alpha t^{n_\alpha} \in I \text{ for any unit } u_\alpha \in R\}$.Then t^N generates the ideal I and thus $I = (t)^N$. Thus R is a principal ideal domain and clearly the unique maximal ideal is (t).

□

Quite often, we will denote a DVR by a pair (R, M), in which case R should be taken to be the ring and M, its unique maximal ideal. Any principal generator of M is referred to as a *uniformizer.*

Note that any nonzero element x of the fraction field K of R can be expressed uniquely as ut^n (If $x = \frac{r}{s}$ where $r, s \in R$ such that $r = ut^n$ and $s = vt^m$, then $x = \frac{u}{v}t^{n-m}$. That this expression is well defined is easily checked), with u an unit of R and $n \in \mathbb{Z}$. This defines a *valuation* on the elements of K as follows :

$$v : K \to \mathbb{Z} \cup \{\infty\} \text{ where } v(0) = \infty \text{ and } v(ut^n) = n \text{ with u a unit in R}$$

v satisfies the following properties

- $v(xy) = v(x) + v(y) \forall x, y \in K$
- $v(x + y) \geq \min(v(x), v(y)) \forall x, y \in K$

Sometimes $v(k)$ is also denoted by $\mathrm{ord}_M(k)$ if the maximal ideal in the DVR is to be emphasised.

Corollary A.2. *Thus a DVR is a local principal ideal domain which is not a field and any non trivial ideal is a power of the maximal ideal. Therefore the only nonzero prime ideal of the DVR is the maximal ideal.*

Proposition A.3. *If R is a DVR and K, its fraction field, then for any $x \in K$, either $x \in R$ or $\frac{1}{x} \in R$.*

Proof. If $x \notin R$, then $x = ut^{-n}$ where $n \in \mathbb{N}$ and u a unit of R. Thus $\frac{1}{x} = \frac{1}{u}t^n \in R$. □

Proposition A.4. *(R, M), a DVR, is integrally closed in its field of fractions K, (ie) any element of K satisfying a monic polynomial equation with coefficients in R belongs to R.*

Proof. Let $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ for some $x \in K$ and $a_0, a_1, \ldots, a_{n-1} \in R$. If $x \notin R$, then $\frac{1}{x} \in R$ by the above proposition. Dividing the equation by x^{n-1}, we get $x = -\left(a_{n-1} + \ldots + \frac{a_0}{x^{n-1}}\right)$. The expression on the righthand side is in R and hence $x \in R$.

□

A ring R is said to be a *Dedekind domain* if it is a noetherian domain, integrally closed in its field of fractions with every nonzero prime ideal being maximal. An interesting property (which can even be used as an alternative definition) that it enjoys is that every nonzero ideal of R can be uniquely factorised into prime ideals (See *Serre, Local fields* for a reference). Not surprisingly, discrete valuation rings and dedekind domains are interrelated as the next proposition shows.

Proposition A.5. *If R is a dedekind domain and M, a nonzero maximal ideal, then R_M, (which is the localization of R with respect to the multiplicatively closed set $R \setminus M$) is a DVR.*

Proof. Since R is a noetherian domain, so is R_M. The latter is also clearly local. By unique factorisation of ideals into prime ideals, $M \neq M^2$. Hence choose a $y \in M \setminus M^2$. As $M^2 \subsetneq Ry + M^2 \subseteq M$, we find that $M = Ry + M^2$.

The maximal ideal $\mathfrak{m}$ of R_M is generated by M. Thus $\mathfrak{m} = \mathfrak{m}^2 + R_M y$ and so

$$\frac{\mathfrak{m}}{R_M y} = \frac{R_M y + \mathfrak{m}\mathfrak{m}}{R_M y} = \mathfrak{m}\left(\frac{\mathfrak{m}}{R_M y}\right).$$

Applying the nakayamma lemma, we get $\frac{\mathfrak{m}}{R_M y} = 0$ which implies that the maximal ideal $\mathfrak{m} = R_M y$ is principal and hence R_M is a DVR.

□

Appendix B

Adele rings and Weil differentials

To define the notion of an adele ring, we need the concepts of completion of fields and DVRs.

Completion of local rings

A purely algebraic way of completing local rings involves the construction of what is known as an *inverse* limit which we describe below.

The inverse limit

A collection of rings $\{A_i\}_{i\in I}$ where I is a poset along with ring homomorphisms $\{f_{ij} : A_j \to A_i | i \leq j\}$ is said to be an *inverse system* of rings if the following properties are satisfied:

- f_{ii} is the identity map on A_i.
- $f_{ij} \circ f_{jk} = f_{ik}$ for any $i \leq j \leq k$.

The inverse limit of an inverse system of rings A_i is then defined as follows:

$$A = \varprojlim A_i := \{(a_i)_{i\in I} \in \prod_{i\in I} A_i | f_{ij}(a_j) = a_i \forall j \geq i\}$$

Note that A acquires a ring structure (operations carry over component wise) and comes with natural projection maps $\pi_i : A \to A_i$ which satisfy $\pi_i = f_{ij} \circ \pi_j$.

For the categorically minded, inverse limits satisfy the following universal property:

If X is any ring with ring homomorphisms $\pi'_i.X \to A_i$ for all $i \in I$ such that $\pi'_i = f_{ij} \circ \pi'_j$ for all $i \leq j$, then there exists a unique ring homorphism $\theta : X \to A$ such that $\pi'_i = \pi_i \circ \theta$ for every i.

In other words, the following diagram commutes:

$$\begin{tikzcd}
& X \arrow[ddl, "\pi'_i"'] \arrow[d, "!\theta"] \arrow[ddr, "\pi'_j"] & \\
& A \arrow[dl, "\pi_i"] \arrow[dr, "\pi_j"'] & \\
A_i & & A_j \arrow[ll, "f_{ij}"]
\end{tikzcd}$$

To verify that our definition of inverse limit does indeed satisfy the above property, let us construct the ring homomorphism θ. Note that if $\theta(x) = (a_i)_{i \in I}$, then we want $\pi_i(\theta(x)) = \pi'_i(x)$. So we are forced to define $\theta(x) = (\pi'_i(x))_{i \in I}$ (and hence the uniqueness of θ follows). Now it is easy to check that $\theta(x) \in A$ because $f_{ij}(\pi'_j(x)) = \pi'_i(x)$ which is the i^{th} co-ordinate of $\theta(x)$. And clearly $\pi_i \circ \theta = \pi'_i$.

The property is universal because if there exists any other ring B with ring homomorphisms $\chi_i : B \to A_i \forall i \in I$ such that $\chi_i = \chi_j \circ f_{ij} \forall i \leq j$ which satisfies the property, then B is isomorphic as a ring to A, our inverse limit. This follows from the commutative diagram below :

$$\begin{tikzcd}
 & & A \arrow[d, "\psi"] \arrow[dddll, "\pi_i"'] \arrow[dddrr, "\pi_j"] & & \\
 & & B \arrow[d, "\theta"] \arrow[ddll, "\chi_i"'] \arrow[ddrr, "\chi_j"] & & \\
 & & A \arrow[dll, "\pi_i"] \arrow[drr, "\pi_j"'] & & \\
A_i & & & & A_j \arrow[llll, "f_{ij}"]
\end{tikzcd}$$

(Since A, B both satisfy the property, we find ring homomorphisms $\theta : B \to A$ and $\psi : A \to B$ which makes the above diagram commute. Now $\pi_i \circ \theta = \chi_i$ and $\chi_i \circ \psi = \pi_i \; \forall i \in I$. This implies that $\pi_i \circ (\theta \circ \psi) = \pi_i$ for all $i \in I$. So $\theta \circ \psi : A \to A$ is the unique homomorphism that satisfies $\pi_i \circ (\theta \circ \psi) = \pi_i$ for all $i \in I$. However the identity map I_A of A also does the job. Thus by the uniqueness of the homormorphism, we get $\theta \circ \psi = I_A$. Arguing similarly, we find $\psi \circ \theta = I_B$ and thus $A \cong B$ as rings and the ring isomorphism is compatible with the homomorphisms χ_is and π_is.)

And finally, the completion of a local ring (R, M) is defined to be the inverse limit of the system $\left(\frac{R}{M^n}\right)_{n\in\mathbb{N}}$ where the $f_{ij} : \frac{R}{M^j} \to \frac{R}{M^i}$ for $j \geq i$ sends $r + M^j \rightsquigarrow r + M^i$.

$$\hat{R} := \varprojlim \frac{R}{M^n}$$

Our original ring R (if it is noetherian) sits inside its completion $\hat{R}$ as $r \hookrightarrow \hat{r} = (r + M^i)_{i\in\mathbb{N}}$. Note that $\hat{R}$ so defined is a local ring itself. One can show this by checking that the set of nonunits of $\hat{R} = \{(\bar{a}_i)_{i\in\mathbb{N}} | a_i \in M\}$ (where $\bar{a}_i = a_i + M^i$) which is an ideal[1]. In fact, completion of a DVR turns out to be a DVR and we record it as a proposition below:

Proposition B.1. *If (R, M) is a DVR, then so is $\hat{R}$.*

Proof. If $z = (a_i + M^i)_{i\in\mathbb{N}}$ is a nonzero nonunit, then find the least integer N such that $a_{N+1} + M^{N+1} \neq 0$. Let $a_i = u_i t^{x_i}$ where u_is are units of R. So clearly for all $i \leq N$, $x_i \geq i$, and $x_{N+1} < N + 1$. Note that

[1] $(\bar{a}_i)_{i\in\mathbb{N}}$ is a unit iff $a_1 \notin M$ because if $a_i \notin M$, then a_1 is a unit of R and so is every a_i and hence $(\bar{a}_i)\left(\overline{\frac{1}{a_i}}\right) = 1 \in \hat{R}$. If $(\bar{a}_i)$ is a unit, clearly $\bar{a}_1 \neq 0$ as $\frac{R}{M}$ is a field and so $a_1 \notin M$

$$u_it^{x_i} + M^{N+1} = u_{N+1}t^{x_{N+1}} + M^{N+1} \forall i \geq N+1$$

Hence $x_i \leq N$ for all $i > N$. Also $x_i \geq x_j$ if $i \geq j$. This forces $x_n = N \forall n \geq N$.

Also because $u_{N+i}t^N - u_{N+j}t^N \in M^{N+j}$, we have $u_{N+i} - u_{N+j} \in M^j$. Thus $u = (u_{N+i} + M^i)_{i \in \mathbb{N}} \in \hat{R}$ and $u\hat{t}^N = z$ where $\hat{t} = (t + M^i)_{i \in mathbbN}$ (for $z = (a_i + M^i)_{i \in \mathbb{N}} \in \hat{R} \implies a = (a_{J+i} + M^i)_{i \in \mathbb{N}}$ for any $J \in \mathbb{N}$).

Observe that u is a unit of $\hat{R}$ as $u_{N+1} \notin M$ and $\hat{t}$ is a uniformizer of $\hat{R}$. The fact that $\hat{R}$ is a domain should be clear from the above discussion.

We would also like to observe that $\operatorname{ord}_M(r) = ord_{\hat{M}}(\hat{r})$ for $r \in R$ where $\hat{M}$ is the maximal ideal of $\hat{R}$.

□

Completion of fields

An absolute value on a field K is a function $|\ | : K \to \mathbb{R}_+ \cup \{0\}$ such that it satsifies the following properties :

- $|x| = 0$ iff $x = 0$.
- $|xy| = |x||y|$ for all $x, y \in K$.
- $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

The absolute value $|\ |$ defines a metric on K given by

$$d(x, y) = |x - y|.$$

K is said to be *complete* under $|\ |$ if all Cauchy sequences of K converge when K is given the metric induced by $|\ |$.

A *completion* of K is defined to be a field $\hat{K}$ with an absolute value $||\ ||$ such that $K \hookrightarrow \hat{K}$, $||\ |||_K = |\ |$, and K is dense is $\hat{K}$ under the metric induced by $||\ ||$.

Theorem B.2. *Given any field K and an absolute value $|\ |$ on it, there exists a completion of it which is unique upto isomorphism.*

Proof. From now on, K will be given the metric induced by $|\ |$. Let S denote the commutative ring[2] of all Cauchy sequences of K. Let

$$M = \{(x_n)_{n\in\mathbb{N}} | \lim_{n\to\infty} x_n = 0$$

Claim: M is a maximal ideal of S

It is clear that M is an ideal of S. To see that it is maximal, pick a Cauchy sequence which doesn't tend to 0, say $x = (x_n)_{n\in\mathbb{N}}$. As the limit of this Cauchy sequence is non zero, there exists an N such that for all $n \geq N$, $x_n \neq 0$, in fact $\exists r > 0$ such that $|x_n| > r$ for large enough n. The sequence

$$y = (\underbrace{0, 0, \ldots, 0}_{N-1}, \frac{1}{x_N}, \frac{1}{x_{N+1}}, \ldots)$$

is hence itself a Cauchy sequence. And the following equation shows that M is maximal.

$$xy + (\underbrace{1, 1, \ldots, 1}_{N-1}, 0, 0, \ldots, 0, \ldots) = (1, 1, \ldots, 1, \ldots)$$

Define $\hat{K} := \frac{S}{M}$.

Note that K sits inside $\hat{K}$ as $k \hookrightarrow (k, k, k, \ldots, k, \ldots)$.

The absolute value $||\ ||$ is given by $||(x_n)_{n\in\mathbb{N}}|| = \lim_{n\to\infty} |x_n|$. Note that this exists because $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence in K and hence $(|x_n|)_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{R}$, which is complete. That $||\ ||$ is well defined and indeed an absolute value can be checked easily. And $||(k, k, k \ldots)|| = |k|$ and hence is compatible with $|\ |$.

Claim: $\hat{K}$ is complete with respect to $||\ ||$

This is proved by the usual diagonalisation trick.

Let $X_1 + M, X_2 + M, \ldots$ be a Cauchy sequence in $\hat{K}$ where each X_i is a Cauchy sequence of K which represents the coset $X_i + M$.

[2] $|x_n y_n - x_m y_m| \leq |y_n||x_n - x_m| + |x_m||y_n - y_m|$ and $\{x_n\}$, $\{y_n\}$ being Cauchy sequences are bounded.

$$\begin{array}{cccccc}
X_1: & x_1^1 & x_2^1 & \dots & x_n^1 & \dots \\
X_2: & x_1^2 & x_2^2 & \dots & x_n^2 & \dots \\
X_3: & x_1^3 & x_2^3 & \dots & x_n^3 & \dots \\
. & . & . & . & . & . \\
. & . & . & . & . & . \\
X_k: & x_1^k & x_2^k & \dots & x_n^k & \dots \\
. & . & . & . & . & . \\
. & . & . & . & . & .
\end{array}$$

Assume that any two terms of X_i lie within $\frac{1}{i}$ distance of each other, (ie) $|x_r^i - x_s^i| < \frac{1}{i}$. This can be done by chopping off the first few terms of each of the X_is. Note that the chopped sequence also lies in the same coset as the previous one.

Construct a sequence $\xi = (x_1^1, x_2^2, \dots, x_n^n, \dots)$ by the famed diagonalisation procedure.

ξ is a Cauchy sequence because given $\epsilon > 0$, for large enough n, m, you can choose a large enough i so that

$$\begin{aligned}
d(x_n^n, x_m^m) &\leq d(x_n^n, x_i^n) + d(x_i^n, x_i^m) + d(x_i^m, x_m^m) \\
&< \frac{1}{n} + \frac{\epsilon}{3} + \frac{1}{m}
\end{aligned}$$

We leave it to the reader to verify that $\xi + M$ is indeed the limit of the sequence $X_1 + M, X_2 + M, \dots, X_n + M \dots$

And finally, given any Cauchy sequence $x = (x_n)_{n \in \mathbb{N}} \in \hat{K}$, given $\epsilon > 0$, there exists an N such that for all $n \geq N$, $v(x_n - x_N) < \epsilon$. Hence the sequence $(x_N, x_N, \dots, x_N \dots) \in K \hookrightarrow \hat{K}$ lies in the ϵ ball around x. This shows that K is dense in $\hat{K}$.

For the uniqueness part, if $(T, |\ |_t)$ and $(S, |\ |_s)$ are two completions of $(K, |\ |)$ such that $k \in K$ sits as $k_s \in S$ and $k_t \in T$, let us define a map $\psi : S \to T$ which sends $k_s \in K \rightsquigarrow k_t$.

If $x \in S \setminus T$, then as K is dense in S, there exists a Cauchy sequence $(x_n)_{n \in \mathbb{N}}$ with $x_i \in K \hookrightarrow S$ for all i such that x is the limit of the sequence. Now as $|\ |_s|_K = |\ |_t|_K = |\ |$, $(\psi(x_n))_{n \in \mathbb{N}}$ is a Cauchy sequence in T whose limit is say y (because T is complete). Define $\psi(x) = y$.

This is well-defined because if $(x_n)_{n \in \mathbb{N}}, (y_n)_{n \in \mathbb{N}}$ with $x_i, y_i \in K \forall i$ tend to x, then

$(x_n - y_n)_{n\in\mathbb{N}}$ tends to 0 in S and hence $(\psi(x_n - y_n))_{n\in\mathbb{N}}$ tends to 0 in T also.

ψ is a field homomorphism by the way it has been constructed and can be shown to be bijective by using the fact that K is dense in T, S again.

□

Now let (R, P) be a discrete valuation ring with fraction field K. It defines an absolute value $|\ |_P$ on K as given below :

$$|k|_P = 2^{-\operatorname{ord}_P(k)} \forall k \neq 0 \text{ and } |0|_P = 0$$

$\hat{R}$, the completion of (R, P) as we have defined earlier, turns out to be the closure of $R \hookrightarrow \hat{K}$, which we shall call $\bar{R}$, under the topology induced by the absolute value $|\ |_P$.We will prove this by giving a bijective map ψ between $\hat{R}$ and the closure of R in $\hat{K}$, which we shall denote by $\bar{R}$.

Let S denote the ring of Cauchy sequences in K, M, the maximal ideal consisting of all sequences which tend to 0. Firstly note that

$$\bar{R} = \{\bar{r} = (r_i)_{i\in\mathbb{N}} + M | \bar{r} \text{ is a Cauchy sequence in } K, r_i \in R \forall i\}^3$$

Let $\hat{x} = (x_i + P^i)_{i\in\mathbb{N}}$ be an element of $\hat{R}$ with $x_i \in R$ for all i. Define

$$\psi(\hat{x}) = (x_i)_{i\in\mathbb{N}} + M$$

Observe that $\hat{x} \in \hat{R}$ implies that $(x_i)_{i\in\mathbb{N}}$ is a Cauchy sequence in K (as for large enough $m \geq n$, $x_m - x_n \in P^n$ implies $d(x_m, x_n) = 2^{-\operatorname{ord}_P(x_m - x_n)} \leq 2^{-n}$).

To check that ψ is well-defined, it is enough to note that

$$\begin{aligned} &(x_i + P^i)_{i\in\mathbb{N}} = (y_i + P^i)_{i\in\mathbb{N}} \in \hat{R} \\ \implies &x_i - y_i \in P^i \forall i \\ \implies &\lim_{i\to\infty} |x_i - y_i|_P \leq \lim_{i\to\infty} 2^{-i} = 0. \end{aligned}$$

[3] Given any sequence $\bar{x} = (x_i)_{i\in\mathbb{N}} + M$ which is the limit of the sequence $f = \bar{r_1}, \bar{r_2}, \ldots$, where $\bar{r_i}$ denotes the coset containing the constant sequence $(r_i, r_i, \ldots, r_i, \ldots)$, then afortiori f is a Cauchy sequence and hence so is $r = (r_1, r_2, \ldots, r_n, \ldots)$. It is also clear that $r + M$ is the limit of f and hence $r + M = \bar{x}$

And as $x_i \in R$ for all i, $(x_i)_{i \in \mathbb{N}} \in \bar{R}$.

Claim: ψ is bijective

If $\hat{x} = (x_i + P^i)_{i \in \mathbb{N}}$ and $\hat{y} = (y_i + P^i)_{i \in \mathbb{N}}$ map to the same element under ψ in $\bar{R}$, this would mean that the sequence $(x_i - y_i)_{i \in \mathbb{N}}$ tends to 0. Thus given any integer N, $x_i - y_i \in P^N$ for suitably large i. However $x_i - x_N \in P^N \forall i \geq N$ as $x \in \hat{R}$ and so also for y_i. Thus $x_N - y_N \in P^N \forall N$, which means that $x = y$ and hence ψ is injective.

To show that it is surjective as well, take $\bar{r} = (r_i)_{i \in \mathbb{N}} + M$, $r_i \in R \forall i$, to be an element of $\bar{R}$. Pick a subsequence of $\bar{r}$, say $\bar{q} = (q_i)_{i \in \mathbb{N}}$ such that $d(q_n, q_m) < 2^{-i}$ for all $n, m \geq i$. This you can do because $\bar{r}$ is a Cauchy sequence. Note that $\bar{q}$ is a Cauchy sequence itself as it is a subsequence of a Cauchy sequence and is in fact equivalent to $\bar{r}$, (ie) $\bar{r} - \bar{s} \in M$.

The element $\hat{q} = (q_i + P^i)_{i \in \mathbb{N}}$ is in $\hat{R}$ and $\psi(\hat{q}) = \bar{q}$.

As a final remark, we observe that $\hat{K}$ is indeed the fraction field of the DVR $\hat{R}$, as one would expect.

The adele ring

Let us begin by fixing some notations :

- K is a finitely generated function field in one variable over F such that F is algebraically closed in K.
- S_K denotes the set of all prime divisors of K
- $| \,|_P$ is the absolute value on K as described in the previous section
- $\hat{K}_P$ refers to the completion of K with respect to the above absolute value
- $\hat{O}_P$ denotes the completion of the local ring O_P under the same absolute value and $\hat{P}$ - the maximal ideal of $\hat{O}_P$.

Now we are ready to define the *adele ring* A_K of K as :

$$A_K = \{(a_P)_{P \in S_K} \in \prod_{P \in S_K} \hat{K}_P | a_P \in \hat{O}_P \text{ for all but finitely many } Ps\}$$

Note that K sits inside A_K as $k \hookrightarrow (k, k, \ldots, k \ldots)$. Apart from a ring structure, A_K also has a K vector space structure because $k(x_P)_{P \in S_K} = (kx_P)_{P \in S_K}$. Hence it is also an F vector space.

For each divisor $D = \sum_{P \in S_K} n(P)P$ of K, we associate an F subspace[4] of A_K as follows:

$$A_K(D) = \{(x_P)_{P \in S_K} | ord_{\hat{P}}(x_P) \geq -n(P)\}$$

The Weil differential

$\omega : A_K \to F$, an F-linear map is said to be a Weil differential if the following conditions hold

- $\omega(K) = 0$
- $\omega(A_K(D)) = 0$ for some divisor D of K.

The set of all Weil differentials will play an important role in the proof of the Riemann-Roch theorem and hence we give it a name -

$$\Omega_K := \{\omega | \omega \text{ is a Weil differential}\}$$

It can be made into a K vector space by defining $k\omega : A_K \to F$ to be a map which sends $\xi \rightsquigarrow \omega(k\xi)$. Note that $k\omega$ is also a Weil-differential because

- $k\omega(f\xi) = \omega(fk\xi) = f\omega(k\xi) = f(kw)(\xi)$ and hence it is an F-linear map.
- $k\omega(k') = \omega(kk') = 0$ as $kk' \in K$ and $\omega \in \Omega_K$.
- We prove a little lemma first

  Lemma B.3. *$\xi \in A_K((k) + D)$ iff $k\xi \in A_K(D)$*

[4] To see that this is indeed an F vector space, it is enough to observe that if $(x_P)_{P \in S_K} \in A_K(D)$, then $ord_{\hat{P}}(fx_P) = ord_{\hat{P}}(f) + ord_{\hat{P}}(x_P) \geq -n(P)$ because $ord_{\hat{P}}(f) \geq 0$ since $F \subseteq O_P \subseteq \hat{O}_P$.

Proof. Let $D = \sum_{P \in S_K} n(P)P$. Then

$$\begin{aligned}
&\xi = (x_P)_{P \in S_K} \in A_K((k) + D) \\
&\iff \operatorname{ord}_{\hat{P}}(x_P) + n(P) + \operatorname{ord}_P(k) \geq 0 \forall P \\
&\iff \operatorname{ord}_{\hat{P}}(kx_P) + n(P) \geq 0 \forall P (\operatorname{ord}_P(k) = \operatorname{ord}_{\hat{P}}(k)) \\
&\iff (kx_P)_{P \in S_K} \in A_K(D)
\end{aligned}$$

□

Since ω is a Weil-differential, $\omega(A_K(D)) = 0$ for some divisor D, and therefore $k\omega(A_K((k) + D)) = 0$ ($k\omega(\xi) = \omega(k\xi) = 0$ if $\xi \in A_K((k) + D)$ because then $k\xi \in A_K(D)$).

Another object which will be of use to us is

$$\Omega_K(D) = \{\omega | \omega \in \Omega_K, \omega(A_K(D)) = 0\}.$$

Appendix C

Riemann-Roch

Let us define a quantity $r(D)$ for each divisor D as follows:

$$r(D) := \deg(D) - l(D)$$

Note that if $D \sim C$, then $r(D) = r(C)$.

Lemma C.1. *If D, C are two divisors of K such that $D \leq C$, then $r(D) \leq r(C)$.*

Proof.

$$\begin{aligned} r(C) - r(D) &= (\deg(C) - l(C)) - (\deg(D) - l(D)) \\ &= (\deg(C) - \deg(D)) - (l(C) - l(D)) \end{aligned}$$

Clearly $\dim_F \frac{L(C)}{L(D)} = l(C) - l(D)$.

Claim: $\dim_F \frac{A_K(C)}{A_K(D)} = \deg(C) - \deg(D)$

To see this first note that $C \geq D$ implies $A_K(C) \supseteq A_K(D)$. As C is the sum of D and finitely many primes, it is enough to show that for any prime P,

$$\dim_F \frac{A_K(D+P)}{A_K(D)} = \deg(P)$$

One way to show this is the following. Let $D = \sum_{Q \in S_K} n(Q)Q$. Choose t to be a uniformizer of $\hat{O}_P$ and define a map

$$T : A_K(D+P) \to \frac{\hat{O}_P}{\hat{P}} \text{ by } (a_Q)_{Q\in S_K} \rightsquigarrow a_P t^{n(P)+1} + \hat{P}$$

Note that

$$\begin{aligned} &(a_Q)_{Q\in S_K} \in A_K(D+P) \\ &\implies \operatorname{ord}_{\hat{P}}(a_P) \geq -n(P) - 1 \\ &\implies \operatorname{ord}_{\hat{P}}(a_P t^{n(P)+1}) \geq 0 \\ &\implies a_P t^{n(P)+1} \in \hat{O}_P \end{aligned}$$

and hence T is well-defined. Any element $a = (a_Q)_{Q\in S_K}$ which belongs to the kernel of T must have $\operatorname{ord}_{\hat{P}} a_P \geq -n(P)$ which implies that $a \in A_K(D)$. The other inclusion , namely $A_K(D) \subseteq \text{kernel}(T)$ is clear.

Now let us do some algebraic manipulation of vector spaces to get a vector space of dimension $r(C) - r(D)$. It should be clear that $L(C) = A_K(C) \cap K$ and similarly for D. However $L(D) \subseteq L(C) \subseteq K$ and hence $L(D) = A_K(D) \cap L(C)$. Thus we have

$$\frac{L(C)}{L(D)} = \frac{L(C)}{A_K(D) \cap L(C)} = \frac{A_K(D) + L(C)}{A_K(D)}.$$

Therefore we have,

$$\frac{\frac{A_K(C)}{A_K(D)}}{\frac{A_K(D)+L(C)}{A_K(D)}} = \frac{A_K(C)}{A_K(D) + L(C)}$$

with the dimension of this vector space being $r(C) - r(D)$ which hence has to be non-negative.

□

Theorem C.2 (Riemann inequality)**.** *Let K be an algebraic function field over F with the latter as its constant field (ie) F is algebraically closed in K. Then $\exists! g \in \mathbb{Z}_+ \cup \{0\}$ such that $\deg(D) - g + 1 \leq l(D) \forall D$, divisors of K.*

*This integer g is called the **genus** of K.*

Also there exists a constant c such that for any divisor D with $\deg(D) \geq c$*, then* $l(D) = \deg(D) - g + 1$.

Idea of the proof : We construct an increasing sequence of divisors D_m and show that $\{r(D_m)\}$ is uniformly bounded above. Thus $r(D_m)$ will become a constant for large enough m and the constant we call $g - 1$. Then we show that for any divisor D, there exists an equivalent divisor C such that $r(C) \leq r(D_m)$ for some m.

Proof. Choose an $x \in K \setminus F$. Thus $K/F(x)$ is a finite extension of say, degree n. Let $B = (x)_\infty$. As proved in Proposition 1.2 in the first section $\deg(B) = [K : F(x)]$. Thus

$$r(mB) = \deg(mB) - l(mB) = mn - l(mB) \forall m \in \mathbb{N}.$$

We want to give an uniform upper bound for $r(mB)$ and thus need a lower bound for $l(mB)$. We can do so by finding some F linearly independent elements $y_i \in L(mB)$ which we recall is $\{0\} \cup \{k \in K^*, (k) + mB \geq 0\}$. If $y \in L(mB)$, then $(y) + mB \geq 0$ which means that y should have all its poles (if at all) only at the primes that are in the prime support of B.

A good place to look for such elements is in the integral closure of $F[x]$ (denoted by R) in K because $\mathrm{ord}_P(x) \geq 0$ implies that $x \in O_P$ which in turn implies $F[x] \subseteq O_P$. Hence $R \subseteq O_P$ as O_P is integrally closed in K, which means that $\mathrm{ord}_P(y) \geq 0$ if $y \in R$.

Let $\rho_1, \rho_2, \ldots, \rho_n$ be an $F(x)$ basis of K with $\rho_i \in R \forall i$ (as the fraction field of R is K). Choose m_0 big enough so that $(\rho_i) + m_0 B \geq 0 \forall i \leq n$. Thus

$$\rho_i \in L(mB) \forall m \geq m_0.$$

In fact, we can find many more F linearly independent elements in $L(mB)$, namely

$$\{x^j \rho_i | 0 \leq j \leq m - m_0, 1 \leq i \leq n\}.$$

This is so because

$$\begin{aligned}(x^j\rho_i)+mB &= j(x)+(m-m_0)B+m_0B+(\rho_i)\\ &\geq j(x)+(m-m_0)B(\text{ as } \rho_i\in L(m_0B))\\ &\geq 0(\text{ as } 0\leq j\leq m-m_0 \text{ and } (x)=(x)_0-B)\end{aligned}$$

These are clearly F-linearly independent because $\{\rho_i\}$ forms an $F(x)$ basis of K.

Thus we have found $(m-m_0+1)(n)$ F linearly independent elements in $L(mB)$ which gives us that $l(mB)\geq mn-m_0n+n$ which implies that $r(mB)\leq m_0n-n\forall m$.

Thus we have an increasing sequence of divisors

$$m_0B\leq(m_0+1)B\ldots\leq mB\leq\ldots$$

and using lemma C.1 and the fact that $r(mB)$ is uniformly upper bounded, choose $g-1$ to be the supremum of the set $\{r(mB)\}_{m\geq m_0}$. As $0\leq mB$ for any non negative integer m, $r(0)=-1\leq r(mB)\leq g-1$ and hence $g\geq 0$.

Now given any divisor D, we would like to find an equivalent divisor C such that $C\leq mB$ for some m. This would imply that $r(D)=r(C)\leq r(mB)\leq g-1$. Thus we want an element $f\in F[x]$ such that $D\leq mB+(f)$ for some non-negative integer m. This translates to finding an f such that $0\leq mB+(f)-D$.

Let $-D=D_1+D_2$ where x has no pole at any prime in the prime support of D_1, whereas x has a pole at every prime in the prime support of D_2. Now if P is a prime in the prime support of D_1, then as $\mathrm{ord}_P(x)\geq 0$, $x\in O_P$ and therefore $F[x]\subseteq O_P$. Let $F[x]\cap P=F[x]g_P$ where $g_P\in F[x]$. Thus $\mathrm{ord}_P(g_P)\geq 1$ and thus $\exists$ some positive integer, say b_P such that the coefficient of P in $(g_P^{b_P})+D_1$ is non-negative. Also $\mathrm{ord}_Q(g_P)\geq 0$ for any prime Q which lies in the prime support of D_1 as again, $F[x]\in O_Q$. Let

$$f=\prod_{P\in\text{ support of } D_1} g_P^{b_P}.$$

Then if the coefficient of P, a prime, in $(f)+D_1$ is negative, then it has to lie in the prime support of B. Since D_2's prime support has only primes at which x has a pole, we have that any prime for which $(f)+D_1+D_2=(f)-D$ has a negative coefficient lies in the prime support of B. And thus $\exists m\in\mathbb{N}$ such that

$$(f) - D + mB \geq 0$$

To find the constant c, find an m_1 large enough so that $r(m_1B) = g - 1$. We want to say that $\deg(D) \geq c \implies r(D) \geq r(m_1B)$. So we would like to find a $y \in K$ such that $D+(y)-m_1B \geq 0$ because $D+(y) \sim D$ and hence $r(D) = r(D+(y))$. Thus we have to pick a $0 \neq y$ from $L(D - m_1B)$ and we are done.

So, finally, we want $l(D - m_1B)$ to be greater than or equal to 1. By Riemann's inequality, $l(D - m_1B) \geq \deg(D - m_1B) - g + 1 \geq c - m_1n - g + 1$. Thus choosing $c \geq m_1n + g$ does the job.

The uniqueness of g can be easily shown by taking a divisor D of degree greater than c (for example, one can take $D = (c + 1)P$ for some prime P) and using the fact that $l(D) = \deg(D) - g + 1$.

□

The next step in proving the Riemann-Roch theorem is to convert the Riemann inequality into an equation as seen in the proposition below :

Proposition C.3. *Given any divisor D of K, $\Omega_K(D)$ is a finite dimension F vector space and*

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

Proof. For any divisor $C \geq D$, we have

$$\begin{aligned} r(C) - r(D) &= \dim_F \frac{A_K(C)}{A_K(D) + L(C)} \text{ (Refer to proof of lemma C.1)} \\ &= \dim_F \frac{A_K(C)}{A_K(D) + (K \cap A_K(C))} \text{ (As } L(C) = A_K(C) \cap K) \\ &= \dim_F \frac{A_K(C)}{A_K(C) \cap (A_K(D) + K)} \text{ (As } P + (Q \cap R) = Q \cap (P + R) \text{ if } P \subseteq Q) \\ &= \dim_F \frac{A_K(C) + A_K(D) + K}{A_K(D) + K} \\ &= \dim_F \frac{A_K(C) + K}{A_K(D) + K} \end{aligned}$$

Find a divisor C_0 such that $\deg(C_0) \geq c$ and $C_0 \geq D$. Let $C_0 = \sum_{P \in S_K} n_P(C_0)P$.

Therefore $r(C_0) = g - 1$ by Riemann's inequality. This implies that

$$r(C_0) - r(D) = g - 1 + l(D) - \deg(D) = \dim_F \frac{A_K(C_0) + K}{A_K(D) + K}.$$

Claim : $A_K = A_K(C_0) + K$.

This is because for any $\xi = (x_P)_{P \in S_K} \in A_K$, $x_P \in \hat{O}_P$ for all but finitely many Ps. Let $m_P = |\text{ord}_P(x_P)|$.

Choose $n_P(C) = \max(m_P, n_P(C_0))$ and construct a divisor $C = \sum n_P(c)P$.

Clearly $C \geq C_0$ and $\xi \in A_K(C)$. Therefore $r(C) = g - 1$ and hence $r(C) - r(C_0) = \dim_F \frac{A_K(C)+K}{A_K(C_0)+K} = 0$. This implies $A_K(C) + K = A_K(C_0) + K$. Thus

$$l(D) = \deg(D) - g + 1 + \dim_F \frac{A_K}{A_K(D) + K}$$

The dual of $\frac{A_K}{A_K(D)+K}$ is nothing but the vector space $\Omega_K(D)$.

For any F- linear map $\omega' : \frac{A_K}{A_K(D)+K} \to F$ defines an F-linear map

$$\omega : A_K \to F \text{ which sends } \xi \rightsquigarrow \omega'(\xi + A_K(D) + K).$$

And given any $\omega \in \Omega_K(D)$, $\omega(K) = \omega(A_K(D)) = 0$ and hence defines a well-defined map

$$\omega' : \frac{A_K}{A_K(D) + K} \text{ such that } \xi + A_K(D) + K \rightsquigarrow \omega(\xi).$$

□

Our task now is to associate a divisor to each non-zero Weil differential.

Lemma C.4. *Given any $\omega \neq 0 \in \Omega_K$, there exists a unqiue divisor D such that $\omega(A_K(D)) = 0$ and if for any other divisor D' $\omega(A_K(D')) = 0$, then $D' \leq D$.*

Such a D is denoted by (ω).

Proof. Consider the set $S = \{D' | \omega(A_K(D')) = 0\}$.

It is non-empty because ω is a Weil differential. Also if $\deg(D') \geq c$, then $A_K = A_K(D') + K$ and hence $D' \in S$ would mean $\omega(A_K(D')) = 0$. $\omega(K)$ is anyway zero as it is a Weil differential and hence $\omega(A_K) = 0$ which means $\omega = 0$.

Pick a $D = \sum_{P \in S_K} n_P(D)P \in S$ with maximum degree. This we claim is the required divisor.

For any other $D' = \sum_{P \in S_K} n_P(D')P \in S$, construct the divisor

$$X = \sum_{P \in S_K} n_P([D, D'])P \text{ where } n_P([D, D']) = \max(n_P(D), n_P(D')).$$

$$A_K(X) = A_K(C) + A_K(D).$$

(A verification : If $\xi = (x_P)_{P \in S_K} \in A_K(X)$, then define $\xi' = (y_P)_{P \in S_K}$ such that $y_P = x_P$ if $\mathrm{ord}_P(x_P) \geq -n_P(D)$ and 0 otherwise. Thus $\xi' \in A_K(D)$. $\xi - \xi'$ is then in $A_K(C)$. The other direction is clear).

Therefore $X \in S$. However $\deg(X) \geq \deg(D)$ and D has maximum degree in S. Hence

$$\begin{aligned} &\deg(X) = \deg(D) \\ &\implies n_P([D, D']) = n_P(D) \geq n_P(D') \\ &\implies D' \leq D \forall D' \in S. \end{aligned}$$

The uniqueness of D follows immediately.

□

Lemma C.5. *If $k \in K^*$ and $\omega \in \Omega_K$, then $(k\omega) = (k) + (w)$.*

Proof. Let $(\omega) = D$ which implies $\omega(A_K(D)) = 0$. By lemma B.3, $\xi \in A_K((k)+ D)$ iff $k\xi \in A_K(D)$. Thus

$$\begin{aligned} &k\omega(\xi) = \omega(k\xi) = 0 \\ &\implies (k) + D = (k) + (\omega) \leq (k\omega). \end{aligned}$$

Now $\omega = k^{-1}k\omega$. Therefore applying the above inequality, we get

$$\begin{aligned} &(k^{-1}) + (k\omega) \leq (\omega) \\ &\implies (\omega) = (k^{-1}) + (k) + (\omega) \leq (k^{-1}) + (k\omega) \leq (\omega). \end{aligned}$$

Hence the inequalities in the above line are all equalities and $(k) + (\omega) = (k\omega)$.

□

We will show the following:

$$\Omega_K(D) \cong_F L((\omega) - D) \text{ for any } \omega \neq 0 \in \Omega_K.$$

And in addition we will also prove that there exists a divisor class C which we shall call the *canonical* class where $C = \{(\omega) | \omega \neq 0 \in \Omega_K\}$.. These two together with proposition C.3 will conclude the proof of the Riemann-Roch theorem.

Theorem C.6. *Ω_K is a one dimensional K vector space.*

Proof. Given any non-zero $\omega \in \Omega_K$ and any divisor D, $L((\omega) - D)\omega \subseteq \Omega_K(D)$ for if $k \in L((\omega) - D)$, then $(k) + (\omega) \geq D$ which gives us that $(k\omega) \geq D$ and hence $k\omega$ vanishes on $A_K(D)$ ($D \leq (k\omega) \implies A_K(D) \subseteq A_K((k\omega))$, and $k\omega$ vanishes on the latter).

Now if ω and ω' are two non-zero Weil differentials, we will find a suitable divisor D such that $L((\omega) - D)\omega \cap L((\omega') - D)\omega' \neq (0)$ which will mean that $\exists k, k' \in K^*$ such that $k\omega = k'\omega'$. Hence the two Weil differentials will be K dependent.

The dimension arguement is used to say that the two vector spaces have non-zero intersection.

$$\dim_F(\Omega_K(D)) = l(D) + g - 1 - \deg(D) \text{ (By proposition C.3)}$$

Using Riemann's inequality, we get

$$\begin{aligned} \dim_F L((\omega) - D)\omega = \dim_F L((\omega) - D) \geq \deg((\omega)) - \deg(D) - g + 1 \\ \dim_F L((\omega') - D)\omega' = \dim_F L((\omega') - D) \geq \deg((\omega')) - \deg(D) - g + 1 \end{aligned}$$

Hence $\dim_F L((\omega')-D)+\dim_F L((\omega')-D) \geq \deg((\omega))+\deg((\omega'))-2\deg(D)-2g+2.$

From the theory of vector spaces, we know that if U, W are two subspaces of an F vector space V, then

$$\begin{aligned} \dim_F(V) \geq \dim_F(U+W) &= \dim_F(U) + \dim_F(W) - \dim_F(U \cap W) \\ \implies \dim_F(U \cap W) &\geq \dim_F(U) + \dim_F(W) - \dim_F(V) \end{aligned}$$

Thus if we can find a divisor D such that

$$\deg((\omega))+\deg((\omega'))-2\deg(D)-2g+2 > \dim_F \Omega_K(D) = l(D)+g-1-\deg(D),$$

then we are assured of a non-zero intersection. So we need a divisor D such that $-\deg(D) > l(D) + 3g - 3 - \deg((\omega)) - deg((\omega'))$.

An ideal choice for D is $-nP$ where n is a suitable large positive integer. Note that $l(D) = 0$ because if $y \in L(-nP)$, then $(y) - nP \geq 0$, which means that y has no pole and a zero at P and hence is 0.

□

The above theorem shows that if ω, ω' are two nonzero Weil differentials, then $\exists k \in K^*$ such that $k\omega = \omega'$. Hence $(k) + (\omega) = (\omega')$. and hence $(\omega) \sim (\omega')$. Also if $D \sim (\omega)$, then $D = (k) + (\omega)$ and hence is equal to $(k\omega)$ which is the divisor of a Weil differential again.

Now in the course of the proof of the above theorem, we have shown that $L((\omega) - D)\omega \subseteq \Omega_K(D)$. To show the other inclusion, pick any $\omega' \in \Omega_K(D)$. Thus $D \leq (\omega') = (k) + (\omega)$ for some $k \in K^*$. Therefore $(k) \geq D - (\omega)$ and hence $k \in L((\omega) - D)$. And thus we have shown that

$$L((\omega) - D) \cong_F L((\omega) - D)\omega = \Omega_K(D)$$

And finally,

Theorem C.7 (Riemann-Roch)**.** *Given K as above, there exists a unique integer $g \geq 0$ and a class C of the Picard group Cl_K such that for any divisor A and any $X \in C$, we have*

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

g is called the genus of K and C, the canonical class of K.

Appendix D

Language of curves

We assume that the reader has some familiarity with projective curves ((ie) knows the definitions of a projective space and a smooth projective curve). In this appendix we give a very brief summary about the correspondence between primes of a function field and points of a smooth projective curve.

Let $\overline{F}$ denote the algebraic closure of finite field F. Let $C \subseteq \mathbb{P}^N(\overline{F})$ be a smooth projective curve defined[1] over F with vanishing ideal $I(C) \subseteq \overline{F}[x_0, x_1, \ldots, x_N]$.

$I(C)$ is the ideal generated in $\overline{F}[x_0, x_1, \ldots x_N]$ by the homogeneous polynomials with coefficients in F which vanish on C.

K consists of all rational functions $\frac{f}{g}$ such that

- f and g are homogeneous polynomials of the same degree in $F[x_0, x_1, \ldots, x_N]$.
- $g \notin I(C)$
- Two functions $\frac{f}{g}$ and $\frac{f'}{g'}$ are identified if $fg' - f'g \in I(C)$.

Likewise any element of $\overline{K}$ looks like $\frac{\bar{f}}{\bar{g}}$ where $\bar{f}, \bar{g}$ are homogeneous polynomials of the same degree, this time in $\overline{F}[x_0, x_1, \ldots, x_N]$ such that $\bar{g}$ does not vanish entirely on C with a similar identification process.

Given a point α of C, one can define a discrete valuation ring

[1] That just means that the set of polynomials in $\overline{F}[x_0, x_1, \ldots, x_N]$ which vanish on C is generated by homogeneous polynomials in $F[x_0, x_1, \ldots, x_N]$

$$\mathfrak{O}_\alpha = \left\{ \frac{f}{g} \in \overline{K} | g(\alpha) \neq 0 \right\},$$

with maximal ideal $\mathfrak{P}_\alpha$ given by

$$\mathfrak{P}_\alpha = \left\{ \frac{f}{g} \in \overline{K} | g(\alpha) \neq 0, f(\alpha) = 0 \right\}.$$

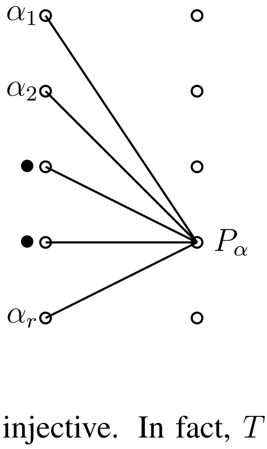
The fact that $(\mathfrak{O}_\alpha, \mathfrak{P}_\alpha)$ is a discrete valuation ring follows because C is a smooth curve. The fraction field of $\mathfrak{O}_\alpha$ is $\overline{K}$ and thus we have found a prime of $\overline{K}$ for every point α of C! Let us give this association a name.

$$\overline{T} : C \rightarrow \text{ Primes of } \overline{K} \text{ which sends } \alpha \rightsquigarrow \mathfrak{P}_\alpha.$$

It turns out that $\overline{T}$ is actually a bijective map and thus primes of $\overline{K}$ correspond exactly to points of C.

A natural step is to try to associate points of C with primes of K by sending α to the prime of K which lies below $\overline{T}(\alpha)$. Let $(\mathcal{O}_\alpha, P_\alpha)$ denote the prime of K lying under $(\mathfrak{O}_\alpha, \mathfrak{P}_\alpha)$. Then we have

$$T : C \rightarrow \text{ Primes of } K,$$



T is a surjective map but not injective. In fact, $T^{-1}(P_\alpha)$ is the Galois orbit of α, where the group action is that of the Galois group $\text{Gal}\left(\overline{F}/F\right)$ naturally acting on C and hence rational primes of K are in one one correspondence with Galois orbits of C.

It turns out that the degree of the prime P_α is the cardinality of the Galois orbit of α. To see this , observe that $\frac{\mathcal{O}_\alpha}{P_\alpha}$ is isomorphic to $F(1, \alpha_1, \alpha_2, \dots, \alpha_N)$ where $\alpha = [1, \alpha_1, \alpha_2, \dots, \alpha_N]$ say.

We reiterate,

$$\deg(P_\alpha) = |T^{-1}(P_\alpha)| = |\text{ Galois orbit of } \alpha|.$$

We will be primarily interested in rational primes of K, (ie) primes of K with degree 1. Not surprisingly, they correspond exactly to what are called F *rational points* of C.

The set of F-rational points of the projective space $\mathbb{P}^N(\overline{F})$ is defined as

$$\mathbb{P}^N(F) := \{[a_0, a_1, \dots, a_N] \in \mathbb{P}^N(\overline{F}) | a_i \in F \forall i \leq N\}.$$

It turns out that another characterisation for F-rational points is to think of them as the fixed points of the map $\phi : \mathbb{P}^N(\overline{F}) \to \mathbb{P}^N(\overline{F})$ which is the natural extension of the Frobenius automorphism π of $\overline{F}$.

Recall that π sends $x \rightsquigarrow x^q$. The fixed points of π form the field F because $x^q - x = 0$ has exactly q roots and elements of F satisfy the afore mentioned equation. π naturally defines an automorphism ϕ of the projective space $\mathbb{P}^N(\overline{F})$ by sending

$$[\beta_0, \beta_1, \dots, \beta_N] \rightsquigarrow [\beta_0^q, \beta_1^q, \dots, \beta_N^q].$$

Now pick a point $a = [a_0, \dots, a_N] \in \mathbb{P}^N(\overline{F})$ which is fixed by ϕ. One of the a_is is nonzero, say a_0. So $a = [1, \frac{a_1}{a_0}, \dots, \frac{a_N}{a_0}]$. Since $\phi(a) = a$, the following tuples are proportional

$$\left(1, \left(\frac{a_1}{a_0}\right)^q, \dots, \left(\frac{a_N}{a_0}\right)^q\right) \text{ and } \left(1, \frac{a_1}{a_0}, \dots, \frac{a_N}{a_0}\right).$$

That is $\exists \lambda \in \overline{F}^*$ such that

$$\left(\frac{a_i}{a_0}\right)^q = \lambda \left(\frac{a_i}{a_0}\right) \forall i \leq N.$$

Taking $i = 0$ gives $\lambda = 1$ and thus $\left(\frac{a_i}{a_0}\right)^q = \left(\frac{a_i}{a_0}\right) \forall i$ which implies $\frac{a_i}{a_0} \in F$ which gives us that $a \in \mathbb{P}^N(F)$. That each point of $\mathbb{P}^N(F)$ is fixed by ϕ is trivial to check.

The set of rational points in C, denoted by $C(F)$ is the set $C \cap \mathbb{P}^N(F)$ for any curve defined over F. As C is a curve defined over F, ϕ maps $C(\overline{F})$ to itself [2]. Thus the rational points of C are nothing but the fixed points of ϕ in $C(\overline{F})$.

Since the Frobenius map π generates $\mathrm{Gal}\left(\overline{F}/F\right)$, the fixed points of ϕ have Galois orbits of size 1 and hence correspond to primes of degree 1 of K.

[2] C is the zero set of some homogeneous polynomials in $F[x_0, x_1, \ldots, x_N]$ and $f([\beta_0^q, \ldots, \beta_N^q]) = (f([\beta_0, \ldots, \beta_N]))^q$ if f is a homogeneous polynomial with coefficients in F.

Bibliography

[1] William Fulton, Algebraic curves : an introduction to algebraic geometry, Springer.

[2] Serge Lang, Algebra, Springer.

[3] Carlos Moreno, Algebraic curves over finite fields, Cambridge University Press.

[4] Michael Rosen, Number Theory in Function Fields, Springer

[5] Joseph H.Silverman, The arithmetic of elliptic curves, Springer.