Algebraic Curves: An Algebraic Approach

Pete L. Clark

Contents

Preface

These are notes from my graduate course *Algebraic Curves: An Algebraic Approach* taught at UGA in Fall 2020. This course was taught remotely (via zoom) during the COVID-19 pandemic. I am grateful to the students for their interest and attention during a very difficult time.

There are three approaches to the study of algebraic curves. The first is the complex analytic approach, which is valid when the ground field is $\mathbb{C}$. This was historically the first approach (by almost 100 years): it showcases a deep connection between algebra and analysis that remains of crucial importance. The second is the approach via valuations on function fields, developed principally by Weil in the second quarter of the 20th century. The third approach is via the theory of schemes and sheaf cohomology, as is exposed for instance by Hartshorne [**He**] in the case of an algebraically closed ground field and by Liu [**Li**] in the general case.

The somewhat daunting truth is that in the 21st century a student or practitioner of arithmetic geometry needs to have some exposure to all three approaches. In Fall 2008 I taught the same course at UGA from the scheme-theoretic approach using [**Li**]. I found that much of the course had to be devoted to developing foundational aspects of scheme theory and that I did not have as much time as I wished to cover "applications." Because of this for several years I had wanted to teach a course from the valuation theoretic approach.

I did so in the Fall 2020 course whose lectures are collected here. My main reference was Stichtenoth's text [**St**], but I also drew from other recent texts that expose this approach, for instance [**G**], [**GSX00**], [**VS**]. (It turns out that although the valuation theoretic approach is no longer the most favored one in the arithmetic geometry community, it seems to be the preferred approach for those mathematicians concentrating on curves over finite fields with applications to coding theory.)

Looking back on the course, it seems to me that my desire to avoid "foundational issues" was not so fully realized: a lot of the course still concerns foundations! However, to those whose core interests lie more in algebraic number theory than algebraic geometry, the foundations drawnn upon may be more familiar and of more intrinsic interest: in these notes we draw upon field theory, basic commutative algebra, and algebraic number theory. Especially, the relatively abstract perspective of modern algebraic number theory – whose main setting is a Dedekind domain A, its fraction field K, a finite degree field extension L/K, and the integral closure B of A in L – is leveraged wonderfully in this approach, and in some respects is brought to fuller fruition here than in the most classical case of $A = \mathbb{Z}$. For instance, the

notion of the different ideal of the extension $A \subset B$ is present in Algebraic Number Theory I but in the study of algebraic number fields plays a relatively ancillary role. On the other hand, in the function field context the different ideal is the key to understanding the Riemann-Hurwitz formula, one of the main results of the course.

As an exposition, these notes distinguish themselves mainly by being tailored to an audience of algebraic number theory students: whereas in [**St**] Stichtenoth is remarkably self-contained, which by necessity requires many *ad hoc* arguments, in these notes we draw upon my prior notes in field theory [**FT**], commutative algebra [**CA**], and algebraic number theory [**NTII**]. We also discuss some relatively recent work on algebraic curves over finite fields, though more in the spirit of a quick survey rather than the deep, robust attention that this material deserves.

Anyway, I very much enjoyed teaching the course. I hope these notes are of some value to you. If so; if you find any typos or more serious errors; if you want to draw my attention to a new reference; or if you are hoping these notes will at some future point be modified so as to treat some other topic, please let me know!

CHAPTER 0

Preliminaries

1. Some Recalled Facts on Field Extensions

Let k be any field.

Recall that a field extension l/k is **finitely generated** if there are elements $x_1, \ldots, x_n$ of l such that $l = k(x_1, \ldots, x_n)$: that is, the only subfield of K that contains k and the elements $x_1, \ldots, x_n$ is l itself. More concretely, every element of l can be expressed as a quotient of two polynomials in the elements $x_1, \ldots, x_n$ with the coefficients in k.

EXERCISE 0.1. *There three notions of finite generation in play for a field extension l/k: (i) l is finitely generated as a k-module (equivalently, finite-dimensional as a k-vector space) – we also say that l/k has finite degree – (ii) l is finitely generated as a k-algebra: there are $x_1, \ldots, x_n \in l$ such that $l = k[x_1, \ldots, x_n]$: every element of l can be expressed as a polynomial in $x_1, \ldots, x_n$ with coefficients in k. (iii) l/k is finitely generated as a field extension.*

a) *Show: l/k finitely generated as a module implies l/k finitely generated as a k-algebra implies l/k finitely generated as a field extension.*
b) *Let $k(t)$ be the rational function field over k – the fraction field of the polynomial ring $k[t]$. Show: $k(t)/k$ is finitely generated as a field extension but is not finitely generated as a k-algebra.*
c) *Show: $k[t]/k$ is finitely generated as a k-algebra but not as a k-module. (However $k[t]$ is not a field!)*
d) *Can you exhibit a field extension l/k such that l is finitely generated as a k-algebra but not as a k-vector space?*
(Hint: no, you can't – this is a famous result of commutative algebra!)
e) *Suppose l/k is algebraic and finitely generated as a field extension. Show that l/k has finite degree.*

Notice that when we say a field extension l/k is finitely generated, it is understood that we mean "as a field extension." In theory this could be ambiguous, but in practice I hope it will not be.

The following is a nontrivial, and very useful, result about finitely generated field extensions.

THEOREM 0.1. *Let $F \subset K \subset L$ be field extensions. Then L/F is finitely generated if and only if L/K is finitely generated and K/F is finitely generated.*

PROOF. See [**FT**, Thm. 11.19]. □

Let k be a field. For any set S we have the polynomial ring $k[\{t_i\}_{i\in S}]$ in a set of indeterminates Eed by S. Its fraction field is $k(\{t_i\}_{i\in S}$ is, by definition, a rational function field of several variables. A field extension K/k is **purely transcendental** if it is isomorphic, as a k-algebra, to a rational function field.

If l/k is a field extension, a subset $\{x_i\}_{i\in I}$ of elements of l are **algebraically independent** over k if they satisfy no nonzero polynomial equation with coefficients in k. If this holds, then $k(\{x_i\}_{i\in I})$ is a purely transcendental extension of k.

In these notes, when we write $k(t)$, $k(t_1,\dots,t_n)$ or $k(\{t_i\}_{i\in I})$, then by our use of "t's" it is understood that we have independent indeterminates (equivalently, algebraically independent elements). Otherwise we will specify when we mean the indeterminates to be independent.

THEOREM 0.2. *Let l/k be a field extension.*

a) *There is a subset $\{x_i\}_{i\in I}$ of l of elements algebraically independent over k such that $l/k(\{x_i\}_{i\in I}$ is an algebraic field extension.*

b) *If $\{y_j\}_{j\in J}$ is another subset of l of elements algebraically independent over k such that $l/k(\{y_j\}_{j\in J}$ is algebraic, then $\#I = \#J$.*

PROOF. a) See [**FT**, Cor. 11.4b)]. b) See [**FT**, Thm. 11.11]. □

The subset $\{x_i\}_{i\in I}$ asserted to exist in Theorem 0.2a) is called a **transcendence basis** for the extension l/k. Transcendence bases in field theory bear a family resemblance to bases in vector space theory. In fact both are important special cases of a common algebraic structure called a **matroid**, in which the notions of independence, spanning and bases are axiomatized. Because of this (but also not because of this: the theory of transcendence degrees was also a precursor to the general matroid theory) many fundamental results about vector spaces have analogues for field extensions. Theorem 0.2b) is the first such result: it says that any two transcendence bases for the same field extension have the same cardinality. Whereas in linear algebra we call the common cardinality of any basis of a vector space its dimension, in field theory we call the common cardinality of any transcendence basis the **transcendence degree** of l/k. A field extension is algebraic iff it has transcendence degree zero.

THEOREM 0.3. *For fields $F \subset K \subset L$, we have*

$$\operatorname{trdeg}(L/F) = \operatorname{trdeg}(K/F) + \operatorname{trdeg}(L/K).$$

PROOF. See [**FT**, Thm. 11.18]. □

LEMMA 0.4. *Let $K = k(x_1,\dots,x_n)/k$ be a finitely generated field extension. Then we have* $\operatorname{trdeg} K/k \leq n$, *with equality iff l/k is purely transcendental.*

PROOF. If $F(x)/F$ is a monogenic field extension, the transcendence degree is 1 if x is transcendental over F and 0 if x is algebraic over F. So by Theorem 0.3, the transcendence degree of $k(x_1,\dots,x_n)$ is equal to the number of $1 \leq i \leq n$ such that $k(x_1,\dots,x_i)$ is transcendental over $k(x_1,\dots,x_{i-1})$. The result follows. □

2. Function Fields

Thus a field extension K/k that is finitely generated but of infinite degree has transcendence degree $0 < d < \aleph_0$. We call such a field a **function field in d**

variables. In this course we will be interested in the case of $d = 1$. On the one hand, the field theory of one variable function fields is simpler. On the other hand, the relationship between function fields and algebraic varieties is much simpler in dimension 1 – so much so that one does not even really need an *a priori* definition of an algebraic curve: all of the needed objects and results can be defined and worked with directly out of its function field. That is going to be our perspective in this course: it is essentially a very algebraic number theorist's take on the theory of algebraic curves, using function fields and valuations on them.

Here is an example of a result that we will prove later in the course.

THEOREM 0.5 (Lüroth's Theorem). *Let k be a field, and let $k \subsetneq l \subsetneq k(t)$. Then there is $f \in k(t)$ such that $l = k(f)$.*

More generally, the **Luröth Problem** asks, for fixed f and d, whether a subextension l of $k(t_1, \ldots, t_d)/k$ such that $k(t_1, \ldots, t_d)/l$ has finite degree must be purely transcendental. Castelnuovo gave an affirmative answer when $d = 2$ and $k = \mathbb{C}$ (or, in fact, when k is algebraically closed of characteristic 0). In 1958 Zariski gave a negative answer when k is algebraically closed of (any) positive characteristic [**Za58**]. When $d \geq 3$ there are counterexamples even over $\mathbb{C}$, the first such being given by Clemens and Griffiths in 1972 [**CG72**].

EXERCISE 0.2. *Let k be a field, let G be a finite group of order n, and let $G \hookrightarrow S_n$ be the Cayley embedding. Permutation of variables gives a natural action of S_n and hence also G on $k(t_1, \ldots, t_n)$. Put $l := k(t_1, \ldots, t_n)^G$, so $k(t_1, \ldots, t_n)/l$ is a finite Galois extension with automorphism group G. Notice that this is an instance of the Lüroth problem.*

a) *Let $k = \mathbb{Q}$. Show: if $l/\mathbb{Q}$ is purely transcendental, then G occurs as a Galois group over $\mathbb{Q}$. Thus: an affirmative answer to the Lüroth problem yields an affirmative answer to the Inverse Galois Problem over $\mathbb{Q}$. (Suggestion: This holds whenever k is a Hilbertian field.)*
b) *Alas, $l/\mathbb{Q}$ need not be purely transcendental. Explore the literature on this – the first example was due to Swan, where G is cyclic of order 47.*

For a field extension K/k, we let $\kappa(K)$ be the algebraic closure of k in K, i.e., the set of all elements of K that satisfy a polynomial equation with coefficients in k. (This is a special case of integral closure.) The extension $\kappa(K)/k$ is the maximal algebraic subextension of K/k. In particular, if $k = \overline{k}$ is algebraically closed then we always have $\kappa(K) = k$.

Suppose now that K/k is a function field, i.e., is finitely generated. In this case we call $\kappa(K)$ the **constant subfield** of K. By Theorem 0.1 we have that $\kappa(K)/k$ has finite degree and $K/\kappa(K)$ is finitely generated, hence $K/\kappa(K)$ is itself a function field. In this way we can always reduce to the case in which there is no nontrivial constant subextension. For most (but not all – I will give a near and dear example later) purposes this is indeed the right thing to do.

3. Base Extension

In the study of function fields just as for so many other things, a key construction in **base extension**. If we have an affine algebraic variety defined by a

system of polynomial equations over a field k and l/k is a field extension, then we may regard the polynomial equations as being defined over l and thereby get an "extended variety" defined over l. A slightly more algebraic take on this is: if the polynomial equations are $P_1, \ldots, P_r \in k[t_1, \ldots, t_n]$, then the affine coordinate ring is

$$k[V] := k[t_1, \ldots, t_n]/\langle P_1, \ldots, P_r \rangle.$$

The passage from $k[V]$ to $l[V]$ simply involves "replacing k with l," but a better take on this is as follows:

$$l[V] = k[V] \otimes_k l.$$

That is, base extension comes by applying $\otimes_k l$.

Can we do this with function fields? Well, we can try. If K/k is a function field and l/k is a field extension, we can form the tensor product $K \otimes_k l$, which is a commutative k-algebra. Is it a field??

Sometimes it is and sometimes it isn't. Here is a first exercise.

EXERCISE 0.3. a) *Let l/k be an algebraic field extension. Show: $l \otimes_k l$ is a domain iff $l = k$.*

b) *Let l/k be any field extension. Show: $k(t) \otimes_k l$ is always a domain with fraction field $l(t)$. It is already a field iff l/k is algebraic.*

In general, understanding "what happens" to the tensor product of fields is a non-trivial, interesting and useful question that does not seem to get the attention it deserves in standard texts. So let us present some of these results.

PROPOSITION 0.6. *Let K_1/k and K_2/k be field extensions and suppose that $K_1 \otimes_k K_2$ is a domain. The following are equivalent:*

(i) *We have that $K_1 \otimes_k K_2$ is a field.*

(ii) *At least one of the extensions K_1/k and K_2/k is algebraic.*

PROOF. See [**FT**, Prop. 12.7, Thm. 12.8]. □

In view of Proposition 0.6 we may as well shift attention to when $K_1 \otimes_k K_2$ is a domain. Then, if either K_1/k or K_2/k is algebraic, it will be a field. If not, okay: we will take the fraction field.

Now we make an observation: if K/k is a field extension and $\overline{k}$ is an algebraic closure of k, then if $K \otimes_k \overline{k}$ is a domain, we must have $\kappa(K) = k$. Indeed (since k is a field, tensoring with k preserves exact sequences!) we have

$$\kappa(K) \otimes_k \kappa(K) \hookrightarrow K \otimes_k \overline{k},$$

and now we apply Exercise 0.3a).

EXERCISE 0.4. *Describe the $\mathbb{R}$-algebra $\mathbb{C}(t) \otimes_{\mathbb{R}} \mathbb{C}$.*

It is honestly a pretty reasonable guess that if K/k is an extension such that $\kappa(K) = k$, then $K \otimes_k \overline{k}$ is a field. In fact this turns out to be true in characteristic 0. In characteristic $p > 0$, there are additional issues: $K \otimes_k \overline{k}$ is a domain, then so is $K \otimes_k k^{p^{-1}}$. This is a known condition in field theory: it says that the (probably not algebraic!) extension K/k is **separable**: among other equivalent conditions, this means that every finitely generated subextension of K/k has a

separating transcendence basis, that is a transcendence basis for which the resulting algebraic extension is separable.

EXAMPLE 0.1. *Let $k := \mathbb{F}_p(a,b)$, a rational function field in two variables over $\mathbb{F}_p$. Let $A := k[x,y]/(ax^p + b - y^p)$, a domain. Let K be the fraction field of A. Then k is algebraically closed in K but K/k is not separable: in $\overline{k}$ we have unique α, β such that $\alpha^p = a$, $\beta^p = b$, and thus $ax^p + b - y^p = (\alpha x + \beta - y)^p$, so $A \otimes_k \overline{k}$ is not a domain.*

That was rather technical. Anyway, notice that this condition is vacuous if $k = k^{p^{-1}}$, that is if k is **perfect**, which holds for both finite fields and algebraically closed fields.

Here comes the main theorem:

THEOREM 0.7. *For a field extension K/k, the following are equivalent:*

(i) *We have $\kappa(K) = k$ and K/k is separable.*
(ii) *We have that $K \otimes_k \overline{k}$ is a domain (equivalently, a field).*
(iii) *For* all *field extensions l/k, we have that $K \otimes_k l$ is a domain.*

*A field extension satisfying these equivalent conditions is called **regular**.*

PROOF. See [**FT**, Thm. 12.20]. □

We mention in passing that the implication (ii) $\implies$ (iii) in Theorem 0.7 is rather curious. Although we are trying to do pure field theory as a middlebrow foundation for some arithmetic geometry, the proof of this result uses the fact that if k is algebraically closed and R_1, R_2 are domains that are finitely generated as k-algebras, then $R_1 \otimes_k R_2$ is also a domain. In other words, we need to show that over an algebraically closed field, the product of two integral affine varieties is again an integral affine variety. The proof of that uses Hilbert's Nullstellensatz!

EXERCISE 0.5. a) *Show: $k(t)/k$ is regular.*
b) *Show: every purely transcendental extension is regular.*
c) *Show: every extension K/k is regular iff k is algebraically closed.*
d) *Show: K/k is regular iff every finitely generated s subextension is regular.*

EXAMPLE 0.2. $\mathbb{Q}(X(N))$

To sum up: the class of function fields for which base extension works well at the field-theoretic level are precisely the regular function fields. If k is perfect, then a function field K/k is regular iff $\kappa(K) = k$ and every function field is regular when viewed as a function field over $\kappa(K)$. This provides some motivation to work with function fields over a perfect ground field, which indeed will be the case for some of the coming results.

4. Polynomials Defining Function Fields

We will give a more concrete description of regular function fields of one variable.

EXERCISE 0.6. *Let R_1 and R_2 be two k-algebras that are also domains, with fraction fields K_1 and K_2. Show that $R_1 \otimes_k R_2$ is a domain iff $K_1 \otimes_k K_2$ is a domain.*

Let k be a field, with algebraic closure $\overline{k}$. A polynomial $f \in k[t_1, \ldots, t_n]$ of positive degree is **geometrically irreducible** if the image of f in $\overline{k}[t_1, \ldots, t_n]$ is irreducible. Notice that geometrically irreducible polynomials are irreducible, and the concept is only interesting if $n \geq 2$: when $n = 1$ the geometrically irreducible polynomials are precisely the linear polynomials.

Let $f \in k[t_1, \ldots, t_n]$ be irreducible. Since $k[t_1, \ldots, t_n]$ is a UFD [**CA**, Thm. 15.26], the ideal (f) is prime, so $k[t_1, \ldots, t_n]/(f)$ is a domain. We define K_f to be its field of fractions. For $1 \leq i \leq n$, let x_i denote the image of t_i under the composite map $k[t_1, \ldots, t_n] \to k[t_1, \ldots, t_n]/(f) \hookrightarrow K_f$. Then $K_f = k(x_1, \ldots, x_n)$.

EXERCISE 0.7. *Show that every finitely generated field extension $K = k(x_1, \ldots, x_n)$ is the fraction field of a quotient of $k[t_1, \ldots, t_n]$ by a (not necessarily principal) prime ideal.*

PROPOSITION 0.8. *Let $f \in k[t_1, \ldots, t_n]$ be geometrically irreducible. Then:*

a) *The function field K_f/k is regular.*
b) *For every field extension l/k, f is irreducible as an element of $l[t_1, \ldots, t_n]$.*

PROOF. There is a canonical isomorphism $k[t_1, \ldots, t_n]/(f) \otimes_k \overline{k} = \overline{k}[t_1, \ldots, t_n]/(f)$, so by definition of geometrically irreducible, the ring $k[t_1, \ldots, t_n]/(f) \otimes_k \overline{k}$ is a domain. By Exercise 0.6 we get that $K_f \otimes_k \overline{k}$ is a a domain, hence a field by Proposition 0.6, which by Theorem 0.7 shows that K_f/k is regular. It then follows that $K_f \otimes_k l$ is a domain for all field extensions l/k, hence is its subring $k[t_1, \ldots, t_n]/(f) \otimes_k l = l[t_1, \ldots, t_n]/(f)$. □

EXERCISE 0.8. *Let k be a field, let $d \geq 2$ be such that $4 \nmid d$, and let $p(x) \in k[x]$ be a polynomial of positive degree. In $\overline{k}[t]$ we factor p as $(x - a_1)^{e_1} \cdots (x - a_r)^{e_r}$ with $a_1, \ldots, a_r$ distinct elements of $\overline{k}$ and $e_1, \ldots, e_r \in \mathbb{Z}^+$. Suppose that there is some $1 \leq i \leq r$ such that $d \nmid e_i$. Show that the*

$$f(x, y) = y^d - p(x) \in k[x, y]$$

is geometrically irreducible and thus the fraction field of $k[x, y]/(y^d - p(x))$ is a regular one variable function field over k.
(Suggestion: use [**FT**, Thm. 9.21]*.)*

EXERCISE 0.9. *Let k be a field of characteristic different from 2.*

a) *Show that the function field K_f attached to $f(x, y) = x^2 - y^2 - 1$ is rational: i.e., there is $z \in K$ such that $K_f = k(z)$.*
b) *Show that the function field K_f attached to $f(x, y) = x^2 + y^2 - 1$ is rational.*
c) *If $k = \mathbb{C}$, show that the function field K_f attached to $f(x, y,) = x^2 + y^2 + 1$ is rational.*
d) *If $k = \mathbb{R}$, is the function field attached to $f(x, y) = x^2 + y^2 + 1$ rational? (Answer: it is not, but at the moment we have precisely no tools to show that a regular function field is not rational, so I don't know how you could prove this. But keep it in mind – as we develop more theory, it will become possible, then easy, then clear.)*

So we have seen that a good way to give regular function fields is via a geometrically irreducible polynomial. In one variable it turns out that this is the only way:

THEOREM 0.9. *Let K/k be a one variable function field.*

a) *If K/k is separable, then there are $x, y \in K$ such that $K = k(x, y)$.*
b) *If K/k is moreover regular, then $K \cong K_f$ for a geometrically irreducible polynomial $f \in k[x, y]$.*

PROOF. a) A finitely generated separable field extension has a separable transcendence basis: there is $x \in K$ such that $K/k(x)$ is separable algebraic. By Theorem 0.1, we have that $K/k(x)$ has finite degree. So by the Primitive Element Corollary [**FT**, Cor. 7.2], there is $y \in K$ such that $K = k(x, y)$.
b) As above, we may write $K = k(x, y)$ with y separable over $k(x)$, so y satisfies an irreducible polynomial of degree n, say, with coefficients in $k(x)$. Since $k(x)$ is the fraction field of the UFD $k[x]$, we may clear denominators just enough to get a "primitive relation": for $0 \leq i \leq n$ there are $a_i(x) \in k[x]$ such that $\langle a_0(x), \ldots, a_n(x) \rangle = 1$ and

$$f(x, y) \coloneqq \sum_{i=0}^{n} a_i(x) y^i = 0.$$

Step 1: We claim that f is geometrically irreducible. Because K/k is regular, we have that $L \coloneqq K \otimes_k \overline{k}$ is a field: equivalently, we have that $\overline{k}$ and K are linearly disjoint over k. The fields $\overline{k}(x)$ and K are linearly disjoint over $k(x)$ and $[L : \overline{k}(x)] = [K : k(x)] = n$. Thus y cannot satisfy a polynomial of degree less than n over $\overline{k}(x)$. If $f(x, y) = g(x, y)h(x, y) \in \overline{k}[x, y]$ then one factor, say g, must be a polynomial in x alone hence $g(x) \mid a_i(x)$ for all x, but this implies that g is a constant.
Step 2: Thus we get a k-algebra homomorphism $\varphi : k[t_1, t_2]/(f) \to k[x, y] \subset K$. Since $k[x, y]$ is a domain, the kernel of φ corresponds to a prime ideal of $k[t_1, t_2]$ containing the height one prime (f). But every prime ideal of $k[x, y]$ properly containing (f) is a maximal ideal [**CA**, Cor. 12.17], so if φ were not injective, then by Zariski's Lemma its image would be algebraic over k. However $\varphi : t_1 + (f) \to x$, so this is not the case and φ is an injection and thus an isomorphism, so the induced mapping on fraction fields maps K_f isomorphically to K. □

4.1. Further Exercises.

EXERCISE 0.10. *Let k be any field, and let $\frac{p(t)}{q(t)} \in k(t)$ be a nonconstant rational function. Show:*

$$\deg[k(t) : k(p/q)] = \max \deg(p), \deg(q).$$

CHAPTER 1

Valuations on One Variable Function Fields

1. Valuation Rings and Krull Valuations

We now recall some rudiments of the algebraic approach to valuation theory. In [**NTII**, §1.1] we took the *analytic* approach to valuations: namely that a valuation on a field K is a map

$$v : K \to \mathbb{R} \cup \{\infty\},\ v(K^\times) \subset \mathbb{R},\ v(0) = \infty$$

of the form $\log |\cdot|$, where $|\cdot| : K \to \mathbb{R}$ is an ultrametric norm. In particular, a valuation comes with a value group $\Gamma = v(K^\times)$, which is a subgroup of $(\mathbb{R}, +)$.

The algebraic approach to valuations begins with the following definition (cf. [**CA**, Ch. 17]): a subring R of a field K is a **valuation ring** if for all $x \in K^\times$, at least one of x and x^{-1} lies in R. A valuation ring is **trivial** if it is a field, and otherwise nontrivial.

Exercise 1.1. *Let R be a valuation ring with fraction field K. Let F be a subfield of K. Show: $R \cap F$ is a valuation ring with fraction field F. We call it the "restriction of R to F."*

Let us rephrase things so as to make contact with the above notion of a valuation. In any domain R with fraction field K, we define the **group of divisibility** $G(R) = K^\times / R^\times$. This is a commutative group under multiplication; despite this, when thinking about $G(R)$ abstractly, we will denote the group law by $+$. (Why we do this should become clear shortly.) But it is not just a group: it has extra structure coming from the divisibility relation on $R^\bullet$. Namely, for $x, y \in K^\times$, we write $x \mid y$ if $\frac{y}{x} \in R$. Thus for instance if $R = \mathbb{Z}$ then we have $\frac{1}{2} \mid 7$ because $\frac{7}{1/2} = 14 \in \mathbb{Z}$. On $K^\times$ itself this divisibility relation is almost but not quite a partial ordering: we have $x \mid y$ and $y \mid x$ iff $\frac{y}{x} \in R^\times$, so we only get antisymmetry if $R^\times$ is trivial. Well then, we have well-motivated the passage from $K^\times$ to $G(R) = K^\times / R^\times$: the divisibility relation remains well-defined on the quotient and induces a partial ordering that is compatible with the group structure, making $G(R)$ into a **partially ordered commutative group**.

Now suppose that R is a valuation ring. Then for any $x, y \in K^\times$ we have either $\frac{y}{x} \in R$ or $\frac{x}{y} \in R$, and thus $G(R)$ is not just partially ordered but totally ordered. (Conversely, a domain with totally ordered group of divisibility is a valuation domain.) We can now write down the associated valuation

$$v : K^\times \to G(R);$$

it is just the quotient map $x \mapsto xR^\times$, and as in more classical cases we put $v(0) := \infty$. We now find that this has the formal properties of a valuation:

(VRK1) For all $x, y \in K^\times$, we have $v(xy) = v(x) + v(y)$.
(VRK2) For all $x, y \in K^\times$ such that $x + y \neq 0$, we have $v(x + y) \geq \min v(x), v(y)$.

EXERCISE 1.2. *In the setting of (VRK2), suppose that $v(x) \neq v(y)$. Show: $v(x + y) = \min v(x), v(y)$.*

Thus a valuation ring yields a map v that is like a classical valuation v but with values in a totally ordered commutative group $(G, +)$ instead of $(\mathbb{R}, +)$...which is nothing else than a particular totally ordered commutative group. And the converse also holds: if $(G, +)$ is a totally ordered group and $v : K^\times \to G$ is a map satisfying (VRK1) and (VRK2), then

$$R_v \coloneqq \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$$

is a valuation ring. The second construction makes it immediately clear that a valuation ring is local, with unique maximal ideal

$$\mathfrak{m}_v \coloneqq \{x \in K^\times \mid v(x) > 0\} \cup \{0\}.$$

We denote the residue field $R_v/\mathfrak{m}_v$ by k_v.

The two constructions are essentially (but not literally) mutually inverse: there is a natural equivalence relation on valuations which for purposes is most cleanly enunciated by saying that two valuations on a field K are equvialent if they have the same valuation ring. Compare with [**NTII**, Thm. 1.8] to see that this is an acceptable definition of equivalence. One consequence of this is that if $v_1 : K^\times \to G_1$ and $v_2 : K^\times \to G_2$ are equivalent valuations on a field K, then their **value groups** $\Gamma_1 \coloneqq v_1(K^\times)$ and $\Gamma_2 \coloneqq v_2(K^\times)$ are isomorphic as totally ordered commutative groups.

A valuation is **trivial** if its value group is trivial. This holds iff the valuation ring is K itself. A valuation is **discrete** if its value group is isomorphic to $(\mathbb{Z}, +)$: *a priori* we understand this to mean an isomorphism of ordered commutative groups, but it is easy to see that the standard ordering on $\mathbb{Z}$ (inherited from the standard ordering on $\mathbb{R}$) is the unique ordering that is compatible with the group structure, so a valuation is discrete iff its value group is infinite cyclic. This holds iff the valuation ring R is a discrete valuation ring (i.e., a local principal ideal domain) that is not a field.

From the algebraic perspective, discrete valuation rings are a very small subclass of the class of all valuation rings: it turns out that every totally ordered commutative group is a group of divisibility [**CA**, Thm. 17.10]. A totally ordered commutative group has **rank one** if it is nontrivial and can be embedded in $\mathbb{R}$ as an ordered group. Thus discrete valuations have rank 1, and the extension of a discrete valuation to an algebraic closure of the field has value group isomorphic to $\mathbb{Q}$ and thus is rank 1 but not discrete. For $n \geq 2$, the group $\mathbb{Z}^n$ equipped with the lexicographic ordering is an ordered group that does not have rank 1 (in fact every ordered commutative group has a well-defined **rank**, a cardinal number [**CA**, §17.2.1], and indeed $\mathbb{Z}^n$ has rank n). A valuation of rank greater than one does not induce a "norm" on the field in the sense of [**NTII**, §1], though in spirit it is not necessarily so diffrerent: essentially we are extending the definition of a metric space to allow the metric function to take values in something more general than $\mathbb{R}$.

2. The Zariski-Riemann Space

If A is a subring of a field K, a valuation $v : K^\times \to (G, +)$ on K is **A-regular** if $v(A^\bullet) \subset G^{\geq 0}$. If R is the valuation ring, this holds iff $A \subset R$. In this case, the maximal ideal $\mathfrak{m}_v$ of R pulls back to a prime ideal $\mathfrak{p} := \mathfrak{m}_v \cap A$ of A.

We denote by $\Sigma(K/A)$ the set of all valuation rings $A \subset R \subsetneq K$ such that K is the fraction field of R. This is a very general definition, and you would be forgiven for not being excited by it. However, it is really very exciting! In this course we will consider $\Sigma(K/k)$ where K/k is a one variable function field. As we will see, $\Sigma(K/k)$ is actually a geometric object: from a more sophisticated algebraic geometric perspective (e.g. using scheme theory) one can show that $\Sigma(K/k)$ is precisely the set of closed points of the unique complete, nonsingular algebraic curve $C_{/k}$ with function field $k(C) \cong K$. However, the advantage of the valuation theoretic approach is that one doesn't need any of this scheme theory: we can use $\Sigma(K/k)$ to extract geometry from the field extension K/k *directly*, without needing to define sheaves, schemes and so forth. This exciting idea goes back to Zariski. Accordingly $\Sigma(K/k)$ is often called the **Zariski-Riemann space** attached to K/k.

Though we will not pursue the thread here, if K/k is a function field in $d \geq 2$ variables, then the set $\Sigma(K/k)$ is a much more complicated (and interesting) object. It has more points than the closed points on any one complete nonsingular variety $V_{/k}$ with function field $k(V) \cong K$ because (in some cases this remains a conjecture) there are infinitely many nonisomorphic such varieties, related by blowups and other birational transformations, and there are at least as many points on the Zariski-Riemann surface as there are closed points on all of these models. (This is meant as quite a loose statement, to match my own quite loose understanding.)

Well, we will not pursue the thread *much*. Once you see Galois connections, it is hard to unsee them.

EXERCISE 1.3. *Let A be a subring of a field K.*

a) *For a subring $A \subset R \subset K$, let $\Phi(R)$ be the set of all R-regular valuation rings of K. Observe that we have $\Phi(R) = \Sigma(K/R)$. For a subset $Y \subset \Sigma(K/A)$, let $\Psi(Y) = \bigcap_{v \in \Sigma(K/A)} R_v$. Show that (Φ, Ψ) forms an antitone Galois connection from the partially ordered set of A-subalgebras of K to the partially ordered set $2^{\Sigma(K/A)}$ of all subsets of $\Sigma(K/A)$.*
(Suggestion: show that this is the Galois connection induced by the relation $\mathcal{R} \subset K \times \Sigma(K/A)$ defined by $(f, v) \in \mathcal{R}$ iff $f \in R_v$.)

b) *Recall that an antitone Galois connection yields Moore closure operators*

$$R \subset \overline{R} := \Psi(\Phi(R)),\ Y \subset \overline{Y} = \Phi(\Psi(Y)),$$

such that Φ and Ψ restrict to mutually inverse antitone bijections on the closed subsets. Show: $\overline{R}$ is the integral closure of R in K.
(This is a restatement of a standard, nontrivial result of commutative algebra. It can be found in [**CA**, §17]*, for instance – note that I am not telling you exactly where!)*

c) *Suppose that A is a Dedekind domain with fraction field K. Show that $\overline{R} = R$ for all $A \subset R \subset K$ and $\overline{Y} = Y$ for all $Y \subset \Sigma(K/A)$.*

3. Places on a function field

Now let K/k be a function field *in one variable*, and let $v \in \Sigma(K/k)$, so v corresponds to a valuation ring $k \subsetneq R_v \subsetneq K$. Our first orders of business are to show that v is necessarily discrete and to classify all possible v in some sense. This is very similar to some material in [**NTII**, §1.1.8], but it is not identical and it is important enough to cover again. We will also take a more "algebraic" approac' here, in contrast to the (relatively) "analytic" approach of those notes. Accordingly, we begin with

THEOREM 1.1. *Let A be a subring of a field K. Then the integral closure of A in K is the intersection of all valuation rings $A \subset R \subset K$.*

PROOF. See [**CA**, Thm. 17.17]. □

From Theorem 1.1 it follows that $\bigcap_{v \in \Sigma(K/k)} R_v = \kappa(K)$, the algebraic closure of k in K. Since K/k has transcendence degree 1 and $\kappa(K)/k$ has transcendence degree zero, this shows that $\Sigma(K/k)$ is not empty. We will see soon enough that it is infinite. (More precisely, we have $\#\Sigma(K/k) = \max(\#k, \aleph_0)$. This will be a straightforward exercise eventually.)

Let $v \in \Sigma(K/k)$. Since $R_v \subsetneq K$ and has fraction field K, R_v is nontrivial; let $t \in \mathfrak{m}_v \setminus \{0\}$. Then $k[t] \subset R_v$ and $\mathfrak{m}_v \cap k[t]$ is a prime ideal of $k[t]$ containing t so $\mathfrak{m}_v \cap k[t] = (t)$. In particular, $\mathfrak{m}_v$ does not contain any other monic irreducible element p. Since $k = k[t]^\times \subset R_v^\times$, associate elements of $k[t]$ map to the same element of the value group $G(R_v) = K^\times / R_v^\times$ and every element of $k[t]^\times$ is associate to a product of monic polynomials, it follows that the image of $k[t]^\bullet$ in $G(R_v)$ is a copy of $(\mathbb{N}, +)$ generated by the image of t. The image of $k(t)^\times$ in $G(R_v)$ is therefore infinite cyclic, generated by the image of t. In other words, we've shown that the restriction of v to $k(t)$ is a discrete valuation. If a valuation becomes discrete when restricted to a finite index subfield, then it was already discrete [**NTII**, Cor. 1.60], so we conclude that v is discrete.

EXERCISE 1.4. *Let k be a field, and let $K = k(t_1, \ldots, t_n)$ be a rational function field in n indeterminates. Let $G \coloneqq \mathbb{Z}^n$, with the lexicographic ordering. Let $G^{\geq 0} = \mathbb{N}^n$ (it is indeed the submonoid of non-negative elements for the given ordering).*

a) *Observe/recall that the polynomial ring $k[t_1, \ldots, t_n]$ can be viewed as the semigroup algebra $k[G^{\geq 0}]$.*
b) *Define a map $v : k[G^{\geq 0}]^\bullet \to G^{\geq 0}$ by mapping each polynomial to the smallest monomial in it support.*
c) *Extend v to a surjective map $K^\bullet \to G$ that satisfies (VRK1) and (VRK2). Show that $R_v \coloneqq v^{-1}(G^{\geq 0}) \cup \{0\}$ is a valuation ring with value group G. In particular, if $n \geq 2$ then K carries a valuation of rank $n \geq 2$.*
d) *Suppose now that L/k is any function field in n variables. Show that L carries a valuation of rank n. (It suffices to know that higher rank valuations on a field can be exended to a a finite degree field extension. This is true, although it is not discussed in* [**NTII**]*.)*

For any field K, let A be a Dedekind domain with fraction field K. Recall that for every maximal ideal $\mathfrak{p} \in \operatorname{MaxSpec} A$ we get a discrete valuation $v_\mathfrak{p}$ on K, as follows:

for $x \in K^\times$, we factor the principal fractional ideal

$$(x) = Ax = \prod_{\mathfrak{p} \in \operatorname{MaxSpec} A} \mathfrak{p}^{a_\mathfrak{p}}$$

with $a_\mathfrak{p} \in \mathbb{Z}$ and $a_\mathfrak{p} = 0$ for all but finitely many primes $\mathfrak{p}$. Then we put

$$v_\mathfrak{p}(x) = a_\mathfrak{p}.$$

This gives a map $\operatorname{MaxSpec} A \to \Sigma(K/A)$. This map is injective: since distinct maximal ideals are incomparable, if $\mathfrak{p} \neq \mathfrak{q} \in \operatorname{MaxSpec} A$, there is $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_2$ and thus $x^{-1} \in A_{\mathfrak{p}_2} \setminus A_{\mathfrak{p}_1}$.

PROPOSITION 1.2. *Let K/k be a one variable function field, and let $k \subset A \subset K$. If A is a Dedekind domain with fraction field K, then*

$$\Sigma(K/A) = \operatorname{MaxSpec} A.$$

PROOF. Let $v \in \Sigma(K/A)$, so $A \subset R_v$. Then $\mathfrak{m}_v \cap A$ is a prime ideal of the Dedekind domain A. If it were the zero ideal, then we would have $A^\bullet \subset R_v^\times$ and then, since K is the fraction field of A, that $K^\times \subset R_v^\times$, so v is trivial, contrary to the definition of $\Sigma(K/A)$. Thus $\mathfrak{m}_V \cap A = \mathfrak{p}$ is a maximal ideal of A and since $A \setminus \mathfrak{p} \subset R_v^\times$, we get $A_\mathfrak{p}^\bullet \subset R_v^\bullet$. An inclusion of two discrete valuation rings within the same fraction field is an equality, so $A_\mathfrak{p} = r_v$ and thus v is equivalent to $v_\mathfrak{p}$. □

Let us now focus on the case of $K = k(t)$, a one variable rational function field. By Proposition 1.2 we get that $\Sigma(k(t)/k[t]) = \operatorname{MaxSpec} k[t]$, which can in turn be identified with the set of monic irreducible polynomials $p(t) \in k[t]$. The remaining issue is to classify the k-regular valuations v of $k(t)$ for which $t \notin R_v$. Well, if $t \notin R_v$ then $t^{-1} \in R_v$, so v is $k[1/t]$-regular and indeed $\frac{1}{t} \in \mathfrak{m}_v$. In fact $k[1/t]$ is a Dedekind domain with fraction field $k(t)$ that is even isomorphic to $k[t]$, so what we have done already determines v: it must be the $\frac{1}{t}$-adic valuation on $k[1/t]$. In other words, if we write a rational function f as $(1/t)^n \frac{a(1/t)}{b(1/t)}$ where $a, b \in k[1/t]$ are polynomials with nonzero constant term, then $v_{1/t}(f) = n$.

EXERCISE 1.5. *Define a map $v_\infty : k(t)^\times \to \mathbb{Z}, x = \frac{p(t)}{q(t)} \mapsto \deg q - \deg p$.*

a) *Show that v_∞ is a $k[1/t]$-regular discrete valuation on $k(t)$.*
b) *Deduce from the above discussion that the valuations v_∞ and $v_{1/t}$ are equivalent: i.e., have the same valuation ring.*
c) *Show that $v_\infty = v_{1/t}$.*

We deduce:

THEOREM 1.3.

$$\Sigma(k(t)/k) = \operatorname{MaxSpec} k[t] \coprod \{v_\infty\}.$$

A description of $\Sigma(K/k)$ for a general one variable function field follows from this using (hopefully!) familiar arguments from algebra and number theory. Let's do it.

THEOREM 1.4. *Let A be a domain with fraction field K. Suppose that A is finitely generated as an algebra over a field k. Let L/K be a finite degree field extension. Let B be the integral closure of A in L. Then:*

a) *The ring B is finitely generated as an A-module.*
b) *The ring B is an integrally closed domain with fraction field L that is finitely generated as a k-algebra.*

c) *We have* $\dim A = \dim B$ *(Krull dimension).*
d) *If A is a Dedekind domain, then so is B.*

PROOF. a) See [**CA**, Thm. 18.4] (and note the lack of separability hypotheses!). b) Since B is finitely generated as an A-module, it is certainly finitely generated as an A-algebra. The property of being finitely generated as an algebra is transitive, so B is finitely generated as a k-algebra. The rest is similarly straightforward. c) Since B is finitely generated as an A-module, by [**CA**, Thm. 14.1] we have that B is an integral extension of A. Integral extensions preserve Krull dimension [**CA**, Cor. 14.17]. d) If A is a Dedekind domain, then by parts a), b) and c) B is an integrally closed domain of dimension at most one that is finitely generated as a module over a Noetherian ring, hence it is a Dedekind domain. □

PROPOSITION 1.5. *Let L/K be a finite degree field extension, and let v be a valuation on L. Let A be a subring of K and let B be the integral closure of A in L. Then v is A-regular iff it is B-regular.*

PROOF. Since $A \subset B$, clearly if v is B-regular then it is A-regular. Conversely, suppose that $A \subset R_v$, and let $x \in B$. There are then elements $a_0, \ldots, a_{n-1} \in A$ such that

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0.$$

Seeking a contradiction, we suppose that $v(x) < 0$ (in the group of divisibility of R_v). Then for all $0 \leq i \leq n-1$ we have

$$v(a_i x^i) = v(a_i) + iv(x) \geq iv(x) > nv(x) = v(x^n),$$

and thus

$$v(-(a_{n-1}x^{n-1}+\ldots+a_1x+a_0)) = v(a_{n-1}x^{n-1}+\ldots+a_1x+a_1x+a_0) \geq \min_i v(a_i x^i) > v(x^n),$$

so $v(x^n) \neq v(-a_{n-1}x^{n-1}-\ldots-a_1x-a_0)$ and $x^n \neq -a_{n-1}x^{n-1}-\ldots-a_1x-a_0$. □

Now let K/k be a one variable function field. We wish to understand $\Sigma(K/k)$. We do this by choosing a transcendental element $t \in K$, which gives a finite degree field extension $K/k(t)$, say of degree n. Restricting valuations from K to $k(t)$ gives us a map

$$r : \Sigma(K/k) \to \Sigma(k(t)/k).$$

As a special case of our study of valuation theory in [**NTII**, §1.3] we know that each fiber of r is nonempty and of size at most n. In fact we have the following much more precise result.

THEOREM 1.6 (Degree Equality). *Let K be a field and let v be a rank one valuation on K, with valuation ring R. Let L/K be a field extension of degree n. Let $w_1, \ldots, w_g$ be the valuations on L extending v. For $1 \leq i \leq g$, let $e_i(L/K)$ be the ramification index of w_i/v, namely the order of $w_i(L^\times)/v(K^\times)$ and let $f_i(L/K)$ be the degree of the extension of residue fields.*

a) *We have*

$$\sum_{i=1}^{g} e_i(L/K) f_i(L/K) \leq [L:K]. \tag{1}$$

b) *If v is discrete and the integral closure S of R in L is finitely generated as an R-module, then equality holds in (1).*

Let K/k is a one variable function field, let L/K be a finite degree field extension, and let $v \in \Sigma(K/k)$. We claim that the integral closure S of R_v in L is a finitely generated R_v-module, and thus the degree equality (1) holds. Recall that the finite generation is automatic if L/K is separable [**CA**, Thm. 18.1], hence always in characteristic 0. However we do not wish do – and do not need to – make that hypothesis. Instead, choose a uniformizing element $t \in K$ for v, and consider the finite degree extension $K/k(t)$. Then v is $k[t]$-regular. Let A be the integral closure of $k[t]$ in K and let B be the integral closure of $k[t]$ in L. By Theorem 1.4 we get that A is a Dedekind domain with fraction field K, B is a Dedekind domain with fraction field L, and both A and B are finitely generated $k[t]$-modules. It follows that B is finitely generated as an A-module. Since v is $k[t]$-regular, it follows from Proposition 1.5 that v is A-regular, and thus it follows from Proposition 1.2 that $v = v_{\mathfrak{p}}$ for a unique $\mathfrak{p} \in \operatorname{MaxSpec} A$. In turn this gives that $R = A_{\mathfrak{p}}$ and $S = B_{\mathfrak{p}} = B \otimes_A A_{\mathfrak{p}}$, and since finite generation is preserved by base change we deduce that is S a finitely generated R-module and thus (1) holds.

Remark 1. *Since all the valuations in play are discrete, there is not really any "Number Theory II" going on here – in the setting of Theorem 1.6 one could just as well take R to be a Dedekind domain and speak in terms of the prime factorization of $\mathfrak{p}S$. It comes to the same – and in particular, is not easier. If one consults a suitably algebraic number theory text that states the Degree Inequality for general extensions of Dedekind domains, say* [**Lo**, Thm. 3.5]*, one still finds the hypothesis that S be finitely generated over R, which is again automatic and easy to show in case L/K is separable. Our present setting – in which our global Dedekind domains are finitely generated over a field – is more favorable than the general case.*

Corollary 1.7. *Let $n \in \mathbb{Z}^+$, and let L/K be a degree n extension of one variable function fields over k. Then the restriction map*

$$r : \Sigma(L/k) \to \Sigma(l/k)$$

is surjective and each fiber has cardinality at most n.

Exercise 1.6. *Let K/k be a one-variable function field.*

a) *Show that $\Sigma(K/k)$ is infinite.*

b *) More precisely, show that the cardinality of $\Sigma(K/k)$ is equal to the number of monic irreducible polynomials $p \in k[t]$, which is $\#\max(\#k, \aleph_0)$.*

4. The Degree of a Place

Let K/k be a one variable function field, and let $v \in \Sigma(K/k)$. Then we have a **residue field** $k(v) \coloneqq R_v/\mathfrak{m}_v$, which is a field extension of k via $k \hookrightarrow R_v \to R_v/\mathfrak{m}_v$. We claim that $[k(v) : k]$ is finite. To show this: we have seen above that there is a Dedekind domain A that is finitely generated as a k-algebra such that v is A-regular and $R_v = A_{\mathfrak{p}}$ for a unique $\mathfrak{p} \in \operatorname{MaxSpec} A$. Thus we also have $k(v) = A/\mathfrak{p}$, so $k(v)$ is a finitely generated k-algebra. By Zariski's Lemma [**CA**, Thm. 11.1], $k(v)$ is a finite degree field extension of k.

Exercise 1.7. *In* [**St**]*, Stichtenoth gives a different proof of the finiteness of $[k(v) : k]$. He chooses $f \in K$ such that $v(f) = 1$ and shows that $[k(v) : k] \leq [K : k(f)]$. Show this by showing first that if $\overline{v}$ is the restriction of v to $k(f)$ then $k(\overline{v}) = k$ and then applying the Degree Equality (1).*

We denote the quantity $[k(v) : k]$ by $\deg v$ and call it the **degree** of v.

We are epecially interested in the degree one points $v \in \Sigma(K/k)$: let's write $\Sigma_1(K/k)$ for this set. In fact it may be empty. The following exercise gives a sufficient (but far from necessary) condition for this.

EXERCISE 1.8. *Let K/k be a one variable function field with constant field $\kappa(K)$. Show that for all $v \in \Sigma(K/k)$, we have*

$$[\kappa(K) : k] \mid \deg v.$$

In particular, if $\kappa(K) \supsetneq k$, then K has no degree one points.

EXERCISE 1.9. *Let K/k be a one variable function field. Show that the following are equivalent:*

(i) *Every $v \in \Sigma(K/k)$ has degree 1.*
(ii) *The ground field k is algebraically closed.*

EXERCISE 1.10. *For any field k, let $\mathcal{P}^1(k)$ denote the set $k \cup \{\infty\}$. (You can certainly go ahead and think of this as the set of lines through the origin in k^2. However it is not necessary, or even immediately helpful, to think in terms of algebraic varieties.) Show that there is a natural bijection*

$$\Sigma_1(k(t)/k) = \mathcal{P}^1(k).$$

Combining with Exercise 1.9 we get: $\Sigma(k(t)/k) = \mathcal{P}^1(k)$ iff k is algebraically closed.

5. Affine Dedekind Domains

Let k be a field. An **affine domain over k** is a finitely generated k-algebra that is a domain. An affine Dedekind domain is an affine domain that is also a Dedekind domain and not a field – that is, it is a domain that is finitely generated over k, integrally closed, and of dimension 1. An **affine order over k** is an affine domain that has Krull dimension one but need not be integrally closed.

EXERCISE 1.11. *Let $A_{/k}$ be an affine order, with fraction field K. Show: K is a one variable function field over k.*

If A/k is an affine Dedekind domain with fraction field K, then Proposition 1.2 gives an embedding

$$\operatorname{MaxSpec} A = \Sigma(K/A) \hookrightarrow \Sigma(K/k).$$

Let

$$\Sigma(A, \infty) \coloneqq \Sigma(K/k) \setminus \Sigma(K/A)$$

be the complement. For example, we have $\Sigma(k[t], \infty) = \{v_\infty\}$.

PROPOSITION 1.8. *For any affine Dedekind domain A, the set $\Sigma(A, \infty)$ is finite and nonempty.*

PROOF. By Noether Normalization [**CA**, Thm. 14.22], there is $t \in A$ such that A is an integral extension of $k[t]$ (equivalently, finitely generated as a $k[t]$-module), and thus A is the integral closure of $k[t]$ in K. Let $r : \Sigma(K/k) \to \Sigma(k(t)/k)$ be the restriction map. By Proposition 1.5, we have

$$\Sigma(K/A) = r^{-1}(\Sigma(k(t)/k[t])$$

and thus

$$\Sigma(A, \infty) = r^{-1}(\Sigma(k[t], \infty)) = r^{-1}(v_\infty).$$

Now Corollary 1.7 gives that $r(A, \infty)$ is nonempty and finite. □

Thus an affine Dedekind domain A determines a function field K, and the set of places $\Sigma(K/k)$ consists of all the maximal ideals of$A$ together with a finite nonempty set of points. Above we saw that for a one variable function field K/k and $v \in \Sigma(K/k)$ there is an affine domain A with fraction field K such that $v \in \Sigma(K/A)$.

For a subset $Z \subset \Sigma(K/k)$, we put

$$R^Z := \bigcap_{v \in \Sigma(K/k) \setminus Z} R_v.$$

For example we have $R^\varnothing = \kappa(K)$.

EXERCISE 1.12. *Show: If A is an affine Dedekind domain with fraction field K, then we have $A = R^{\Sigma(K/k) \setminus \operatorname{MaxSpec} A}$.*

The following result gives a converse:

THEOREM 1.9. *Let K/k be a one variable function field, and let $Z \subset \Sigma(K/k)$ be finite and nonempty. Then R^Z is an affine Dedekind domain with fraction field Z and* $\operatorname{MaxSpec} R^Z = \Sigma(K/k) \setminus Z$.

PROOF. Step 0: If $Z_1 \subset Z_2$ is an inclusion of finite nonempty subsets of $\Sigma(K/k)$, then we have $R^{Z_1} \subset R^{Z_2} \subset K$. So if R^{Z_1} is a Dedekind domain with fraction field K and $\operatorname{MaxSpec} R^{Z_1} = \Sigma(K/k) \setminus Z_1$, then it follows from the classification of overrings of Dedekind domains [**CA**, §23.2] that R^{Z_2} is a Dedekind domain and $\operatorname{MaxSpec} R^{Z_2} = \operatorname{MaxSpec} R^{Z_1} \setminus Z_2 = \Sigma(K/k) \setminus Z_2$.
Step 1: We treat the case of $K = k(t)$ a rational function field, and here we begin with the case of $\#Z = 1$. We have $R^{v_\infty} = k[t]$. For any monic irreducible polynomial $p \in k[t]$, we have $R^{v_p} \supset k[\frac{1}{p}]$. Let $d = \deg(p)$. Then $k[\frac{1}{p}]$ is an affine PID (it is isomorphic as a k-algebra to $k[t]$) and its fraction field $F = k(\frac{1}{p})$ is a subfield of $k(t)$ such that $[k(t) : F] = d$ (Exercise 1.3). Let A be the integral closure of $k[\frac{1}{p}]$ in $k(t)$. Then A is a Dedekind domain with fraction field $k(t)$ such that $\operatorname{MaxSpec} A = \Sigma(k(t)/k) \setminus \{v_p\}$. By Exercise 1.12 we have $A = R^{\{v_p\}}$.

Step 2: Let Z be a finite nonempty subset of $\Sigma(K/k)$. Choose $t \in K \setminus \kappa(K)$, let $r : \Sigma(K/k) \to \Sigma(k(t)/k)$ be the restriction map, and put $\overline{Z} = r(Z)$. Let $A = R^{\overline{Z}}$, and let B be the integral closure of A in K. Then B is an affine Dedekind domain with fraction field K, and if $\tilde{Z} := \Sigma(K/k) \setminus \operatorname{MaxSpec} B$ then $\tilde{Z} \supset Z$. So we have

$$A \subset R^Z \subset B.$$

Since B is finitely generated as an A-module and A is Noetherian, R^Z is therefore finitely generated as an A-module and therefore it is finitely generated as a k-algebra. So R^Z is an affine Dedekind domain, and by Exercise 1.12 we have $\operatorname{MaxSpec} R^Z = \Sigma(K/k) \setminus Z$. □

EXERCISE 1.13. *Let $Z \subset \Sigma(K/k)$ be infinite and proper. Show: R^Z is a Dedekind domain with fraction field K that is* not *finitely generated as a k-algebra.*

EXERCISE 1.14. *Let R be an integrally closed domain such that $k \subset R \subset K$. Show: $R = R^Z$ for a unique subset $S \subset \Sigma(K/k)$.*

These results show an essential equivalence between affine Dedekind domains over k and one-dimensional function fields over k. One can think affine Dedekind domains as giving "coordinate charts" for $\Sigma(K/k)$, but in some sense that makes things overly elaborate: in this case, each chart is so large that it covers all but finitely many points!

EXERCISE 1.15. *Let K/k be a one-variable function field. Show: there are affine Dedekind domains A_1, A_2 over k with fraction field K such that $\Sigma(K/k) = \operatorname{MaxSpec} A_1 \cup \operatorname{MaxSpec} A_2$ (the union is very far from being disjoint).*

LEMMA 1.10. *Let K/k be a one variable function field, and let $f \in K \setminus \kappa(K)$. There is an affine Dedekind domain A containing f.*

PROOF. Since $f \notin \kappa(K)$, it is transcendental over k. We may take A to be the integral closure of $k[f]$ in K. □

LEMMA 1.11. *Let $f \in K \setminus \kappa(K)$.*

a) *The set of $v \in \Sigma(K/k)$ such that $f \notin R_v$ is finite.*
b) *The set of $v \in \Sigma(K/k)$ such that $f \in \mathfrak{m}_v$ is finite.*

PROOF. a) By the previous Lemma, there is an affine Dedekind domain A with fraction field K and containing f. Thus for all $\mathfrak{p} \in \operatorname{MaxSpec} A$ we have $f \in A \subset A_{\mathfrak{p}} = R_{v_{\mathfrak{p}}}$. Since $\Sigma(K/k) \setminus \operatorname{MaxSpec} A$ is finite, this establishes the result.
b) Since $f \in \mathfrak{m}_v$ iff $\frac{1}{f} \notin R_v$, this follows from part a). □

THEOREM 1.12 (Strong Approximation). *Let $X \subsetneq \Sigma(K/k)$ be a proper subset, and let $P_1, \ldots, P_r$ be finitely many distinct elements of X. Let $x_1, \ldots, x_r \in K$ and let $n_1, \ldots, n_r \in \mathbb{Z}$. Then there is $x \in K$ such that*

$$\forall 1 \leq i \leq r,\ v_{P_i}(x - x_i) = n_i,$$
$$\forall P \in S \setminus \{P_1, \ldots, P_r\},\ v_P(x) \geq 0.$$

PROOF. It is no loss of generality to assume that $S \coloneqq \Sigma(K/k) \setminus X$ consists of a single place v. Let R^S be the corresponding affine domain. It is a Dedekind domain, so we may apply the "Dedekind Approximation Theorem" [**NTII**, Prop. 1.17]. (This result uses the Artin-Whaples "weak" approximation theorem and the Chinese Remainder Theorem.) □

5.1. The Jacobian Criterion. The following result is, from the perspective of a principled exposition drawing only on prior courses, a bit of a cheat. However, it is so useful in practice that omitting it seems like a disservice to the student of this area.

THEOREM 1.13 (Jacobian Criterion for Smoothness). *Let k be a field with algebraic closure $\overline{k}$. Let $f \in k[x, y]$ be a geometrically irreducible polynomial. Let $R \coloneqq k[x, y]/(f)$ and $\overline{R} \coloneqq \overline{k}[x, y]/(f)$.*

a) *The following are equivalent:*
   (i) *The ring $\overline{R}$ is a Dedekind domain.*
   (ii) *For all $(a, b) \in \overline{k}$, at least one of $\frac{\partial f}{\partial x}(a, b)$ and $\frac{\partial f}{\partial y}(a, b)$ is nonzero.*
b) *If $\overline{R}$ is a Dedekind domain, then R is a Dedekind domain.*

c) *If k is perfect and R is a Dedekind domain, then $\overline{R}$ is a Dedekind domain.*

PROOF. First we observe that R and $\overline{R}$ are Noetherian domains of dimension one, so they are Dedekind domains iff they are integrally closed. With this in mind, [**Lo**, Thm. II.5.10] gives part a), while [**Lo**, Cor. VII.2.7] gives part b). Part c) is a special case of [**Ei**, Thm. 16.19]. □

6. Completion

In [**NTII**] we develop the general theory of completion of a field with respect to a norm, which includes the case of completion with respect to a rank one valuation. We now apply this to the case of a one variable function field K/k and $P \in \Sigma(K/k)$.

For any field k, recall that $k[[t]] = \{\sum_{n=0}^{\infty} a_n t^n\}$ denotes the ring of formal power series over k, a domain with fraction field

$$k((t)) = \{\sum_{n=N}^{\infty} a_n t^n \mid a_n \in k\}$$

consisting of formal (finite-tailed) Laurent series over k. The map $v : k((t))^\times \to \mathbb{Z}$ that sends a nonzero formal Laurent series to the index of its smallest nonzero coefficient is a discrete valuation, with associated valuation ring $k[[t]]$. The maximal ideal is generated by t. This $k[[t]]$ is a DVR; it is moreover complete, which means on the one hand that the natural map $R \to \varprojlim k[[t]]/(t^n)$ is an isomorphism and on the other that $k((t))$ is complete with respect to "the" associated norm, in a sense that is made precise in the proof of Proposition 1.14 below.

EXERCISE 1.16. *Let k be a perfect field of characteristic p. Show:*

$$k((t))^{1/p} = k((t^{1/p})).$$

(Suggestion: Given $\sum_{n \geq N} a_n t^n \in k((t))$, actually write out its pth root.)

PROPOSITION 1.14. *Let R be a complete discrete valuation ring, with maximal ideal $\mathfrak{m}$ and residue field $R/\mathfrak{m} = k$, and let $q : R \to k$ be the quotient map. **Suppose** there is a homomorphism $\iota : k \hookrightarrow R$ such that $q \circ \iota = 1_k$. If π is a uniformizer for R, there is a k-algebra isomorphism $\varphi : k[[t]] \xrightarrow{\sim} R$ such that $\varphi(t) = \pi$.*

PROOF. Let K be the fraction field of R, and let $v : K^\times \to \mathbb{Z}$ be the discrete valuation. As usual we can define an associated non-Archimedean metric on K by $|x| := 2^{-v(x)}$. (Any other positive real number would work just as well as 2. There are circumstances in which it is useful to choose the constant with some care; this is not one.) That R is complete means (in one equivalent formulation) that K is complete with respect to the metric $d(x, y) := |x - y|$. In the metric topology, the subring R is both the open unit ball centered at 0 and the closed unit ball centered at 0; in particular, R, being closed in a complete metric space, is itself complete. In particular this gives us a notion of convergence of infinite sequences and series in K and R, and because of the completeness, a sequence in K or R converges iff it is Cauchy. In fact, because the metric is non-Archimedean – namely $|x+y| \leq \max |x|, |y|$, the theory of convergence of infinite series simplifies

conisderably: a series $\sum_{n=0}^{\infty} a_n$ in K converges iff $a_n \to 0$ iff $v(a_n) \to \infty$.
The map φ is given by

$$\sum_{n=0}^{\infty} a_n t^n \mapsto \sum_{n=0}^{\infty} \iota(a_n)\pi^n.$$

This is well-defined because $v(\iota(a_n)\pi^n) = n + v(\iota(a_n)) \geq n$. It is straightforward to check that φ is a k-algebra homomorphism. Moreover, if $\sum_{n=0}^{\infty} \iota(a_n)\pi^n = 0$ then we must have $\iota(a_n) = 0$ for all n: for if not, let N be the least natural number n such that $\iota(a_n) \neq 0$. Since $q(\iota(a_n)) = a_n \neq 0$ in the residue field k, we get $v(\iota(a_N)) = 0$. We then get

$$\iota(a_N)\pi^N = \sum_{n=N+1}^{\infty} -a_n,$$

and the left hand side has valuation N while the right hand side has valuation at least $N+1$, a contradiction.

It remains to show that φ is surjective, so let $x \in R$. Let $a_0 \coloneqq q(x)$. Then

$$q(x - \iota(a_0)) = q(x) - q(\iota(a_0)) = q(x) - a_0 = 0,$$

so $x - \iota(a_0)$ lies in the maximal ideal and thus is of the form πx_1 for a unique $x_1 \in R$. Let $a_1 \coloneqq q(x_1)$. Then as above we have $q(x_1 - \iota(a_1)) = 0$, so $x_1 - \iota(a1) = \pi x_2$ for a unique $x_2 \in R$, and thus overall we have

$$x - \iota(a_0) - \iota(a_1)\pi = \pi(x_1 - \iota(a_1)) = \pi^2 x_2.$$

Continuing in this way, we define a sequence $\{a_n\}_{n=0}^{\infty}$ of elements of k such that for all $N \in \mathbb{N}$ we have

$$x - \sum_{n=0}^{N} \iota(a_n)\pi^n \in \mathfrak{m}^{n+1},$$

from which it follows that

$$\sum_{n=0}^{\infty} \iota(a_n)\pi^n = x. \qquad \square$$

We remark that the isomorphism φ is continuous for the associated topologies on $k[[t]]$ and R and is in fact the unique continuous map having the properties asserted in Proposition 1.14.

The next question is for which CDVRs R there exists a homomorphism $\iota : k \hookrightarrow R$ such that $q \circ \iota = 1_k$. There is one case in which this certainly *cannot* occur. Namely, if R has characteristic 0 and k has characteristic p, then an embedding of k into R would embed $\mathbb{F}_p$ into a characteristic 0 ring, which is impossible. This is the case for instance when $R = \mathbb{Z}_p$ or more generally is the completion of the ring of integers $\mathbb{Z}_K$ of a number field K with respect to the valuation $v_{\mathfrak{p}}$ attached to a nonzero prime ideal $\mathfrak{p}$. In this case we say that R has **mixed characteristic**, and otherwise we say that R has **equicharacteristic**. In fact:

THEOREM 1.15. *Let R be an equicharacteristic CDVR with residue field k. Then there is a homomorphism $\varphi : k \hookrightarrow R$ and thus $R \cong k[[t]]$.*

The case of equicharacteristic 0 is rather easy, and the case in which the residue field k is perfect of positive characteristic is not much harder. The general case follows from Cohen's structure theory of complete local rings, which for me is quite

serious commutative algebra.

The hardest part of these results is to show that an equicharacteristic CDVR contains any field whatsoever. This at least is clear in equicharacteristic 0: if p is any prime number, then we cannot have $p \in \mathfrak{m}$ since then the residue field $R/\mathfrak{m}$ would have charactersitic p. So every prime number is invertible in R, hence $\mathbb{Q} \subset R$. Happily, in our intended application the existence of a subfield comes for free.

Namely, let K/k be a one variable function field, and let $P \in \Sigma(K/k)$ be a place. Let K_P be the completion of K with respect to the discrete valuation v_P, so K_P is a complete discretely valued field with residue field $R_P/\mathfrak{m}_P = k_P$, which as we know is a finite degree field extension of k. Let $\hat{R}_P$ be the valuation ring of K_P, so $\hat{R}_P$ is the competion of the DVR R_P. Indeed we have

$$k \subset R_P \subset \hat{R}_P.$$

Thus it follows from Theorem 1.15 that $\hat{R}_P \cong k_P[[t]]$, though we have not explained exactly why. Notice that the easiest case is certainly that in which P has degree 1: then $k_P = k$ and the homomorphism ι is simply the inclusion $k \hookrightarrow \hat{R}_P$ mentioned above. It turns out that the pleasant case is that in which the finite degree extension k_P/k is separable.

PROPOSITION 1.16. *Suppose that $P \in \Sigma(K/k)$ is such that the k_P/k is a separable extension (which is automatic when k is perfect, hence always in characteristic 0). Then there is a unique k-algebra homomorphism $\iota : k_P \hookrightarrow \hat{R}_P$ such that $q \circ \iota = 1_{k_P}$. It follows that for every uniformizer π for P we have $\hat{R}_P = k_P[[\pi]]$.*

PROOF. Since k_P/k is separable, it is monogenic: we have $k_P = k[a]$ for some $a \in k_P$. Let $f \in k[x]$ be the minimal polynomial for a. Since k_P/k is separable, f is separable and thus $f'(a) \neq 0$. But because k embeds in $\hat{R}_P$ we may also view $f \in \hat{R}_P[x]$. It now follows from Hensel's Lemma that there is a unique $\alpha \in R$ such that $q(\alpha) = a$ and $f(\alpha) = 0$. If $d = [k_P : k]$ then every element of k_P has a unique expression as $\sum_{i=0}^{d-1} c_i a^i$ with $c_i \in k$, and therefore the unique k-algebra homomorphism $\iota : k[x] \to \hat{R}_P$ such that $\iota(x) = \alpha$ induces a k-algebra homomorphism $\iota : k_P \hookrightarrow \hat{R}_P$ such that $q(\iota(a)) = a$ and thus $q \circ \iota = 1_{k_P}$. The uniqueness of ι follows: a k-algebra homomorphism $\iota : k_P \hookrightarrow \hat{R}_P$ is determined by where it sends a; it must send a to a root of $f(x)$, and α is the only root of $f(x)$ that maps under q to a. □

Thus, if $P \in \Sigma(K/k)$ is a place with separable residue field, then any choice of uniformizing element π at P yields a embedding

$$K \hookrightarrow k_P((\pi)),$$

so that we get a series representation $f = \sum_{n=N}^{\infty} a_n \pi^n$ of any element $f \in K$. This is an algebraic analogue of the Laurent series expansion of a meromorphic function of one complex variable at a point, and it is similarly useful: for instance, the coefficient a_{-1} is in some sense a residue,[1] and there will be a Residue Theorem.

[1]This is not quite right: the a_{-1} coefficient certainly depends on the choice of the uniformizing element so is not capturing anything intrinsic about f at P. Later we will define the residue at P of the meromorphic differential $f d\pi$, which *will* be independent of the choice of π.

CHAPTER 2

The Riemann-Roch Theorem

In this chapter we will prove the Riemann-Roch Theorem for curves over an arbitrary ground field. Our treatment follows [**St**], who follows André Weil's spectacular approach using repartitions (a.k.a. "small adeles") and Weil differentials.

Starting in this chapter, when we say "function field" we will mean "one-variable function field."

1. Divisors

Let K/k be a function field. The **divisor group** $\operatorname{Div} K$ is the free commutative group on the set $\Sigma(K/k)$ of places of K. That is, $\operatorname{Div} K$ consists of formal $\mathbb{Z}$-linear combinations $\sum_P n_P P$ with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many places P. A divisor is **effective** if $n_P \geq 0$ for all P. The effective divisors form a free commutative monoid on the set of places.

For $D_1, D_2 \in \operatorname{Div} K$, we write $D_1 \leq D_2$ if $D_2 - D_1$ is effective. This endows $\operatorname{Div} K$ with a partial ordering that is compatible with the commutative group structure (i.e., if $A \leq B$ and $C \leq D$ then $A + C \leq B + D$) .

The **support** of a divisor $D = \sum_P n_P P$ is the set of P such that $n_P \neq 0$. This is a finite subset of $\Sigma(K/k)$.

Every divisor has a **degree**,

$$\deg(\sum_P n_P P) = \sum_P n_p \deg P \in \mathbb{Z}.$$

The degree defines a homomorphism $\deg : \operatorname{Div} K \to \mathbb{Z}$. The kernel is denoted by $\operatorname{Div}^0 K$, the degree zero divisors.

We define the **index** $I(K)$ of K to be the size of the cokernel of the degree map. In other words, the index is the least positive degree of a divisor on K.

Exercise 2.1. *Let K/k be a one variable function field.*

a) *Show: If $\Sigma_1(K/k) \neq \varnothing$, then K has index 1.*
b) *We will see later that if k is finite, K always has index 1 but $\Sigma(K/k)$ may be empty. You can try to prove this now if you like!*
c) *Deduce: if k is algebraically closed, then K has index 1.*
d) *Show: The index of K is divisible by $[\kappa(K) : k]$.*

Lemma 2.1. *For $f \in K^\times$ we have $v_P(f) = 0$ for all but finitely many $P \in \Sigma(K/k)$.*

PROOF. If $f \in \kappa(K)$ then we have $v_P(f) = 0$ for all $P \in \Sigma(K/k)$. Otherwise, let A be the integral closure of $k[f]$ in K. This is an affine Dedekind domain containing f. Then $v_{\mathfrak{p}}(f) \geq 0$ for all $\mathfrak{p} \in \operatorname{MaxSpec} A$, hence $v_{\mathfrak{p}}(f) \geq 0$ for all but finitely many $\mathfrak{p}$. Like any nonzero element in a Dedekind domain, f is divisible by only finitely many prime ideals (the ones appearing in its prime factorization!), and ths completes the proof. □

Let $f \in K^\times$. We define the **divisor of f**,

$$(f) \coloneqq \sum_P v_P(f)P.$$

Here we are using Lemma 2.1 that $v_P(f) = 0$ for almost every P (throughout these notes, "almost every" will mean " for all but finitely many").

EXERCISE 2.2. *Show:* $(f) = 0$ *iff* $f \in \kappa(K)$.

We can uniquely write any element $D \in \operatorname{Div} K$ as $D_+ - D_-$, where D_+ and D_- are effective divisors with disjoint support. For the divisor (f) of a function $f \in K$, we refer to $(f)_+$ as the **divisor of zeroes** of f and $(f)_-$ as the **divisor of poles** of f.

PROPOSITION 2.2. *For $f \in K \setminus \kappa(K)$, consider the extension of function fields $K/k(f)$.*

a) *Let B_0 be the integral closure of $k[f]$ in K, an affine domain with fraction field K. If we factor $fB_0 = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$, then the divisor of zeroes of f is*

$$a_1\mathfrak{p}_1 + \ldots + a_r\mathfrak{p}_r.$$

b) *Let B_∞ be the integral closure of $k[1/f]$ in K, an affine Dedekind domain with fraction field K. If we factor $1/fB_\infty = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_s}$, then the divisor of poles of f is*

$$b_1\mathfrak{p}_1 + \ldots + b_r\mathfrak{p}_s.$$

PROOF. a) For $P \in \Sigma(K/k)$, we have that $v_P(f) \geq 0$ iff $f \in R_v$ iff $R_v \supset k[f]$. When these conditions hold, we have $\mathfrak{m}_v \cap k[f] = (f)$, so the places P for which $v_P(f) > 0$ are precisely the places lying over the valuation v_f of $k(f)$. Thus the support of the divisor of zeros of f is precisely the set of primes of B_0 lying over (f). As usual, in a Dedekind domain, if $fB_0 = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$, then $v_{\mathfrak{p}_i}(f) = a_i$.
b) It is almost the same as part a), with $\frac{1}{f}$ in place of f. Details are left to you. □

COROLLARY 2.3. *Let $f \in K \setminus \kappa(K)$.*

a) *We have* $\deg(f)_+ = [K : k(f)] = \deg(f)_-$.
b) *We have* $\deg(f) = 0$.

PROOF. a) We have $\deg(f)_+ = \sum_i a_i \deg \mathfrak{p}_i$. As we saw above, in the extension $K/k(f)$, the places $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ all lie above the degree one place v_f of $k(f)$, so $\deg \mathfrak{p}_i$ is also the residual degree f_i. Therefore by the Degree Equality we have $\deg(f)_+ = [K : k(f)]$. The argument that $\deg(f)_- = [K : k(f)]$ is almost identical.
b) Since $(f) = (f)_+ - (f)_-$, we have

$$\deg(f) = \deg(f)_+ - \deg(f)_- = [K : k(f)] - [K : k(f)] = 0.$$ □

We define the **degree** of a function $f \in K \setminus k$ to be the common quantity $[K : k(f)] = \deg(f)_+ = \deg(f)-$. Thus we must distinguish the degree of a rational function – which is a positive integer – from the degree of its divisor – which is 0.

EXERCISE 2.3. *Let $K = k(t)$, and let $f \in K \setminus k$. Write $f = \frac{p(t)}{q(t)}$ for relatively prime polynomials p and q (equivalently, p and q have no common root in an algebraic closure of k). Show:*

$$\deg(f) = \max(\deg(p), \deg(q)). \tag{2}$$

The divisor of a rational function is called **principal**.

EXERCISE 2.4. *Let $f, g \in K^\times$.*

a) *Show: $(\frac{1}{f}) = -(f)$.*
b) *Show: $(fg) = (f) + (g)$.*
c) *Deduce the principal divisors form a subgroup of $\operatorname{Div}^0 K$, denoted $\operatorname{Prin} K$.*

We say that two divisors are **linearly equivalent** if their difference is principal. We define the **divisor class group**

$$\operatorname{Cl} K = \operatorname{Div} K / \operatorname{Prin} K.$$

Since principal divisors have degree 0, the degree map factors through

$$\deg : \operatorname{Cl} K \to \mathbb{Z}.$$

We define the **degree zero divisor class group**

$$\operatorname{Cl}^0 K = \operatorname{Div}^0 K / \operatorname{Prin} K.$$

EXERCISE 2.5. a) *Show that every degree zero divisor on $k(t)$ is the divisor of a rational function.*
b) *Deduce that the degree map induces an isomorphism $\operatorname{Cl} k(t) \xrightarrow{\sim} \mathbb{Z}$ and that $\operatorname{Cl}^0 k(t) = (0)$.*

In almost every other case the groups $\operatorname{Cl} K$ and $\operatorname{Cl}^0 K$ are more interesting!

2. Rosen's Theorem

The following result apepars in a 1973 paper of Rosen [**Ro73**], in which he explains that in some form it goes back to F.K. Schmidt. For many years now it has been one of my favorite results in the area, because it directly links the divisor class group of a function field K/k to the ideal class groups of (all of!) its affine Dedekind domains.

THEOREM 2.4. *Let K/k be a one variable function field with $\kappa(K) = k$, and let $S \subset \Sigma(K/k)$ be finite and nonempty, so $R^S := \bigcap_{v \in \Sigma(K/k) \setminus S} R_v$ is an affine Dedekind domain with fraction field K. Let $D^0(S)$ be the subgroup of $\operatorname{Div}^0 K$ of degree 0 divisors supported on S, and let $P(S) = \operatorname{Prin}(K) \cap D^0(S)$ be the principal divisors supported on S. Let d be the least positive degree of a divisor supported on S (so $d = 1$ if S contains a degree one place), and let $I(K)$ be the index of K: the least positive degree of a divisor on K. Then there are exact sequences*

$$1 \to k^\times \to (R^S)^\times \to P(S) \to 0 \tag{3}$$

and

$$0 \to D^0(S)/P(S) \xrightarrow{\iota} \operatorname{Cl}^0(K) \xrightarrow{\alpha} \operatorname{Cl} R^S \xrightarrow{\beta} C(d/I(K)) \to 0, \tag{4}$$

where $\operatorname{Cl} R^S$ is the ideal class group of the Dedekind domain R^S and $C(d/i)$ is a finite cyclic group of order d/i.

PROOF. The homomorphism $(R^S)^\times \to P(S)$ is the restriction to $(R^S)^\times$ of the map that associates to a nonzero rational function its associated divisor. That it is well-defined and surjective follows immediately from the definitions, and its kernel is the set of rational functions without zeros or poles, i.e., $k^\times$. This establishes (3).

The map ι is induced by mapping a degree zero divisor supported on S to its class in $\mathrm{Cl}^0 K = \mathrm{Div}^0 / \mathrm{Prin}(K)$; the kernel of this map is $\mathrm{Prin}\, K \cap D^0(S)$, so ι is injective. The map α is induced by the map $\mathrm{Div}^0 K \to \mathrm{Frac}\, R^S$ in which we simply remove the components of the divisor at places corresponding to S. Under this map, the divisor of a rational function f gets sent to the principal fractional ideal generated by f, hence we get a well-defined map $\mathrm{Cl}^0 K \to \mathrm{Cl}\, R^S$. Under this map, a degree zero divisor class represented by D maps to 0 iff there is a rational function f such that $D - (f)$ is supported on S, so the kernel of α is the image of ι.

The map β is the most interesting. We claim that an element of $\mathrm{Cl}\, R^S$ has a degree that is well-defined up to a multiple of d. Indeed, let I represent an element of $\mathrm{Cl}\, R^S$. Then if $D \in \mathrm{Div}\, K$ is any divisor that maps to I and X is any divisor supported on S, then also $D + X$ is a divisor that maps to I. (Modifying I within its equivalence class does not change the degree, since the degree of any principal divisor is 0.) Since the degree of every divisor supported on S is a multiple of d, there is a well-defined homomorphism $\mathrm{Cl}\, R^S \to \mathbb{Z}/d\mathbb{Z}$. The kernel of this homomorphism consists of divisors whose degree is a multiple of d, and thus the divisor X supported on S can be suitable chosen so that $\deg(X + S) = 0$ and thus I lies in the image of α. Conversely, any divisor lying in the image of α has degree a multiple of d, so the kernel of β is the image of α. The image of β is the set of all multiples of the least positive degree of a divisor on C, i.e., i. Thus the map β may be viewed as a surjection onto a finite cyclic group of order $\frac{d}{i}$, completing the proof. □

EXERCISE 2.6. *We maintain the setting of Theorem 2.4.*

a) *Show:* $D^0(S) \cong \mathbb{Z}^{\#S-1}$.

b) *Suppose that* $S = \{P\}$ *consists of a single place, of degree* $d \in \mathbb{Z}^+$. *Show that (4) simplifies to*

$$0 \to \mathrm{Cl}^0(K) \xrightarrow{\alpha} \mathrm{Cl}\, R^S \xrightarrow{\beta} C(d/I(K)) \to 0.$$

Deduce that in this case α *is an isomorphism iff* $I(K) = d$.

c) *Deduce that if* S *consists of a single degree* 1 *place, then* $\alpha : \mathrm{Cl}^0 K \xrightarrow{\sim} \mathrm{Cl}\, R^S$.

EXERCISE 2.7. *We maintain the setting of Theorem 2.4.*

a) *Suppose that* $\mathrm{Cl}^0 K$ *is finite. Show that every affine Dedekind domain* R^S *in* K *has finite ideal class group.*[1]

b) *Suppose* $\mathrm{Cl}^0 K$ *is infinite and finitely generated. Show that for any nonempty finite subset* $S \subset \Sigma(K/k)$, *there is a nonempty finite subset* $S' \supset S$ *such that* $\mathrm{Cl}\, R^{S'}$ *is finite.*

The following is an elementary, but striking, result.

[1]Later we will show that $\mathrm{Cl}^0 K$ is always finite when k is a finite field. Thus this exercise shows the finiteness of all the class groups $\mathrm{Cl}\, R^S$, which is the function field analogue of the finiteness of the class group of the ring of integers (or better, of the rings of S-integers; but the latter follows easily from the former) of a number field.

THEOREM 2.5 (Trotter [**Tr88**]). *The ring* $\mathbb{R}[\cos\theta, \sin\theta]$ *of real trigonometric polynomials is not a unique factorization domain, while the ring* $\mathbb{C}[\cos\theta, \sin\theta]$ *of complex trigonometric polynomials is a PID.*

Trotter in fact proceeds quite directly: he shows that in $\mathbb{R}[\cos\theta, \sin\theta]$ the elements $\sin\theta$, $1 + \cos\theta$ and $1 - \cos\theta$ are nonassociate irreducibles, and thus the identity

$$\sin^2\theta = 1 - \cos^2\theta$$

is an instance of non-unique factorization. Using Theorem 2.4 we can show more:

EXERCISE 2.8. a) *Show:* $\mathbb{R}[\cos\theta, \sin\theta] \cong \mathbb{R}[x, y]/(x^2 + y^2 - 1)$. *Show that the latter is an affine Dedekind domain. By Exercise 0.9, its fraction field* K *is isomorphic to* $\mathbb{R}(t)$.

b) *Use Rosen's Theorem to show that* $\operatorname{Cl}\mathbb{R}[\cos\theta, \sin\theta] \cong \mathbb{Z}/2\mathbb{Z}$.

c) *Show:* $\mathbb{C}[\cos\theta, \sin\theta] = \mathbb{C}[e^{i\theta}, e^{-i\theta}]$ *and deduce that* $\mathbb{C}[\cos\theta, \sin\theta]$ *is a PID.*

d) *Use Rosen's Theorem to show that* $\operatorname{Cl}\mathbb{C}[\cos\theta, \sin\theta]$ *is trivial.*

3. Riemann-Roch Spaces

The rational function field $k(t)$ has the following property: for any degree one place $P \in \Sigma(k(t)/k)$, there is a rational function $f \in k(t)$ whose divisor of poles is precisely P. Indeed, if $P = \infty$ we may take $f = t$; otherwise P corresponds to an element $t - a$ for $a \in k$, and we may take $f = \frac{1}{t-a}$.

This is in fact a characteristic property of rational function fields: indeed, if K/k is a function field and there is $f \in K$ whose divisor of poles has degree 1, then $[K : k(f)] = \deg(f)_- = 1$, so $K = k(f)$. So in general it cannot be that easy. (Admittedly, it does not follow from any of the results we have given so far that non-rational function fields exist. But they do, and this will be remedied!) It is interesting to ask a weaker version: in any function field K/k, if $P \in \Sigma(K/k)$, is there $f \in K$ with a pole only at P? If so, can we bound the order of the pole?

This motivates the notion of Riemann-Roch space and the most important theorem about them, the Riemann-Roch Theorem.

For $D \in \operatorname{Div} K$, the **Riemann-Roch space** associated to D is

$$\mathcal{L}(D) := \{f \in K^\times \mid (f) \geq -D\} \cup \{0\}.$$

For $f \in \mathcal{L}(D)^\bullet$, we have that $D + (f)$ is effective and linearly equivalent to D.

EXERCISE 2.9. *In* $k(t)$*, show that for* $n \geq 0$*, the Riemann-Roch space* $\mathcal{L}(n\infty)$ *is the set of* $f \in k[t]$ *such that* $\deg f \leq n$.

LEMMA 2.6. *For* $D \in \operatorname{Div} K$*, we have* $\mathcal{L}(D) \neq (0)$ *iff* D *is linearly equivalent to an effective divisor.*

PROOF. If $f \in \mathcal{L}(D)^\bullet$, then $(f) + D$ is an effective divisor linearly equivalent to D. Conversely, if D' is an effective divisor that is linearly equivalent to D, then there is $f \in K^\times$ such that $D' = D + (f)$, so $(f) = D' - D \geq -D$. □

As a first key example, $\mathcal{L}(0)$ consists of rational functions such that $(f) \geq 0$, i.e., rational functions without poles. Thus $\mathcal{L}(0) = \kappa(K)$, the constant subfield of K. For those with some familiarity with this subject, that is not exactly what we wanted

to hear: rather, we want $\mathcal{L}(0)$ to be a one-dimensional k-vector space. Thus it is time to do what we said we could do for the entire course so far:

From now on, we will assume that $\kappa(K) = k$. Again, we can always achieve this by replacing k by $\kappa(K)$.

EXERCISE 2.10. *Show that $\mathcal{L}(D)$ is a k-vector space.*

EXERCISE 2.11. *Show: if $D, D' \in \operatorname{Div} K$ are linearly equivalent divisors, then the Riemann-Roch spaces $\mathcal{L}(D)$ and $\mathcal{L}(D')$ are isomorphic as k-vector spaces.*

EXERCISE 2.12. *Suppose $D \in \operatorname{Div} K$ has degree 0. Show that the following are equivalent:*

(i) *We have $\dim \mathcal{L}(D) \geq 1$.*
(ii) *We have $\dim \mathcal{L}(D) = 1$.*
(iii) *The divisor D is principal.*

EXERCISE 2.13. *Let $\mathbb{P}\mathcal{L}(D)$ be the projective space associated to the k-vector space $\mathcal{L}(D)$, i.e., the set of one-dimensional linear subspaces of $\mathcal{L}(D)$. Show that $\mathbb{P}\mathcal{L}(D)$ may be viewed as the set of all effective divisors linearly equivalent to D.*

LEMMA 2.7. *Let $A \leq B \in \operatorname{Div} K$. Then:*

a) *We have $\mathcal{L}(A) \subset \mathcal{L}(B)$.*
b) *We have $\dim \mathcal{L}(B)/\mathcal{L}(A) \leq \deg B - \deg A$.*

PROOF. a) If $A \leq B$ and $(f) \geq -A$, then $-A \geq -B$, so $f \geq -B$.
b) An easy induction argument reduces us to the case $B = A+P$ for some place (not necessarily of degree 1) $P \in \Sigma(K/k)$. Choose $t \in K$ such that $v_P(t) = v_P(B) = v_P(A) + 1$. For $f \in \mathcal{L}(B)$, we have $v_P(f) \geq -v_P(B) = -v_P(t)$, so $ft \in R_v$. This gives us a k-linear map

$$\Psi : \mathcal{L}(B) \to k_P, \ f \mapsto ft \mod \mathfrak{m}_v.$$

The kernel of this map consists of $f \in \mathcal{L}(B)$ such that $v_P(f) \geq -v_P(B) + 1 = -v_P(A)$, hence the kernel is $\mathcal{L}(A)$. This shows that

$$\dim \mathcal{L}(B)/\mathcal{L}(A) \leq [k_P : k] = \deg P. \qquad \square$$

COROLLARY 2.8. *For $A \in \operatorname{Div} K$. If $\deg A \geq 0$, then we have $\dim \mathcal{L}(A) \leq \deg A + 1$. In particular, $\mathcal{L}(A)$ is finite-dimensional.*

PROOF. Step 1: If A is not linearly equivalent to an efective divisor, then Lemma 2.6 gives $\mathcal{L}(A) = 0$, so $\dim \mathcal{L}(A) = 0 =< 1 \leq \deg A + 1$. So we may assume that A is linearly equivalent to an effective divisor D. By Exercise 2.11 and Corollary 2.3, neither $\dim \mathcal{L}(A)$ nor $\deg A$ changes if we replace A by a linearly equivalent divisor, so we may assume that $A = D$ is effective.

Writing $D = P_1 + \ldots + P_r$ for not necessarily distinct P_i and successively applying Lemma 2.7b), we get

$$\begin{aligned} \dim \mathcal{L}(D) - \dim \mathcal{L}(0) &= \sum_{i=0}^{r-1} \dim \mathcal{L}(P_1 + \ldots + P_{i+1}) - \dim \mathcal{L}(P_1 + \ldots P_i) \\ &\leq \sum_{i=1}^{r} \deg P_i = \deg D. \end{aligned}$$

Since $\dim \mathcal{L}(0) = 1$, we get $\dim \mathcal{L}(D) \leq \deg D + 1$. $\square$

EXERCISE 2.14. *Show: if* $A \in \operatorname{Div} k(t)$, *then* $\dim \mathcal{L}(A) = \begin{cases} \deg A + 1 & \deg A \geq 0 \\ 0 & \deg A < 0 \end{cases}$.

For $D \in \operatorname{Div} K$, we put $\ell(D) := \dim \mathcal{L}(D)$.

We are interested in computing or at least bounding $\ell(D)$. Our motivating problem can be asked in these terms: for a fixed place $P \in \Sigma(K/k)$, show that there is a positive integer n such that $\ell(nP) \geq 0$. What can be said about the least such n?

Corollary 2.8 can be rewritten as: for all $A \in \operatorname{Div} K$ with $\deg A \geq 0$, we have

$$\deg A - \ell(A) \geq -1.$$

In order to deduce the existence of rational functions with prescribed poles, we would like to have a corresponding upper bound. Here is one such result, the first of several preliminary forms of the Riemann-Roch Theorem.

PROPOSITION 2.9. *For a function field* K/k, *there is an integer* γ *such that for all* $A \in \operatorname{Div} K$, *we have*

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

PROOF. We begin by observing that a restatement of Lemma 2.7b) is: for $A_1, A_2 \in \operatorname{Div} K$,

$$A_1 \leq A_2 \implies \deg A_1 - \ell(A_1) \leq \deg A_2 - \ell(A_2).$$

Step 1: Choose $x \in K \setminus k$, and put $B := (x)_-$. We claim that there is an effective divisor C on K such that

$$\forall n \in \mathbb{N},\ \ell(nB + C) \geq (n+1) \deg B.$$

To see this, choose a $k(x)$-basis $u_1, \ldots, u_d$ for K and an effective divisor C such that $(u_i) \geq -C$ for $1 \leq i \leq d$. Since $u_1, \ldots, u_d$ are $K(x)$-linearly independent, for $n \in \mathbb{N}$, the functions $\{x^i u_j\}_{0 \leq i \leq n, 1 \leq j \leq d}$ are k-linearly independent elements of $\mathcal{L}(nB + C)$, which gives $\ell(nB + C) \geq (n+1)d = (n+1) \deg B$.
Step 2: On the other hand, Lemma 2.7b) gives $\ell(nB + C) \leq \ell(nB) + \deg C$. Combining these inequalities gives

$$\ell(nB) \geq \ell(nB+C) - \deg C \geq (n+1) \deg B - \deg C = \deg(nB) + ([K : k(x)] - \deg C),$$

so taking $\gamma := [K : k(x)] - \deg C$, we get

$$\forall n \in \mathbb{N},\ \deg(nB) - \ell(nB) \leq \gamma. \tag{5}$$

Step 3: We claim that for $A \in \operatorname{Div} K$ there are $A_1, D \in \operatorname{Div} K$ and $n \in \mathbb{N}$ such that $A \leq A_1$, $A_1 \sim D$ and $D \leq nB$. To see this, choose any $A_1 \geq \max(A, 0)$. Then using Lemma 2.7b) and (5), for $n >> 0$ we get

$$\ell(nB - A_1) \geq \ell(nB) - \deg A_1 \geq \deg(nB) - \gamma - \deg A_1 > 0,$$

so there is $z \in \mathcal{L}(nB - A_1)^\bullet$. Putting $D := A_1 - (z)$, we have that D is linearly equivalent to A_1 and $D \leq A_1 + (nB - A_1) = nB$, proving the claim.
Step 4: Now for any $A \in \operatorname{Div} K$, as in the claim we choose $n \in \mathbb{N}$ and A_1, D such that $A \leq A_1$, $A_1 \sim D$ and $D \leq nB$. Then we have

$$\deg A - \ell(A) \leq \deg A_1 - \ell(A_1) = \deg D - \ell(D) \leq \deg(nB) - \ell(nB) \leq \gamma. \quad \square$$

Theorem 2.9 allows us to define a crucially important invariant of the function field K, its genus. This particular definition is quite awkward (but correct): we will soon gain a better understanding of it.

We define the **genus** of K/k as

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

Notice that Proposition 2.9 precisely ensures that this maximum exists.

As a simple example, for $K = k(t)$, we saw that $\ell(A) = \deg A + 1$ for all divisors A of non-negative degree. Thus the genus of $k(t)$ is 0.

THEOREM 2.10 (Riemann's Inequality). *Let K/k be a function field of genus g.*

a) *For all $A \in \operatorname{Div} K$, we have*

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

b) *There is $c = c(K) \in \mathbb{Z}$ such that for all divisors A with $\deg A \geq c$ we have*

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

PROOF. a) By definition of the genus, for all $A \in \operatorname{Div} K$ we have $\deg A - \ell(A) + 1 \leq g$, so $\ell(A) \geq \deg A - g + 1$.
b) Also by definition of the genus, there is $A_0 \in \operatorname{Div} K$ with $g = \deg A_0 - \ell(A_0) + 1$. Put $c := \deg A_0 + g$. If $\deg A \geq c$, then by part a) we have

$$\ell(A - A_0) \geq \deg(A - A_0) + 1 - g \geq c - \deg A_0 + 1 - g = 1,$$

so there is $z \in \mathcal{L}(A - A_0)^\bullet$. Put $A' := A + (z)$. Then $A' \geq A_0$. Lemma 2.7b) gives

$$\deg A - \ell(A) = \deg A' - \ell(A') \geq \deg A_0 - \ell(A_0) = g - 1. \qquad \square$$

4. The Riemann-Roch Theorem

In view of Riemann's Theorem, it is natural to consider for $D \in \operatorname{Div} K$ the quantity

$$\iota(D) := \ell(A) - \deg A + g - 1.$$

This is called the **index of speciality** of D (though I find that a bit hokey and will just call it $\iota(D)$). Then Riemann's Inequality says that $\iota(D) \geq 0$ for all D and is equal to 0 when $\deg D$ is sufficiently large. However it does not tell us *how* large is sufficiently large nor give us any further information about $\iota(D)$. The following improved result does.

THEOREM 2.11 (Riemann-Roch Theorem). *For a function field K/k of genus g, there is a divisor $\mathcal{K} \in \operatorname{Div} K$ such that for all $D \in \operatorname{Div} K$ we have*

$$\iota(D) = \ell(\mathcal{K} - D).$$

Equivalently, for all $D \in \operatorname{Div} K$ we have

$$\ell(D) - \ell(\mathcal{K} - D) = \deg D - g + 1. \tag{6}$$

EXERCISE 2.15. *Deduce the following from the Riemann-Roch Theorem.*

a) *We have $\ell(\mathcal{K}) = g$ and $\deg \mathcal{K} = 2g - 2$.*
b) *In particular, we have $g \geq 0$.*
c) *If $g \geq 1$, then the least $d \in \mathbb{Z}$ such that $\iota(D) = 0$ if $\deg D > d$ is $d = 2g-2$.*

EXERCISE 2.16. a) *Show that the Riemann-Roch Theorem characterizes the genus: that is, there is at most one $g \in \mathbb{Z}$ for which the result can hold.*

b) *Show that if $\mathcal{K}$ is a divisor for which the Riemann-Roch Theorem holds, then the Riemann-Roch Theorem also holds for any linearly equivalent divisor. Conversely, show that if the Riemann-Roch Theorem holds with divisors $\mathcal{K}_1$ and $\mathcal{K}_2$, then $\mathcal{K}_1 \sim \mathcal{K}_2$.*

In view of Exercise 2.16b), the Riemann-Roch Theorem singles out an element of the divisor class group $\operatorname{Div} K$, the class of any divisor $\mathcal{K}$ for which the result holds. This canonical divisor class is called – wait for it – the **canonical class**, and any divisor in this class is called a **canonical divisor**.

PROPOSITION 2.12. *A divisor $D \in \operatorname{Div}(K)$ is canonical iff $\deg(D) = 2g-2$ and $\ell(D) = g$.*

PROOF. It follows from Exercises 2.15 and 2.16 that any canonical divisor D has $\deg(D) = 2g-2$ and $\ell(D) = g$. Fix any canonical divisor $\mathcal{K}$ and let D be a divisor with $\deg(D) = 2g-2$ and $\ell(D) = g$. Then by Riemann-Roch we have

$$\ell(\mathcal{K} - D) = \ell(D) - \deg(D) + g - 1 = 1.$$

Since $\deg(\mathcal{K} - D) = 0$, by Exercise 2.12 we have $D \sim \mathcal{K}$, hence D is canonical. □

EXERCISE 2.17. *Let K/k be a function field of genus 0.*

a) *Show that $\mathrm{Cl}^0 K = (0)$: that is, every degree 0 divisor is principal.*

b) *Show: a divisor $\mathcal{K} \in \operatorname{Div} K$ is canonical iff $\deg \mathcal{K} = -2$.*

c) *Show: The index $I(K)$ of K (recall this the least positive degree of a divisor on K) is either 1 or 2.*

d) *Show that the following are equivalent:*

(i) *We have $K \cong k(t)$.*

(ii) *We have $\Sigma_1(K/k) \neq \varnothing$.*

(iii) *We have $I(K) = 1$.*

EXERCISE 2.18. *Let P be a degree 1 point on K. Then we have $\ell(P) \in \{1, 2\}$. Show that $\ell(P) = 2 \iff K \cong k(t)$.*

EXERCISE 2.19. *Let K be a function field of genus one. Show that a divisor $\mathcal{K} \in \operatorname{Div} K$ is canonical iff it is principal.*

5. Weil's Proof of Riemann-Roch

For a one variable function field K/k with $\kappa(K) = k$, we define the ring of **repartitions** (or the **small adele ring**) $\mathcal{A}_K$ as the restricted direct product of the family of fields $\{K\}_{v \in \Sigma(K/k)}$ with respect to the family of subrings $\{R_v\}_{v \in \Sigma(K/k)}$: that is $\mathcal{A}_K$ is the set of tuples x_v in the direct product $\prod_{v \in \Sigma(K/k)} K$ such that $x_v \in R_v$ for all but finitely many v.

REMARK 2. *The adele ring $\mathbb{A}_K$ would be formed by replacing the factor K in the vth place with its completion K_v and R_v with the valuation ring $\hat{R}_v$ in the completion. When k is finite, this adele ring features in* [**NTII**, Ch. 3]. *The rings R_v and $\hat{R}_v$ have the same residue field k_v, a finite field extension of k. Thus K_v is locally compact iff $\hat{R}_v$ is compact iff k is finite. As seen in* [**NTII**, Ch. 3], *much of the merit of the "big" adele ring is that it carries a locally compact topology, a*

fact which turn on the local compactness of each of the completions. Because of this there is less merit in considering the "big" adele ring in the case of a general ground field – in fact we could use it, and everything we will do here will still work, but there is no reason to add this layer of complication.

For our purposes here the ring structure of $\mathcal{A}_K$ will not be used. We will only use that it is a K-vector space, and hence also a k-vector space.

We embed $K \hookrightarrow \mathcal{A}_K$ diagonally: this uses the fact that any $f \in K^\times$ has only finitely many poles. Furthermore extend v to a map on $\mathcal{A}_K$ just by pullback:

$$\mathcal{A}_K \stackrel{\pi_v}{\to} K \stackrel{v}{\to} \mathbb{Z} \cup \{\infty\},$$

where π_v denotes projection onto the vth factor.

We now introduce an adelic version of $\mathcal{L}(D)$: for $D \in \operatorname{Div} K$, we put

$$\mathcal{A}_K(D) \coloneqq \{\alpha \in \mathcal{A}_K \mid v_P(\alpha) \geq -v_P(D)\ \forall P \in \Sigma(K/k)\}.$$

EXERCISE 2.20. a) *Show: for all $D \in \operatorname{Div} K$, we have that $\mathcal{A}_K(D)$ is a k-subspace of $\mathcal{A}_K$.*
b) *Show: if $D_1 \leq D_2$ then $\mathcal{A}_K(D_1) \subset \mathcal{A}_K(D_2)$.*

LEMMA 2.13. *Let $A_1 \leq A_2$ be divisors on K. Then $\mathcal{A}_K(A_1) \subset \mathcal{A}_K(A_2)$ and $\dim_k \mathcal{A}_K(A_2)/\mathcal{A}_K(A_1) = \deg A_2 - \deg A_1$.*

PROOF. This result is the adelic analogue of Lemma 2.7b) and is proved in almost the same way: induction reduces us to the case in which $A_2 = A_1 + P$ for $P \in \Sigma(K/k)$. We choose $t \in K^\times$ such that $v_p(t) = v_p(A_2)$. Then

$$\varphi : \mathcal{A}_K(A_2) \to k_P,\ \alpha \mapsto (t\alpha_P) \mod \mathfrak{m}_P$$

is k-linear with kernel $\mathcal{A}_K(A_1)$. The difference is that because $\mathcal{A}(A_2)$ is a larger and simpler object than $\mathcal{L}(A_2)$, it is true – and easy to see – that φ is surjective. □

THEOREM 2.14. *For all D, we have*

$$\dim_k \mathcal{A}_K/(\mathcal{A}_K(D) + K) = \iota(D).$$

In particular, $\mathcal{A}_K(D) + K$ has finite codimension in $\mathcal{A}_K(D)$.

PROOF. Step 1: Let $A_1 \leq A_2$ be divisors on K. We have an exact sequence of k-vector spaces

$$0 \longrightarrow \mathcal{L}(A_2)/\mathcal{L}(A_1) \stackrel{\sigma_1}{\to} \mathcal{A}_K(A_2)/\mathcal{A}_K(A_1) \stackrel{\sigma_2}{\to} (\mathcal{A}_K(A_2) + K)/(\mathcal{A}_K(A_1) + K) \to 0$$

where the maps σ_1, σ_2 are the evident ones. As for the exactness, the only nontrivial assertion is that the kernel of σ_2 is contained in the image of σ_1. To see this, let $\alpha \in \mathcal{A}_K(A_2)$ be such that $\sigma_2(\alpha + \mathcal{A}_K(A_1)) = 0$. In other words, we have $\alpha \in \mathcal{A}_K(A_1) + K$, so there is $x \in K$ such that $\alpha - x \in \mathcal{A}_K(A_1)$. Since $\mathcal{A}_K(A_1) \subset \mathcal{A}_K(A_2)$ we get $x \in \mathcal{A}_F(A_2) \cap K = \mathcal{L}(A_2)$. So $\alpha + \mathcal{A}_K(A_1) = x + \mathcal{A}_K(A_1) = \sigma_1(x + \mathcal{L}(A_1))$.
Step 2: Using Step 1 and Lemma 2.13 we get

$$\begin{aligned}
&\dim_k(\mathcal{A}_K(A_2) + K)/(\mathcal{A}_K(A_1) + K) \\
&= \dim_k \mathcal{A}_K(A_2)/\mathcal{A}_K(A_1) - \dim_k \mathcal{L}(A_2)/\mathcal{L}(A_1) \\
&= (\deg A_2 - \ell(A_2)) - (\deg A_1 - \ell(A_1)) = \iota(A_1) - \iota(A_2).
\end{aligned}$$

Step 3: In view of Step 2, it is enough to show that for every $A_1 \in \operatorname{Div} K$, there is $A_2 \geq A_1$ such that $\iota(A_2) = 0$ and $\mathcal{A}_K(A_2) + K = \mathcal{A}_K$. By Riemann's Inequality there is always $A_2 \geq A_1$ such that $\iota(A_2) = 0$ since the latter holds whenever A_2 has sufficiently large degree. So the proof will be completed by showing that when $B \in \operatorname{Div} K$ satsifes $\iota(B) = 0$, we have $\mathcal{A}_K = \mathcal{A}_K(B) + K$.

To see this, let $B_1 \geq B$. Then Lemma 2.7b) gives

$$\ell(B_1) \leq \deg B_1 + \ell(B) - \deg(B) = \deg(B_1) - g + 1.$$

On the other hand, Riemann's Inequality gives $\ell(B_1) \geq \deg(B_1) - g + 1$, so

$$\ell(B_1) = \deg B_1 + 1 - g.$$

Let $\alpha \in \mathcal{A}_K$. We may choose $B_1 \geq B$ such that $\alpha \in \mathcal{A}_K(B_1)$. By Step 2, we have

$$\dim_k(\mathcal{A}_K(B_1)+K)/(\mathcal{A}_K(B)+K) = (\deg B_1 - \ell(B_1)) - (\deg B - \ell(B)) = (g-1)-(g-1) = 0$$

and thus $\mathcal{A}_K(B_1) + K = \mathcal{A}_K(B) + K$, and it follows that $\alpha \in \mathcal{A}_K(B) + K$. So $\mathcal{A}_K(B) + K = \mathcal{A}_K$, completing the proof. □

Corollary 2.15. *We have* $\dim_k \mathcal{A}_K/(\mathcal{A}_K(0) + K) = g$.

Proof. Using Theorem 2.15 we have

$$\dim_k \mathcal{A}_K/(\mathcal{A}_K(0) + K) = \iota(0) \coloneqq \ell(0) - \deg 0 + g - 1 = g.$$ □

Exercise 2.21. *It follows from Corollary 2.15 that if $K = k(t)$ is a rational function field, then we have $\mathcal{A}_K(0) + K = \mathcal{A}_K$. Show this directly.*

Next we define Weil differentials, which are certain k-linear functionals on $\mathcal{A}_K$. For $D \in \operatorname{Div} K$, let $\Omega_K(D)$ be thet set of all k-linear maps $\omega : \mathcal{A}_K \to k$ whose kernel contains $\mathcal{A}_K(D) + K$. Thus elements of $\Omega_K(D)$ factor through the quotient space $\mathcal{A}_K/(\mathcal{A}_K(D) + K)$, which by Theorem 2.15 is finite-dimensional, so $\Omega_K(D)$ is canonically isomorphic to the dual space of $\mathcal{A}_K/(\mathcal{A}_K(D) + K)$ and therefore is finite-dimensional of dimension $\iota(D)$. If $D_1 \leq D_2$ then $\mathcal{A}_K(D_1) \subset \mathcal{A}_K(D_2)$, so if a linear form vanishes on $\mathcal{A}_K(D_2)$ it also vanishes on $\mathcal{A}_K(D_1)$, and thus we get $\Omega_K(D_2) \subset \Omega_K(D_1)$. By Theorem 2.15 and Riemann's Inequality (Theorem 2.10) it follows that $\Omega_K(D) = 0$ if $\deg D \mathfrak{g} 0$.

We put

$$\Omega_K \coloneqq \bigcup_{D \in \operatorname{Div} K} \Omega_K(D) \subset \mathcal{A}_K^\vee.$$

Then Ω_K is a directed union of finite-dimensional k-vector spaces, hence a k-vector space. We call elements of Ω_K **Weil differentials**.

Exercise 2.22. *Let K/k be a function field.*

a) *Let $D \in \operatorname{Div} K$ be such that $\deg D < 0$. Show: $\dim_k \Omega_K(D) \geq |\deg D| - 1$. Deduce that $\Omega_K(D)$ is nontrivial if $\deg D \leq -2$.*
b) *Show: $\dim_k \Omega_K \geq \aleph_0$.*
c) *You can think about computing $\dim_k \Omega_K$ as an infinite cardinal, but don't work too hard: the next result will give the answer much more easily.*

To say where we are going: to every nonzero Weil differential we will attach a divisor. All Weil divisors of Weil differentials will be linearly equivalent, and any divisor linearly equivalent to a a divisor of a Weil differential will be the divisor of a Weil differential, so we specify one full linear equivalence class of divisors this way.

This will turn out to be the canonical class.

We claim that whereas each $\Omega_K(D)$ is a k-vector space, their union Ω_K is a K-vector space. This is defined in the obvious way:

$$\forall x \in K, \forall \omega \in \Omega_K,\ (x\omega)(\alpha) \coloneqq \omega(x\alpha).$$

Certainly $x\omega$ is still a k-linear functional on $\mathcal{A}_K$. Moreover, if ω vanishes on $A_K(D) + K$ then $x\omega$ vanishes on $A_K(D + (x)) + K$, so indeed $x\omega \in \Omega_K$.

PROPOSITION 2.16. *We have* $\dim_K \Omega_K = 1$.

PROOF. Exercise 2.22 tells us that Ω_K is nontrivial. So let $\omega_1, \omega_2 \in \Omega_K^\bullet$. We must show that there is $z \in K$ such that $\omega_2 = z\omega_1$. Choose divisors A_1, A_2 such that $\omega_i \in \mathcal{A}_K(A_i)$ for $i = 1, 2$. For a divisor B to be specified later, we consider the injective, k-linear maps

$$\varphi_i : \mathcal{L}(A_i + B) \to \Omega_K(-B), x \mapsto x\omega_i.$$

We claim that there is B such that $\varphi_1(\mathcal{L}(A_1 + B)) \cap \varphi_2(\mathcal{L}(A_2 + B)) \neq (0)$.
Step 1: Assume that the claim holds, and for $i = 1, 2$ choose $x_i \in \mathcal{L}(A_i + B)$ suhc that $x_1\omega = x_2\omega_2 \neq 0$. Then $\omega_2 = (x_1 x_2^{-1})\omega_1$, completing the proof.
Step 2: Now we establish the claim. First recall the following fact from linear algebra: if U_1, U_2 are subspaces of a finite-dimensional vector space V, then $\operatorname{codim}(U_1 \cap U_2) \leq \operatorname{codim} U_1 + \operatorname{codim} U_2$. Rearranging this, we get

$$\dim(U_1 \cap U_2) \geq \dim U_1 + \dim U_2 - \dim V.$$

Now, by Riemann's Inequality, if we take $B \in \operatorname{Div} K$ to have sufficiently large (in particular, positive!) degree, then for $i = 1, 2$ we have

$$\ell(A_i + B) = \deg(A_i + B) - g + 1.$$

Put $U_i \coloneqq \varphi_i(\mathcal{L}(A_i + B)) \subset \Omega_K(-B)$. Then

$$\dim_k \Omega_K(-B) = \iota(-B) = \ell(-B) - \deg(-B) + g - 1 = \deg B + g - 1,$$

so

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

The above parenthesized quantity is independent of B, so the entire quantity is positive so long as B has sufficiently large degree, and thus $\dim(U_1 \cap U_2) \geq 1$, establishing the claim and completing the proof. □

LEMMA 2.17. *Let $\omega \in \Omega_K^\bullet$. The set of divisors A such that $\omega \in \Omega_K(A)$ has a top element: that is, a divisor W such that $\omega \in \Omega_K(W)$ and for all $A \in \operatorname{Div} K$, if $\omega \in \Omega_K(A)$ then $A \leq W$.*

PROOF. As we've observed before, if $\deg A \gneq 0$ then $\iota(A) = \dim_k \Omega_K(A) = 0$, so among all divisors A such that $\omega \in \Omega_K(A)$ we may choose such a divisor W of maximal degree. We claim that this our desired divisor (equivalently, that there is a unique such divisor of maximal degree). We argue by contradiction: if not, there is A_0 such that $\omega \in \Omega_K(A_0)$ and $A_0 \not\leq W$: this means there is $Q \in \Sigma(K/k)$ such

that $v_Q(A_0) > v_Q(W)$.

Let $\alpha = (\alpha_P) \in \mathcal{A}_K(W+Q)$. We write $\alpha = \alpha' + \alpha''$, where

$$\alpha'_P = \begin{cases} \alpha_P & P \neq Q \\ 0 & P = Q \end{cases}, \ \alpha''_P = \begin{cases} 0 & P \neq Q \\ \alpha_Q & P = Q \end{cases}.$$

Then $\alpha' \in \mathcal{A}_K(W)$, $\alpha'' \in \mathcal{A}_K(A_0)$, so

$$\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0,$$

so $\omega \in \Omega_K(W+Q)$, contradicting the maximality of $\deg W$. □

Thus Lemma 2.17 assigns to each nonzero Weil differential ω a divisor W, the unique maximal divisor A such that ω vanishes on $\mathcal{A}_K(A) + K$. We denote this differential by (ω). Moreover, for $P \in \Sigma(K/k)$, we put $v_P(\omega) \coloneqq v_P(((\omega))$.

Exercise 2.23. *Show that*

$$\Omega_K(A) = \{\omega \in \Omega_K^\bullet \mid (\omega) \geq A\}.$$

We also introduce some terminology carried over from divisors of rational functions: for $\omega \in \Omega_K^\bullet$ and $P \in \Sigma(K/k)$ we say that ω has a **zero** at P if $v_P(\omega) > 0$, is **regular** at P if $v_P(\omega) \geq 0$ and has a **pole** at P if $v_P(\omega) < 0$.

We say that ω is **regular** or **holomorphic** if ω is regular at *all* places $P \in \Sigma(K/k)$. The latter makes sense also for functions but is much more interesting, since the only functions that are regular everywhere are the constant functions, but this need not be the case for differentials. Thus by Exercise 2.23 we get that $\Omega_K(0)$ is the space of regular differentials, and its dimension is $\iota(0) = \ell(0) - \deg 0 + g - 1 = g$.

Proposition 2.18. *Let K/k be a function field.*

a) *For all $x \in K^\times$ and $\omega \in \Omega_K^\bullet$, we have $(x\omega) = (x) + (\omega)$.*
b) *The set of divisors of nonzero Weil differentials comprise one full linear equivalence class of divisors on K.*

Proof. a) If $\omega \in \Omega_K(A)$, then $x\omega \in \Omega_K(A + (x))$, so we have

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

The same argument gives

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

so

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

b) This follows from part a) and the fact that $\dim_K \Omega_K = 1$. □

As advertised we call a divisor **canonical** if it is the divisor of a differential. And now comes the payoff.

Theorem 2.19 (Duality Theorem). *Let $\mathcal{K} = (\omega)$ be a canonical divisor.*

a) *For all $A \in \operatorname{Div} K$, the map*

$$\mu : \mathcal{L}(\mathcal{K} - A) \to \Omega_K(A), \ x \mapsto x\omega$$

is a k-vector space isomorphism.
b) *We have $\ell(\mathcal{K} - A) = \iota(A)$.*

PROOF. a) For $x \in \mathcal{L}(\mathcal{K} - A)$, we have

$$(x\omega) = (x) + (\omega) \geq -(\mathcal{K} - A) + \mathcal{K} = A,$$

so $x\omega \in \Omega_K(A)$. It is immediate that μ is k-linear and injective. As for the surjectivity, let $\nu \in \Omega_K(A)^\bullet$. Because $\dim_K \Omega_K = 1$, we may write $\nu = x\omega$ for a (unique) $x \in K$. Since

$$(x) + \mathcal{K} = (x) + (\omega) = (x\omega) = (\nu) \geq A,$$

we get $(x) \geq A - \mathcal{K}$, so $x \in \mathcal{L}(\mathcal{K} - A)$.
b) By part a) and Theorem 2.15, we get

$$\ell(\mathcal{K} - A) = \dim_k \mathcal{L}(\mathcal{K} - A) = \dim_k \Omega_K(A) = \dim_k \mathcal{A}_K/(\mathcal{A}_K(A) + K) = \iota(A). \quad \square$$

Theorem 2.19b) is precisely the Riemann-Roch Theorem.

6. Local components of Weil differentials

Let K/k be a function field. Previously we considered the diagonal embedding of K into $\mathcal{A}_K$. However, we may also embed $K \hookrightarrow \mathcal{A}_K$ by fixing a place $P \in \Sigma(K/k)$ and defining

$$\iota_P(x) \coloneqq \begin{cases} x & \text{in the } P \text{ component} \\ 0 & \text{in every other component} \end{cases}.$$

Now for $\omega \in \Omega_K$ and $P \in \Sigma(K/k)$, we define k-linear functional

$$\omega_P : K \to k,\ \omega_P(x) \coloneqq \omega(\iota_P(x)).$$

We will see shortly that for each place $P \in \Sigma(K/k)$ the k-linear map $\omega \mapsto \omega_P$ is injective, and thus we can represent Weil differentials as linear functionals on K. (Since ω_K is a one-dimensional K-vector space, this is not really surprising.)

PROPOSITION 2.20. *Let $\omega \in \Omega_K$ and let $\alpha = (\alpha_P) \in \mathcal{A}_K$.*

a) *We have $\omega_P(\alpha_P) = 0$ for all but finitely many $P \in \Sigma(K/k)$.*
b) *We have*

$$\omega(\alpha) = \sum_{P \in \Sigma(K/k)} \omega_P(\alpha_P).$$

c) *If $\alpha \in K$ (diagonally embedded in $\mathcal{A}_K$!), then we have*

$$\sum_{P \in \Sigma(K/k)} \omega_P(\alpha) = 0. \tag{7}$$

PROOF. a) Everything holds trivially if $\omega = 0$, so we may assume that $\omega \in \Omega_K^\bullet$. Let $W \coloneqq (\omega)$. There is a finite subset $S \subset \Sigma(K/k)$ such that for all $P \in \Sigma(K/k) \setminus S$ we have $v_P(W) = 0$ and $v_P(\alpha_P) \geq 0$. We define $\beta = (\beta_P) \in \mathcal{A}_K$ by

$$\beta_P \coloneqq \begin{cases} 0 & P \in S \\ \alpha_P & P \notin S \end{cases}.$$

Then $\beta \in \mathcal{A}(W)$ and

$$\alpha = \beta + \sum_{P \in S} \iota_P(\alpha_P),$$

so $\omega(\beta) = 0$ and thus

$$\omega(\alpha) = \sum_{P \in S} \omega_P(\alpha_P).$$

On the other hand, if $P \notin S$ then $\iota_P(\alpha_P) \in \mathcal{A}_K(W)$, so

$$\omega_P(\alpha_P) = \omega(\iota_P(\alpha_P)) = 0,$$

which shows part a) and also that

$$\omega(\alpha) = \sum_{P \in S} \omega_P(\alpha_P) = \sum_{P \in \Sigma(K/k)} \omega_P(\alpha_P),$$

establishing part b). Part c) follows since every Weil differential vanishes on the diagonally embedded copy of K. □

Later we will see that (7) is a sort of embryonic form of the Residue Theorem.

PROPOSITION 2.21. *Let $\omega \in \Omega_K^\bullet$, and let $P \in \Sigma(K/k)$.*

a) *We have*

$$v_P(\omega) = \max\{n \in \mathbb{Z} \mid \omega_P(x) = 0 \text{ for all } x \in K \text{ such that } v_P(x) \geq -n\}. \tag{8}$$

b) *It follows that $\omega_P \neq 0$.*

c) *If $\omega, \eta \in \Omega_K$ are such that $\omega_P = \eta_P$ for some $P \in \Sigma(K/k)$, then $\omega = \eta$.*

PROOF. a) Put $W := (\omega)$, and let $m := v_P(\omega) = v_P(W)$. If $x \in K$ has $v_P(x) \geq -m$, then $\iota_P(x) \in \mathcal{A}_K(W)$, so $\omega_P(x) = \omega(\iota_P(x)) = 0$. This shows that the maximum occurring in the right hand side of (8) is at least $v_P(\omega)$. Seeking a contradiction, suppose now that $\omega_P(x) = 0$ for all $x \in K$ with $v_P(x) \geq -m-1$, and let $\alpha = (\alpha_Q) \in \mathcal{A}_K(W+P)$. Then

$$\alpha = (\alpha - \iota_P(\alpha_P)) + \iota_P(\alpha_P)$$

with $\alpha - \iota_P(\alpha_P) \in \mathcal{A}_K(W)$ and $v_P(\alpha_P) \geq -m-1$, so

$$\omega(\alpha) = \omega(\alpha - \iota_P(\alpha_P)) + \omega_P(\alpha_P) = 0.$$

This shows that ω vanishes on $\mathcal{A}_K(W+P)$, in contradiction to the definition of W.
b) This follows from part a): if $\omega_P = 0$, the maximum of part a) would not exist.
c) By part b), the kernel of the k-linear map $\omega \mapsto \omega_P$ is zero, so if $0 = \omega_P - \eta_P = (\omega - \eta)_P$, then $\omega - \eta = 0$. □

EXERCISE 2.24. *Let $K = k(x)$ be a rational function field.*

a) *Show: there is a unique $\omega \in \Omega_K$ such that $(\omega) = -2P_\infty$ and $\omega_{P_\infty}(\frac{1}{x}) = -1$.*

b) *For $a \in k$, let P_a be the place corresponding to the irreducible polynomial $x - a$. Show that for the Weil differential ω of part a), we have*

$$\omega_{P_\infty}((x-a)^n) = \begin{cases} 0 & n \neq -1 \\ -1 & n = -1 \end{cases}$$

and

$$\omega_{P_a}((x-a)^n) = \begin{cases} 0 & n \neq -1 \\ 1 & n = -1 \end{cases}.$$

Suggestion: for $n \neq -1$, use Proposition 2.21. For $n = -1$, also use

$$\frac{1}{x-a} = \frac{a}{x(x-a)} + \frac{1}{x}.$$

7. Applications of Riemann-Roch

7.1. Conic Function Fields. Let K/k be a function field of genus 0 (and constant field k, as usual). Let $\mathcal{K} \in \operatorname{Div} K$ be a canonical divisor. Then $\deg \mathcal{K} = -2$, so $\deg(-\mathcal{K}) = 2$, and Riemann-Roch gives $\ell(-\mathcal{K}) = 3$. It follows that there is an effective degree 2 divisor D on K and a basis $1, x, y$ for $\ell(D)$. We claim that $K = k(x, y)$.

Case 1: Suppose that either x or y has degree 1. Then $K = k(x)$ or $K = k(y)$, so the result is clear.

Case 2: Now suppose that $\deg x = \deg y = 2$, so $[K : k(x)] = 2$. Since a degree 2 field extension admits no proper subextensions, it suffices to show that $y \notin k(x)$. Seeking a contradiction, suppose that $y \in k(x)$. Since also $[K : k(y)] = 2$, this means that $k(x) = k(y)$, and thus that y is a degree 1 rational function in x, so $y = \frac{ax+b}{cx+d}$ for $a, b, c, d \in k$. Since x and y live in $\mathcal{L}(D)$ and have degree 2, so we must have $(x)_- = (y)_- = D$, and since $x, y \in k(x)$ this means that y is regular away from the infinite place in $k(x)$, so $c = 0$ and $y = ax + b$, contradicting the k-linear independence of 1, x and y.

Now consider the six functions 1, x, y, x^2, xy, y^2 in K. They all live in $\mathcal{L}(2D)$, which by Riemann-Roch has dimension 5, so there must be a linear relation among them: i.e., there are $a, b, c, d, e, f \in k$, not all zero, such that

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

We cannot have $a = b = c = 0$ because once again that would give a linear dependence relation among 1, x and y. Similarly the polynomial

$$f(X, Y) \coloneqq aX^2 + bXY + cY^2 + dX + eY + f \in k[X, Y]$$

must be irreducible, for otherwise it would have a linear factor, yielding a linear relation among 1, x and y. Thus we have shown the following result.

THEOREM 2.22. *Let K/k be a genus zero function field. Then there are $a, b, c, d, e, f \in k$ with a, b, c not all zero such that $K = K_f$, where $f(X, Y) = aX^2 + bXY + cY^2 + dX + eY + f$.*

EXERCISE 2.25. *Suppose that the characteristic of k is different from 2. Show that if K/k is a genus zero function field, then K/k is regular and there are $a, b, c \in k^\times$ and $c \in k$ such that $K = K_f$, where $f(X, Y) = aX^2 + bY^2 + c$.*

One could – and should – study conic function fields more deeply. It turns out that to every conic function field over k one can attach a quaternion algebra over k, which gives a bijection on isomorphism classes. We will return to this later.

7.2. Elliptic Function Fields. We say a function field K/k is **elliptic** if it has genus 1 and a degree one place O. Using this place we define a map

$$\Phi_O : \Sigma_1(K/k) \to \operatorname{Pic}^0 K, \ P \mapsto [P - O].$$

PROPOSITION 2.23. *The map Φ_O is a bijection.*

PROOF. Let P_1 and P_2 be degree one places on K such that $[P_1 - O] = [P_2 - O]$. Then P_1 is linearly equivalent to P_2, so there is $f \in K^\bullet$ such that $(f) = P_1 - P_2$. Then $f \in \mathcal{L}(P_2)$. If $P_1 \neq P_2$ then f is not contant, so $\ell(P_2) \geq 2$. However, the

Riemann-Roch Theorem in genus one says that for all divisors D of positive degree we have $\ell(D) = \deg D$, so $\ell(P_2) = \deg P_2 = 1$, a contradiction. Thus $P_1 = P_2$ and Φ_O is injective.

Let $D \in \operatorname{Div}^0 K$. Then $D = (D + O) - O$, and $\deg(D + O) = 1$. By Riemann-Roch again we have $\ell(D + O) = 1$, so there is a unique effective divisor linearly equivalent to $D + O$, which since it has degree 1 must be a degree one place P, and thus

$$[D] = [D + O] - [O] = [P] - [O] - [P - O],$$

so Φ_O is surjective. □

Using "transport of structure" from Φ_O we can endow $\Sigma_1(K/k)$ with the structure of a commtuative group. In other words, for $P_1, P_2 \in \Sigma_1(K/k)$, we put

$$P_1 + P_2 \coloneqq \Phi_O^{-1}(\Phi_O(P_1) + \Phi_O(P_2)).$$

Does this group law depend on the choice of O? Most certainly it does: indeed it makes O into the additive identity. However, this dependence is totally innocuous: the group laws are certainly isomorphic to each other, since each is isomorphic to $\operatorname{Pic}^0 K$. In fact the isomorphism is given by "translation," as the following exercise makes precise.

EXERCISE 2.26. a) *Show that* $\operatorname{Cl}^0 K$ *acts on* $\Sigma_1(K/k)$ *by defining* $[D]+P$ *to be the unique effective divisor linearly equivalent to* $D + P$*. Show that this action is simply transitive: i.e., there is a single orbit, and all the stabilizers are trivial.*

b) *Let* $O_1, O_2 \in \Sigma_1(K/k)$*. Show that* $P \in \Sigma_1(K/k) \mapsto [O_2 - O_1] + P$ *gives an isomorphism from the group law on* $\Sigma_1(K/k)$ *obtained from* Φ_{O_1} *to the group law on* $\Sigma_1(K/k)$ *obtained from* Φ_{O_2}*.*

In fact, for any genus one function field K/k, the divisor class group $\operatorname{Cl}^0 K$ acts on K by k-algebra automorphisms, giving an embedding

$$\operatorname{Pic}^0 K \hookrightarrow \operatorname{Aut}(K/k).$$

In particular this shows that $\operatorname{Aut}(K/k)$ is infinite when k is algebraically closed. Unfortunately I don't see how to define this action using the material we have developed so far.

7.3. Weierstrass Points. Let $P \in \Sigma_1(K/k)$ be a degree one point. We say that $n \in \mathbb{N}$ is a **pole order at P** if

$$\ell(nP) > \ell((n-1)P).$$

Thus n is a pole order at P iff there is a rational function $f \in K$ that has a pole of order n at P and is regular at every other point. Let $W(P) \subset \mathbb{N}$ be the set of pole orders at P. Some easy observations:

• If $g = 0$, then Riemann-Roch gives $\ell(nP) = n + 1$ for all $n \in \mathbb{N}$, so $W(P) = \mathbb{N}$.
• If $g = 1$, then we have $\ell(0) = 1$ and $\ell(nP) = n$ for all $n \in \mathbb{Z}^+$, so $W(P) = \mathbb{N} \setminus \{1\}$.

Thus the case of interest if $g \geq 2$, which we now assume.

• By Exercise 2.18, we have $\ell(0) = \ell(P) = 1$, so $0 \in W(P)$ and $1 \notin W(P)$.
• The set $W(P)$ is a **numerical semigroup**: that is, it is a submonoid of $(\mathbb{N}, +)$.

Indeed, $m, n \in W(P)$ then there is a rational function f with a pole of order m at P and regular away from P and a rational function g with a pole of order n at P and regular away from P and then fg has a pole of order $m+n$ at P and is regular away from P, so $m + n \in W(P)$.
• In fact $W(P)$ is a **primitive numerical semigroup**: the elements generate the unit ideal of $\mathbb{Z}$. In fact, any such semigroup contains all suffiicently large natural numbers. You can prove that on your own time, because we will immediately show something more precise: by Riemann-Roch, for all $n \geq 2g-1$ we have $\ell(nP) = n - g + 1$, and thus for all $n \geq 2g$ we have $\ell(nP) - \ell((n-1)P) = 1$. Thus $W(P)$ contains all $n \geq 2g$.
• So the question is which of $2, \ldots, 2g-1$ lie in $W(P)$. Well, we have $\ell(0) = \ell(P) = 1$, $\ell((2g-1)P) = g$ and for all $n \in \mathbb{Z}^+$ we have $\ell(nP) - \ell((n-1)P) \in \{0, 1\}$. It follows that there are precisely $g-1$ integers $1 \leq n \leq 2g-1$ such that $n \in W(P)$ and thus there are g **gaps**, i.e., elements $n \in \mathbb{N} \setminus W(P)$. This result is called the **Weierstrass Gap Theorem**.

For example, suppose that $g = 2$. Then $W(P)$ contains 0 and all integers $n \geq 4$ and omits precisely two non-negative integers. One of these gaps is $n = 1$, as we've seen already. This leaves two possibilities for $W(P)$: it is either $\{0, 3, 4, 5, \ldots\}$ or $\{0, 2, 4, 5, \ldots\}$. It turns out that if $k = \mathbb{C}$, both possibilities arise on every curve of genus 2.

A little thought shows that for any $g \geq 2$ one numerical semigroup that satisfies all the constraints is $\mathbb{W} := \{0, \ldots, g+1, g+2, \ldots\}$, i.e., the gaps are precisely the integers between 1 and g. In some naive sense this answer is "expected," since Riemann's Inequality shows that $\ell(nP) \geq 2$ for all $n \geq g+1$, but neither it nor Riemann-Roch can be used to show that $\ell(nP) \geq 2$ for any smaller value of n. We say that P is a **Weierstrass point** if W_P is anything other than $\mathbb{W}$: equivalently, if there is $1 \leq n \leq g$ such that $\ell(nP) \geq 2$. (Yet another equivalent characterization is that gP has positive index of speciality.)

To understand the set of Weierstrass points as a whole, it is better to assume that k is algebraically closed (later we will gain a clearer understanding between points over a given field K and points over $K \otimes_k \overline{k}$), but if k is perfect it turns out that every point P of degree d corresponds to a family of d "geometric points" on $K \otimes_k \overline{k}$.

From now until the end of this section we assume that k is algebraically closed of characteristic 0. In this case the set of Weierstrass points is finite and nonempty. When $g \geq 3$ the number of Weierstrass points on a curve of genus g depends on the curve, so we get a cleaner result if we count them with a certain "weight." Namely, for any point P (necessarily of degree 1 since k is algebraically closed), let $a_1 < \ldots < a_g$ be the g Weierstrass gaps. We define the **Weierstrass weight of P**

$$w_P := \sum_{i=1}^{g} (a_i - i).$$

Now if P is *not* a Weierstrass point, then we have $a_i = i$ for all i, so $w_P = 0$. So if P is a Weierstrass point we must have $a_i > i$ for at least one i and thus $w_P > 0$. Thus P is a Weierstrass point iff it has positive Weierstrass weight.

THEOREM 2.24. *Let k be algebraically closed of characteristic 0, and let K/k be a function field of genus $g \geq 2$. Then we have*

$$\sum_{P \in \Sigma(K/k)} w_P = g^3 - g.$$

PROOF. One can reduce to the case of $k = \mathbb{C}$, for which see [**ACGH**, C-15, p. 38] or [**ACGH**, E-8, p. 43]. □

It follows that there are at most $g^3 - g$ Weierstrass points, with equality iff every Weierstrass point has Weierstrass weight 1.

EXERCISE 2.27. *Let $P \in \Sigma(K/k)$, where k is algebraically closed of characteristic 0 and K has genus $g \geq 2$.*

a) *Show that $w_P = 1$ iff the gap sequence is $1 < 2 < \ldots < g-1 < g+1$. Such a Weierstrass point is called **normal**.*
b) *Show that $w_P \leq \frac{g(g-1)}{2}$, and deduce that there are at least $2g+2$ Weierstrass points.*
c) *Show that the following are equivalent:*
   (i) *We have $w_P = \frac{g(g-1)}{2}$.*
   (ii) *We have $\mathbb{N} \setminus \mathbb{W}(P) = \{1, 3, 5, \ldots, 2g-1\}$.*
   (iii) *We have $2 \in \mathbb{W}(P)$.*

If a curve has a point P with $2 \in \mathbb{W}(P)$, then there is $f \in K$ with polar divisor $2P$. Thus f has degree 2, so $K/k(f)$ is a quadratic extension. Function fields that are quadratic extensions of rational function fields are called **hyperelliptic** and will be studied in more detail later. If you already know what a hyperelliptic curve is, you should make a guess about what are the Weierstrass points and their weights on a hyperelliptic curve. (The most reasonable such guess is correct.)

The existence of Weierstrass points is a very striking difference between curves of genus 0 and 1 and curves of genus at least 2. For function fields of genus 0 and 1 over an algebraically closed field of constants, the automorphism group $\mathrm{Aut}(K/k)$ acts transitively on $\Sigma(K/k)$: every point looks the same as every other point. On the other hand, because of their instrinsic nature, for a curve of genus $g \geq 2$ the group $\mathrm{Aut}(K/k)$ must map Weierstrass points to Weierstrass points, so there is a finite subset of "special" points on the curve. In fact the use of Weierstrass points is one way to show that $\mathrm{Aut}(K/k)$ is a finite group when $g \geq 2$.

7.4. Weierstrass Normal Form. Let K/k be a function field of genus $g \geq 1$, and let P be a degree one place of K. (To be sure, we are making an assumption that such a place exists, which as mentioned above forces $\kappa(K) = k$, though we have assumed that already.) Let d be the least positive integer such that $\ell(dP) \geq 2$, and let e be the least positive integer that is coprime to d and such that $\ell(eP) > \ell((e-1)P)$. If $g = 1$ then by Riemann-Roch we have $\ell(nP) = n$ for all $n \geq 1$ so $d = 2$ and $e = 3$. If $g \geq 2$ then for all $n \geq 2g-1$ Riemann-Roch gives $\deg(nP) = n - g + 1 \geq g \geq 2$, so d and e exist and e is bounded above by any $n \geq 2g$ that is coprime to d.

Choose any nonconstant $x \in \ell(dP)$. By the minimality of d, the polar divisor of x is dP, so $[K : k(x)] = d$. Choose any $y \in \ell(eP) \setminus \ell((e-1)P)$, so the polar

divisor of y if eP and $[K : k(y)] = e$. We have

$$[K : k(x, y)] \mid [K : k(x)] = d,\ [K : k(x, y)] \mid [K : k(y)] = e,$$

and since $\gcd(d, e) = 1$ we conclude that $[K : k(x, y)] = 1$ and $K = k(x, y)$. By Exercise 0.7, there is a prime ideal $\mathfrak{p}$ of $k[t_1, t_2]$ such that $k(x, y)$ is the fraction field of $k[t_1, t_2]/(\mathfrak{p})$. Since the transcendence degree of the fraction field of $k[t_1, t_2]/(\mathfrak{p})$ is the Krull dimension of $k[t_1, t_2]/(\mathfrak{p})$ ([**CA**, Thm. 14.22b)]), it follows that $\mathfrak{p}$ must have height 1 in the UFD $k[t_1, t_2]$ and thus be principal. That is, there is an irreducible polynomial $f(t_1, t_2) \in k[t_1, t_2]$ satisfied by x and y. We call $f(x, y) = 0$ a **Weierstrass Normal Form** for K.

As a technical remark, we did not assume here that K/k is regular, or equivalently that K/k is separable. So this proves the 2-generation of K/k when k is algebraically closed in K and has a degree 1 place.

Let us now look further at some special cases.

Suppose that K has genus 1. As mentioned above the function x has degree 2 (by which we mean that $[K : k(x)] = 2$) and the function y has degree 3. We can be more explicit about the polynomial f in this case: the k-vector space $\mathcal{L}(6P)$ has dimension 6, and here are 7 elements of it: $1, x, y, x^2, xy, x^3, y^2$. So there must exist a linear relation among these 7 functions. Since the rational functions 1, x, y, x^2 all have different degrees which are also different from the degrees of x^3 and y^2, the linear dependence relation must involve both x^3 and y^2 with nonzero coefficients. I leave to you to check that we can scale each of x and y by nonzero elements of x so as to make the coefficients of x^2 and y^3 equal, and then we can divide by this common nonzero quantity, to get an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 = 0.$$

EXERCISE 2.28. *Suppose that the characteristic of k is not 2. Show that $K = K_f$ where f has the form*

$$y^2 - x^3 - a_2x^2 - a_4x - a_6,$$

and deduce that every genus one function field is regular.

Next we suppose that $d = 2$. This means that $2 \in \mathbb{W}(P)$ and that P is a Weierstrass point. By Exercise 2.27, the Weierstrass semigroup at P is $\{0, 2, 4, 6, \ldots, 2g, 2g + 1, \ldots\}$, and it follows that $e = 2g + 1$. (In that exercise we assumed that k was algebraically closed of characteristic 0, but this part holds true anyway.) Choose nonconstant $x \in \mathcal{L}(2P)$ and $y \in \mathcal{L}((2g + 1)P) \setminus \mathcal{L}(2gP)$. Again we get that $K = k(x, y)$.

EXERCISE 2.29. a) *Show that after rescaling x and y by elements of $k^\times$, there is a polynomial $a(x) \in k[x]$ of degree at most g and a monic polynomial $p(x) \in k[x]$ of degree $2g + 1$ such that*

$$y^2 + a(x)y = p(x).$$

b) *Suppose that the characteristic of k is not 2. Show that there is $x \in \mathcal{L}(2P) \setminus \mathcal{L}(P)$ and $y \in \mathcal{L}((2g + 1)P) \setminus \mathcal{L}(2gP)$ and a monic polynomial $p(x) \in k[x]$ of degree $2g + 1$ such that $K = K_f$ where $f(x, y) = y^2 - p(x)$.*

c) *Deduce that if the characteristic of k is not 2, then K/k is a regular function field.*

Next we suppose that $g \geq 2$ and that P is *not* a Weierstrass point. Then $d = g+1$ and $e = g+2$. I leave it to you to show that $K = K_f$, where $f \in k[x,y]$ is an irreducible polynomial of **bidegree** $(g+2, g+1)$ (in other words, viewed as an element of $(k[y])[x]$, it has degree $g+2$, while viewed as an element of $(k[x])[y]$, it has degree $g+1$). In fact, even if P is a Weierstrass point such a representation exists; it is just not the Weierstrass representation because $d < g+1$.

EXERCISE 2.30. *Suppose that k has characteristic $p > d$. Show that every Weierstrass polynomial $f \in k[t_1, t_2]$ is geometrically irreducible and K/k is geometrically regular.*

7.5. Clifford's Theorem. Let's check back in on the Riemann-Roch problem, which is to compute the dimension $\ell(D)$ of the Riemann-Roch space $\mathcal{L}(D)$ attached to a divisor $D \in \operatorname{Div} K$ for a function field K/k.

We know:

- If $\deg D < 0$, then $\ell(D) = 0$.
- If $\deg D \geq 0$, then $\ell(D) \leq \deg D + 1$.
- If $\deg D = 0$, then $\ell(D) = \begin{cases} 1 & D \text{ is principal} \\ 0 & \text{otherwise} \end{cases}$
- If $g = 0$ and $\deg D \geq 0$, then $\ell(D) = \deg D + 1$.
- If $g \geq 1$ and $\deg D \geq 2g-1$, then $\ell(D) = \deg(D) - g + 1$.
- If $g \geq 1$ and $\deg D = 2g-2$, then $\ell(D) = \begin{cases} g & D \textbf{ is canonical} \\ g-1 & \textbf{otherwise} \end{cases}$.

These give complete results for $g = 0$ and $g = 1$, so suppose $g \geq 2$. In this case we also know:

- If $\deg D = 1$, then $\ell(D) \in \{0, 1\}$.

Indeed, if $\deg D = 1$, $\ell(D) \geq 1$ iff $D \sim P$ for a degree one place P, so $\ell(D) = \ell(P) = 1$, because otherwise K would admit a rational function with polar divisor P, hence a rational function of degree 1, making K a rational function field, hence of genus 0.

This also gives a reasonable good answer to the Riemann-Roch problem when $g = 2$, with one exception: we would like a better understanding of when a genus 2 divisor is canonical. For instance, above we claimed that when k is algebraically closed of characteristic 0 there is always $P \in \Sigma_1(K/k)$ such that $\ell(2P) = 2$, or equivalently that $2P$ is canonical. We will come back to this later after establishing the Riemann-Hurwitz formula.

When $g \geq 2$ and $0 \leq \deg D \leq 2g-2$ we would like to improve our understanding. As far as I know there is no complete answer, and it does not seem reasonable to expect one: for instance a sufficiently simple answer would render the theory

of Weierstrass points simpler than it can demonstrably be shown to be. However there are some further results. We will content ourselves with this classical one.

THEOREM 2.25 (Clifford's Theorem). *Let $g \geq 2$, and let $D \in \operatorname{Div} K$ be such that $0 \leq \deg D \leq 2g-2$. Then we have*

$$\ell(D) \leq 1 + \frac{\deg D}{2}. \tag{9}$$

Before giving the proof we note some consequences:

• First of all we get again that if $\deg D = 1$, then $\ell(D) \in \{0, 1\}$.
• Next we get that if $\deg D = 2$, then $\ell(D) \leq 2$. When $g = 2$ then $g = 2g - 2$ and we knew this already; when $g \geq 3$ it is new information.
• If $g \geq 3$, we get that if $\deg D = 3$ then $\ell(D) \leq 2$. In this case if $D = 3P$ for a degree one place P then we new this already from our analysis of the Weierstrass semigroup.

EXERCISE 2.31. *Does Clifford's Theorem impose any new restrictions on the Weierstrass semigroup of a degree one place?*

At the moment we will prove Clifford's Theorem when the ground field k is infinite. Later we will remedy this. For instance, later we will study the effect of base extension on Riemann-Roch spaces, and that will allow us to pass from a finite field to its infinite algebraic closure.

We will deduce Clifford's Theorem from the following result.

LEMMA 2.26. *Let K be a function field over an infinite field of constants k. Let $A, B \in \operatorname{Div} K$ be such that $\ell(A), \ell(B) > 0$. Then we have*

$$\ell(A) + \ell(B) \leq 1 + \ell(A + B).$$

PROOF. Since $\ell(A), \ell(B) > 0$, there are effective divisors $A_0 \sim A$ and $B_0 \sim B$. Consider the set

$$\mathcal{X} \coloneqq \{D \in \operatorname{Div} K \mid D \leq A_0 \text{ and } \mathcal{L}(D) = \mathcal{L}(A_0)\}.$$

Since $A_0 \in \mathcal{X}$, the set $\mathcal{X}$ is nonempty. Moreover every element of $\mathcal{X}$ has positive degree, so there is some $D_0 \in \mathcal{X}$ of minimal degree. It follows that for all $P \in \Sigma(K/k)$ we have

$$\ell(D_0 - P) < \ell(D_0) = \ell(A).$$

We CLAIM that

$$\ell(D_0) + \ell(B_0) \leq 1 + \ell(D_0 + B_0).$$

If so, then

$$\ell(A) + \ell(B) = \ell(D_0) + \ell(B_0) \leq 1 + \ell(D_0 + B_0) \leq 1 + \ell(A_0 + B_0) = 1 + \ell(A + B).$$

Let $P_1, \ldots, P_r$ be the places in the support of B_0. Then for $1 \leq i \leq r$ we have that $\mathcal{L}(D_0 - P_i)$ is a proper k-subspace of $\mathcal{L}(D_0)$. Since we are assuming that k is infinite, a k-vector space is not a union of finitely many proper subspaces [**Cl12**, Main Theorem], so there is $z \in \mathcal{L}(D_0) \setminus \bigcup_{i=1}^{r} \mathcal{L}(D_0 - P_i)$.

The k-linear map

$$\varphi : \mathcal{L}(B_0) \to \mathcal{L}(D_0 + B_0)/\mathcal{L}(D_0),\ x \mapsto xz \pmod{\mathcal{L}(D_0)}$$

has kernel k, so

$$\ell(B_0) - 1 \leq \ell(D_0 + B_0) - \ell(D_0),$$

establishing the claim. □

PROOF OF CLIFFORD'S THEOREM: Certainly (9) holds if $\ell(A) = 0$. Similarly, if for a canonical divisor $\mathcal{K}$ we have $\ell(\mathcal{K} - A) = 0$, then Riemann-Roch gives

$$\ell(A) = \deg(A) - g + 1 = 1 + \frac{\deg(A)}{2} + \frac{\deg(A) - 2g}{2} < 1 + \frac{\deg(A)}{2}.$$

So suppose $\ell(A)$ and $\ell(\mathcal{K} - A)$ are both positive. Then Lemma 2.26 gives

$$\ell(A) + \ell(\mathcal{K} - A) \leq 1 + \ell(\mathcal{K}) = 1 + g, \tag{10}$$

while the Riemann-Roch Theorem gives

$$\ell(A) - \ell(\mathcal{K} - A) = \deg(A) - g + 1. \tag{11}$$

Adding (10) and (11) gives (9).

7.6. More on Hyperelliptic Function Fields. Recall that a function field K/k is **hyperelliptic** if there is a degree 2 rational function $f \in K$: equivalently, K is a quadratic extension of a rational function field.

EXERCISE 2.32. a) *Show: a hyperelliptic function field has index* 1 *or* 2.
b) *Show: every function field of genus* 0 *is hyperelliptic.*
c) *Show: every elliptic function field is hyperelliptic.*
d) *[Harder] Show: there are genus one function fields that are not hyperelliptic. (Cf.* [**Cl04**]*)*

THEOREM 2.27. *For a function field K/k of genus $g \geq 1$, the following are equivalent:*

(i) *The function field K/k is hyperelliptic.*
(ii) *There is a divisor $D \in \mathrm{Div}(K)$ with $\deg(D) = 2$ and $\ell(D) = 2$.*

PROOF. (i) $\implies$ (ii): Let $f \in K$ be a rational function of degree 2, and put $D := (f)_-$, so D has degree 2. Since D is effective and $f \in \mathcal{L}(D)$, we have $\ell(D) \geq 2$. By Clifford's Theorem (Theorem 2.25) we have $\ell(D) \leq 1 + \frac{\deg D}{2} = 2$, so $\ell(D) = 2$. (ii) $\implies$ (i): Since $\ell(D) \geq 1$, we may assume without loss of generality that D is effective. Since $\ell(D) \geq 2$ there is a nonconstant f such that $(f) \geq -D$, so $\deg f = \deg(f)_- \in \{1, 2\}$. If f had degree 1 then $K = k(f)$ would be rational and thus of genus 0, so f has degree 2. □

Theorem 2.27 fails in genus 0: every genus 0 function field is hyperelliptic, but in a genus zero function field every divisor D of degree 2 has $\ell(D) = 3$.

THEOREM 2.28. *Every function field of genus* 2 *is hyperelliptic.*

PROOF. In genus 2, a canonical divisor $\mathcal{K}$ has $\deg \mathcal{K} = 2$ and $\ell(\mathcal{K}) = 2$. □

CHAPTER 3

Extensions of Function Fields

Throughout this chapter, a function field K/k means a field extension that is finitely generated, of transcendence degree 1 and such that k is algebraically closed in K.

1. Algebraic Extensions of Function Fields

Let K/k and L/l be function fields. We write $K/k \subset L/l$ and say that **L/l is an extension of K/k** if $k \subset l$ and $K \subset L$.

LEMMA 3.1. *Let $K/k \subset L/l$ be an extension of function fields.*

a) *We have that L/K is algebraic iff l/k is algebraic. We call an extension satisfying these equivalent conditions* ***algebraic****.*
b) *We have that $[L : K]$ is finite iff $[l : k]$ is finite. We call an extension satisfying these equivalent conditions* ***finite****.*
c) *If $K/k \subset L/l$ is algebraic, then $K \cap l = k$.*

PROOF. a) We have

$$\begin{aligned} \operatorname{trdeg}(L/K) + 1 &= \operatorname{trdeg}(L/K) + \operatorname{trdeg}(K/k) \\ &= \operatorname{trdeg}(L/k) = \\ \operatorname{trdeg}(L/l) + \operatorname{trdeg}(l/k) &= \operatorname{trdeg}(l/k) + 1, \end{aligned}$$

so

$$\operatorname{trdeg}(L/K) = \operatorname{trdeg}(l/k).$$

b) If $[l : k]$ is finite, then l/k is algebraic, so by part a) we have that L/K is algebraic. L/l and l/k are both finitely generated, so L/k is finitely generated. It follows that L/K is finitely generated and algebraic, so $[L : K]$ is finite. The argument for the converse is almost identical and left to the reader.
c) Since $(K \cap l)/k$ is an algebraic subextension of K/k, we must have $K \cap l = k$. □

LEMMA 3.2. *Let $K/k \subset L/l$ be an algebraic extension of function fields. Suppose that K/k is regular and L/K is separable. Then l/k and L/l are separable.*

PROOF. Since K/k is regular, it is separable. Since L/K and K/k are both separable, we have that L/k is separable [**FT**, Cor. 12.17b)]. It follows that l/k is separable [**FT**, Cor. 12.17a)] and then, since l/k is algebraic by Lemma 3.1a), that L/l is separable [**FT**, Cor. 12.17c)]. □

An extension $K/k \subset L/l$ is **constant** if $L = Kl$. This definition includes not necessarily algebraic extensions, in which case the subring $K[l]$ generated by K and l need not be a field. When the extension is algebraic, $K[l]$ is already a field. An extension L/k of a regular function field K/k is **geometric** if $l = k$. Thus for

a regular function field K/k, every algebraic extension of K/k is geometric iff k is algebraically closed, and a general algebraic extension $K/k \subset L/l$ decomposes as

$$K \subset Kl \subset L,$$

hence as a a geometric extension of a constant extension.

We claim that for any algebraic extension $K/k \subset L/l$ we have a restriction map

$$r : \Sigma(L/l) \to \Sigma(K/k)$$

that is surjective with finite fibers. Let $Q \in \Sigma(L/l)$, with corresponding discrete valuation v_Q. We wish to take $r(Q)$ to be the place corresponding to the ring $R_Q \cap K$. By Exercise 1.1 this is a valuation ring of K. Since $l \subset R_Q$, $k = l \cap K \subset R_Q \cap K$. There is just one thing to check: that $R_Q \cap K \subsetneq K$. To see this, let $\pi \in R_Q$ be a uniformizing element. Since $\pi \in L$ and L/K is algebraic, there is a monic polynomial

$$P = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in K[t]$$

such that $P(\pi) = 0$. We claim that there is at least one i such that $a_i \neq 0$ and $v_Q(a_i) \neq 0$, which suffices since then $a_i^{-1} \in K \setminus R_Q$. If not, then taking $a_n = 1$, for each i such that $a_i \neq 0$ we have $v_Q(a_i t^i) = i$, hence we have a finite sum of elements of distinct valuations equal to 0, a contradiction.

This shows that for every $Q \in \Sigma(L/l)$, we have $r(Q) = R_Q \cap K$ is a nontrivial discrete valuation ring of K/k, thus defines a unique place $P = r(Q) \in \Sigma(K/k)$. We say that Q **lies over** P and write $Q \mid P$. Notice that the situation here is a bit more interesting than the standard one considered in algebraic number theory, because the extension L/K is allowed to be algebraic of infinite degree.

EXERCISE 3.1. *Let k be a field with algebraic closure $\overline{k}$, let $K = k(t)$, $l = \overline{k}$ and $L = Kl = \overline{k}(t)$, so $k(t)/k \subset \overline{k}(t)/k$ is a constant algebraic extension.*

a) *A place $Q \in \Sigma(\overline{k}(t)/\overline{k})$ corresponds to a monic irreducible polynomial $t - \alpha$ for $\alpha \in \overline{k}$. Let $P(t) \in k[t]$ be the minimal polynomial. Show that Q lies over P, viewed as a place of $k(t)/k$.*

b) *Deduce that the map $r : \Sigma(\overline{k}(t)/\overline{k}) \to \Sigma(k(t)/k)$ is surjective with finite fibers. Show that if $[\overline{k} : k]$ is infinite (by [**FT**, X.X], this happens iff k is neither algebraically closed nor real-closed, and in particular when $[\overline{k} : k] > 2$), the fibers can have arbitrarily large cardinality.*

LEMMA 3.3. *Let $K/k \subset L/l$ be an algebraic extension of function fields, let $Q \in \Sigma(L/l)$, and let $P = r(Q) \in \Sigma(K/k)$.*

a) *Let R_Q (resp. R_P) be the valuation ring of Q (resp. of P) in L (resp. K), and let $\mathfrak{m}_Q$ (resp. $\mathfrak{m}_P$) be the maximal ideal of R_Q (resp. of R_P). Then*

$$\mathfrak{m}_Q \cap K = \mathfrak{m}_P.$$

b) *Let π be a uniformizer for v_Q, and let*

$$e(Q/P) \coloneqq v_P(\pi).$$

Then we have

$$(v_Q)|_K = v_P.$$

PROOF. a) By definition of P we have $R_P = R_Q \cap K$, so under the inclusion map $R_P \hookrightarrow R_Q$ the maximal ideal $\mathfrak{m}_Q$ pulls back to a prime ideal of R_P. Above we saw that there is $a \in K^\times$ such that $v_Q(a) \neq 0$, hence, passing from a to a^{-1} if necessary, there is a nonzero element in $\mathfrak{m}_Q \cap K$. Since R_P is a DVR its only nonzero prime ideal if $\mathfrak{m}_P$, so we must have $\mathfrak{m}_Q \cap K = \mathfrak{m}_P$.
b) Let $x \in K^\times$. Since $R_P = R_Q \cap K$, we have $v_P(x) \geq 0$ iff $v_Q(x) \geq 0$, and by part a) we have $v_P(x) > 0$ iff $v_Q(x) > 0$. So

$$v_Q(x) = v_Q(x\pi^{-v_P(x)}) + v_Q(\pi^{v_P(x)}) = 0 + v_P(x)v_Q(\pi) = e(Q/P)v_P(x). \qquad \square$$

It follows that for an algebraic extension $K/k \subset L/l$ of function fields and $Q \in \Sigma(L/l)$ lying over $P \in \Sigma(K/k)$, then just as in the finite case we have an extension of residue fields

$$k_P = R_P/\mathfrak{m}_P \hookrightarrow R_Q/\mathfrak{m}_Q = k_Q.$$

It is easy to see, by reducing to the finite case, tha k_Q/k_P is algebraic. However it need not have finite degree: for instance, in Exercise 3.1 suppose that $k = \mathbb{Q}$. Then for all Q we have $k_Q = \overline{Q}$, while k_P is a finite degree extension of $\mathbb{Q}$. The possibility of an infinite degree algebraic residue extension is the only real change from the usual finite degree case. We still put

$$f(Q|P) \coloneqq [k_Q : k_P],$$

with the understanding that this is now a cardinal number.

We say that the place P is **ramified** in L/K if for some $Q \mid P$ we have either that $e(Q|P) > 1$ or that the residue extension k_Q/k_P is inseparable.

Consider a finite extension $K/k \subset L/l$. First of all, the data of k, K, L determines l in this case as the algebraic closure of k in L. The restriction $r : \Sigma(L/l) \to \Sigma(K/k)$ is essentially the pullback of maximal ideals familiar from algebraic number theory: for any $P \in \Sigma(K/k)$, choose an affine Dedekind domain A of K such that $A \subset R_P$; then we may identify P with a maximal ideal of A. The integral closure B of A in L is a Dedekind domain that is finitely generated as an A-module, and the places $Q \in \Sigma(L/l)$ lying over P correspond to the maximal ideals of B that lie over P. In particular, there is at least one and only finitely many such Q. Moreover the residue field at P is $A/P = k_P$, and the residue field at Q is $B/Q = l_Q$. Writing the places Q lying over P as $Q_1, \ldots, Q_r$, we have the usual degree equality

$$\sum_{i=1}^{r} e(Q_i|P)f(Q_i|P) = [L : K].$$

It follows that $f(Q_i|P)$ is finite, which is half of part a) of the following result.

PROPOSITION 3.4. *Let $K/k \subset L/l$ be an algebraic extension of function fields. Let $Q \in \Sigma(L/l)$ lie over $P \in \Sigma(K/k)$.*

a) *We have that $f(Q|P)$ is finite iff L/K is finite.*
b) *Suppose we have a tower $K/k \subset L/k \subset M/m$ of algebraic extensions, and let $P \in \Sigma(K/k)$, $Q \in \Sigma(L/l)$, $R \in \Sigma(M/m)$, with $R \mid Q \mid P$. Then:*

$$e(R|P) = e(R|Q)e(Q|P),$$

$$f(R|P) = f(R|Q)f(Q|P).$$

PROOF. a) We saw above that if L/K is finite, then $[l_Q : k_P]$ is finite. Now suppose that $[l_Q : k_P]$ is finite. Since $[k_P : k]$ is finite, we get that $[l_Q : k]$ is finite and thus that $[l : k]$ is finite. Now Proposition 3.1b) gives that $[L : K]$ is finite.
b) We have $(v_R)|_L = e(R|Q)v_Q$ and $(v_Q)|_K = e(Q|P)v_K$, so

$$e(R|P)v_P = (v_R)|_K = e(R|Q)e(Q|P)v_P$$

and thus $e(R|P) = e(R|Q)e(Q|P)$. Moreover we have

$$f(R|P) = [m_R : k_P] = [m_R : l_Q][l_Q : k_P] = f(R|Q)f(Q|P). \qquad \square$$

Interestingly, even when L/K is algebraic of infinite degree, we retain the following result.

THEOREM 3.5. *Let $K/k \subset L/l$ be an algebraic extension of function fields. Then the restriction map*

$$r : \Sigma(L/l) \to \Sigma(K/k)$$

is surjective with finite fibers.

PROOF. Let $P \in \Sigma(K/k)$. By Riemann-Roch there is $f \in K$ that has a zero at P and at no other place of K/k. We claim that for $Q \in \Sigma(L/l)$, we have that Q lies over P iff $v_Q(f) > 0$. First of all if $Q|P$, we have $v_Q(f) = e(Q|P)v_P(f) > 0$. Conversely, if $v_Q(f) > 0$, let $P' = Q \cap K$. Then

$$v_{P'}(f) = \frac{1}{e(Q|P')} v_Q(f) > 0,$$

so $P' = P$.

Since f is transcendental over k and l/k is algebraic, we have $f \in L \setminus l$ and thus the set of zeroes of f in $\Sigma(L/l)$ is finite and nonempty. $\square$

These considerations suggest that even infinite degree algebraic extensions are still governed by Dedekind domains. This seems initially surprising, because if A is a Dedekind domain with fraction field $K \supsetneq A$ and L/K is an algebraic extension of infinite degree, then in general the integral closure B of A in L need not be a Dedekind domain. For instance, take $A = \mathbb{Z}$, $K = \mathbb{Q}$ and $L = \overline{\mathbb{Q}}$, so $B = \overline{\mathbb{Z}}$ is the ring of all algebraic integers. This ring is Noetherian and integrally closed (as B will always be in the above setup) but fails to be Noetherian: $(2) \subset (2^{1/2}) \subset (2^{1/4}) \subset \ldots$ is an infinite properly ascending chain of ideals. However, things work out better for affine Dedekind domains.

EXERCISE 3.2. *Let $K/k \subset L/l$ be an algebraic extension of function fields, and let $r : \Sigma(L/l) \to \Sigma(K/k)$ be the restriction map. Let $S \subset \Sigma(K/k)$ be a finite nonempty subset, and let $T \coloneqq r^{-1}(S)$. Show: the integral closure of the Dedekind domain R^S in the (possibly infinite degree!) field extension L/K is the Dedekind domain R^T.*

For an extension $\iota : A \subset B$ of Dedekind domains,the pushforward ι_* on nonzero ideals gives a monoid homomorphism from the nonzero ideals of A under multiplication to the nonzero ideals of B under multiplication. This extends uniquely to a group homomorphism $\operatorname{Frac} A \to \operatorname{Frac} B$ on the groups of fractional ideals. This pushforward evidently carries principal fractional ideals to principal fractional ideals, so induces a homomorphism of class groups $\operatorname{Cl} A \to \operatorname{Cl} B$.

Given an algebraic extension $K/k \subset L/l$ of function fields, we can define a similar pushforward map on divisors, which is (for some reason!) usually called the **conorm**. Namely, for $P \in \Sigma(K/k)$ we put

$$\iota_{L/K}(P) \coloneqq \sum_{Q|P} e(Q|P)Q \in \operatorname{Div} L.$$

Since $\operatorname{Div} K$ is the free commutative group on the set of places, this extends uniquely to a homomorphism

$$\iota_{L/K} : \operatorname{Div} K \to \operatorname{Div} L, \sum_P n_P P \mapsto \sum_Q e(Q|r(Q))n_{r(Q)}Q.$$

LEMMA 3.6. a) *Let $K/k \subset L/l \subset M/m$ be a tower of algebraic extensions of function fields. Then we have*

$$\iota_{M/K} = \iota_{L/K} \circ \iota_{M/L}.$$

b) *Let $K/k \subset L/k$ be an algebraic extension of function fields, and let $f \in K^\times$. Then we have*

$$\iota_{L/K}((f)) = (\iota_{L/K}(f)),$$
$$\iota_{L/K}((f)_+) = (\iota_{L/K}(f))_+,$$

and

$$\iota_{L/K}((f)_-) = (\iota_{L/K}(f))_-.$$

EXERCISE 3.3. *Prove Lemma 3.6.*

It follows from Lemma 3.6b) that we get an induced homomorphism

$$\iota_{L/K} : \operatorname{Cl}(K) \to \operatorname{Cl}(L).$$

It would be more interesting to get an induced homomorphism on the degree zero divisor class groups. The next result tells us when this occurs.

PROPOSITION 3.7. *Let $K/k \subset L/l$ be a finite extension of function fields. Then for all $D \in \operatorname{Div} K$ we have*

$$\deg \iota_{L/K}(D) = \frac{[L:K]}{[l:k]} \deg D.$$

PROOF. If we can show this for a prime divisor $P \in \Sigma(K/k)$, the general case follows by linearity. And indeed we have

$$\deg \iota_{L/K}(P) = \deg(\sum_{Q|P} e(Q|P)Q) = \sum_{Q|P} e(Q|P)[l_Q : l]$$

$$= \left(\sum_{Q|P} e(Q|P)f(Q|P)\frac{[l_Q : l]}{[l_Q : k_P][k_P : k]}\right)\deg(P)$$

$$= \left(\frac{1}{[l:k]}\right)\left(\sum_{Q|P} e(Q|P)f(Q|P)\right)\deg(P)$$

$$= \frac{[L:K]}{[l:k]} \deg P. \qquad \square$$

The following is an immediate consequence.

COROLLARY 3.8. *Let K/k be a regular function field, let l/k be a finite degree extension, and let L be the constant extension $K \otimes_k l$. Then $\iota_{L/K}$ preserves degrees and thus induces a homomorphism*

$$\iota_{L/K} : \mathrm{Cl}^0 K \to \mathrm{Cl}^0 L.$$

We will see later that in the case of a separable constant extension the map $\iota_{L/K} : \mathrm{Cl}\, K \to \mathrm{Cl}\, L$ is injective, and moreover both of these facts continue to hold for separable algebraic constant extensions of infinite degree.

The following result is a version of Eisenstein's Irreducibility Criterion.

PROPOSITION 3.9. *Let K/k be a function field, and let $f = a_n x^n + \ldots + a_1 x + a_0 \in K[x]$ be a polynomial. Suppose that there is a place $P \in \Sigma(K/k)$ such that one of the following conditions holds:*

(i) *We have $v_P(a_n) = 0$; for $1 \leq i \leq n-1$ we have $v_P(a_i) \geq v_P(a_0) > 0$; and $\gcd(n, v_P(a_0)) = 1$.*
(ii) *We have $v_P(a_n) = 0$; for $1 \leq i \leq n-1$ we have $v_P(a_i) \geq 0$; $v_P(a_0) < 0$ and $\gcd(n, v_P(a_0)) = 1$.*

Then $f \in F[x]$ is irreducible. Let $L = K[x]/(f)$, and let l be the algebraic closure of k in L. Then there is a unique place $Q \in \Sigma(L/l)$ lying over P and we have $e(Q|P) = n$, $f(Q|P) = 1$.

PROOF. In an algebraic closure $\overline{K}$ of K, let y be a root of K, and put $L \coloneqq K(y)$. Then $[K : L] \leq n$, with equality iff f is irreducible. Let l be the algebraic closure of k in L, and let $Q \in \Sigma(L/l)$ be a place lying over P. Since $f(y) = 0$, we have

$$-a_n y^n = a_{n-1} y^{n-1} + \ldots + a_1 y + a_0.$$

First assume (i). Put $e \coloneqq e(Q|P)$, so $v_Q|_K = e v_P$. Thus $v_Q(a_n) = 0$ and $v_(a_i) > 0$ for all $0 \leq i \leq n-1$, and it follows that $v_Q(y) > 0$. Moreover we get $v_Q(a_0) = e v_P(a_0)$ and $v_Q(a_i y^i) = e v_P(a_i) + i v_Q(i) > e v_P(a_0)$ for all $1 \leq i \leq n-1$, so it follows that

$$n v_Q(y) = v_Q(-a_n y^n) = e v_P(a_0).$$

Since $\gcd(n, v_P(a_0)) = 1$, we conclude that $n \mid e$ and thus that $n \leq e$. Since $[L : K] \leq n$ we conclude that $[L : K] = n = e$ and thus f is irreducible and $e(Q|P) = n$, so $f(Q|P) = 1$. It follows from the Degree Equality that Q must be the only place of L/l lying over P.
Now assume (ii)... □

2. Review on the Discriminant and Different Ideals

Let us recall some important algebraic number theory. Let R be a Dedekind domain with fraction field K, let L/K be a *separable* field extension of finite degree n, and let S be the integral closure of R in L. Then S is a Dedekind domain and (because L/K is separable) finitely generated as an R-module.

Let us denote by $T_{L/K}$ the **trace map** from L down to K: among other things, for $x \in L$, $T_{L/K}(x)$ really is the trace of the K-linear map $x\bullet : y \in K \mapsto xy$. Let

$$\langle \cdot, \cdot \rangle : L \to K$$

be the **trace form**, defined by $\langle x, y \rangle = T_{L/K}(xy)$. A basic fact is that the trace form is a symmetric bilinear form that is nondegenerate since L/K is separable:

indeed its nondegeneracy is equivalent to the separability of L/K. Among other things, nondegneracy means that if we choose a basis $e_1, \ldots, e_n$ for L/K, then the associated **Gram matrix**

$$M(i,j) \coloneqq \langle e_i, e_j \rangle$$

is nonsingular, so its discriminant is nonzero. We denote this quanity by $\Delta(e_1, \ldots, e_n)$. If we switched to a different K-basis $e_1', \ldots, e_n'$ then there is a change of basis matrix P carrying e_i to e_i' and then the new Gram matrix is $P^T M P$ and thus we have

$$\Delta(e_1', \ldots, e_n') = (\det P)^2 \Delta(e_1, \ldots, e_n),$$

so overall there is a well-defined **discriminant class** $\Delta_{L/K} \in K^\times / K^{\times 2}$.

We now define $\Delta_{S/R}$ to be the ideal of R generated by all the elements $\Delta(x_1, \ldots, x_n)$ such that $e_1, \ldots, e_n$ are elements of S that are K-linearly independent. Because R is integrally closed, we have $\Delta(x_1, \ldots, x_n) \in R^\bullet$, so $\Delta_{S/R}$ is a nonzero ideal of R. Therefore it factors as $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.

If S is a free R-module and $e_1, \ldots, e_n$ is an R-basis for S, then it is easy to see that $\Delta_{S/R} = \Delta(e_1, \ldots, e_n)$. In the general case if we replace R by the DVR $R_\mathfrak{p}$ then we have $\Delta_{S/R} R_\mathfrak{p} = \Delta_{S R_\mathfrak{p} / R_\mathfrak{p}}$ since there is an $R_\mathfrak{p}$-basis of $S_\mathfrak{p}$ consisting of elements of S. Thus the discriminant ideal can be computed locally, but we needed the two lines of global definition to see that for all but finitely many $\mathfrak{p} \in \operatorname{MaxSpec} R$ we have that $\Delta_{S R_\mathfrak{p} / R_\mathfrak{p}}$ is the unit ideal.

Here is the main theorem on discriminants:

THEOREM 3.10. *Let R be a Dedekind domain with fraction field K, let L/K be a finite degree separable field extension, and let S be the integral closure of R in L. For $\mathfrak{p} \in \operatorname{MaxSpec} R$, the following are equivalent:*

(i) *The prime $\mathfrak{p}$ ramifies in S: that is, write $\mathfrak{p}S = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$. Then for some $1 \leq i \leq r$ either $e_i > 1$ or the residual extension $(R/\mathfrak{p}) \subset (S/\mathcal{P}_i)$ is inseparable.*

(ii) *The prime $\mathfrak{p}$ divides the discriminant $\Delta_{S/R}$.*

The major weakness of this theorem is that it gives information on the prime divisors of the discriminant but not on their multiplicities.

Let R be a Dedekind domain with fraction field K, let V be a finite-dimensional K-vector space, and let $\langle \cdot, \cdot \rangle$ be a nondegenerate symmetric bilinear form on V. A **lattice** in V is a finitely generated R-sumodule of V that spans V as a K-vector space. For any lattice $\Lambda \subset V$ we define the **dual lattice**

$$\Lambda^* \coloneqq \{x \in V \mid \langle x, \Lambda \rangle \subset R\}.$$

As the name suggests, Λ^* is indeed another R-lattice in V; as an R-module we have

$$\Lambda^* \cong \Lambda^\vee \coloneqq \operatorname{Hom}_R(\Lambda, R).$$

Moreover we have that $\Lambda^{**} = \Lambda$. For proofs, see e.g. [**Su.5**].

We now return to the previous setup, in which R is a Dedekind domain with fraction field K, L/K is a field extension of finite degree n, S is the integral closure of R in L, and $\langle \cdot, \cdot \rangle$ is the trace form. Then a fractional S-ideal $\mathfrak{a}$ is a nonzero finitely generated S-submodule of L; since S is finitely generated as an R-module,

we have that $\mathfrak{a}$ is also finitely generated as an R-module. Moreover the K-span $\mathfrak{a}$ is all of L, so $\mathfrak{a}$ is a lattice in R. It is not hard to show that the dual lattice $\mathfrak{a}^*$ is also a fractional S-ideal of L [**Su.12**, Lemma 12.1].

Let us apply this with $\mathfrak{a} = S$: the dual lattice is $S^* = \{x \in L \mid \langle x, S\rangle \subset R\}$. Since $T_{L/K}(S) \subset R$, we have $S^* \supset S$. Moreover S^*, being finitely generated as an R-module, is certainly finitely genreated as an S-module: that is, S^* is a fractional S-ideal of L that contains S. Therefore its inverse as a fractional ideal is an integral ideal of S, called the **different ideal** $\mathbb{D}_{S/R}$.

As for any nonzero integral ideal in a Dedekind domain, the different can be factored into a product of primes:

$$\mathbb{D}_{S/R} = \prod_{\mathcal{P} \in \operatorname{MaxSpec} S} \mathcal{P}^{d(\mathcal{P}|\mathfrak{p})}.$$

Here $\mathfrak{p} = \mathcal{P} \cap R$, and we refer to the non-negative integer $d(\mathcal{P}|\mathfrak{p})$ as the **local different exponent** at $\mathcal{P}$.

Let us collect some known facts about the different ideal for future use.

PROPOSITION 3.11. *Formation of the different ideal commutes with both localization and completion. That is: let R be a Dedekind domain with fraction field K, let L/K be a finite degree separable field extension, and let S be the integral closure of R in L. Then:*

a) *Let M be a multiplicative subset of R. Then we have*

$$M^{-1}\mathbb{D}_{S/R} = \mathbb{D}_{M^{-1}S/M^{-1}R}.$$

b) *Let $\mathfrak{p} \in \operatorname{MaxSpec} R$ and $\mathcal{P} \in \operatorname{MaxSpec} S$ with $\mathcal{P} \mid \mathfrak{p}$. Then*

$$\mathbb{D}_{\hat{S}_{\mathcal{P}}/\hat{R}_{\mathfrak{p}}} = \mathbb{D}_{S/R}\hat{S}_{\mathcal{P}}.$$

PROOF. See [**Su.12**, Prop. 12.3] and [**Su.12**, Prop. 12.4]. □

We now want to introduce the **ideal norm**, a group homomorphism

$$N_{S/R} : \operatorname{Frac} S \to \operatorname{Frac} R.$$

There is a right way to do this and a slightly wrong way to do this. The slightly wrong way is equivalent to the right way under the assumption that the field extension L/K is separable, whereas in the inseparable case it doesn't work...hence the name slightly wrong. However, for now we will take advantage of the separability hypothesis that we have already imposed and give the slightly wrong definition. Namely, if $\mathcal{P} \in \operatorname{MaxSpec} S$ and $\mathcal{P}$ lies over $\mathfrak{p} = \mathcal{P} \cap R$, let $f(\mathcal{P}|\mathfrak{p}) = [S/\mathcal{P} : R/\mathfrak{p}]$ be the residual degree. Then we define

$$N_{S/R}(\mathcal{P}) \coloneqq \mathfrak{p}^{f(\mathcal{P}|\mathfrak{p})}.$$

Having defined the norm on a basis for the free $\mathbb{Z}$-module of fractional S-ideals, it extends uniquely to a group homomorphism on $\operatorname{Frac} S$.

(Notice that in the classical case $R = \mathbb{Z}$, we are trying to define $N_{S/\mathbb{Z}}(\mathcal{P})$ as a nonzero ideal in $\mathbb{Z}$. If $\mathfrak{p} = (p)$ for a prime number p, then our definition gives $N_{S/R}(\mathcal{P}) = (p^{f(\mathcal{P}:\mathfrak{p})})$. Notice that $p^{f(\mathcal{P}:\mathfrak{p})}$ is the cardinality of the residue field $S/\mathcal{P}$.

By multiplicativity, for any nonzero integral ideal I of $S = \mathbb{Z}_L$, we are getting $N_{S/Z}(I) = \#S/I$. This idea that the norm of an ideal is measuring its index can be extended to the general case with some module-theoretic considerations, leading to the right definition of the ideal norm.)

THEOREM 3.12. *Let R be a Dedekind domain with fraction field K, let L/K be a finite degree separable field extension, and let S be the integral closure of R in L. Let $I \in \operatorname{Frac} B$, and let $N_{L/K} : L \to K$ be the field norm. Then:*

a) *We have that $N_{S/R}(I)$ is $\langle N_{L/K}(\alpha) \mid \alpha \in I \rangle$.*
b) *If $I = (\alpha)$ is principal, then $N_{S/R}(I) = (N_{L/K}(\alpha))$.*

THEOREM 3.13. *Let R be a Dedekind domain with fraction field K, let L/K be a finite degree separable field extension, and let S be the integral closure of R in L. Then we have:*

a)
$$N_{S/R}(\mathbb{D}_{S/R}) = \Delta_{S/R}.$$
b) *For $\mathcal{P} \in \operatorname{MaxSpec} S$, let $\mathfrak{p} = \mathcal{P} \cap R$. Then $d(\mathcal{P}|\mathfrak{p}) \geq 1$ iff $\mathcal{P}/\mathfrak{p}$ is ramified: that is, either $e(\mathcal{P}|\mathfrak{p}) > 1$ or the residual extension is inseaprable.*

PROOF. a) See [**Su.12**, Thm. 12.16]. b) See [**Su.12**, Thm. 12.19]. □

Thus the different ideal $\mathbb{D}_{S/R}$ is an "upstairs version" of the discriminant ideal $\Delta_{S/R}$, first in the sense that the norm of the different is the discriminant, and second that whereas the discriminant is measuring, in particular, which downstairs primes are ramified, the different is measuring, in particular, which upstairs primes are ramified.

The definition we gave of the discriminant allows for a straightforward computation of it provided one has an explicit basis for S/R. In general, S need not be a free R-module, but that is not necessarily the sticking point since the discriminant can be computed locally and just by computing the discriminant $\Delta(x_1, \ldots, x_n)$ of any set of F-linearly independent elements of S one gets an upper bound on the set of primes of R that could divide $\Delta_{S/R}$. However, even computing local integral bases is not trivial.

For the different, in contrast, the definition we gave involves computing a lattice dual and then inverting the ideal, which is a bit less explicit. The following results allow one to do better.

THEOREM 3.14. *Let R be a Dedekind domain with fraction field K, let L/K be a finite degree separable field extension, and let S be the integral closure of R in L.*

a) *Suppose that S is monogenic over R: that is, $S = R[x]$ for some $x \in S$. Let $f \in R[t]$ be the minimal polynomial of x. Then*
$$\mathbb{D}_{S/R} = (f'(x)).$$
b) *In general, for an element $x \in B$, let $f_x \in R[t]$ be its minimal polynomial. Then $\mathbb{D}_{S/R}$ is the ideal generated by all elements $f'(x)$ such that $x \in S$ and $L = K(x)$.*

Keeping the above situation, if we have $\mathcal{P} \in \operatorname{MaxSpec} S$ lying over $\mathfrak{p} \in \operatorname{MaxSpec} R$, we say that $\mathcal{P}$ is **tamely ramified** if the ramification index $e(\mathcal{P}|\mathfrak{p})$ is not divisible by the characteristic of $R/\mathfrak{p}$, the characteristic of the residual fields and the residual

extension $R/pp \subset S/\mathcal{P}$ is separable. Two immediate comments: first, this means that if the residual characteristic is 0 – which in the function field case holds iff the ground field k has characteristic 0 – then this holds automatically. Second, unramified implies tamely ramified.

THEOREM 3.15 (Dedekind). *Let R be a Dedekind domain with fraction field K, let L/K be a finite degree separable field extension, and let S be the integral closure of R in L. Suppose that $\mathcal{P} \in \operatorname{MaxSpec} S$ lies over $\mathfrak{p} \in \operatorname{MaxSpec} R$ and is tamely ramified. Then*

$$d(\mathcal{P}|\mathfrak{p}) = e(\mathcal{P}|\mathfrak{p}) - 1.$$

We say that an extension S/R is **tame** if every $\mathcal{P} \in \operatorname{MaxSpec} R$ is tamely ramified: again, this is automatic if all the residue fields have characteristic 0, which occurs for instance if R contains a field of characteristic 0. Thus in the tamely ramified case Theorem 3.15 reduces the computation of the different to the question of which upstairs primes are ramified.

3. The Different of a Finite Separable Extension of Function Fields

Let K/k be a regular function field. And let L/K be a finite degree separable extension with constant field l. It will turn out to be exceedingly fruitful to consider the analogues of the discriminant ideal and the different ideal in this case.

First we can define an effective divisor $\Delta(L/K) \in \operatorname{Div}^+(K)$. Namely, let R be an affine Dedekind domain with fraction field K, and let S be its integral closure in in L. Since L/K is separable, $\Delta(S/R)$ is a nonzero ideal of the Dedekind domain R and thus is expressed as $\prod_{P \in \operatorname{MaxSpec} R} P^{\delta_P(S/R)}$. The discriminant can be computed locally in the sense that if we let S_P be the integral closure of R_P in L, then S_P is a semilocal Dedekind domain whose maximal ideals correspond to the finite nonempty set of places Q of L lying over P. Then we have

$$\Delta(S_P/R_P) = (PR_P)^{(\delta_{S/R})_P}.$$

This shows in particular that the non-negative integer $(\delta_{S/R})_P$ is independent of the chosen affine coordinate chart, and that for all put finitely many $P \in \Sigma(K/k)$ we have $(\delta_{S/R})_P = 0$. Therefore we get a well-defined effective divisor

$$\Delta_{L/K} \coloneqq \sum_{P \in \Sigma(K/k)} \delta_P(S_P/R_P)P \in \operatorname{Div}^+(K).$$

Moreover, NTI shows that $\Delta_{S/R}$ is supported at the set of places of K that ramify in L: that is, for which there is at least one place $Q \mid P$ of L such that $e(Q|P) > 1$ or the residual extension l_Q/k_P is inseparable.

In a similar way we can define a **different divisor**

$$\mathbb{D}(L/K) \coloneqq \sum_{P \in \Sigma(K/k)} \mathbb{D}(L/K)_P \in \operatorname{Div}^+(L).$$

Here $\mathbb{D}(L/K)_P$ is the different ideal of the extension S_P/R_P of Dedekind domains, viewed as an effective divisor with support contained in the set of $Q \in \Sigma(L/)$ such that $Q \mid P$. For all $P \in \Sigma(K/k)$ we have

$$N_{L/K}(\mathbb{D}(S_P/R_P)) = \Delta(S_P/R_P),$$

so $\mathbb{D}(L/K)_P = 0$ for all but finitely many P. For $Q \in \Sigma(L/l)$ with $Q \mid P$, the coefficient of Q in $\mathbb{D}(L/K)$ is nonzero iff $e(Q|P) > 1$ or l_Q/k_P is inseparable.

4. The Differential Pullback Theorem and the Riemann-Hurwitz Formula

Let K/k be a regular function field, and let L/K be a finite degree separable extension, and let l be the algebraic closure of k in L. By Lemmas 3.1 and 3.2, the extension l/k is separable of finite degree and the function field L/l is regular.

Let $\omega \in \Omega_K^\bullet$ be a nonzero Weil differential. In this section we will define a canonical pullback $\omega^* \in \Omega_L^\bullet$. We will also compare the divisors (ω^*) and $\iota_{L/K}(\omega)$: the former is obtained by pulling back first and then taking the divisor, while the latter is obatined by taking the divisor first and then pulling back the divisor. One might hope that (ω^*) and $\iota_{L/K}((\omega))$ are equal. It turns out that this holds iff the extension L/K is everywhere unramified. In fact the truth is much more interesting and more useful: the difference between the divisors turns out to be the different $\mathbb{D}(L/K)$, and taking degrees will give us a relation among the genus of K, the genus of L, and the ramification in the extension, the Riemann-Hurwitz formula.

We begin by defining an adelic trace map. The domain is however not all of $\mathcal{A}_L$ but the following L-subspace:

$$\mathcal{A}_{L/K} \coloneqq \{\alpha \in \mathcal{A}_L \mid \alpha_{Q_1} = \alpha_{Q_2} \text{ if } Q_1, Q_2 \mid P\}.$$

For $D \in \mathrm{Div}(L)$ we put

$$\mathcal{A}_{L/K}(D) \coloneqq \mathcal{A}_{L/K} \cap \mathcal{A}_L(D).$$

We define a K-linear trace map

$$\mathrm{Tr}_{L/K} : \mathcal{A}_{L/K} \to \mathcal{A}_K,$$

as follows: for $\alpha \in \mathcal{A}_{L/K}$ and $P \in \Sigma(K/k)$, we put

$$(\mathrm{Tr}_{L/K}(\alpha))_P \coloneqq \mathrm{Tr}_{L/K}(\alpha_Q) \text{ for any } Q \mid P\ .$$

This map is well-defined precisely because any two components of α corresponding to places of L lying over the same place of K are equal. If $Q \mid P$, then since R_P is integrally closed, we have $\mathrm{Tr}_{L/K}(R_Q) \subset R_P$, and since for each $v_Q(\alpha_Q) \geq 0$ for all but finitely many Q, it follows that $v_Q(\mathrm{Tr}_{L/K}(\alpha_Q)) \geq 0$ for all but finitely many P, so $\mathrm{Tr}_{L/K}(\alpha) \in \mathcal{A}_K$.

THEOREM 3.16. *Let K/k be a regular function field and let L/K be a finite degree separable extension, with constant field l. Let $\omega \in \Omega_K$. There is a unique differential $\omega^* \in \Omega_L$ such that*

$$\forall \alpha \in \mathcal{A}_{L/K},\ \mathrm{Tr}_{l/k}\, \omega^*(\alpha) = \omega(\mathrm{Tr}_{L/K}(\alpha)). \tag{12}$$

Our notation ω^* is a bit light: it does not exhibit the field extension L/K. When necessary to include this in the notation, we write $\mathrm{Cotr}_{L/K}(\omega)$ for ω^*.

We will prove Theorem 3.16 along with another result to be stated soon, but first we state a corollary that shows how to take advantage of the uniqueness of ω^* subject to (12).

COROLLARY 3.17. *Maintain the setup of Theorem 3.16.*

a) *For $\omega_1, \omega_2 \in \Omega_K$, we have $(\omega_1 + \omega_2)^* = \omega_1^* + \omega_2^*$.*
b) *For $f \in K$ and $\omega \in \Omega_K$, we have $(f\omega)^* = f\omega^*$.*
c) *If M/L is finite separable, then we have*

$$\mathrm{Cotr}_{M/K}(\omega) = \mathrm{Cotr}_{L/K}(\mathrm{Cotr}_{M/L}(\omega)).$$

PROOF. a) For all $\alpha \in \mathcal{A}_{L/K}$, we have

$$\mathrm{Tr}_{l/k}((\omega_1^* + \omega_2^*)(\alpha)) = \mathrm{Tr}_{l/k}(\omega_1^*(\alpha) + \omega_2^*(\alpha))$$

$$= \mathrm{Tr}_{l/k}(\omega_1^*(\alpha)) + \mathrm{Tr}_{l/k}(\omega_2^*(\alpha)) = \omega_1(\mathrm{Tr}_{L/K}(\alpha)) + \omega_2(\mathrm{Tr}_{L/K}(\alpha))$$

$$= (\omega_1 + \omega_2)(\mathrm{Tr}_{L/K}(\alpha)).$$

By the uniqueness of pullback subject to (12), this shows that $(\omega_1+\omega_2)^* = \omega_1^*+\omega_2^*$.
b) For all $\alpha \in \mathcal{A}_{L/K}$, we have

$$\mathrm{Tr}_{l/k}((f\omega^*)(\alpha)) = \mathrm{Tr}_{l/k}(\omega^*(f\alpha))$$

$$= \omega(\mathrm{Tr}_{L/K}(f\alpha)) = \omega(f\,\mathrm{Tr}_{L/K}(\alpha)) = (f\omega)(\mathrm{Tr}_{L/K}(\alpha)),$$

so as above we deduce that $f\omega^* = (f\omega)^*$.
c) Let m be the constant subfield of M. The key fact is that for a tower of finite degree field extensions $A \subset B \subset C$ we have $\mathrm{Tr}_{C/A} = \mathrm{Tr}_{B/A} \circ \mathrm{Tr}_{C/B}$. Then for all $\alpha \in \mathcal{A}_{M/K}$, we have

$$\omega(\mathrm{Tr}_{M/K}(\alpha)) = \omega(\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha)))$$

$$= \mathrm{Tr}_{l/k}(\mathrm{Cotr}_{L/K}(\omega)(\mathrm{Tr}_{M/L}(\alpha)))$$

$$= \mathrm{Tr}_{l/k}(\mathrm{Tr}_{m/l}(\mathrm{Cotr}_{M/L}(\mathrm{Cotr}_{L/K}(\omega)))(\alpha))$$

$$= \mathrm{Tr}_{m/k}(\mathrm{Cotr}_{M/L}(\mathrm{Cotr}_{L/K}(\omega))(\alpha)),$$

so as above we have $\mathrm{Cotr}_{M/L}(\mathrm{Cotr}_{L/K}(\omega)) = \mathrm{Cotr}_{M/K}(\alpha)$. □

THEOREM 3.18. *Let $K/k \subset L/l$ be a finite separable extension of function fields, let $\omega \in \Omega_K^\bullet$ be a nonzero Weil differential on K, and let ω^* be its pullback to Ω_L. Then we have*

$$(\omega^*) = \iota_{L/K}(\omega) + \mathbb{D}(L/K). \tag{13}$$

COROLLARY 3.19 (Riemann-Hurwitz Formula). *Let $K/k \subset L/l$ be a finite separable extension of function fields. Let g_K be the genus of K and let g_L be the genus of L.*

a) *We have*

$$2g_L - 2 - \frac{[L:K]}{[l:k]}(2g_K - 2) + \deg \mathbb{D}(L/K). \tag{14}$$

b) *Suppose that L/K is a tame extension: that is, for all $P \in \Sigma(K/k)$ and all $Q \in \Sigma(L/l)$ with $Q \mid P$, we have that $e(Q|P)$ is indivisible by the characteristic of k and the residual extension l_Q/k_P is separable. Then we have*

$$2g_L - 2 = \frac{[L:K]}{[l:k]}(2g_K - 2) + \sum_{Q \in \Sigma(L/l)} (e(Q|P) - 1)\deg(Q). \tag{15}$$

PROOF. a) This comes from taking degrees in (13), since the divisor of a nonzero Weil differential on a function field of genus g has degree $2g-2$ (Exercise 2.15) and that $\deg \iota_{L/K}(D) = \frac{[L:K]}{l:k} \deg(D)$ (Proposition 3.7).
b) We have

$$\deg \mathbb{D}(L/K) = \sum_{Q \in \Sigma(L/K} d(Q|P) \deg(Q).$$

Since each $\mathcal{P} \mid \mathfrak{p}$ is tame, by Theorem 3.15 we have $d(Q|P) = e(Q|P) - 1$. Plugging this into (14), we get (15). □

EXERCISE 3.4. *Let $K/k \subset L/l$ be a finite, separable degree n extension of function fields. Let g_K be the genus of K, and let g_L be the genus of L.*

a) *Suppose that L/K is unramified. Show:*

$$g_L = 1 + n(g_K - 1).$$

b) *Suppose $g_K = 1$. Show that $g_L = 1$ iff L/K is unramified.*

5. Proofs of Theorems 3.16 and 3.18

5.1. Uniqueness of ω^*.

LEMMA 3.20. *For all $D \in \operatorname{Div} L$, we have*

$$\mathcal{A}_L = \mathcal{A}_{L/K} + \mathcal{A}_L(D).$$

PROOF. Let $\alpha \in \mathcal{A}_L$. By Artin-Whaples Approximation [**NTII**, Thm. 1.9], for all $P \in \Sigma(K/k)$ there is $x_P \in L$ such that

$$\forall Q \mid P,\ v_Q(\alpha_Q - x_P) \geq -v_Q(D). \tag{16}$$

Away from a finitely many Q's we have $-v_Q(D) = 0$ and $v_Q(\alpha_Q) \geq 0$, so we must have $v_Q(x_P) \geq 0$ or otherwise $v_Q(\alpha_Q - x_P) = v_Q(x_P) < 0$, contradicting (16). So taking $\beta_Q = x_P$ we get $\beta \in \mathcal{A}_{L/K}$. Moreover by construction we have $\alpha - \beta \in \mathcal{A}_L(D)$, so

$$\alpha = \beta + (\alpha - \beta) \in \mathcal{A}_{L/K} + \mathcal{A}_L(D).$$ □

We now prove that there is at most one $\omega^* \in \Omega_L$ satisfying (12). Indeed, suppose that there is also $\eta \in \Omega_L$ such that for all $\alpha \in \mathcal{A}_{L/K}$ we have

$$\operatorname{Tr}_{l/k}(\eta(\alpha)) = \operatorname{Tr}_{l/k}(\omega^*(\alpha)).$$

It follows that for all $\alpha \in \mathcal{A}_{L/K}$ we have

$$\operatorname{Tr}_{l/k}((\eta - \omega^*)(\alpha)) = 0.$$

Since $\eta - \omega^*$ is a Weil differential, there is $D \in \operatorname{Div}(L)$ such that $\eta - \omega^* \in \Omega_L(D))$. It follows that the k-linear functional

$$\lambda : \mathcal{A}_L \to k,\ \lambda(\alpha) \coloneqq \operatorname{Tr}_{l/k}((\eta - \omega^*)(\alpha))$$

vanishes on both $\mathcal{A}_{L/K}$ and $\mathcal{A}_L(D)$, so by Lemma 3.20 we have that $\lambda = 0$. Now $\eta - \omega^* : \mathcal{A}_L \to l$ is an l-linear functional, so if it is nonzero it is surjective; since $\operatorname{Tr}_{l/k}$ is also surjective since l/k is separable, we would have

$$0 = \lambda(\mathcal{A}_L) = \operatorname{Tr}_{l/k}((\eta - \omega^*)(\mathcal{A}_L)) = \operatorname{Tr}_{l/k}(l) = k,$$

a contradiction. Thus $\eta = \omega^*$, completing the proof of uniqueness.

5.2. Existence of ω^* and the Differential Pullback Formula.

LEMMA 3.21. *Let M/L be a finite degree separable field extension, let V be an M-vector space, and let $\mu : V \to L$ be an L-linear functional. There is a unique M-linear functional $\mu_M : V \to M$ such that*

$$\mathrm{Tr}_{M/L} \circ \mu_M = \mu.$$

PROOF. Once again the uniqueness is easier: suppose that also $\eta : V \to M$ is an M-linear functional such that

$$\mathrm{Tr}_{M/L} \circ \eta = \mu.$$

Then

$$0 = \mu - \mu = \mathrm{Tr}_{M/L} \circ \mu_M - \mathrm{Tr}_{M/K} \circ \eta = \mathrm{Tr}_{M/K} \circ (\mu_M - \eta).$$

Since $\mu_M - \eta : V \to M$ is an M-linear functional, if it is not identically zero, it is surjective onto M. Since M/K is separable, the trace map $\mathrm{Tr}_{M/K}$ is surjective onto K. So if $\mu_M \neq \eta$ then $0 = \mathrm{Tr}_{M/K} \circ (\mu_M - \eta) = K$, a contradiction. So $\mu_M = \eta$.

As for the existence, we now write $W^\vee$ for the L-linear dual of an L-vector space (notice that an M-vector space is, in particular, an L-vector space!). Then the trace form $(x, y) \in M \times M \mapsto \mathrm{Tr}_{M/L}(xy)$ is nondegenerate [**FT**, Thm. 6.10]: this means that the associated map

$$M \to M^\vee, m \mapsto (x \in M \mapsto \mathrm{Tr}_{M/L}(mx))$$

is an L-vector space isomorphism. For $v \in V$, define $\lambda_v : M \to L$ by $\lambda_v(a) \coloneqq \mu(av)$. Then $\lambda_v \in M^\vee$, so there is a unique $z_v \in M$ such that for all $a \in M$ we have

$$\mu(av) = \lambda_v(a) = \mathrm{Tr}_{M/L}(z_v a).$$

Put $\mu_M(v) \coloneqq z_v$, so for all $a \in M$ and all $v \in V$ we have

$$\mu(av) = \mathrm{Tr}_{M/K}(a\mu_M(v)).$$

From this expression and the nondegeneracy of the trace form, it follows that μ_M is M-linear: for $v_1, v_2 \in V$ and $a \in M$ we have

$$\mathrm{Tr}_{M/K}(a\mu_M(v_1 + v_2)) = \mu(a(v_1 + v_2)) = \mu(av_1) + \mu(av_2)$$

$$= \mathrm{Tr}_{M/K}(a\mu_M(v_1)) + \mathrm{Tr}_{M/K}(a\mu_M(v_2)),$$

so $\mu_M(v_1 + v_2) - \mu_M(v_1) - \mu_M(v_2))$ lies in the kernel of the trace form hence is zero. Similarly for $v \in V$ and $a, m \in M$ we have

$$\mathrm{Tr}_{M/K}(a\mu_M(mv)) = \mu(a(mv)) = \mu((am)v)$$

$$= \mathrm{Tr}_{M/K}((am)\mu_M(v)) = \mathrm{Tr}_{M/K}(a(m\mu_M(v)),$$

and the nondegeneracy gives $\mu_M(mv) = m\mu_M(v)$. Setting $a = 1$ shows that

$$\mu = \mathrm{Tr}_{M/L} \circ \mu_M. \qquad \square$$

We now begin the proof proper. If $\omega = 0$, then we put $\omega^* = 0$, a trivial case of Theorem 3.16. Henceforth we assume that $\omega \in \Omega_K^\bullet$ is a nonzero Weil differential.

The following remark will be crucial: for $P \in \Sigma(K/k)$, let B_P be the integral closure of the DVR R_P in L, so B_P is a semilocal Dedekind domain. Let C_P denote the codifferent ideal:

$$C_P \coloneqq \{x \in L \mid \mathrm{Tr}_{L/K}(xB_P) \subset R_P\}.$$

This is the fractional B_P-ideal such that factoring the inverse gives us the local different exponents at the places $Q \mid P$. It follows that:

$$\forall\ z \in L,\ z \in C_P \iff \forall Q \mid P,\ v_Q(z) \geq -d(Q|P).$$

Now put

$$W \coloneqq \iota_{L/K}((\omega)) + \mathbb{D}(L/K).$$

Step 1: Put

$$\omega_1 \coloneqq \omega \circ \mathrm{Tr}_{L/K} : \mathcal{A}_{L/K} \to k.$$

This is a k-linear functional on $\mathcal{A}_{L/K}$. We claim that:

(1a) We have $\omega_1(\mathcal{A}_{L/K}(W) + L) = 0$, and

(1b) If $B \in \mathrm{Div}(L)$ is such that $B \not\leq W$, then there is $\beta \in \mathcal{A}_{L/K}(B)$ such that $\omega_1(\beta) \neq 0$.

Proof of (1a): Indeed the adelic trace map maps the diaongally embedded copy of L in $\mathcal{A}_L$ into the diagonally embedded copy of K in $\mathcal{A}_K$, so we wish to show that for $\alpha \in \mathcal{A}_{L/K}(W)$, we have $\omega_1(\alpha) = 0$. For this it is enough to show that for all $P \in \Sigma(K/k)$ and all $Q \mid P$ then

$$v_P(\mathrm{Tr}_{L/K}(\alpha_Q)) \geq -v_P((\omega)),$$

for then we have

$$\mathrm{Tr}_{L/K}(\alpha) \in \mathcal{A}_K((\omega)) \subset \mathrm{Ker}\,\omega.$$

To see this, choose $x \in K$ such that $v_P(x) = v_P((\omega))$. Then

$$v_Q(x\alpha_Q) \geq v_Q(x) + v_Q(\alpha_Q) \geq e(Q|P)v_P(x) - v_Q(W)$$
$$= v_Q(\iota_{L/K}((\omega)) - W) = -v_Q(\mathbb{D}(L/K)) = -d(Q|P).$$

By our remark above this shows that $x\alpha_Q \in C_P$, which by definition gives

$$0 \leq v_P(\mathrm{Tr}_{L/K}(x\alpha_Q)) = v_P(x\,\mathrm{Tr}_{L/K}(\alpha_Q)) = v_P(x) + v_P(\mathrm{Tr}_{L/K}(\alpha_Q))$$
$$= v_P((\omega)) + v_P(\mathrm{Tr}_{L/K}(\alpha_Q)),$$

and thus

$$v_P(\mathrm{Tr}_{L/K}(\alpha_Q)) \geq -v_P((\omega)).$$

Proof of (1b): Since $B \not\leq W$, there is $P_0 \in \Sigma(K/k)$ and $Q_0 \mid P_0$ such that F

$$v_{Q_0}(\iota_{L/K}((\omega)) - B) < -d(Q_0|P_0).$$

Let S_{P_0} be the integral closure of R_{P_0} in L and let C_{P_0} be the codifferent of S_{P_0}/R_{P_0}. Put

$$J \coloneqq \{z \in L \mid v_Q(z) \geq v_Q(\iota_{L/K}((\omega)) - B))\ \forall Q \mid P_0\},$$

a fractional S_{P_0}-ideal. By Weak Approximation, there is $u \in J$ such that

$$v_Q(u) = v_Q(\iota_{L/K}((\omega)) - B)\ \forall Q \mid P_0,$$

so by the remark at the beginning of the proof, we have $J \not\subset C_{P_0}$. Since $JS_{P_0} \subset J$ it follows that

$$\mathrm{Tr}_{L/K}(J) \not\subset R_{P_0}. \tag{17}$$

Choose $\pi \in K$ such that $v_{P_0}(\pi) = 1$. Then, since π has positive valuation at every place $Q \mid P_0$, there is $r \in \mathbb{N}$ such that $\pi^r J \subset S_{P_0}$, and thus

$$\pi^r\,\mathrm{Tr}_{L/K}(J) = \mathrm{Tr}_{L/K}(\pi^r J) \subset R_{P_0}.$$

Since $\pi^r\,\mathrm{Tr}_{L/K}(J_0)$ is an R_{P_0}-ideal and R_{P_0} is a DVR, there is $m \in \mathbb{Z}$ such that

$$\mathrm{Tr}_{L/K}(J) = \pi^m R_{P_0}.$$

By (17) we have $m \leq -1$, and thus

$$\pi^{-1} R_{P_0} \subset \mathrm{Tr}_{L/K}(J). \tag{18}$$

By Proposition 2.21a), there is $x \in K$ such that

$$v_{P_0}(x) = -v_{P_0}(\omega) - 1 \text{ and } \omega_{P_0}(x) \neq 0. \tag{19}$$

Choose $y \in K$ such that $v_{P_0}(y) = v_{P_0}(\omega)$; then

$$xy \in \pi^{-1} R_{P_0}.$$

By (18) there is $z \in J$ such that $\mathrm{Tr}_{L/K}(z) = xy$. Now we define $\beta \in \mathcal{A}_{L/K}$ by

$$\beta_Q \coloneqq \begin{cases} 0 & Q \nmid P_0 \\ y^{-1} z & Q \mid P_0 \end{cases}.$$

Then for all $Q \mid P_0$ we have

$$v_Q(\beta) = -v_Q(y) + v_Q(z) \geq -v_Q(\iota_{L/K}((\omega)) + v_Q(\iota_{L/K}((\omega)) - B) = -v_Q(B),$$

so $\beta \in \mathcal{A}_{L/K}(B)$. Finally, using (19) we get

$$\omega_1(\beta) = \omega(\mathrm{Tr}_{L/K}(\beta)) = \omega(\iota_{P_0}(\mathrm{Tr}_{L/K}(y^{-1} z)))$$

$$= \omega(\iota_{P_0}(y^{-1} \mathrm{Tr}_{L/K}(z))) = \omega(\iota_{P_0}(x)) = \omega_{P_0}(x) \neq 0.$$

Step 2: We define

$$\omega_2 : \mathcal{A}_L \to k$$

as follows: for $\alpha \in \mathcal{A}_L$, by Lemma 3.20 there is $\beta \in \mathcal{A}_{L/K}$ and $\gamma \in \mathcal{A}_L(W)$ such that $\alpha = \beta + \gamma$, and we put

$$\omega_2(\alpha) = \omega_1(\beta).$$

Let us check that ω_2 is well-defined: if $\alpha = \beta_1 + \gamma_1 = \beta_2 + \gamma_2$ with $\beta_i \in \mathcal{A}_{L/K}$ and $\gamma_i \in \mathcal{A}_L(W)$ for $i = 1, 2$, then

$$\beta_2 - \beta_1 = \gamma_1 - \gamma_2 \in \mathcal{A}_{L/K} \cap \mathcal{A}_L(W) = \mathcal{A}_{L/K}(W),$$

so by Step (1a) we have

$$\omega_1(\beta_2) - \omega_1(\beta_1) = \omega(\beta_2 - \beta_1) = 0.$$

The map ω_2 is k-linear and also satisfies:

- (2a) We have $\omega_2(\mathcal{A}_L(W) + L) = 0$, and
- (2b) If $B \in \mathrm{Div}\, L$ is such that $B \not\leq W$, then there is $\beta \in \mathcal{A}_L(B)$ such that $\omega_2(\beta) \neq 0$.

Step 3: The map ω_2 is a Weil differential on L iff $l = k$. If $l \supsetneq k$ we now fix this, as follows: by Lemma 3.21 there is an l-linear functional $\omega^* : \mathcal{A}_L \to l$ such that

$$\mathrm{Tr}_{l/k} \circ \omega^* = \omega_2.$$

Moreover, for $\alpha \in \mathcal{A}_{L/K}$ we have

$$\mathrm{Tr}_{l/k}(\omega^*(\alpha)) = \omega_2(\alpha) = \omega_1(\alpha) = \omega(\mathrm{Tr}_{L/K}(\alpha)). \tag{20}$$

As usual, we claim that

- (3a) We have $\omega^*(\mathcal{A}_L(W) + L) = 0$, and
- (3b) If $B \in \mathrm{Div}(L)$ is such that $B \not\leq W$, then there is $\beta \in \mathcal{A}_L(B)$ such that $\omega^*(\beta) \neq 0$.

Proof of (3a): Since ω^* is l-linear, the image of the l-subspace $\mathcal{A}_L(W) + L$ under ω^* is either 0 or all of l. In the latter case, because $\mathrm{Tr}_{l/k} : l \to k$ is surjective, there is $\alpha \in \mathcal{A}_L(W) + L$ such that

$$0 \neq \mathrm{Tr}_{l/k}(\omega^*(\alpha)) = \omega_2(\alpha),$$

contradicting (2a).
Proof of (3b): By (2b), there is $\beta \in \mathcal{A}_L(B)$ such that

$$0 \neq \omega_2(\beta) = \mathrm{Tr}_{l/k}(\omega^*(\beta)),$$

so $\omega^*(\beta) \neq 0$. This shows that $\omega^* \in \Omega_L^\bullet$ is a nonzero Weil differential that, by (20), satisfies the characteristic property (12) and completes the proof of Theorem 3.16. Moreover, properties (3a) and (3b) together give that W is the largest divisor B such that $\omega^* \in \Omega_L(B)$, so

$$(\omega^*) = W = \iota_{L/K}((\omega)) + \mathbb{D}(L/K),$$

completing the proof of Theorem 3.18.

6. Lüroth's Theorem

We will now apply the Riemann-Hurwitz Formula to give a proof of Lüroth's Theorem, so let k be any field, and let L be a field such that $k \subsetneq L \subset k(x)$. We wish to show that $L = k(f)$ for some $f \in k(x)$.

First, since $k(x)/k$ is regular, we must have $\mathrm{trdeg}(L/k) = 1$, hence $k(x)/L$ has finite degree. Moreover the constant subfield of L is again k, so $L/k(x)$ is a geometric extension.

Case 1: Suppose that the extension $k(x)/L$ is separable. Applying the Riemann-Hurwitz formula, we get

$$-2 = [k(x) : L](2g_L - 2) + \deg \mathbb{D}(k(x)/L).$$

Since the left hand side is negative, so is the right hand side, and the only way for this to happen is for $2g_L - 2$ to be negative, which implies that $g_L = 0$. Moreover, the place P_∞ of $k(x)$ has residue field k, so if $P = P_\infty \cap L$, then we have $k \subset k_P \subset k_{P_\infty} = k$, so also $k_P = k$. Thus L has genus zero and index 1 so is rational by Exercise 2.17: that is, $L = k(f)$ for some $f \in k(x)$.

Case 2: Suppose that the extension $k(x)/L$ is inseparable. There is therefore a subfield M with $k \subset L \subset M \subset k(x)$ such that M/L is separable and $k(x)/M$ is purely inseparable, say of degree p^a. Since $x \in M$, the extension $k(x)/M$ is generated by x, and like any monogenic purely inseparable extension of degree p^a, we have that a is the least positive integer A such that $x^{p^A} \in M$. Thus we have $k \subset k(x^{p^a}) \subset M \subset k(x)$. But by [**FT**, Thm. 11.1] we have that $[k(x) : k(x^{p^a})] = p^a = [k(x) : M]$, so $M = k(x^{p^a})$. We may now apply Step 1 with $k \subset L \subset k(x^{p^a})$ to get that $L = k(f)$.

7. Separable Constant Extensions

Let K/k be a regular function field, and let $\overline{k}$ be an algebraic closure of k. Regularity is equivalent to $K\overline{k} = K \otimes_k \overline{k}$ being a function field over $\overline{k}$. Let $\alpha \in \overline{k}$ and let $f \in k[t]$ be its minimal polynomial. Then

$$k[t]/(f) \cong k(\alpha),$$

so

$$K[t]/(f) = k[t]/(f) \otimes_k K \cong k(\alpha) \otimes_k K = K(\alpha),$$

which shows that f remains irreducible over K and thus

$$[k(\alpha) : k] = \deg(f) = [K(\alpha) : K].$$

Moreover, we have that α is separable over k iff $f \in k[t]$ is separable iff $f' \neq 0$ [**FT**, Prop. 5.2] ifff $f \in K[t]$ is separable iff α is separable over K.

THEOREM 3.22. *Let K/k be a regular function field, let l/k be a **separable** algebraic field extension, and put $L \coloneqq Kl$. Then:*

a) *The extension L/K is everywhere unramified: for all $Q \in \Sigma(L/l)$ and $P \in \Sigma(K/k)$ with $Q \mid P$, we have $e(Q|P) = 1$.*
b) *Let g_K be the genus of K and g_L be the genus of L. Then: $g_K = g_L$.*
c) *For all $D \in \mathrm{Div}(K)$, we have $\deg \iota_{L/K}(D) = \deg D$.*
d) *Let $D \in \mathrm{Div}(K)$. Then every k-basis of $\mathcal{L}(D)$ is an l-basis of $\mathcal{L}(\iota_{L/K}(D))$. In particular we have*

$$\ell(\iota_{L/K}(D)) = \ell(D).$$

e) *For $D \in \mathrm{Div}(K)$, we have that D is canonical iff $\iota_{L/K}(D)$ is canonical.*
f) *The induced maps*

$$\mathrm{Cl}(K) \hookrightarrow \mathrm{Cl}(L), \ \mathrm{Cl}^0(K) \hookrightarrow \mathrm{Cl}(L)$$

are injective.
g) *Let $Q \in \Sigma(L/l)$ and $P \in \Sigma(K/k)$ with $Q \mid P$, then we have*

$$l_Q = k_P l.$$

h) *If l/k has finite degree and $\alpha_1, \ldots, \alpha_n$ is a k-basis for l, then for all $P \in \Sigma(K/k)$, let S_P be the integral closure of R_P in L. Then $\alpha_1, \ldots, \alpha_n$ is a basis for S_P over R_P.*

PROOF. Step 1: First we assume that l/k has finite degree n and prove parts a) and b) in this case as well as part h), which is only stated in this case. Let $l = k(\alpha)$, so $L = K(\alpha)$, and let $f \in k[t]$ be the minimal polynomial of α. Since f is separable we have $f'(\alpha) \in l^\times$ and thus for all $Q \mid P$ we have $v_Q(f'(\alpha)) = 0$. By Theorem 3.14 this implies that the local different exponent $d(Q|P)$ is zero and thus that $e(Q|P) = 1$. The Riemann-Hurwitz formula gives

$$2g_L - 2 = \frac{[L : K]}{[l : k]}(2g_K - 2) + \deg \mathbb{D}(L/K) = 2g_K - 2,$$

so $g_K = g_L$. As for h), consider first the power k-basis $1, \alpha, \ldots, \alpha^{n-1}$ of l. As for any k-basis of a finite degree separable field extension l/k we have $\Delta(1, \alpha, \ldots, \alpha^{n-1}) \in l^\times$. Now viewing $1, \alpha, \ldots, \alpha^{n-1}$ as elements of S_P, the same calculation shows that

$\Delta(1,\dots,\alpha^{n-1})$ has valuation 0 at every place $Q \mid P$, which implies that the R_P-module spanned by $1,\alpha,\alpha^{n-1}$ must be all of S_P. If $\gamma_1,\dots,\gamma_n$ is any other k-basis of l, we see immediately that

$$\langle \gamma_1,\dots,\gamma_n\rangle_{R_p} = \langle 1,\alpha,\dots,\alpha^{n-1}\rangle_{R_p} = S_P.$$

Step 2: We suppose that l/k is algebraic and prove parts a) through g).
a) Let $Q \in \Sigma(L/l),\ P \in \Sigma(K/k)$ with $Q \mid P$. Let $t \in L$ be a uniformizer at Q. There is a subfield $k \subset k_1 \subset l$ such that $[k_1 : k]$ is finite and $t \in K_1 \coloneqq Kk_1$. Let

$$P_1 \coloneqq Q \cap K_1.$$

Then we have

$$1 = v_Q(t) = e(Q|P_1)v_{P_1}(t),$$

so $e(Q|P_1) = 1$. By Step 1 we have $e(P_1|P) = 1$, and thus

$$e(Q|P) = e(Q|P_1)e(P_1|P) = 1.$$

c) It is enough to consider the case of a prime divisor $P \in \Sigma(K/F)$. By Riemann-Roch there is $f \in K$ such that $(f)_+ = rP$ for some $r \in \mathbb{Z}^+$. Let D_+ be the positive part of the divisor of f viewed as an element of L. By Lemma 3.6 we have

$$D_+ = \iota_{L/K}((f)_+) = r\iota_{L/K}(P).$$

Since $\deg D_+ = [L : l(x)]$, we get

$$r\deg \iota_{L/K}(P) = [L : l(x)] = [K : k(x)] = \deg(f)_+ = r\deg(P),$$

so

$$\deg \iota_{L/K}(P) = \deg(P).$$

b) Let $D \in \mathrm{Div}(K)$. If $x_1,\dots,x_r$ is a k-basis for $\mathcal{L}(D)$ then for all $1 \le i \le r$ we have $x_i \in \mathcal{L}(\iota_{L/K}(D))$, and linear disjointness of K and l over k implies that $x_1,\dots,x_r$ are l-linearly independent, so we have

$$\ell(D) \le \ell(\iota_{L/K}(D)). \tag{21}$$

Now choose $C \in \mathrm{Div}(K)$ satisfying

$$\deg(C) \ge \max(2g_K - 1, 2g_L - 1).$$

By Riemann-Roch we have

$$\ell(C) = \deg(C) - g_K + 1,\ \ell(\iota_{L/K}(C)) = \deg(\iota_{L/K}(C)) - g_L + 1 = \deg(C) - g_L + 1,$$

and combining this with (21) we find that

$$g_K \ge g_L.$$

Next consider a basis $u_1,\dots,u_s$ of $\mathcal{L}(\iota_{L/K}(C))$. There is a field $k \subset k_2 \subset l$ with $[k_2 : k]$ finite and $u_1,\dots,u_s \in K_2 \coloneqq Kl_2$. We have $u_1,\dots,u_s \in \mathcal{L}(\iota_{K_2/K}(C))$, so

$$\ell(\iota_{K_2/K}(C)) \ge \ell(\iota_{L/K}(C)).$$

From Step 1 we know that $g_{K_2} = g_K$, so Riemann-Roch yields

$$\ell(\iota_{K_2/K}(C)) = \deg(C) - g_K + 1.$$

Therefore

$$\deg(C) - g_K + 1 \ge \ell(\iota_{L/K}(C)) = \deg(C) + 1 - g_L,$$

so

$$g_K \le g_L.$$

We conclude that $g_K = g_L$. Henceforth we denote all genera simply by g.
d) Suppose first that $\deg D \geq 2g-1$. Then

$$\ell(\iota_{L/K}(D)) - \deg \iota_{L/K}(D)) - g + 1 = \deg(D) - g + 1 = \ell(D).$$

Above we showed that any k-linearly independent subset of $\mathcal{L}(D)$ remains l-linearly independent in $\mathcal{L}(\iota_{L/K}(D))$, so any k-basis of $\mathcal{L}(D)$ is an l-basis of $\mathcal{L}(\iota_{L/K}(D))$. Now consider an arbitrary divisor $D \in \operatorname{Div}(K)$, and let $x_1, \ldots,_r$ be a k-basis for $\mathcal{L}(D)$. Once again we know that $x_1, \ldots, x_r$ remains l-linearly independent in $\mathcal{L}(\iota_{L/K}(D))$, so it suffices to show that each $z \in \mathcal{L}(\iota_{L/K}(D))$ is an l-linear combination of $x_1, \ldots, x_r$.

To see this we choose distinct $P_1, P_2 \in \Sigma(K/k)$ and put

$$D_1 \coloneqq A + n_1 P_1,\ D_2 \coloneqq A + n_2 P_2$$

for $n_1, n_2 \in \mathbb{N}$ that are sufficiently large so that $\deg(D_i) \geq 2g_K - 1$ for $i = 1, 2$. Our definition of D_1 and D_2 is such that $D = \inf(D_1, D_2)$ in the complete lattice $\operatorname{Div} K$, so for all $x \in K^\times$ we have

$$(x) \geq -D \iff (x) \geq -D_1 \text{ and} (x) \geq -D_2$$

and thus

$$\mathcal{L}(D) = \mathcal{L}(D_1) \cap \mathcal{L}(D_2).$$

We may extend $x_1, \ldots, x_r$ to k-bases $\begin{cases} x_1, \ldots, x_r, y_1, \ldots, y_m \text{ of } \mathcal{L}(D_1) \\ x_1, \ldots, x_r, z_1, \ldots, z_n \text{ of } \mathcal{L}(D_2) \end{cases}$.
We claim that $x_1, \ldots, x_r, y_1, \ldots, y_m, z_1, \ldots, z_n$ are k-linearly independent and hence by the linear disjointness of K and l over k, also l-linearly independent. To see this, let $a_i, b_k, c_k \in k$ be such that

$$\sum_{i=1}^{r} a_i x_i + \sum_{j=1}^{m} b_j y_j + \sum_{k=1}^{n} c_k z_k = 0.$$

Then

$$\sum_{i=1}^{r} a_i x_i + \sum_{j=1}^{m} b_j y_j = -\sum_{k=1}^{n} c_k z_k \in \mathcal{L}(D_1) \cap \mathcal{L}(D_2) = \mathcal{L}(D).$$

This implies that $b_j = 0$ for all j which then in turns forces $a_i = c_k = 0$ for all i and k because $x_1, \ldots, x_r, z_1, \ldots, z_m$ are k-linearly indpendent, establishing the claim.

Now let $z \in \mathcal{L}(\iota_{L/K}(D))$. Since $\deg(A_1), \deg(A_2) \geq 2g-1$, by what we proved above there are $d_i, e_j, f_i, g_k \in l$ such that

$$z = \sum_{i=1}^{r} a_i x_i + \sum_{j=1}^{m} b_j y_j = \sum_{i=1}^{r} c_i x_i + \sum_{k=1}^{n} d_k z_k.$$

The l-linear indendence of the x_i, y_j, z_k implies that $a_i = c_i$ for all $1 \leq i \leq r$, $b_j = 0$ for all $1 \leq j \leq m$ and $d_k = 0$ for all $1 \leq k \leq n$, and thus z lies in the l-span of $x_1, \ldots, x_r$, as we wanted to show.
e) Let $W \in \operatorname{Div}(K/k)$. We now know that

$$\deg \iota_{L/K}(W) = 2g - 2 \text{ and } \ell(\iota_{L/K}(W)) = g.$$

By Proposition 2.12, it follows that W is canonical iff $\iota_{L/K}(W)$ is canonical.
f) It is enough to show that the homomorphism $\mathrm{Cl}(K) \to \mathrm{Cl}(L)$ is injective, for then the homomorphism $\mathrm{Cl}^0(K) \to \mathrm{Cl}^0(L)$ is obtained by restricting to the subgroup $\mathrm{Cl}^0(K)$ (and has image contained in $\mathrm{Cl}^0(L)$ by part c)), so is certainly injective. So

let $D \in \mathrm{Div}(K)$ be such that $\iota_{L/K}(D)$ is principal. This means that $\deg \iota_{L/K}(D)) = 0$ and $\ell(\iota_{L/K}(D)) = 1$. By parts c) and d) it follows that $\deg(D) = 0$ and $\ell(D) = 1$, which by Exercise 2.12 implies that D is principal.
g) Let $P \in \Sigma(K/k)$, $Q \in \Sigma(L/l)$ with $Q \mid P$: we want to show that $l_Q = k_P l$. Certainly l_Q contains both l and k_P, so $l_Q \supset k_P l$; the matter of it is to show the reverse inclusion.

We denote the reduction map $R_Q \to R_Q/\mathfrak{m}_Q = l_Q$ by $z \mapsto \overline{z}$. Let $z \in R_Q$. Then there is a subextension $k \subset k_3 \subset l$ with $z \in K_3 := Kk_3$ and $[k_3 : k] = n < \infty$. Let $\tilde{P}_1 = Q \cap K_3$ and let $\tilde{P}_2, \ldots \tilde{P}_r$ be the other places of $\Sigma(K_3/k_3)$ lying over P (if any: it may be that $r = 1$). By Weak Approximation, there is $u \in K_3$ such that

$$v_{\tilde{P}_1}(z - u) > 0, \ \forall 2 \le i \le r, \ v_{\tilde{P}_i}(u) \ge 0.$$

Then $\overline{z} = \overline{u}$, and since u has non-negative valuation at all places of K_3 lying over P it lies in the integral closure of R_P in K_3. By part h), there are $\gamma_1, \ldots, \gamma_n \in k_3$ and $x_1, \ldots, x_n \in R_P$ such that

$$u = \sum_{i=1}^n \gamma_i x_i,$$

so

$$\overline{z} = \overline{u} = \sum_{i=1}^n \gamma_i \overline{x_i} \in k_3 k_P \subset k_P l.$$

It follows that $l_Q \subset k_P l$ and thus $l_Q = k_P l$. □

Exercise 3.5. *We stated Clifford's Theorem (Theorem 2.25) for function fields over any field k, but in §2.6.5 we proved it only when k is infinite. Show that Clifford's Theorem holds also when k is finite.*

Now we assume that k is perfect: equivalently, we assume that any algebraic closure $\overline{k}$ of k is a separable field extension. In this case (and, alas, only in this case), we may apply Theorem 3.22 with $L = K\overline{k}$. Let us consider the restriction map

$$r : \Sigma(L/\overline{k}) \to \Sigma(K/k).$$

By Theorem 3.5, the map r is surjective with finite fibers. But in this case we can be much more precise:

Proposition 3.23. *Let $P \in \Sigma(K/k)$ have degree d and residue field k_P. There are exactly d places of $\Sigma(L/k)$ lying over P.*

Proof. Consider the subextension Kk_P/k_P, which is a separable extension of K/k that is finite of degree d. By Theorem 3.22g), for every place Q of Kk_P lying over P, the residue field is $k_P k_P = k_P$. One the one hand, this means that all the places $Q \mid P$ have degree 1, and on the other hand it means that $f(Q|P) = 1$ for all Q, and since we are unramified it follows that P splits completely: there are precisely d such places Q. Now we consider places R of $\Sigma(K\overline{k}/\overline{k})$ lying over any such place Q. If there were $R_1 \neq R_2$ each lying over the same Q, then there is $f \in K\overline{k}$ such that $v_{R_1}(f) \neq v_{R_2}(f)$. But every element $f \in K\overline{k}$ lives in Kl for some subextension $k_P \subset l \subset \overline{k}$ with l/k_P finite. Let $S_i := R_i \cap Kl$. Then

$$v_{S_1}(f) = \frac{v_{R_1}(f)}{e(S_1|R_1)} = v_{R_1}(f) \neq v_{R_2}(f) = \frac{v_{R_2}(f)}{e(S_2|R_2)} = v_{S_2}(f),$$

which shows that Q splits into at least two places S_1 and S_2 over the finite degree extension Kl/l. But this is impossible: Theorem 3.22g) implies that every degree 1 place is inert in every finite degree separable constant extension. This contradiction shows that there are indeed precisely d places of $L/\overline{l}$ lying over each $P \in \Sigma_d(K/k)$. □

EXERCISE 3.6. *Let K/k be a regular function field. Let $P \in \Sigma(K/k)$ such that the reisdue field k_P is separable of degree d over k. Let l/k be a separable algebraic field extension, and put $L \coloneqq Kl$. Show that the following are equivalent:*

(i) *There are at least d places $Q \in \Sigma(L/l)$ such that $Q \mid P$.*
(ii) *There are exactly d places $Q \in \Sigma(L/l)$ such that $Q \mid P$.*
(iii) *We have $k_P \subset l$.*

Still under the assumption that k is perfect, we put

$$L \coloneqq K\overline{k}$$

and consider

$$\mathfrak{g}_k \coloneqq \mathrm{Aut}(\overline{k}/k),$$

the absolute Galois group of k. Each $\sigma \in \mathfrak{g}_K$ extends uniquely to an element of $\mathrm{Aut}(L/K)$. Indeed, we have $L = K \otimes_k \overline{k}$, so we may – and must – put

$$\sigma\left(\sum_{i=1}^{n} x_i \otimes \alpha_i\right) \coloneqq \sum_{i=1}^{n} x_i \otimes \sigma(\alpha_i). \tag{22}$$

This defines a map $\mathfrak{g}_k \to \mathrm{Aut}(L/K)$.

EXERCISE 3.7. *Let K/k be a regular function field, and let l/k be any algbraic extension (not necessarily of finite degree). Let $L \coloneqq Kl = K \otimes_k l$.*

a) *Show: the formula (22) works to define a map $\Phi : \mathrm{Aut}(l/k) \to \mathrm{Aut}(L/K)$, which is an isomorphism of groups.*
b) *Show: l/k is normal iff L/K is normal.*
c) *Show: l/k is separable iff L/K is separable.*
d) *Show: l/k is Galois iff L/K is Galois, and in this case the isomorphism Φ is also a homeomorphism when both Galois groups are given the Krull topology.*

There is an induced action of $\mathfrak{g}_K$ on $\Sigma(L/\overline{l})$. For $Q \in \Sigma(L/\overline{l})$ and $\sigma \in \mathfrak{g}_K = \mathrm{Aut}(L/K)$, the image $\sigma(R_Q)$ of the discrete valuation ring under the field automorphism σ is again a discrete valuation ring of L containing $\sigma(\overline{k}) = \overline{k}$, so there is a unique place $\sigma(Q) \in \Sigma(L/\overline{l})$ such that

$$\sigma(R_Q) = R_{\sigma(Q)}.$$

EXERCISE 3.8. *Let $Q \in \Sigma(L/\overline{k})$ and $\sigma \in \mathfrak{g}_k = \mathrm{Aut}(L/K)$.*

a) *Show:*
$$v_{\sigma(Q)} = v_Q \circ \sigma^{-1}.$$
b) *Show: if $Q \mid P$, then $\sigma(Q) \mid P$.*

Thus we have an action of $\mathfrak{g}_k$ on $\Sigma(L/\overline{k})$ that preserves the fibers of the map

$$r : \Sigma(L/\overline{k}) \to \Sigma(K/k).$$

PROPOSITION 3.24. *Let K/k be an algebraic function field over a perfect field k. Let $L := K\overline{k}$.*

a) *The fibers of the map $r : \Sigma(L/\overline{k}) \to \Sigma(K/k)$ are precisely the $\mathfrak{g}_k$-orbits on $\Sigma(L/\overline{k})$.*
b) *It follows that if $P \in \Sigma(K/k)$ has degree d, then for all $\tilde{P} \in \Sigma(L/\overline{k})$ with $\tilde{P} \mid P$, the $\mathfrak{g}_k$-orbit on $\tilde{P}$ has size d.*

PROOF. Let l be the Galois closure of k_P/k, so l/k is finite Galois, and put $L' := Kl$. By Exercise 3.7 the extension L'/K is finite Galois, with automorphism group canonically isomorphic to $\mathrm{Aut}(l/k)$. By Exercise 3.5 there are precisely d places $Q_1, \ldots, Q_d$ of $\Sigma(L'/l)$ lying over P. Choose an affine Dedekind domain A of K such that $A \subset R_P$, and let B be the integral closure of A in L'. Then $P \in \mathrm{MaxSpec}\, A$ and $Q_1, \ldots, Q_d$ are precisely the maximal ideals of B that lie over P, so by NTI we have that $\mathrm{Aut}(L'/K) = \mathrm{Aut}(l/k)$ acts transitively on the Q_i's. By Exercise 3.7 (so really, by the proof of Proposition 3.24), none of Q_i's split any further in L'/L: for $1 \leq i \leq d$ there is a uique $\tilde{P}_i \in \Sigma(L/\overline{k})$ with $\tilde{P}_i \mid Q_i$. It follows that for all $\sigma \in \mathfrak{g}_l = \mathrm{Aut}(\overline{k}/l)$ and all $1 \leq i \leq d$ we have $\sigma(\tilde{P}_i) = \tilde{P}_i$ and thus the $\mathfrak{g}_k$-action on $\{\tilde{P}_1, \ldots, \tilde{P}_d\} = r^{-1}(P)$ factors through $\mathrm{Aut}(l/k)$ and coincides with the transitive $\mathrm{Aut}(l/k)$-action on $\{Q_1, \ldots, Q_d\}$. This proves part a), and part b) follows from part a) and Proposition 3.23. □

Contemplation of the $\mathfrak{g}_k$-action on $\Sigma(L/\overline{k})$ is a big part of the way I think about rational points (and lack thereof) on algbraic curves. In particular, the "rational points on the curve corresponding to K' – that is, the degree 1 places of K – can be identified with the fixed points of the $\mathfrak{g}_k$-action on $\Sigma(L/\overline{k})$ and that the least degree of a place on K is the least size of a $\mathfrak{g}_k$-orbit on $\Sigma(L/\overline{k})$, which is *also* equal to the minimal degree of a constant extension necessary in order to attain a degree 1 place.

Since $\mathfrak{g}_k$ acts on $\Sigma(L/\overline{k})$, it also acts on $\mathrm{Div}\, L$ simply by mapping P to $\sigma(P)$ and extending $\mathbb{Z}$-linearly. Now we have an action of $\mathfrak{g}_K$ on a $\mathbb{Z}$-module, or in other words, a "$\mathfrak{g}_k$-module structure" on $\mathrm{Div}\, L$. Whenever a G acts on a $\mathbb{Z}$-module M by $\mathbb{Z}$-linear automorphisms of M, we put

$$M^G := \{x \in M \mid gx = x \ \forall g \in G\}.$$

Since $\iota_{L/K} : \mathrm{Div}\, K \hookrightarrow \mathrm{Div}\, L$ is an injection, we may – and shall – identify $\mathrm{Div}\, K$ with its image in $\mathrm{Div}\, L$.

PROPOSITION 3.25. *We have $(\mathrm{Div}\, L)^{\mathfrak{g}_k} = \mathrm{Div}\, K$.*

PROOF. The image of $\mathrm{Div}\, K$ in $\mathrm{Div}\, L$ consists of divisors D such that $v_{Q_1}(D) = v_{Q_2}(D)$ whenever $Q_1, Q_2 \mid P$. Since $\mathfrak{g}_k$ acts transitively on the set of places Q lying over P, these are precisely the $\mathfrak{g}_k$-invariant divisors as well. □

Proposition 3.25 says that "Galois descent holds for divisors." This fact is sometimes taken as the definition of divisors in a function field over a perfect ground field, cf. [**Si**, §II.3]. The same argument shows that for an everywhere unramified Galois extension of function fields L/K we have ("étale descent")

$$(\mathrm{Div}\, L)^{\mathrm{Aut}(L/K)} = \mathrm{Div}\, K.$$

However, if $e(Q|P) > 1$ for some $Q \mid P$, then we still have

$$\mathrm{Div}\, K \hookrightarrow (\mathrm{Div}\, L)^{\mathrm{Aut}(L/K)},$$

but

$$\sum_{Q|P} Q \in (\operatorname{Div} L)^{\operatorname{Aut}(L/K)} \setminus \operatorname{Div} K.$$

Finally we turn to the problem of Galois descent for the class group and degree 0 class group. For simplicity we stick with the case of k perfect, $l = \overline{k}$ and $L = K\overline{k}$: once again, everthing goes through verbatim for any Galois extension l/k. As we have seen, we have a $\mathfrak{g}_k$-action on L and $\operatorname{Div} L$; for $\sigma \in \mathfrak{g}_k$, we have

$$\sigma((f)) = (\sigma(f))$$

and it follows that the subgroup $\operatorname{Prin} L$ of principal divisors is $\mathfrak{g}_k$-stable (equivalent terminology: a $\mathfrak{g}_k$-submodule). Whenever a group G acts on a $\mathbb{Z}$-module M and stabilizes a $\mathbb{Z}$-submodule N, the group G also acts on the quotient M/N:

$$\sigma(x + N) \coloneqq \sigma(x) + N.$$

It follows that we have a $\mathfrak{g}_k$-action on $\operatorname{Cl} L$. Moreover, in $\operatorname{Div} L$ all prime divisors have degree one and the $\mathfrak{g}_k$-action permutes perime divisors, the $\mathfrak{g}_k$-action also preserves degrees, so we also have a $\mathfrak{g}_k$-action on $\operatorname{Cl}^0 K$.

QUESTION 1. *Must we have* $(\operatorname{Cl} L)^{\mathfrak{g}_k} = \operatorname{Cl} K$ *and* $(\operatorname{Cl}^0 L)^{\mathfrak{g}_k} = \operatorname{Cl}^0(K)$*?*

The answer is **no** in general. There is an easy group-theoretic explanation for why one would not necessarily expect this to be the case. Namely, we have a group G acting on a $\mathbb{Z}$-module M and a G-stable submodule N. Under these circumstances, because $N^G = M^G \cap N$, we always have an injection

$$\frac{M^G}{N^G} \hookrightarrow (M/N)^G,\ x + N^G \mapsto x + N.$$

So in our case we have injections

$$\operatorname{Cl} K = \frac{\operatorname{Div} K}{\operatorname{Prin} K} = \frac{(\operatorname{Div} L)^G}{(\operatorname{Prin} L)^G} \overset{\iota}{\hookrightarrow} (\operatorname{Cl} L)^G = (\frac{\operatorname{Div} L}{\operatorname{Prin} L})^G, \tag{23}$$

$$\operatorname{Cl}^0 K = \frac{\operatorname{Div}^0 K}{\operatorname{Prin} K} = \frac{(\operatorname{Div}^0 L)^G}{(\operatorname{Prin} L)^G} \overset{\iota^0}{\hookrightarrow} (\operatorname{Cl}^0 L)^G = (\frac{\operatorname{Div}^0 L}{\operatorname{Prin} L})^G, \tag{24}$$

In general the map $\frac{M^G}{N^G} \hookrightarrow (M/N)^G$ ned not surjective.[1] For instance, let $G = (\mathbb{R}, +)$ be the additive group of the real numbers, and let $V = \mathbb{R}^2$ be the Euclidean plane, with the following action:

$$a \cdot (x, y) \coloneqq (x + ay, y).$$

(This is "really" the action of the matrix group $G = \{\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \mid a \in \mathbb{R}\}$ on $\mathbb{R}^2$.) Let $W_1 = \mathbb{R} \times \{0\}$. Then we find

$$V^G = W_1 = W_1^G,\ (V/W_1)^G = V/W_1 \cong \mathbb{R},$$

so

$$V^G/W_1^G = 0 \subsetneq (V/W_1)^G.$$

What's happening here is that the subspace W_2 spanned by the second standard basis vector e_2 is is not G-fixed – essentially because the upper right hand entry of

[1]The cognoscnenti will see that this is precisely the assertion that the functor $M \mapsto M^G$ is left exact but not generally exact.

the matrix need not be 0 – but for all $\sigma \in G$ and $v \in W_2$ we have $\sigma(v) - v \in W_1$ – eseentially because the lower right hand entry of the matrix must be 0 – so its isomorphic image in the quotient V/W_1 becomes G-fixed.

Of course this does not give a counterexample in the particular cases of (23) and (24): it just makes us less optimistic. It turns out that counterexamples to these cases exist but lie much deeper. One level deeper is the fact that ι is always an isomorphism when K has a degree 1 place or even has index 1, from which it follows immediately that ι^0 is also an isomorphism. As we will see later, this implies that ι and ι^0 are isomorphisms whenever k is finite. The next level deeper is that for an element of $C \in (\operatorname{Cl} L)^G$ there is a Galois cohomological obstruction to its lying in $\operatorname{Cl} K$: that is, there is a well-defined element of the Brauer group of k that vanishes iff $C \in \operatorname{Cl} K$. Thus ι and ι^0 are isomorphisms whenever the Brauer group of k vanishes (which also happens when k is finite, but for some infinite nonalgebraically closed fields as well). There are however examples of nonsurjectivity of ι over every local and global field. More precisely, it was shown by Roquette and Lichtenbaum that if k is a p-adic field, for every genus one function field without a degree 1 place the map ι fails to be surjective.

8. Kummer Extensions

We begin by recalling the following fact of field theory.

THEOREM 3.26. *Let $n \in \mathbb{Z}^+$, and let K be a field containing a primitive nth root of unity ζ_n. Let L/K be a degree n field extension.*

a) *The following are equivalent:*
   (i) *The extension L/K is cyclic, i.e., is a Galois extension with cyclic Galois group $\operatorname{Aut}(L/K)$.*
   (ii) *There is $u \in K^\times$ such that u has order n in $K^\times/K^{\times n}$ and such that if $u^{1/n}$ is any nth root of u in an algebraic closure of L, then $L = K(u^{1/n})$.*

b) *When the equivalent conditions of part a) are satisfied, there is a unique element $\sigma \in \operatorname{Aut}(L/K)$ such that $\sigma(u^{1/n}) = \zeta_n u^{1/n}$, and σ generates $\operatorname{Aut}(L/K)$.*

PROOF. See [**FT**, §9.2]. □

A **Kummer extension** is a degree n extension of fields L/K satisfying the equivalent conditions of Theorem 3.26a). In this section we will apply Riemann-Hurwitz to give a general genus formula for a Kummer extension of function fields.

LEMMA 3.27. *Let v be a nontrivial discrete valuation on a field K, and let $n \geq 2$ be such that $v(n) = 0$. Let $u \in K^\times$ be such that u has order n in $K(\mu_n)^\times/K(\mu_n)^{\times n}$, and let $L \coloneqq K(u^{1/n})$. Also put*

$$r \coloneqq \gcd(n, v(u)).$$

Let w be a discrete valuation on L such that $w|_K = v$ Then we have

$$e(w|v) = \frac{n}{r_p}.$$

PROOF. Step 1: We may first of all replace K by K_v and L by L_w and thereby assume that K and L are both complete. Moreover, since taking the compositum with an unramified extension does not change the ramification index, we may assume that K contains the nth roots of unity μ_n: by our hypothesis, after adjoining the nth roots of unity, u still has order n in $K^\times/K^{\times n}$, so $[L:K] = n$. The degree equality in the local case gives

$$e(w|v)f(w|v) = n.$$

Because of this it suffices to show that $\frac{n}{r} \mid e(w|v)$ and $r \mid f(w|v)$.
Step 2: We have $e(w|v) = e(L/K) = [w(L^\times) : v(K^\times)]$. This quantity is divisible by $[\langle w(u^{1/n})\rangle : v(K^\times)]$, which a quick contemplation involving cyclic groups shows to be $\frac{n}{r}$. Thus $\frac{n}{r} \mid e(w|v)$.
Step 3: We have $K \subset K(u^{1/r}) \subset K(u^{1/n})$. Since $[K(u^{1/r}) : K] = r$, it suffices to show that the extension $K(u^{1/r})/K$ is unramified. To see this, let π be a uniformizer of K and put $u' \coloneqq \frac{u}{\pi^{v(u)}}$. Then $\frac{u}{u'} = \pi^{v(u)} \in K^{\times r}$, so we have $K(u^{1/r}) = K(u'^{1/r})$. It follows that we may replace u with u'. Let R_v be the valuation ring of K and $k_v \coloneqq R_v/(\pi)$ the residue field. Since $v(n) = 0$ also $v(r) = 0$, and by Hensel's Lemma reduction modulo π induces an isomorphism $R_v^\times/R_v^{\times r} \xrightarrow{\sim} k_v^\times/k_v^{\times r}$. Thus adjoining the rth root of a unit in R_v yields an unramified extension. □

THEOREM 3.28. *Let $n \geq 2$, and let k be a field containing a primitive nth root of unity. Let K/k be a function field. Let $u \in K^\times$ have order n in $K^\times/K^{\times n}$. Put $L \coloneqq K(u^{1/n})/K$, and let l be the algebraic closure of k in L. By Theorem 3.26, the extension L/K is cyclic Galois of degree n, so for for all $P \in \Sigma(K/k)$ and all $Q, Q' \in \Sigma(L/l)$ such that $Q, Q'|P$ we have*

$$e(Q|P) = e(P) = e(Q'|P).$$

For $P \in \Sigma(K/k)$, put

$$r_P \coloneqq \gcd(n, v_P(u)).$$

Then we have

$$g_L = 1 + \frac{n}{[l:k]}\left(g_K - 1 + \frac{1}{2}\sum_{P \in \Sigma_{K/k}} (1 - \frac{r_P}{n}) \deg P\right). \tag{25}$$

PROOF. Riemann-Hurwitz gives us

$$g_L = 1 + \frac{n}{[l:k]}(g_K - 1) + \frac{1}{2}\deg \mathbb{D}(L/K).$$

The key observation is that Lemma 3.27 applies to give

$$e(Q|P) = \frac{n}{r_P},$$

and so if k has characteristic $p > 0$, the existence of a primitive nth root of unity forces $p \nmid n$ and thus also $p \nmid e(Q|P)$. Furthermore, since L/K is Galois, the residual degree $f(Q|P)$ also divides n and thus is indivisible by p, so the extension L/K is tame. So Theorem 3.15 gives

$$\deg \mathbb{D}(L/K) = \sum_{P \in \Sigma_{K/k}} \sum_{Q|P} d(Q|P) \deg(Q)$$

$$= \sum_{P \in \Sigma(K/k)} \sum_{Q|P} (e(P)-1) \deg Q = \sum_{P \in \Sigma(K/k)} \left(\frac{n}{r_P} - 1 \right) \sum_{Q|P} \deg Q,$$

so let us compute $\sum_{Q|P} \deg Q$. We have

$$\sum_{Q|P} \deg Q = \frac{1}{e(P)} \deg \left(\sum_{Q|P} e(Q|P) Q \right)$$

$$= \frac{1}{e(P)} \deg \iota_{L/K}(P) = \frac{r_P}{n} \frac{n}{[l:k]} \deg P = \frac{r_P}{[l:k]} \deg P.$$

Thus we get

$$\deg \mathbb{D}(L/K) = \sum_{P \in \Sigma(K/k)} \left(\frac{n}{r_P} - 1 \right) \sum_{Q|P} \deg Q$$

$$= \frac{n}{[l:k]} \sum_{P \in \Sigma(K/k)} \left(1 - \frac{r_P}{n} \right) \deg P. \qquad \square$$

COROLLARY 3.29. *Let $n \geq 2$, and let k be a field containing a primitive nth root of unity. Let K/k be a function field. Let $u \in K^\times$, and put $L \coloneqq K(u^{1/n})$. **Let us moreover suppose** that there is a separable place $P_\bullet \in \Sigma(K/k)$ such that*

$$r_{P_\bullet} \coloneqq \gcd(n, v_{P_\bullet}(u)) = 1.$$

Then:

a) *The element u has order n in $K^\times / K^{\times n}$.*
b) *The algebraic closure l of k in L is k.*
c) *If K/k is regular, then L/k is regular.*
d) *We have*

$$g_L = 1 + n(g_K - 1) + \frac{1}{2} \sum_{P \in \Sigma(K/k)} (n - r_p) \deg P.$$

PROOF. a) Consider the discrete valuation $v_{P_\bullet}$ on K. Then we have a short exact sequence

$$1 \to R_{P_\bullet}^\times \to K^\times \xrightarrow{v_{P_\bullet}} \mathbb{Z} \to 0.$$

Choosing a uniformizer for $v_{P_\bullet}$ gives us a splitting

$$K^\times = R_{P_\bullet}^\times \times \mathbb{Z},$$

and passing to the cokernel of multiplication by n gives a canonical isomorphism

$$K^\times / K^{\times n} = R_{P_\bullet}^\times / R_{P_\bullet}^\times \times \mathbb{Z}/n\mathbb{Z}.$$

The associated map $K^\times / K^{\times n}$ is just $x \mapsto v_{P_\bullet}(x) \pmod{n\mathbb{Z}}$, so the hypothesis that $\gcd(n, v_{P_\bullet}(u)) = 1$ means that $v_{P_\bullet}(x)) \pmod{n\mathbb{Z}}$ has order n, so certainly the image of u in $K^\times / K^{\times n}$ has order n.
b) Notice that by Lemma 3.26 our assumption that $r_{P_\bullet} = 1$ is equivalent to $P_\bullet$ being totally ramified in L. Since k is regular, we have $[l:k] = [Kl:K] \mid [L:K] = n$, and since in characteristic p we have $p \nmid n$, the extension l/k is separable. A separable constant field extension of a separable place has ramification index 1, so we cannot have a nontrivial such subextension of a totally ramified extension: $l = k$.
c) A field extension E/F is regular if F is algebraically closed in E and E/F is separable. We just saw that k is algebraically closed in L. If K/k is regular then it is separable, and once again for degree reasons the extension L/K is separable, so

it follows from [**FT**, Cor. 12.17b)] that L/k is separable and thus L/k is regular.
d) Since $[l : k] = 1$, this follows immediately from (25). □

EXERCISE 3.9. *Suppose that $n \geq 2$ and that k is a field such that the characteristic of k does not divide n, so that there is a primitive nth root of unity ζ_n in a separable closure k^{sep} of k. Let K/k be a function field, and let $u \in K^\times$ have order n in $K^\times/K^{\times n}$. Let $u^{1/n}$ be an nth root of u in $\overline{K}$, and let $L \coloneqq K(u^{1/n})$.*

a) *Let $\tilde{k} \coloneqq k(\zeta_n)$, $\tilde{K} = K\tilde{k} = K(\zeta_n)$ and $\tilde{L} \coloneqq \tilde{k}L = K(\zeta_n, u^{1/n})$. Suppose that u still has order n in $\tilde{K}$. Show that $g_{\tilde{K}} = g_K$ and $g_{\tilde{L}} = g_L$ and thus Theorem 3.28 and Corollary 3.29 still work to compute g_L.*
b) *Under what circumstances does u still have order n in $\tilde{K}$? (See* [**FT**, Thm. 9.21]*.)*

9. Artin-Schreier Extensions

In the previous section our running hypothesis was that k contained an nth root of unity. As shown in Exercise 3.9, for the most part we can still use Kummer Theory to compute the genus of $K(u^{1/n})$ so long as the characteristic of k does not divide n. What happens when k has positive characteristic p and $p \mid n$? In this section we treat the simplest case of that: cyclic p extensions in characteristic p, with the aid of Artin-Schreier Theory. This seems less familiar than Kummer Theory, so rather than immediately recalling the results from [**FT**] we motivate them a bit.

EXERCISE 3.10. *Let k be a field of characteristic p. Let $a, b \in k$ be two elements whose images in $k/\wp(k)$ generate the same cyclic subgroup of $k/\wp(k)$. Show: $k(\wp^{-1}(a)) = k(\wp^{-1}(b))$.*

LEMMA 3.30. *Let k be a perfect field of characteristic $p > 0$, let K/k be a function field, let $u \in K$, and let $P \in \Sigma(K/k)$.*

a) *There is $z \in K$ such that $v_P(u - (z^p - z))$ is either*
   (i) *Non-negative or*
   (ii) *Negative and prime to p.*
b) *There is at most one integer m that is negative and prime to p such that $v_P(u - (z^p - z)) = m$ for some $z \in K$. If such an m exists, it is characterized as*

$$\max\{v_P(u - (z^p - z)) \mid z \in K\}.$$

It follows that precisely one of the two alternatives in part a) holds.

PROOF. Step 1: We claim that for all $x_1, x_2 \in K^\times$ with $v_P(x_1) = v_P(x_2)$, there is $y \in K^\times$ such that

$$v_P(y) = 0 \text{ and } v_P(x_1 - y^p x_2) > v_P(x_1).$$

PROOF OF CLAIM: For $x \in R_P$ we denote by $\overline{x}$ its reduction modulo the maximal ideal. Since $\frac{\overline{x_2}}{\overline{x_1}} \in k_P^\times$ and k_P is perfect (being a finite degree extension of the perfect field k), there is $y \in R_P$ such that $\frac{\overline{x_2}}{\overline{x_1}} = \overline{y}^p$. Thus $v_P(y) = 0$ and $v_P(\frac{x_2}{x_1} - y^p) > 0$, so $v_P(x_2 - y^p x_1) > v_P(x_1)$.
Step 2: We claim that if $z_1 \in K$ is such that $v_P(u - (z_1^p - z_1))$ is negative and divisible by p, then there is $z_2 \in K$ such that

$$v_P(u - (z_2^p - z_2)) > v_P(u - (z_1^p - z_1)).$$

PROOF OF CLAIM: Suppose $v_P(u-(z_1^p-z_1))=\ell p$. We may choose $t\in K$ such that $v_P(t)=\ell$. Then

$$v_P(u-(z_1^p-z_1))=v_P(t^p),$$

so by Step 1 there is $y\in K$ such that $v_P(y)=0$ and

$$v_P(u-(z_1^p-z_1)-(yt)^p))>\ell p.$$

Since $v_P(yt)=\ell>\ell p$, we have

$$v_P(u-(z_1^p-z_1)-((yt)^p-yt))>\ell p.$$

Step 3: We generate a sequence of elements as follows: put $z_0=0$ and $v(0):=v_P(u-(z_0^p-z_0))=v_P(u)$. If $v(0)$ is negative and divisible by p, then by Step 2 there is $z_1\in K$ such that $v(1):=v_P(u-(z_1^p-z_1))>v(0)$. If $v(1)$ is still negative and divislbe by p, then by Step 2 there is $z_2\in K$ such that $v(2):=v_P(u-(z_2^p-z_2))>v(1)$. Continuing in this way, we get a sequence of integers $v(0)<v(1)<\ldots$, so at some point one of them must either be non-negative or negative and not divisible by p, which proves a).
Step 4: Suppose there is $z\in K$ such that $v_P(u-(z^p-z))=m$ is negative and not divisible by p. Now let $w\in K$. Since $\gcd(p,m)=1$, we have that $v_P((w-z)^p)=pv_P(w-z)$ is not equal to m, so there are two cases.
Case 1: Suppose that $v_P((w-z)^p)>m$. Then

$$v_P((w-z)^p-(w-z))>m$$

and

$$v_P(u-(w^p-w))=v_P(u-(z^p-z)-((w-z)^p-(w-z))=m.$$

Case 2: Suppose that $v_P((w-z)^p)<m$. Then

$$v_P(u-(w^p-w))=v_P(u-(z^p-z)-((w-z)^p-(w-z))=v_P((w-z)^p)<m.$$

This proves part b). □

THEOREM 3.31. *Let k be a perfect field of characteristic $p>0$, let K/k be a function field, let $u\in K$ and put $L:=K(\wp^{-1}(u))$. For $P\in\Sigma(K/k)$, put*

$$M_P=\begin{cases}|m| & \text{if there is } z\in K \text{ such that } v_P(u-(z^p-z))=m \text{ with } m<0 \text{ and prime to } p\\ -1 & \text{if there is } z\in K \text{ such that } v_P(u-(z^p-z))\geq 0\end{cases}.$$

Then:

a) *If $M_P=-1$, then P is unramified in L.*
b) *If $M_P\geq 1$ then P is totally ramified in L. Let $\tilde{P}$ be the unique place of L lying over P. Then we have*

$$d(\tilde{P}|P)=(p-1)(M_P+1).$$

c) *Suppose that there is at least one place $P\in\Sigma(K/k)$ with $M_P\geq 1$. Then $[L:K]=p$, L/k is regular and we have*

$$g_L=pg_K+\frac{p-1}{2}\left(-2+\sum_{P\in\Sigma(K/k)}(M_P+1)\deg(P)\right). \tag{26}$$

PROOF. Step 1: Suppose that $M_P = -1$. By definition, this means there is $z \in K$ such that $v_P(u - z^p - z) \geq 0$. By Exercise 3.10 we have $K(\wp^{-1}(u)) = K(\wp^{-1}(u-(z^p-z)))$, so we may replace u by $u-(z^p-z)$ and thereby assume that $v_P(u) \geq 0$. Choose $\alpha \in \overline{K}$ such that $\alpha^p - \alpha = u$, so $L = K(\alpha)$. For any place $Q|P$ of $\Sigma(L/\kappa(L))$, we have $v_Q(u) = e(Q|P)v_P(u) \geq 0$, and the equation $\alpha^p - \alpha = u$ implies that $v_Q(\alpha) \geq 0$. The minimal polynomial of α over K is $\varphi(t) = t^p - t - u$. So α is integral over R_P and $K(\alpha) = L$, so by Theorem 3.14b) we have

$$d(Q|P) \leq v_Q(\varphi'(\alpha)) = v_Q(-1) = 0.$$

Thus L is unramified over P.
Step 2: Suppose that $M_P \geq 1$. Choose $z \in K$ such that $v_P(u - (z^p - z)) = m$ is negative and prime to p. As in Step 1 without loss of generality we may replace u by $u - (z^p - z)$ and thereby assume that $v_P(u) = m$. Choose $\alpha \in \overline{K}$ such that $\alpha^p - \alpha = u$, and let $Q|P$ be a place of L. We have

$$v_Q(u) = e(Q|P)v_P(u) = me(Q|P) < 0,$$

which implies that $v_Q(\alpha) < 0$ and thus we have

$$me(Q|P) = v_Q(u) = v_Q(\alpha^p - \alpha) = pv_Q(\alpha).$$

So $p \mid me(Q|P)$, and since $\gcd(m, p) = 1$ we get

$$p \mid e(Q|P) \mid [L : K] \mid p$$

and also

$$v_Q(\alpha) = m.$$

Thus $[L : K] = p = e(Q|P)$, so P is totally ramified and thus there is a unique place of L lying over it, which we denote by $\tilde{P}$. As in the proof of Corollary 3.29, this shows that $\kappa(L) = k$. Since k is perfect, this means that L/K is regular.
Step 3: It remains to compute the local different exponent $d(\tilde{P}|P)$. For this, let $\pi \in K$ be a uniformizer at P. Choose $i, j \in \mathbb{N}$ such that $1 = ip - jM_P$, and put

$$x \coloneqq \pi^i \alpha^j \in L.$$

Then

$$v_{\tilde{P}}(x) = iv_{\tilde{P}}(\pi) + jv_{\tilde{P}}(\alpha) = ie(\tilde{P}|P) - jM_P = 1.$$

so x is a uniformizer at $\tilde{P}$. Let $\varphi(t) \in K[t]$ be its minimal polynomial. As in the proof of Theorem 3.28, the total ramification implies that $R_{\tilde{P}} = R_P[x]$ and thus $d(\tilde{P}|P) = v_{\tilde{P}}(\varphi'(x))$.

Let $G \coloneqq \mathrm{Aut}(L/K)$ and put $G^\bullet \coloneqq G \setminus \{1\}$. Then

$$\varphi(T) \coloneqq \prod_{\sigma \in G} (T - \sigma(x)) = (T - x)h(T),$$

where

$$h(T) = \prod_{\sigma \in G^\bullet} (T - \sigma(x)).$$

So

$$\varphi'(T) = h(T) + (T - x)h'(T),\ \varphi'(x) = h(x)$$

and thus

$$d(\tilde{P}|P) = v_{\tilde{P}}\left(\prod_{\sigma \in G^\bullet} (x - \sigma(x))\right).$$

Well, keep calm and compute: by X.X we know that each $\sigma \in G^\bullet$ is of the form $\sigma(\alpha) = \alpha + k$ for $1 \leq k < p$. So

$$x - \sigma(x) = \pi^i \alpha^j - \pi^i(\alpha + k)^j = -\pi^i \sum_{\ell=1}^{j} \binom{j}{l} \alpha^{j-l} k^l.$$

The factors $\binom{j}{\ell}$ and k^ℓ are all integers prime to p, so have valuation zero. Since once again $v_{\tilde{P}}(\alpha) < 0$, the $\ell = 1$ term is the unique term in the sum of smallest valuation, so

$$v_{\tilde{P}}(x - \sigma(x)) = v_{\tilde{P}}(\pi^i \alpha^{j-1}) = ip - (j-1)M_P = ip - jM_P + M_P = M_P + 1.$$

Since this holds for each $\sigma \in G^\bullet$ and there are $p-1$ such elements, we get

$$d(\tilde{P}|P) = (p-1)(M_P + 1),$$

completing the proof of part b).
Finally, if there is a totally ramified place, then as above we know that $\kappa(L) = k$. Using this, our calculation of the local different exponents, and the Riemann-Hurwitz formula, yields (26). □

The following very special case of Theorem 3.31 is already quite interesting.

COROLLARY 3.32. *Let k be a perfect field of characteristic $p > 0$. Let d be a positive integer such that $\gcd(p, d) = 1$, and let $f \in k[x]$ be a polynomial of degree d. Let $L = K(\wp^{-1}(f))$. Then $[L : K] = p$ and L/k is a regular function field of genus $\frac{(p-1)(d-1)}{2}$ that is unramified away from ∞.*

PROOF. We have $v_{P_\infty}(f) = -d$ is negative and prime to P, so in the notation of Theorem 3.31 we have $M_{P_\infty} = d \geq 1$, so $[L : K] = p$ and L/k is regular. For every finite place $P \in \Sigma(k(x)/k)$, we have $v_P(f) \geq 0$, so Theorem 3.31 implies that L is unramified over P and $M_P = -1$. Therefore (26) gives

$$g_L = p \cdot 0 + \frac{p-1}{2}(-2 + (d+1)(1)) = \frac{(p-1)(d-1)}{2}.$$ □

10. Inseparable Extensions

10.1. A dark corner of algebraic number theory.

PROPOSITION 3.33. *Let R be an integrally closed domain with fraction field K, let L/K be a purely inseparable algebraic extension (possibly of infinite degree), and let S be the integral closure of R in L. For each prime ideal $\mathfrak{p}$ of R, the ideal $\operatorname{rad} \mathfrak{p}S$ of S is prime and is the unique prime ideal of S lying over $\mathfrak{p}$.*

PROOF. We recall that purely inseparable extensions are characterized by the fact that for all $x \in L$, there is $n \in \mathbb{N}$ such that $x^{p^n} \in K$ [**FT**, Prop. 5.4].
Step 1: We claim that

$$\operatorname{rad}(\mathfrak{p}S) = \{x \in S \mid x^n \in \mathfrak{p} \text{ for some } n \in \mathbb{Z}^+\}.$$

First, if $x^n \in \mathfrak{p}$ then $x^n \in \mathfrak{p}S$, so $x \in \operatorname{rad}(\mathfrak{p}S)$. Conversely, if $x \in \operatorname{rad}(\mathfrak{p}S)$ then $x^n \in \mathfrak{p}S$ for some $n \in \mathbb{Z}^+$. This means that there are elements $a_1, \ldots, a_r \in \mathfrak{p}$ and $b_1, \ldots, b_r \in S$ such that

$$x^n = a_1 b_1 + \ldots + a_n b_n.$$

There is $N \in \mathbb{Z}^+$ such that for all $1 \leq i \leq r$ we have $b_i^{p^N} \in K$. Since also $b_i^{p^N} \in S$ and R is integrally closed, we have $b_i^{p^N} \in R$. It follows that $x^n \in \mathfrak{p}$.

Step 2: Let $x, y \in S$ be such that $xy \in \operatorname{rad}(\mathfrak{p}S)$. By Step 1, there is $n \in \mathbb{Z}^+$ such that $x^n y^n = (xy)^n \in \mathfrak{p}$. Choose $N \in \mathbb{Z}^+$ such that $x^{p^N}, y^{p^N} \in K$. Then

$$x^{np^N} y^{np^N} = (xy)^{np^N} \in \mathfrak{p},$$

and since $x^{np^N}, y^{np^N} \in K$ and $\mathfrak{p}$ is a prime ideal, we have $x^{np^N} \in \mathfrak{p}$ or $y^{np^N} \in \mathfrak{p}$. It follows that at least one of x and y lies in $\operatorname{rad}(\mathfrak{p}S)$, so $\operatorname{rad}(\mathfrak{p}S)$ is a prime ideal.
Step 3: Let $\mathcal{P} \in \operatorname{Spec} S$ be such that $\mathcal{P} \cap R = \mathfrak{p}$. Let $x \in \mathcal{P}$. There is $n \in \mathbb{N}$ such that $x^{p^n} \in K \cap S = R$, hence $x^{p^n} \in \mathcal{P} \cap R = \mathfrak{p}$, so $x \in \operatorname{rad}(\mathfrak{p}S)$. Thus $\mathcal{P} \subset \operatorname{rad}(\mathfrak{p}S)$.
Step 4: Similarly, if $x \in \operatorname{rad}(\mathfrak{p}S) \cap R$ then $x \in R$ and $x^n \in \mathfrak{p}$ for some $n \in \mathbb{Z}^+$, so $x \in \mathfrak{p}$, and thus $\operatorname{rad}(\mathfrak{p}S)$ is a prime ideal lying over $\mathfrak{p}$. In an integral extension $R \subset S$ one cannot have prime ideals $\mathcal{P}_1 \subsetneq \mathcal{P}_2$ each pulling back to the same prime ideal of R [**CA**, Cor. 14.15]. So it follows from Step 3 that $\operatorname{rad}(\mathfrak{p}S)$ is the unique prime ideal of S that pulls back to $\mathfrak{p}$. □

COROLLARY 3.34. *Let R be a Dedekind domain, with fraction field K of characteristic $p > 0$. Let L/K be a finite degree purely inseparable field extension, so $[L : K] = p^a$ for some $a \in \mathbb{Z}^+$. Let S be the integral closure of R in L, a Dedekind domain. Let $\mathfrak{p} \in \operatorname{MaxSpec} R$.*

a) *We have*
$$S = \{x \in L \mid x^{p^a} \in R\}.$$
b) *There is a unique prime ideal $\mathcal{P}$ of S lying over R. Thus we have*
$$\mathfrak{p}S = \mathcal{P}^e$$
for some $e \in \mathbb{Z}^+$. The residual extension $k := R/\mathfrak{p} \subset S/\mathcal{P} =: l$ is purely inseparable, say of degree f.
c) *If S is finitely generated over R (which always occurs when R is an affine domain) then we have $ef = p^a$.*
d) *If k is perfect, then we have $e = p^a$.*

EXERCISE 3.11. *Prove Corollary 3.34.*

Recall that in a finite degree extension of Dedekind domains $R \subset S$ – let us assume that S is finitely generated over R so as not to make too much trouble – we say that a prime $\mathfrak{p} \in \operatorname{MaxSpec} R$ **ramifies** in S if *either* $\mathfrak{p} = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_g^{e_g}$ with $\max e_i > 1$ or if at least one of the residual extensions $R/\mathfrak{p} \subset S/\mathcal{P}_i$ is inseparable. Thus Corollary 3.34 shows that when the extension of fraction fields is purely inseparable, every prime ramifies. From this one deduces:

EXERCISE 3.12. *Let R be a Dedekind domain with fraction field K, let L/K be a finite degree inseparable field extension, and let S be the integral closure of R in L. We suppose that S is finitely generated as an R-module. Show: every prime $\mathfrak{p} \in \operatorname{MaxSpec} R$ is ramified in S.*

In fact the preceding exercise follows from a suitably general version of the result that the primes that ramify in an extension of Dedekind domains are precisely those that divide the discriminant – see e.g. [**Lo**, Thm. 5.6] – together with the fact that the discriminant of an extension of Dedekind domains is nonzero iff the field extension is separable [**Lo**, Rem. 5.10].

COROLLARY 3.35. *Let k be a perfect ground field, and let $K/k \subset L/l$ be a finite extension of function fields, with L/K purely inseparable. Then $l = k$ and L is isomorphic to K as a K-algebra. In particular we have $g_K = g_L$.*

PROOF. Let $[L : K] = p^a$. Since k is perfect, [**FT**, Exc. 13.18] gives $L = K^{p^{-a}}$. The map $\mathrm{Fr} : K^{p^{-a}} \to K$ by $x \mapsto x^{p^a}$ is a field isomorphism such that $\mathrm{Fr}(k) = k^{p^a} = k$. □

EXERCISE 3.13. *Let k be a perfect field, and let $K/k \subset L/l$ be a finite extension of function fields. Let g_K be the genus of K, and let g_L be the genus of L. Show: $g_L \geq g_K$.*

The following example shows that over an imperfect ground field, the genus can drop upon inseparable base extension, even when the function field is regular.

EXERCISE 3.14. *Let $p \geq 3$ be a prime number, let k be an imperfect field of characteristic p, and let $a \in k \setminus k^p$. Put*

$$f(x, y) \coloneqq y^2 - x^p + a.$$

a) *Show that $f \in k[x, y]$ is geometrically irreducible, so the fraction field K of of $k[x, y]/(f)$ is a regular function field.*
b) *Show that K has genus $\frac{p-1}{2}$.*
c) *Let $l \coloneqq k(a^{1/p})$, and let $L = Kl = K \otimes_k l$. Show that L has genus 0.*

A classic paper of Tate [**Ta52**] studies the genus change in purely inseparable extensions of a function field. He shows in particular the following result.

THEOREM 3.36 (Tate). *Let K/k be a function field of genus g_K.*

a) *Let L/K be a purely inseparable extension of finite degree, of genus L. Then we have*
$$\frac{p-1}{2} \mid g_L - g_K.$$
b) *If $g_K < \frac{p-1}{2}$, then for every constant extension l/k, we have $g_{K \otimes_k l} = g_K$.*

PROOF. a) This is [**Ta52**, Cor. 1]. b) This is [**Ta52**, Cor. 2]. □

11. Castelnuovo's Inequality

If a function field L/k is obtained as the composite of two subfields K_1/k and K_2/k, it is natural to ask for a bound on the genus of L in terms of the genera of K_1 and K_2 and the indices $[L : K_1]$ and $[L : K_2]$. The main result of this section, Castelnuovo's Inequality, does exactly this, in the case that the ground field is perfect.[2]

PROPOSITION 3.37. *Let $K/k \subset L/k$ be an extension of function fields with $[L : K] = n$. Let g_K be the genus of K/k and let g_L be the genus of L/k. Let $z_1, \ldots, z_n$ be a K-basis for L, and choose $D \in \operatorname{Div} L$ such that $z_i \in \mathcal{L}(D)$ for all $1 \leq i \leq n$. Then we have*

$$g_L \leq 1 + n(g_K - 1) + \deg(D). \tag{27}$$

PROOF. Let $A_1 \in \operatorname{Div}(K)$ have degree at least $\max(2g_K - 1, \frac{2g_L - 1 - \deg(D)}{n})$. Then A_1 is nonspecial, so

$$t \coloneqq \ell(A_1) = \deg(A_1) + 1 - g_K.$$

Choose a k-basis $x_1, \ldots, x_t$ of $\mathcal{L}(A_1)$, and put

$$A \coloneqq \iota_{L/K}(A_1) \in \operatorname{Div}(L).$$

[2]All treatments of this result that I have seen include the hypothesis that the ground field is perfect. I would be interested to know if there are counterexamples in the general case.

Then the elements $\{x_i z_j \mid 1 \leq i \leq t,\ 1 \leq j \leq n\}$ lie in $\mathcal{L}(A+D)$ and are k-linearly independent, as a k-linear dependence relation among the $x_i z_j$ yields a K-linear dependence relation among the z_j. Therefore

$$\ell(A+D) \geq nt = n\deg(A_1) + n(1-g_K). \tag{28}$$

On the other hand, since

$$\deg(A+D) = n\deg(A_1) + \deg(D) \geq 2g_L - 1,$$

the divisor $A+D$ is nonspecial, so

$$\ell(A+D) = \deg(A+D) + 1 - g_L = n\deg(A_1) + \deg(D) + 1 - g_L. \tag{29}$$

Combining (28) and (29), we get (27). □

LEMMA 3.38. *Let k be an algebraically closed field, and let $K/k \subset L/k$ be an extension of function fields, with L/K separable of degree $n > 1$. Choose $y \in L$ such that $L = K(y)$. Then for all but finitely many $P \in \Sigma(K/k)$, we have that there are n places $P_1, \ldots, P_n \in \Sigma(L/k)$ lying over P and their restrictions to $k(y)$ yield n places of $k(y)/k$.*

PROOF. Let A be an affine Dedekind domain of K, and let B be its integral closure in L. Then $A[y]$ is an A-order in B. Since the extension L/K is separable, the discriminant $\Delta = \Delta(A[y]/A)$ is a nonzero ideal of A. Let S be the finite set of maximal ideals of A that divide Δ. Replacing A with $S^{-1}A$ and B with $S^{-1}B$ (which is also the integral closure of $S^{-1}A$ in L), we have reduced to the case in which $B = A[y]$ is an unramified extension of A. Let $\mathfrak{p} \in \operatorname{MaxSpec} A$; since k is algebraically closed, we have $A/\mathfrak{p} = k$. Let $f \in A[t]$ be the minimal polynomial of y, so $B \cong A[t]/(f)$. The maximal ideals of B lying over $\mathfrak{p}$ correspond to the maximal ideals of $B/\mathfrak{p}B \cong k[t]/(f)$. Because B is unramified over A and k is algebraically closed, there must be $n = [L:K] = \deg(f)$ maximal ideals of $k[t]/(f)$, which means that the polynomial $f \in k[t]$ splits into distinct linear factors:

$$f = (t-b_1)\cdots(t-b_n), b_i \in k.$$

It follows that the maximal ideals of B lying over $\mathfrak{p}$ are

$$\mathcal{P}_i = \langle \mathfrak{p}, y - b_i \rangle,\ 1 \leq i \leq n.$$

For the corresponding place P_i of L we have $v_{P_i}(y-b_i) > 0$, and thus $(P_i)|_{k(y)}$ is the place corrsesponding to $y - b_i$. □

LEMMA 3.39. *Let $S \subset \Sigma_1(K/k)$ be a set of degree 1 places of cardinality at least $g = g(K)$. Then there is an effective, nonspecial divisor D with $\deg D = g$ and $\operatorname{supp} D \subset S$.*

PROOF. If $g = 0$, then we may (and must) take $D = 0$. So suppose $g \geq 1$.[3]
Step 1: We claim that given distinct $P_1, \ldots, P_g \subset S$ and an effective divisor $A \in \operatorname{Div}(K)$ such that

$$A \geq 0,\ \ell(A) = 1,\ \deg(A) \leq g-1,$$

then there is $1 \leq i \leq g$ such that $\ell(A+P_i) = 1$. Indeed, suppose not: then for all $1 \leq i \leq g$ we have $\ell(A+P_i) \geq 2$ and thus there is $z_i \in \mathcal{L}(A+P_i) \setminus \mathcal{L}(A)$. Since

$$v_{P_i}(z_i) = -v_{P_i}(A) - 1 \text{ and } \forall j \neq i,\ v_{P_j}(z_i) \geq -v_{P_j}(A),$$

[3]The case of $g = 1$ is almost as easy, so one could certainly assume that $g \geq 2$, but the argument to come does encompass the $g = 1$ case.

if $a_0, a_1, \ldots, a_g \in k$ are such that

$$a_0 + a_1 z_1 + \ldots + a_g z_g = 0,$$

then if $a_i \neq 0$ the term $a_i z\_i$ is the unique term of minimal P_i-adic valuation, so the sum cannot be zero. Therefore $a_1 = \ldots = a_g = 0$, which implies that $a_0 = 0$.

Since $\Sigma(K/k) \neq \varnothing$ and $\deg(A + P_1 + \ldots + P_g) \leq 2g - 1$, there is $B \in \mathrm{Div}(K)$ such that

$$B \geq A + P_1 + \ldots + P_g, \ \deg B = 2g - 1.$$

Then $1, z_1, \ldots, z_g \in \mathcal{L}(B)$, so $\ell(B) \geq g + 1$, but by Riemann-Roch we have

$$\ell(B) = 2g - 1 - g + 1 = g,$$

a contradiction. This completes the proof of Step 1.

Step 2: We now proceed inductively using Step 1.

We put $A_0 \coloneqq 0$. Inductively, for $0 \leq i \leq g - 1$, having defined an effective divisor A_i with $\deg(A_i) = i$, $\ell(A_i) = 1$ and $\mathrm{supp}(A_i) \subset S$, by Step 1 there is $P_{i+1} \in S$ such that $\ell(A_i + P_{i+1}) = 1$. We put

$$A_{i+1} \coloneqq A_i + P_{i+1}.$$

Then A_{i+1} is effective, has degree $i + 1$, has $\ell(A_{i+1}) = 1$ and has $\mathrm{supp}(A_{i+1}) \subset S$.

Now take $D \coloneqq A_g$. Then $D \geq 0$, $\deg(D) = g$, $\mathrm{supp}(D) \subset S$, and we have

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

so D is nonspecial. □

THEOREM 3.40 (Castelnuovo Inequality). *Let k be a perfect field. Let K_1, K_2, L be function fields over k such that $L = K_1 K_2$. Put*

$$g_1 = g(K_1), g_2 = g(K_2), \ n_1 = [L : K_1], \ n_2 = [L : K_2], \ g_L = g(L).$$

Then we have

$$g_L \leq n_1 g_1 + n_2 g_2 + (n_1 - 1)(n_2 - 1). \tag{30}$$

PROOF. Under the hypothesis that k is perfect, it is no loss of generality to suppose that k is algebraically closed, because the genera are unchanged by separable field extensions and moreover since k is perfect all function fields are regular and thus $[L\overline{k} : K_i\overline{k}] = [L : K_i]$. Moreover we may assume that L/K_1 is separable, because if k has characteristic $p > 0$ and L/K_1 and K/K_2 were both inseparable, then $K_1, K_2 \subset L^p$ and thus $K_1 K_2 \subset L^p \subsetneq L$. Since $L = K_1 K_2$, there are $y_1, \ldots, y_s \in K_2$ such that $L = K_1(y_1, \ldots, y_s)$. Since L/K_1 is separable, and k is infinite, by a refined form of the Primitive Element Corollary [**FT**, Cor. 7.3] there are $a_1, \ldots, a_s \in k$ such that for

$$y \coloneqq \sum_{i=1}^{s} a_i y_i \in K_2,$$

we have

$$L = K_1(y).$$

By Lemma 3.39 there is $A_0 \in \mathrm{Div}(K_2)$ such that $A_0 \geq 0$, $\deg A_0 = g_2$ and $\ell(A_0) = \deg(A_0) - g_2 + 1 = 1$. Let $P_0 \in \Sigma(K_2/k)$ be a place that is not in the support of A_0 and put $B_0 \coloneqq A_0 - P_0 \in \mathrm{Div}(K_2)$. Since $\mathcal{L}(A_0) = k$, we have

$$\deg B_0 = g_2 - 1, \ \ell(B_0) = 0. \tag{31}$$

By Lemma 3.38 there is a place $P \in \Sigma(K_1/k)$ that has n_1 extensions $P_1, \ldots, P_{n_1}$ to L and such that the restrictions

$$Q_i \coloneqq P_i \cap K_2 \in \Sigma(K_2/k)$$

are pairwise distinct and such that for all $1 \leq n_1$ we have that $Q_i \notin \operatorname{supp}(B_0)$. (Indeed, by Lemma 3.38 the restrictions of $P_1, \ldots, P_n$ to $k(y)$ are all distinct, so they must remain distinct in the intermediate function field K_2. The support condition holds for all but finitely many P, so by Lemma 3.38 it may be enforced.) By Riemann-Roch we have

$$\forall 1 \leq i \leq n_1,\ \ell(B_0 + Q_i) \geq \deg(B_0 + Q_i) + 1 - g_2 = 1. \tag{32}$$

Combining (31) and (32) we get for all $1 \leq i \leq n_1$ an element $u_i \in K_2$ such that

$$(u_i) \geq -B_0 - Q_i,\ v_{Q_i}(u_i) = -1. \tag{33}$$

We claim that $u_1, \ldots, u_{n_1}$ form a K_1-basis for L. There are n_1 of them, so it suffices to show that they are K_1-linearly independent. Suppose not, and let

$$\sum_{i=1}^{n_1} x_i u_i,\ x_i \in K_1$$

be a nontrivial linear combination. Choose $1 \leq j \leq n_1$ such that

$$v_P(x_j) \leq v_P(x_i)\ \forall i.$$

Since $P_j \mid P$ is unramified we have $v_{P_j}|_{K_1} = v_P$; also by (33) we have

$$v_{P_j}(u_j) = e(P_j|Q_j) v_{Q_j}(u_j) \leq -1,$$

so

$$v_{P_j}(x_j u_j) = v_P(x_j) + v_{P_j}(u_j) \leq v_P(x_j) - 1.$$

By construction of u_i it has a pole at Q_i but at no other Q_j, so for $i \neq j$ we have

$$v_{P_j}(x_i u_i) = v_P(x_i) + v_{P_j}(u_i) \geq v_P(x_i) \geq v_P(x_j),$$

so

$$v_{P_j}\left(\sum_{i=1}^{n_1} x_i u_i\right) = v_P x_j u_j < \infty,$$

a contradiction. So $u_1, \ldots, u_{n-1}$ is a K_1-basis for L. Finally, we consider

$$D \coloneqq \iota_{L/K_2}(B_0 + \sum_{i=1}^{n_1} Q_i) \in \operatorname{Div}(L).$$

We have

$$deg(D) = n_2 \deg(B_0 + \sum_{i=1}^{n_1} Q_i) = n_2(g_2 - 1 + n_1).$$

By (33) the elements $u_1, \ldots, u_{n_1}$ all lie in $\mathcal{L}(D)$. Therefore Proposition 3.37 applies to give

$$g_L \leq 1 + n_1(g_1 - 1) + \deg(D) = 1 + n_1(g_1 - 1) + n_2(g_2 - 1) + n_1 n_2$$

$$= n_1 g_1 + n_2 n_2 + (n_1 - 1)(n_2 - 1),$$

completing the proof. □

COROLLARY 3.41 (Riemann's Inequality). *Let k be a perfect field. Suppose $L = k(x, y)$ is a function field, and let g be the genus of L. Then:*

$$g \leq ([L : k(x)] - 1)([L : k(y)] - 1).$$

PROOF. We apply Castelnuovo's Inequality with $K_1 = k(x)$, $K_2 = k(y)$. □

Let K/k be a function field. Let us say that two rational functions $f, g \in K$ are **independent** if $K = k(f, g)$. Then Riemann's Inequality says that the genus of K can be bounded above in terms of the degrees of any two independent rational functions. Because

$$[K : k(f, g)] \mid [K : k(f)] = \deg(f),\ [K : k(f, g)] \mid [K : k(g)] = \deg(g),$$

two rational functions are certainly independent if their degrees are coprime. This special case of Riemann's Inequality is a very useful result:

COROLLARY 3.42. *Let K/k be a function field of genus g.*

a) *Let $d, e \in \mathbb{Z}^+$ be coprime positive integers. If K/k admits rational functions of degrees d and e, then*

$$g \leq (d - 1)(e - 1).$$

b) *If K/k is hyperelliptic and admits a rational function of odd degree e, then*

$$g \leq e - 1.$$

PROOF. a) This is immediate from Corollary 3.41 and the above discussion.
b) We apply part a) with $d = 2$. □

EXERCISE 3.15. *Let k be a perfect field, let $n \geq 3$ be odd, and suppose that the characteristic of k does not divide n.*

a) *Show that for all $d \in \mathbb{Z}^+$, there is a separable polynomial $f \in k[x]$ of degree d. For such a polynomial, show that the function field K attached to the geometrically irreducible polynomial $y^n - f(x)$ has genus*

$$g = \frac{(n-1)(d-1)}{2} - \frac{\gcd(n, d) - 1}{2}.$$

Show: if $g \geq n - 1$ then K is not hyperelliptic.

b) *Suppose $n = p$ is an odd prime. Then*

$$g = \begin{cases} \frac{(p-1)(d-1)}{2} & p \nmid d \\ \frac{(p-1)(d-2)}{2} & p \mid d \end{cases}. \tag{34}$$

c) *Show that for $p = 3$ the set of genera that are of the form in part b) form a subset of $\mathbb{Z}^+$ of asymptotic density $\frac{2}{3}$. Show that for $p = 5$, the set of genera that are of the form in part b) form a subset of $\mathbb{Z}^+$ of asymptotic density $\frac{2}{5}$, and show that union of the two sets of genera obtained using $p = 3$ and $p = 5$ has asymptotic density $\frac{4}{5}$.*

d) *What is the asymptotic density of the set of positive integers g of the form (34) as we take the union over all odd prime numbers p?*

EXERCISE 3.16. *Let k be a perfect field. Show: for all $\gamma \in \mathbb{Z}^+$ there is a function field K/k with gonality at least γ – that is, every nonconstant rational function $f \in K$ has degree at least γ.*

An interesting application of Castelnuovo's Inequality to the gonality of modular curves in characteristic $p > 0$ was given by Poonen [**Po07**].

CHAPTER 4

Kähler Differentials and the Residue Theorem

1. Relative Kähler Differentials of a Function Field

For an extension $R \subset S$ of commutative rings, one normally writes $\Omega_{S/R}$ for the R-module of Kähler differentials. For a function field K/k, we have already defined the Weil differentials Ω_K of K. We now wish to explore the Kähler differentials of associated to $k \subset K$ and compare them to Weil differentials. **In order to reduce confusion we will use a more distinct notation for Kähler differentials in these notes, writing $\Lambda_{R/S}$ in place of $\Omega_{R/S}$.** In particular, $\Lambda_{K/k}$ is the K-module of Kähler differentials of K/k.

We refer to [**FT**, §13.2] for a discussion of Kähler differentials and their relation to derivations. Here we will only recall some of the most essential points. First of all we have the following crucial (but easy) result [**FT**, Prop. 13.19].

PROPOSITION 4.1. *Let $B \subset A$ be an extension of commutative rings. If M is an A-module and $D : A \to M$ is a B-derivation, then there is a unique A-module homomorphism $f : \Lambda_{A/B} \to M$ such that $D = f \circ d$. In other words, we have a natural isomorphism*

$$\mathrm{Der}_B(A, M) = \mathrm{Hom}_A(\Lambda_{A/B}, M). \tag{35}$$

If in (35) we take $M = A$, we get

$$\mathrm{Der}_B(A) = \mathrm{Hom}_A(\Lambda_{A/B}, A) = \Lambda_{A/B}^{\vee}. \tag{36}$$

The case of interest to us here is when $A = K$ and $B = L$ are both fields and $K \subset L$ is a finitely generated field extension. In this case we have $\mathrm{Der}_K(L)$ is a finite-dimensional L-vector space [**FT**, Prop. 13.4] which is the L-dual space of the L-vector space $\Lambda_{L/K}$, and it follows that $\Lambda_{L/K}$ is also a finite-dimensional L-vector space. Using the natural isomorphism from a finite-dimensional vector space to its second dual space, we have

$$\Lambda_{L/K} \xrightarrow{\iota} \Lambda_{L/K}^{\vee\vee} = \mathrm{Der}_K(L)^{\vee}.$$

In other words, each of $\Lambda_{L/K}$ and $\mathrm{Der}_K(L)$ is the L-dual of the other, which is perhaps best expressed by means of a perfect bilinear pairing $\Lambda_{L/K} \times \mathrm{Der}_K(L) \to L$. This pairing is quite concrete: for

$$\sum_{i=1}^{n} a_i dx_i \in \Lambda_{L/K},\ D \in \mathrm{Der}_K(L) \mapsto \left(\sum_{i=1}^{n} a_i dx_i\right)(D) = \sum_{i=1}^{n} a_i D(x_i) \in L.$$

EXERCISE 4.1. *Let $k \subset K$ be a field extension such that $K = k(S)$. Show: $\langle ds \mid s \in S \rangle_K = \Lambda_{K/k}$.*

Let K/k be a field extension. A subset $S \subset k$ is a **differential basis** of K/k if the mapping $S \to \Lambda_{K/k}$ given by $s \mapsto ds$ is injective and $\{ds \mid s \in S\}$ is a K-basis for $\Lambda_{K/k}$.

THEOREM 4.2. *Let K/k be a finitely generated field extension.*

a) *A separating transcendence basis for K/k is a differential basis for K/k.*
b) *If K/k is separable, then every differential basis for K/k is a separating transcendence basis for K/k.*

PROOF. This is [**FT**, Thm. 13.21]. □

COROLLARY 4.3. *If K/k is a regular function field, then $\dim_K \Lambda_{K/k} = 1$ and for $f \in K$ we have that df is a basis for $\Lambda_{K/k}$ iff $K/k(f)$ is a separable algebraic extension.*

For a function field K/k we say that $f \in K$ is a **separating element** if it forms a differential basis, i.e., if $K/k(f)$ is separable algebraic.

COROLLARY 4.4. *Let K be a field of characteristic $p > 0$, and let L/K be finitely generated and separable, of transcendence degree 1.*

a) *For $x \in L$, the following are equivalent:*
   (i) *We have that x is a **separating element** for L/K – i.e., x is a separating transcendence basis for L/K.*
   (ii) *We have $dx \neq 0$.*
   (iii) *We have that $x \notin KL^p$.*
   If K is perfect, the conditions are also equivalent to $x \notin L^p$.
b) *For each separating element x of L/K, there is a unique derivation $\delta_x \in \mathrm{Der}_K(L)$ such that $\delta_x(x) = 1$.*
c) *For separating elements x, y of L/K we have*

$$\delta_y = \delta_y(x)\delta_x. \tag{37}$$

d) *For $y \in K$, we have $\delta_x(y) \neq 0$ iff y is a separating element of L/K.*

PROOF. See [**FT**, Cor. 13.23]. □

EXERCISE 4.2. *Let k be a perfect field, and let K/k be a function field. Let $f \in K^\times$ be such that $v_P(f) = 1$ for some $P \in \Sigma(K/k)$. Show: f is a separating element of K/k.*

For a regular function field K/k, the K-vector spaces $\mathrm{Der}_k(K)$ and $\Lambda_{K/k}$ are mutually dual and 1-dimensional. For a separating element $f \in K$, the dual basis to df is a $\delta_f \in \mathrm{Der}_k(K)$ such that

$$1 = \langle \delta_f, df \rangle = \delta_f(f).$$

That is, for each separating f, there is a unique $\delta_f \in \mathrm{Der}_k(K)$ such that $\delta_f(f) = 1$.

If $x, y \in K$ with x a separating element, then dy and dx live in the one-dimensional K-vector space $\Lambda_{K/k}$ with $dx \neq 0$, and thus there is a unique $\alpha \in K$ such that $dy = \alpha dx$. This is the kind of situation that division was made for: we put

$$\frac{dy}{dx} \coloneqq \alpha \in K.$$

PROPOSITION 4.5. *Let $x, y, z \in K$, and suppose that x and y are separating elements. We denote by δ_x (resp. δ_y) the unique element of $\mathrm{Der}_k(K)$ such that $\delta_x(x) = 1$ (resp. such that $\delta_y(y) = 1$).*

a) *We have $\delta_x(y)\delta_y(x) = 1$.*
b) *We have $\frac{dy}{dx} = \delta_x(y)$.*
c) *We have $\frac{dz}{dx} = \frac{dz}{dy}\frac{dy}{dx}$; equivalently, we have $\delta_x(z) = \delta_y(z)\delta_x(y)$.*

PROOF. a) By (4.4) we have $\delta_y = \delta_y(x)\delta_x$ and thus of course also

$$\delta_x = \delta_x(y)\delta_y = \delta_x(y)\delta_y(x)\delta_x.$$

Since $\delta_x \neq 0$, the result follows.
b) There is a unique $\alpha \in K^\times$ such that $dy = \alpha dx$. Evaluating both sides at δ_x gives

$$\delta_x(y) = dy(\delta_x) = (\alpha dx)(\delta_x) = \alpha.$$

c) Indeed $\frac{dz}{dx} = \frac{dz}{dy}\frac{dy}{dx}$ holds just by cancelling the dy's (!!). Since

$$\frac{dz}{dx} = \delta_x(z),\ \frac{dz}{dy} = \delta_y(z),\ \frac{dy}{dx} = \delta_x(y),$$

the identity $\delta_x(z) = \delta_y(z)\delta_x(y)$ follows. □

2. Divisor of a Kähler Differential

In this section we assume that k is a perfect field.

To $\omega \in \Lambda_{K/k}^\bullet := \Lambda_{K/k} \setminus \{0\}$, we will associate a divisor $\operatorname{div}\omega \in \mathrm{Div}(K)$. For $P \in \Sigma(K/k)$, choose a uniformizer t_P at P: by Exercise 4.2 we have $dt_P \neq 0$, so there is a unique $f_P \in K^\times$ such that $\omega = f_P dt_P$. We put

$$v_P(\operatorname{div}\omega) := v_P(f_P) \in \mathbb{Z}.$$

There are two things to check: first that for all places P, the integer $v_P(f_P)$ is independent of the choice of uniformizer t_P, and second that we actually get a divisor: i.e., that $v_P(f_P) = 0$ for all but finitely many $P \in \Sigma(K/k)$.

But even before checking this, let us do the most basic possible example.

EXAMPLE 4.1. *Let k be algebraically closed. We take $K = k(x)$ and $\omega = dx$.*
• *When P is the place with uniformizer $x - a$ for $a \in k$, we take $t_P = x - a$. Then using Proposition 4.5b) we have*

$$\frac{dt_P}{dx} = \delta_x(t_P) = \delta_x(x - a) = 1,$$

so the coefficient of P in $\operatorname{div}\omega$ is

$$\omega = dx = 1dt_P, v_P(1) = 0.$$

• *When $P = P_\infty$ is the infinite place, we take $t_P = \frac{1}{x}$. Then*

$$\frac{dt_P}{dx} = \delta_X(t_O) = \delta_x(\frac{1}{x}) = \frac{-1}{x^2}.$$

So

$$dt_P = \frac{-1}{x^2}dx = \frac{-1}{x^2}\omega \text{ and } \omega = -x^2 dt_{P_\infty},$$

so the coefficient of P_∞ *in* $\operatorname{div}\omega$ *is*

$$v_{P_\infty}(-x^2) = -2.$$

Thus we have

$$\operatorname{div} dx = -2P_\infty.$$

EXERCISE 4.3. *Now let* k *be any perfect field and* $K = k(x)$*. Show that we still have* $\operatorname{div} dx = -2P_\infty$*. (The need for* k *to be perfect should arise during your calculation.)*

Now we show that $v_P(\operatorname{div}\omega)$ is independent of the choice of uniformizing element: if s, t are two uniformizers at P, we need $v_P(\frac{ds}{dt}) = 0$. This is easily verified using Laurent series expansions: write

$$s = \sum_{n=N}^{\infty} a_n t^n,\ a_N \neq 0.$$

Then we have

$$N = v_P(s) = 1,$$

so

$$\frac{ds}{dt} = a_1 + 2a_2 t + \dots$$

and thus $v_P(\frac{ds}{dt}) = 0$.

Finally, we show the finiteness of the support of $\operatorname{div}\omega$, in two steps.

Step 1: Suppose that k is algebraically closed, so $k_P = k$ for all $P \in \Sigma(K/k)$. Choose a separating element $f \in K$. The idea is as follows: away from the finitely many P with $v_P(f) < 0$, put $f(P) \coloneqq f \pmod{\mathfrak{m}_P} \in k$. Then $(f - f(P))(P) = 0$, so $v_P(f - f(P)) \geq 0$. It seems reasonable to hope that for all but finitely many P we have $v_P(f - f(P)) = 1$.

To see this, we observe that the extension $K/k(f)$ is finite separable, so only finitely many places ramify. Thus, for almost every $a \in k$, there are $n = [K : k(f)]$ places P of K such that $P \mid f - a$ and $e(P|f - a) = 1$. So

$$1 = e(P|f-a) = v_P(f-a) = v_P(f - f(P)) = v_P(f - f(P)).$$

Write $\omega = gdf$. For all but finitely many $P \in \Sigma(K/k)$, we take $t_P = f - a$. Then

$$\omega = gdf = gd(f - a).$$

Since g is fixed, we have $v_P(g) = 0$ for all but finitely many P.

Step 2: Now assume that k is perfect, let $f \in K/k$ be a separating element, and write $\omega = gdf$. At this point we have a well-defined element $\operatorname{div}\omega \in \prod_{P\in\Sigma(K/k)} \mathbb{Z}$, and we need to show that it actually lies in the direct sum. For this: the extension $K\overline{k}/\overline{k}(f)$ is finite separable, so f is separating for $K\overline{k}/\overline{k}$. Let $\overline{\omega}$ be $gdf \in \Lambda_{K\overline{k}/\overline{k}}$. Since $K\overline{k}/K$ is everywhere unramified, we find that

$$\operatorname{div}\overline{\omega} = \iota_{K\overline{k}/K} \operatorname{div}\omega.$$

In other words, for all $P \in \Sigma(K/k)$ and each of the finitely many places $Q \in \Sigma(K\overline{k}/\overline{k})$ with $Q \mid P$ we have

$$v_Q(\operatorname{div}(\overline{\omega})) = v_P(\operatorname{div}(\omega)).$$

It follows that $v_P(\mathrm{div}(\omega)) = 0$ for all but finitely many $P \in \Sigma(K/k)$.

3. Residue of a Kähler Differential

In this section we assume that k is a perfect field, except in Exercise 4.4.

Let K/k be a function field. Let $P \in \Sigma(K/k)$, with residue field k_P, and let $t \in K$ be a uniformizing element at P. Since k is perfect, k_P/k is a finite degree separable extension, and the P-adic completion $\hat{K}_P$ of K is canonically isomorphic, as a k-algebra, to $k_P((t))$.

EXERCISE 4.4. *Let k be any field (not necessarily perfect), let $\delta_t \in \mathrm{Der}_k(k(t))$ be the unique k-derivation with $\delta_t(t) = 1$, and let*

$$\hat{\delta} : k((t)) \to k((t)),\ \sum_{n=N}^{\infty} a_n t^n \mapsto \sum_{n=N}^{\infty} n a_n t^{n-1}.$$

a) *Show: $\hat{\delta}$ is a k-derivation of $k((t))$.*
b) *Show: for all $f \in k(t)$ we have $\hat{\delta}(f) = \delta_t(f)$. In particular, $\hat{\delta}(k(t)) \subset k(t)$.*

First of all t is a separating element for K/k: by Corollary 4.4a), this holds iff $t \notin kK^p = k^p K^P = (kK)^p = K^p$, and indeed a uniformizing element is not a pth power. Thus $K/k(t)$ is finite degree separable, so by [**FT**, Cor. 13.7] we have that $\delta_t \in \mathrm{Der}_k(k(t))$ extends uniquely to $\mathrm{Der}_k(K)$, and we continue to call the extension δ_t. Let $c_P : K \hookrightarrow k_P((t))$ be the completion map. Consider the following two k-derivations from K to $k_p((t))$:

$\delta_1 = \hat{\delta}|_K$.
$\delta_2 \coloneqq c_P \circ \delta_t$.

We have $\delta_1, \delta_2 \in \mathrm{Der}_k(K, k_P((t)))$, and upon restriction to $k(t)$ the two derivations are each δ_t (for δ_1 this is Exercise 4.4). If δ_1, δ_2 took values in K, it would follow from [**FT**, Cor. 13.7] that they must be equal, but because they take values in the larger field $k_P((t))$ that result does not apply. The method of proof does, and I plan to modify [**FT**, §13] accordingly. In the meantime, the equality of $\delta_1 = \delta_2$ follows from [**St**, Prop. 4.1.4]. From this and from Proposition 4.5b) we deduce:

COROLLARY 4.6. *For a place $P \in \Sigma(K/k)$ a uniformizer t at P and all $z \in K$, if we write*

$$z = \sum_{n=N}^{\infty} a_n t^n,$$

then we have

$$\frac{dz}{dt} = \delta_t(z) = \sum_{n=N}^{\infty} n a_n t^{n-1} \in K.$$

With notation as in Corollary 4.6, we define

$$\mathrm{res}_{P,t}(z) \coloneqq a_{-1}.$$

Thus we define the residue of an element of K at a place P with respect to a uniformizer t as the -1th Laurent series coefficient. It is clear that the map

$$\mathrm{res}_{P,t} : K \to k_P$$

is a k-linear and vanishes on R_P. This is not quite what we want, because the residue *does* depend on the choice of uniformizer t, however in a precise way:

THEOREM 4.7. *Let $P \in \Sigma(K/k)$, and let s, t be two uniformizers at P. Then for all $z \in K$, we have*

$$\operatorname{res}_{P,s}(z) = \operatorname{res}_{P,t}\left(z\frac{ds}{dt}\right). \tag{38}$$

PROOF. See [**St**, Prop. 4.2.9]. □

A little reflection on (38) with a differential analytic eye reveals that it is saying that the residue is not intrinsic to the function z but rather to the differential 1-form zds. In our algebraic context, this means: for a Kähler differential $\omega \in \Lambda_{K/k}$ and $P \in \Sigma_{K/k}$, we may choose any uniformizer t at P, write

$$\omega = udt$$

and define

$$\operatorname{res}_P(\omega) \coloneqq \operatorname{res}_{P,t}(u).$$

This is well-defined, because if s is another uniformizer at P and we write

$$udt = \omega = vds,$$

then by Theorem 4.7 we have

$$\operatorname{res}_{P,s}(v) = \operatorname{res}_{P,t}\left(v\frac{ds}{dt}\right) = \operatorname{res}_{P,t}(u).$$

We can now state an elegant and powerful result.

THEOREM 4.8 (Residue Theorem). *Let k be an algebraically closed field, let K/k be a function field, and let $w \in \Lambda^{\bullet}_{K/k}$. Then:*

a) *For all but finitely many $P \in \Sigma(K/k)$ we have $\operatorname{res}_P(w) = 0$.*
b) *We have $\sum_{P\in\Sigma(K/k)} \operatorname{res}_P(w) = 0$.*

We will deduce Theorem 4.8 from a later result (that unfortunately we will note prove in this iteration of these notes!), but first let us make some remearks.

• Why did we assume that $\overline{k} = k$? Over any perfect field k, for any $w \in \Lambda_{K/k}$ and $P \in \Sigma(K/k)$ we have $\operatorname{res}_P(w) \in k_P$. In order to add the residues at different places they should all take values in the same field. As we know, we have $k_P = k$ for all $P \in \Sigma(K/k)$ iff k is algebraically closed.

• The Residue Theorem can be viewed as a reciprocity law, a global constraint on local contributions, similar to the Brauer-Hasse-Noether Theorem for the Brauer group of a global field K [**Hi**, Thm. 14.11]:

$$0 \longrightarrow \operatorname{Br}(K) \to \bigoplus_{v\in\Sigma(K)} \operatorname{Br}(K_v) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \to 0.$$

For a wonderful exposition of geometric reciprocity laws related to the Residue Theorem, please consult [**S**].

• In any around, the proof involves a reduction to the case of a rational function field $k(X)$. The case of characteristic 0 is much easier than the case of positive

characteristic. When k is algebraically closed of characteristic 0, one can easily reduce to the case of $k = \mathbb{C}$ (an instance of the so-called "Lefschetz Principle"). The Residue Theorem on a compact Riemann surface is part of complex function theory.

Of course there is a "residue theorem" from more basic complex analysis. Let us now quickly sketch how the residue theorem for $K = \mathbb{C}(z)$ is a consequence of this truly basic and familiar result. We are given a meromorphic function on the Riemann sphere $f : \hat{\mathbb{C}} \to \hat{C}$. Let γ be a positively oriented simple closed curve in $\mathbb{C}$ such that f is regular on the complement of γ. Let $P_1, \ldots, P_m$ be the poles of f *inside* γ and let $Q_1, \ldots, Q_n$ be the poles of f *outside* γ. Then the residue theorem from undergraduate complex analysis tells us

$$\frac{1}{2\pi i}\int_\gamma f = \sum_{i=1}^m \operatorname{res}(f, P_i).$$

However, on the Riemann sphere we can also consider the region *outside* γ and integrate over that:

$$\frac{1}{2\pi i}\int_{\overline{\gamma}} f = \sum_{j=1}^n \operatorname{res}(f, Q_j)$$

Here we write $\overline{\gamma}$ because the choice of a coordinate chart on the exterior of γ involves reversing the orientation on γ. It follows that

$$\sum_{j=1}^n \operatorname{res}(f, Q_j) = \frac{1}{2\pi i}\int_{\overline{\gamma}} f = \frac{-1}{2\pi i}\int_\gamma f = -\sum_{i=1}^m \operatorname{res}(f, P_i),$$

and thus the sum over all the residues of f is 0. Here we integrated a function and not a differential, as is done in classical complex analysis This is permissible because the Riemann sphere comes equipped with the canonical coordinate function z, allowing us to pass back and forth from the function f to the differential $f dz$.

We now come to the larger result that implies Theorem 4.8. We return to the context of a perfect (but not necessarily algebraically closed) field k. By Exercise 5.1, on the function field $k(x)/k$ there is a unique Weil differential η such that

$$(\eta) = -2P_\infty,\ \eta_{P_\infty}(1/x) = -1.$$

Now for a function field L/k we define an L-linear map

$$\partial : L \to \Omega_L$$

as follows:
• if $x \in L$ is *not* a separating element, we put $\partial x \coloneqq 0$.
• If $x \in L$ is a separating element, then $K \coloneqq k(x)$ is such that L/K is a finite separable extension, and we put

$$\partial x \coloneqq \eta^* \in \Omega_L^\bullet,$$

the pullback of η in the finite degree separable extension L/K. Since $\dim_L \Omega_L = 1$, for all $\omega \in \Omega_L$ and all separating elements $x \in L$, there is a unique $z \in L$ such that

$$\omega = z\partial x.$$

Above we entertained a function field L so as to be able to write $K = k(x)$ and use the notation of the pullback of Weil differentials. Having made that definition we notationally revert to a function field K/k.

THEOREM 4.9 (Kähler-Weil Theorem). *Let k be a perfect field, and let K/k be a function field.*

a) *We have $\partial \in \mathrm{Der}_k(K, \Omega_K)$.*
b) *The map $\mu : \Lambda_{K/k} \to \Omega_{K/k}$ given by $zdx \mapsto z\partial x$ is a K-vector space isomorphism.*
c) *We have $\partial = \mu \circ d$. It follows that $\partial : K \to \Omega_K$ is (also!) a universal k-derivation on K.*
d) *If $P \in \Sigma_1(K/k)$, $\omega = z\partial x \in \Omega_K$ and $w = zdx \in \Lambda_{K/k}$, then for all $u \in K$ we have*
$$\omega_P(u) = \mathrm{res}_P(uzdx) = \mathrm{res}_P(uw).$$
In particular we have
$$\mathrm{res}_P(w) = \omega_P(1).$$
e) *If t is a uniformizing element at P and $\omega = z\partial t$, put $w = zdt = \mu^{-1}(\omega)$. Then we have $v_P(\omega) = v_P(z) = v_P(w)$. In other words, we have*
$$(\omega) = \mathrm{div}(w). \tag{39}$$

Thus, although Weil differentials and Kähler differentials look like quite different objects, Theorem 4.9 shows that in the case of a perfect ground field there is a *complete equivalence* between them.

Now suppose that $k = \overline{k}$, so $\Sigma(K/k) = \Sigma_1(K/k)$. Then for all $w \in \Lambda_{K/k}$ and corresponding Weil differential $\omega \coloneqq \mu(w)$, Theorem 4.9d) combined with Proposition 2.20b) gives
$$\sum_{P \in \Sigma(K/k)} \mathrm{res}_P(w) = \sum_{P \in \Sigma(K/k)} \omega_P(1) = \omega(1) = 0.$$
This shows that the Residue Theorem is a consequence of Theorem 4.9.

In the Fall 2020 course we did not have time to prove Theorem 4.9, and unfortunately we do not include a proof in this iteration of these notes. A complete proof can be found in [**St**, §4.3] – it runs about eight pages.

As a final comment on this topic, we explain how the restriction to an algebraically closed ground field in the Residue Theorem is no that serious. For any perfect field k, write $\tilde{K} \coloneqq K\overline{k}$. Then we have a map
$$\Omega_K \hookrightarrow \Omega_{\tilde{K}},\ z\partial x \mapsto z\tilde{\partial} x.$$
If $P \in \Sigma(K/k)$ has degree d, then in the separable algebraic extension $\tilde{K}/K$ the place P splits into degree 1 places $Q_1, \ldots, Q_d$. Then:
$$\forall \omega \in \Omega_K,\ \forall u \in K, \forall P \in \Sigma(K/k),\ \omega_P(u) = \sum_{i=1}^{d} \mathrm{res}_{Q_i}(u\mu^{-1}(\omega)).$$
Thus over any perfect ground field, local components of Weil differentials can be expressed in terms of residues of Kähler differentials.

CHAPTER 5

Function Fields Over a Finite Field

Thorughout this chapter the ground field $k = \mathbb{F}_q$ is finite and K/k is a one variable function field with constant field $\mathbb{F}_q$. Since $\mathbb{F}_q$ is perfect, this means that all our function fields are regular.

For such a field δ we denote the least positive degree of a divisor on K by δ. For a function field over an arbitrary ground field we have already denoted this quantity by $I(K)$ and called it the **index**. We see relatively soon that for curves over a finite field, the index is always equal to 1, so you should keep in mind that δ is a quantity that in due logical course will be shown to be 1. As for curves over any ground field, the existence of the canonical divisor of degree $2g-2$ implies that

$$\delta \mid 2g - 2.$$

1. Finiteness of the Divisor Class Group

LEMMA 5.1. *Let $K/\mathbb{F}_q$ be a function field.*

a) *For all $d \in \mathbb{Z}^+$, there are only finitely many places of degree d.*
b) *For all $n \in \mathbb{N}$, there are only finitely many effective divisors of degree n.*

PROOF. a) If L/K is a finite degree extension of function fields over $\mathbb{F}_q$, then since the restriction map $r : \Sigma(L/\mathbb{F}_q) \to \Sigma(K/\mathbb{F}_q)$ is surjective with finite fibers, the field K has infinitely many points of bounded degree iff the field L has infinitely many points of bounded degree. Thus we can reduce to the case $K = \mathbb{F}_q(t)$, in which case the result asserts that there are only finitely many monic irreducible polynomials $f \in \mathbb{F}_q[t]$ of bounded degree, which is certainly true.
b) Clearly there is a unique effective divisor of degree 0. For $n \in \mathbb{Z}^+$, if N_n is the number of places of degree at most n, then an effective divisor of degree n is a sum of the form $\sum a_P P$ where P has degree at most n and $0 \leq a_P \leq n$ (and all such sums give effective divisors, but perhaps of degree larger than n). So the number of effective divisors of degree n is certainly no more than $(n+1)^{N_n}$. □

PROPOSITION 5.2. *For a function field $K/\mathbb{F}_q$, the degree 0 divisor class group $\mathrm{Cl}^0 K$ is finite.*

PROOF. Let g be the genus of K, and choose a divisor $B \in \operatorname{Div} K$ of degree $n \geq g$. We denote by $\mathrm{Cl}^n K$ the subset of linear equivalence classes of divisors of degree 0. Being a nonempty fiber of the map $\deg : \operatorname{Cl} K \to \mathbb{Z}$ it is a coset of Cl^0, so it has the same cardinality as Cl^0 and it suffices to show that Cl^n is finite. By Riemann-Roch, every element of Cl^n is represented by an effective divisor, and by Lemma 5.1 there are only finitely many effective divisors of degree n. □

We denote the size of the group $\mathrm{Cl}^0 K$ by h and call it the **class number** of K.

REMARK 3. *It is beyond the scope of this course, but in fact* $\mathrm{Cl}^0 K$ *is the group of* $\mathbb{F}_q$*-rational points of the Jacobian abelian variety.*

For $n \in \mathbb{N}$, let $A_n(K)$ be the number of effective degree n divisors on K. We abbreviate to A_n when K is fixed.

For $D \in \operatorname{Div} K$, since $\deg D$ and $\ell(D)$ depends only on the linear equivalence class of D, we allow ourselves to write $\deg[C]$ and $\ell([C])$ for a class $[C] \in \operatorname{Cl} K$.

LEMMA 5.3. *Let* $K/\mathbb{F}_q$ *be a function field. Recall that* $I(K)$ *is the least positive degree of a divisor on* K*.*

a) *If* $A_n \neq 0$ *then* $I(K) \mid n$*.*
b) *For* $C \in \operatorname{Cl} K$*, the number of effective divisors* A *in the the divisor class* C *is* $\frac{q^{\ell(C)}-1}{q-1}$*.*
c) *For all* $n > 2g-2$ *such that* $I(K) \mid n$*, we have*

$$A_n = \frac{h(q^{n+1-g}-1)}{q-1}.$$

PROOF. a) The image of the degree map is a subgroup of $\mathbb{Z}$, so if its least positive element is $I(K)$ then its image if $I(K)\mathbb{Z}$.
b) As remarked upon before, over any ground field k the set of effective divisors linearly equivalent to a given divisor D can be identified with the projectivization of the Riemann-Roch space $\mathcal{L}(D)$. The projectivization of a d-dimensional vector space over $\mathbb{F}_q$ has size $\frac{q^d-1}{q-1}$.
c) Since $I(K) \mid n$, $\mathrm{Cl}^n K$ is a coset of $\mathrm{Cl}^0 K$, so there are h divisor classes of degree n. By part b) and Riemann-Roch, each such class C contains $\frac{q^{\ell(C)}-1}{q-1} = \frac{q^{n+1-g}-1}{q-1}$ effective divisors. □

2. From K to K_r

Let $K/\mathbb{F}_q$ be a one variable function field over the finite field $\mathbb{F}_q$ with constant subfield $\mathbb{F}_q$. Since $\mathbb{F}_q$ is perfect, the extension $K/\mathbb{F}_q$ is regular. Let $\overline{\mathbb{F}_q}$ be an algebraic closure of $\mathbb{F}_q$. Then for all $r \in \mathbb{Z}^+$ there is a unique degree r subextension $\mathbb{F}_{q^r}$ of $\overline{\mathbb{F}_q}/\mathbb{F}_q$, which is cyclic with Galois group generated by the Frobenius map $x \mapsto x^q$. We denote by K_r the extension $K\mathbb{F}_{q^r} \cong K \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$ and view it as a function field over $\mathbb{F}_{q^r}$.

LEMMA 5.4. *Let* $P \in \Sigma(K/\mathbb{F}_q)$ *be a place of degree* d*. Let* $r \in \mathbb{Z}^+$*. Then there are* $\gcd(d,r)$ *places* Q *of* K_r *lying over* P*, each of degree* $\frac{d}{\gcd(d,r)}$ *and with residue field* $\mathbb{F}_{q^{\operatorname{lcm}(d,r)}}$*.*

PROOF. The extension K_r/K is Galois of degree r, so as ever for a finite Galois extension of Dedekind domains, we have

$$efs = r,$$

where $e = e(Q|P)$, $f = f(Q|P)$ and s is the number of places $Q \mid P$. Since K_r/K is a separable constant field extension, Theorem 3.22 applies. For starters, Theorem 3.22a) gives $e = 1$, so $s = \frac{r}{f}$. Next, by Theorem 3.22g) we get that for all $Q \mid P$, the residue field l_Q is the compositum $k_P l$. We work inside a fixed algebraic closure

of $\overline{\mathbb{F}}_q$, in which for all $N \in \mathbb{Z}^+$ we have a unique finite field $\mathbb{F}_{q^N}$. Thus we may indentify k_P with $\mathbb{F}_{q^d}$ and l with $\mathbb{F}_{q^r}$, so the residue field at Q is

$$l_Q = k_P l = \mathbb{F}_{q^d}\mathbb{F}_{q^r} = \mathbb{F}_q^{\operatorname{lcm}(d,r)},$$

as claimed. Thus we have

$$f = f(Q|P) = [\mathbb{F}_{q^{\operatorname{lcm}(d,r)}} : \mathbb{F}_{q^d}] = \frac{\operatorname{lcm}(d,r)}{d} = \frac{dr/\gcd(d,r)}{d} = \frac{r}{\gcd(d,r)}$$

and

$$s = \frac{r}{f} = \gcd(d,r),$$

as claimed. Since each Q has residue field $\mathbb{F}_{q^{\operatorname{lcm}(d,r)}}$ and the constant subfield of K_r is $\mathbb{F}_{q^r}$, each place $Q \mid P$ has degree

$$\mathbb{F}_{q^{\operatorname{lcm}(d,r)}} : \mathbb{F}_{q^r}] = \frac{\operatorname{lcm}(d,r)}{r} = \frac{dr/\gcd(d,r)}{r} = \frac{d}{\gcd(d,r)}. \qquad \square$$

For $r \in \mathbb{Z}^+$, we put $N_r \coloneqq \#\Sigma_1(K_r/\mathbb{F}_{q^r})$.

COROLLARY 5.5. *Let $K/\mathbb{F}_q$ be a function field. For all $r, s \in \mathbb{Z}^+$, if $r \mid s$ then $N_r \leq N_s$.*

PROOF. Replacing K with K_r and s with $\frac{s}{r}$, we may assume that $r = 1$. Applying Lemma 5.4 with $d = 1$, we find that for every degree one place v of K, there is exactly one place w of K_r lying over v, and this place also has degree 1. $\square$

3. Introducing the Hasse-Weil Zeta Function

For a function field $K/\mathbb{F}_q$, recall that $A_n = A_n(K)$ is the number of effective degree n divisors. We define the **zeta function** of $K/\mathbb{F}_q$ as the formal power series

$$Z(t) = \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}[[t]].$$

PROPOSITION 5.6. *Let $K/\mathbb{F}_q$ be a function field of genus g.*

a) *If $F/\mathbb{F}_q$ has genus zero, then*

$$Z(t) = \frac{1}{q-1}\left(\frac{q}{1-q^\delta t^\delta} - \frac{1}{1-t^\delta}\right).$$

b) *If $g \geq 1$, then $Z(t) = F(t) + G(t)$, with*

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg C \leq 2g-2} q^{\ell(C)} t^{\deg C},$$

the sum extending over all divisor classes C with $0 \leq \deg C \leq 2g-2$, and

$$G(t) = \frac{h}{q-1}\left(\frac{q^{1-g}(qt)^{2g-2+\delta}}{1-(qt)^\delta} - \frac{1}{1-t^\delta}\right).$$

PROOF. a) Suppose $g = 0$. By Exercise 2.17a) we have $h = 1$. Since every $n \in \mathbb{N}$ exceeds $2g-2$, we may compute the zeta function using Lemma 5.3c):

$$\sum_{n=0}^{\infty} A_n t^n = \sum_{n=0}^{\infty} A_{\delta n} t^{\delta n} = \sum_{n=0}^{\infty} \frac{q^{\delta n+1}-1}{q-1} t^{\delta n}$$

$$= \frac{1}{q-1}\left(q\sum_{n=0}^{\infty}(qt)^{\delta n} - \sum_{n=0}^{\infty}t^{\delta n}\right) = \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\delta}} - \frac{1}{1-t^{\delta}}\right).$$

b) We have

$$\sum_{n=0}^{\infty}A_n t^n = \sum_{\deg C\geq 0}\#\{A\in C \mid A\geq 0\}t^{\deg C} = \sum_{\deg C\geq 0}\frac{q^{\ell(C)}-1}{q-1}t^{\deg C}$$

$$\frac{1}{q-1}\left(\sum_{0\leq \deg C\leq 2g-2}q^{\ell(C)}t^{\deg C} + \sum_{\deg C>2g-2}q^{\deg C-g+1}t^{\deg C} - \sum_{\deg C\geq 0}t^{\deg C}\right)$$
$$= F(t)+G(t),$$

where

$$F(t) = \frac{1}{q-1}\sum_{0\leq \deg C\leq 2g-2}q^{\ell(C)}t^{\deg C}$$

and

$$(q-1)G(t) = \sum_{n=\frac{2g-2}{\delta}+1}^{\infty}hq^{n\delta+1-g}t^{n\delta} - \sum_{n=0}^{\infty}ht^{n\delta}$$

$$= hq^{1-g}\sum_{n=\frac{2g-2}{\delta}+1}^{\infty}((qt)^{\delta})^n - \frac{h}{1-t^{\delta}}$$

$$= \frac{hq^{1-g}(qt)^{2g-2+\delta}}{1-(qt)^{\delta}} - \frac{h}{1-t^{\delta}}.$$ □

It follows that $Z(t)\in\mathbb{C}(t)\subset\mathbb{C}((t))$, that is, it is a rational function of t.

EXERCISE 5.1. *Show: the power series $\sum_{n=0}^{\infty}A_n t^n$ is convergent for all $|t|<\frac{1}{q}$.*

4. Some Generalities on Zeta Functions

We digress to give some not-so-deep general facts on zeta functions. At the utmost level of generality (indeed, so general as to be completely divorced from any algebraic or geometric considerations), a zeta function is a kind of generating function for a sequence of numbers.

Let $f:\mathbb{Z}^+\to\mathbb{C}$ be an arithmetic function. To this we associate a Dirichlet series

$$D(f) = \sum_{n=1}^{\infty}\frac{f(n)}{n^s}.$$

We consider this Dirichlet series formally unless otherwise mentioned – issues of convergence are certainly important in some contexts but do not play any role for us here. There is a very simple algebraic formalism for these Dirichlet series: the **Dirichlet ring** $\mathcal{D}(\mathbb{C})$ is the set of all functions $f:\mathbb{Z}^+\to\mathbb{C}$, with

$$(f+g)(n) \coloneqq f(n)+g(n),$$
$$(f\bullet g)(n) \coloneqq \sum_{d|n}f(d)g(\frac{n}{d}).$$

That is, the sum is the expected pointwise one but the product is "Dirichlet convolution." The point of these operations is that

$$\forall f, g \in \mathcal{D}(\mathbb{C}),\ D(f+g) = D(f) + D(g),\ D(f \bullet g) = D(f)D(g).$$

One checks that $(\mathcal{D}(\mathbb{C}), +, \cdot)$ forms a commutative ring with identity element

$$\delta(n) = \begin{cases} 1 & n = 1 \\ 0 & n \geq 2 \end{cases}.$$

THEOREM 5.7 (Cashwell-Everett [**CE59**]). *The ring $\mathcal{D}(\mathbb{C})$ is isomorphic to $\mathbb{C}[[\{t_n\}_{n=1}^{\infty}]]$, i.e., to the formal power series ring over $\mathbb{C}$ in a countably infinite set of indeterminates. It is therefore (by a previously known, though not completely obvious result) a unique factorization domain.*

EXERCISE 5.2. *Let $f \in \mathcal{D}(\mathbb{C})$.*

a) *Recall that f is called **multiplicative** if for all $a, b \in \mathbb{Z}^+$ with $\gcd(a,b) = 1$ we have $f(ab) = f(a)f(b)$. Show: f is multiplicative iff*

$$D(f) = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \ldots + \frac{f(p^n)}{p^{ns}} + \ldots\right).$$

b) *Recall that f is called **completely multiplicative** if for all $a, b \in \mathbb{Z}^+$ we have $f(ab) = f(a)f(b)$. Show: f is completely multiplicative if*

$$D(f) = \prod_p \left(1 - \frac{f(p)}{p^s}\right)^{-1}.$$

For a ring R and $n \in \mathbb{Z}^+$, let $a_n(R)$ be the number of ideals I of R such that $\#R/I = n$. In general this is a cardinal number, but one does not have to assume much about R in order for all the $a_n(R)$'s to be finite.

THEOREM 5.8. *If R is a Noetherian ring, then $a_n(R) < \aleph_0$ for all $n \in \mathbb{Z}^+$.*

PROOF. See [**CA**, Thm. 22.3]. □

So for a Noetherian ring R, one can defne

$$\zeta_R(s) \coloneqq \sum_{n=1}^{\infty} \frac{a_n(R)}{n^s}.$$

We will only consider the case where R is a Dedekind domain that is moreover residually finite: R/I is finite for all noznero ideals I of R. In this case, for an nonzero ideal I of R, we put $|I| \coloneqq \#R/I$.

EXAMPLE 5.1. *Let K be a number field, and let R be the ring of integers of K.*

a) *When $R = \mathbb{Z}$, we have $a_n(R) = 1$ for all $n \in \mathbb{Z}^+$, and thus*

$$\zeta_{\mathbb{Z}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

*This is the **Riemann zeta function** – arguably the most important function in all of mathematics.*

b) *For a general number field K, $\zeta_R(s)$ is the **Dedekind zeta function** of K, which is of critical impotance in algebraic/analytic number theory.*

EXERCISE 5.3. *Let R be a residually finite Dedekind domain.*

a) *Show:*

$$\zeta_R(s) = \prod_{\mathfrak{p} \in \operatorname{MaxSpec} R} \left(1 - |\mathfrak{p}|^{-s}\right)^{-1}.$$

b) Supose R is a DVR with residue field $\mathbb{F}_q$. Show:

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

c) Show:

$$\zeta_R(s) = \prod_{\mathfrak{p} \in \operatorname{MaxSpec} R} \zeta_{R_\mathfrak{p}}(s).$$

EXAMPLE 5.2. *Let R be the affine Dedekind domain $\mathbb{F}_q[t]$. We have*

$$\zeta_R(s) = \sum_{g \ monic} q^{-\deg(g)s} = \sum_{n=0}^{\infty} q^{n-ns} = \left(1 - q^{1-s}\right)^{-1}.$$

Thus if we put $T \coloneqq q^{-s}$, we get

$$\zeta_R(T) = \frac{1}{1 - qT}.$$

Following Serre, we will now consider zeta functions in a more general sense. Our approach is "lightly scheme-theoretic," but many important special cases should make sense without any knowledge of scheme theory. Namely, if X is a finite-type $\mathbb{Z}$-scheme, let $|X|$ denote the set of closed points of X. For each closed point $x \in \overline{X}$, the residue field $k(x)$ is finite, and we denote its cardinality by $N(x)$. We define

$$\zeta(X, s) \coloneqq \prod_{x \in \overline{X}} \left(1 - N(x)^{-s}\right)^{-1}.$$

Let us debrief a bit: if X is a scheme that has finite type over $\mathbb{Z}$ and is moreover **affine**, then $X \cong \operatorname{Spec} R$ for a finitely generated $\mathbb{Z}$-algebra R, and $\overline{X}$ may be identified with $\operatorname{MaxSpec} R$. Let $\mathfrak{p}$ be a maximal ideal in the finitely generated $\mathbb{Z}$-algebra R. By [**CA**, Exc. 12.3, Thm. 12.15], the pullback of $\mathfrak{p}$ to $\mathbb{Z}$ is maximal in $\mathbb{Z}$ and $\mathfrak{p}$ contains a prime number p. It follows that $R/\mathfrak{p}$ is a field that is finitely generated as an $\mathbb{F}_p$-algebra, so by Zariski's Lemma it is a finite field $\mathbb{F}_q$. Let $|\mathfrak{p}| \coloneqq \#R/\mathfrak{p}$. Then we have

$$\zeta(\operatorname{Spec} R, s) = \prod_{\mathfrak{p} \in \operatorname{MaxSpec} R} \left(1 - |\mathfrak{p}|^{-s}\right).$$

As a special case of this, if R is moreover a Dedekind domain that is not a field, then we have

$$\zeta_{\operatorname{Spec} R}(s) = \zeta_R(s)$$

i.e., the zeta function coincides with the zeta function in the above sense. As a warning, this is *not* the case for a general finitely generated $\mathbb{Z}$-algebra. Indeed, in the special case $R = \mathbb{F}_q$ we have

$$\zeta_{\mathbb{F}_q}(s) = \frac{1}{1^s} + \frac{1}{q^s} = 1 + q^{-s},$$

whereas

$$\zeta_{\operatorname{Spec} \mathbb{F}_q}(s) = \left(1 - q^{-s}\right)^{-1} = 1 + q^{-s} + q^{-2s} + \dots.$$

In the general case of a finite type $\mathbb{Z}$-scheme X, it follows directly from the definition that whenever $X = \coprod_{i\in I} X_i$ is a disjoint union of subschemes – a possibly infinite union, in which each X_i can be either open or closed – then we have

$$\zeta(X, s) = \prod_{i\in I} \zeta(X_i, s).$$

With such a permissive notion of admissible decomposition, every finite type $\mathbb{Z}$-scheme can be written as a finite disjoint union of affine schemes: the basic idea is to take an affine open subscheme of each irreducible component, and then the complementary part of the component is a closed subscheme of smaller dimension, allowing an inductive argument. For example, in this way we can write projective N-space over $\mathbb{F}_q$ as

$$\mathbb{P}^N = \mathbb{A}^N \coprod \mathbb{P}^{N-1} = \mathbb{A}^N \coprod (\mathbb{A}^{N-1} \coprod \mathbb{P}^{N-2}) = \ldots = \coprod_{i=0}^{N} \mathbb{A}^i,$$

hence

$$\zeta(\mathbb{P}^N/\mathbb{F}_q, s) = \prod_{i=0}^{N} \zeta(\mathbb{A}^{\mathbb{N}}/\mathbb{F}_q, s).$$

Let us now compute the zeta function of $\mathbb{A}^{\mathbb{N}}/\mathbb{F}_q$, i.e., of $\operatorname{Spec} \mathbb{F}_q[t_1, \ldots, t_n]$. The key is the following result.

PROPOSITION 5.9. *Let R be a finitely generated $\mathbb{Z}$-algebra. Then we have*

$$\zeta(\operatorname{Spec} R[t], s) = \zeta(\operatorname{Spec} R, s-1).$$

PROOF. As above, the ring $\mathbb{Z}$ is Hilbert-Jacobson and R is finitely generated over $\mathbb{Z}$ hence R is also Hilbert-Jacobson. By [**CA**, Thm. 12.15], if $\mathcal{P} \in \operatorname{MaxSpec} R[t]$, then $\mathfrak{p} := \mathcal{P} \cap R$ is a maximal ideal of R. Let $k(\mathfrak{p}) = R/\mathfrak{p}$, a finite field. By [**CA**, §7.3], the set of $\mathcal{P} \in \operatorname{MaxSpec} R[t]$ that pull back to $\mathfrak{p}$ may be identified with $\operatorname{MaxSpec}(R[t] \otimes_R k(\mathfrak{p})) = \operatorname{MaxSpec} k(\mathfrak{p})[t]$. It follows that

$$\zeta(\operatorname{Spec} R[t], s) = \prod_{\mathfrak{p}\in\operatorname{MaxSpec}(R)} \prod_{\mathbb{P}\in\operatorname{MaxSpec} k(\mathfrak{p})[t]} (1 - |\mathcal{P}|^{-s})^{-1}$$

$$= \prod_{\mathfrak{p}\in\operatorname{MaxSpec}(R)} \zeta(k(\mathfrak{p})[t], s) = \prod_{\mathfrak{p}\in\operatorname{MaxSpec}(R)} \left(1 - |k(\mathfrak{p})|^{1-s}\right)^{-1}$$

$$= \zeta(\operatorname{Spec} R[t], s-1). \qquad \square$$

We deduce:

COROLLARY 5.10. *Let q be a prime power, and put $T := q^{-s}$.*

a) *We have*

$$\zeta(\mathbb{A}^N_{/F_q}, s) = \zeta(\operatorname{Spec} \mathbb{F}_q[t_1, \ldots, t_n], s) = (1 - q^{N-s})^{-1}.$$

b) *We have*

$$\zeta(\mathbb{P}^N_{/\mathbb{F}_q}, s) = \frac{1}{(1-q^{-s})(1-q^{1-s})\cdots(1-q^{N-s})}.$$

Now let $X_{/\mathbb{F}_q}$ be a finite type scheme. We will derive a more down-to-earth representation of $\zeta(X,s)$ as a generating function.

For $n \in \mathbb{Z}^+$, let

$$a_n(X) = \#\{x \in \overline{X} \mid N(x) = q^n\}$$

be the number of closed points of degree n, and let $\#X(\mathbb{F}_{q^n})$ denote the number of points of X with values in $\mathbb{F}_{q^n}$.

LEMMA 5.11. *For all $n \in \mathbb{Z}^+$, we have*

$$\#X(\mathbb{F}_{q^n}) = \sum_{k|n} k a_k(X). \tag{40}$$

PROOF. The elements of $X(\mathbb{F}_{q^n})$ are the morphisms $\operatorname{Spec} \mathbb{F}_{q^n} \to X$. In turn such morphisms correspond pairs (x, ι) with $x \in \overline{X}$ and $\iota : \operatorname{Spec} \mathbb{F}_{q^n} \to \operatorname{Spec} k(x)$, i.e., to a field embedding $k(x) \hookrightarrow \mathbb{F}_{q^n}$. Such an embedding exists iff $[k(x) : \mathbb{F}_q] \mid n$, in which case there are precisely $[k(x) : \mathbb{F}_q]$ of them. We're done. □

For $X_{/\mathbb{F}_q}$, we put

$$Z(X,T) = \prod_{x \in \overline{X}} \left(1 - T^{\deg x}\right)^{-1}, \tag{41}$$

so

$$\zeta(X,s) = Z(X, q^{-s}).$$

THEOREM 5.12. *Let $X_{/\mathbb{F}_q}$ be a finite type scheme. Then we have a formal power series identity*

$$\log Z(X,T) = \sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{q^n}) T^n}{n}.$$

PROOF. We have

$$Z'(X,T) = \sum_{x \in X} Z_X(t)(1 - t^{\deg x}) \cdot \left(\frac{(\deg x) t^{\deg x - 1}}{(1 - t^{\deg x})^2} \right),$$

so

$$T(\log Z(X,T))' = T \frac{Z'(X,T)}{Z(X,T)} = \sum_{x \in \overline{X}} \frac{(\deg x) T^{\deg x}}{1 - T^{\deg x}}$$

$$= \sum_{x \in \overline{X}} \sum_{n=1}^{\infty} (\deg x) T^{n \deg x} = \sum_{n=1}^{\infty} \sum_{k|n} k a_k(X) T^n = \sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n}) T^n.$$

Thus

$$(\log Z(X,T))' = \sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n}) T^{n-1},$$

and integrating both sides gives the result. □

EXERCISE 5.4. *Use Theorem 5.12 to show (again; cf. Corollary 5.10) that*

$$Z(\mathbb{A}^n_{/\mathbb{F}_q}, T) = (1 - q^N T)^{-1}$$

and

$$Z(\mathbb{P}^n_{/\mathbb{F}_q}, T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^N t)}.$$

Let $X_{/\mathbb{F}_q}$ be a finite-type $\mathbb{F}_q$-scheme. To compare this zeta function to the zeta function we defined for function fields $K/\mathbb{F}_q$ in the previous section, we need to introduce the group $Z_0(X)$ of 0-cycles: it is the free commutative group on $|X|$, the set of closed points of X. As we've already seen, each $x \in |X|$ corresponds to a maximal ideal in some finite-dimensional $\mathbb{F}_q$-algebra R, and thus the residue field $k(x)$ is a finite extension of $\mathbb{F}_q$. We define the **degree** $\deg(x)$ to be $[k(x) : \mathbb{F}_q]$. There is an induced degree map

$$\deg : Z_0(X) \to \mathbb{Z}, \ \sum n_x x \mapsto \sum n_x \deg(x).$$

A zero-cycle $\sum n_x x$ is **effective** if $n_x \geq 0$ for all $x \in |X|$. Let $Z_0(X)^+$ be the submonoid of effective zero-cycles. Since each X has a finite covering by $\operatorname{Spec} R_i$ where R_i is a finitely generated $\mathbb{F}_q$-algebra, it follows from Theorem 5.8 that for all $d \in \mathbb{Z}^+$ there are only finitely many $x \in |X|$ with $\deg(x) = d$. It follows easily from this that the number A_n of effective 0-cycles on X of degree n is finite.

PROPOSITION 5.13. *For a finite type scheme $X_{/\mathbb{F}_q}$, we have*

$$\zeta(X, s) = \sum_{z \in Z_0(X)^+} q^{-\deg(z)s} = \sum_{n=0}^{\infty} \frac{A_n}{q^{ns}} = \sum_{n=0}^{\infty} a_n T^n.$$

PROOF. We have

$$\zeta(X, s) = \prod_{x \in |X|} (1 - q^{-\deg(x)s})^{-1} = \prod_{x \in |X|} (1 + q^{-\deg(x)s} + q^{-2\deg(x)s} + \ldots)$$

$$= \sum_{z \in Z_0(X)^+} q^{-\deg(z)s}.$$

The latter two identities are even more immediate. □

This shows that if $K/\mathbb{F}_q$ is a one-variable function field and $C_{/\mathbb{F}_q}$ is the complete nonsingular curve with function field K, then we have

$$Z(C, T) = Z(T),$$

i.e., we recover the Hasse-Weil zeta function defined above.

5. Schmidt's Theorem

LEMMA 5.14. *For $m, r \in \mathbb{Z}^+$, put $d := \gcd(m, r)$. We denote by μ_r the group of rth roots of unity in $\mathbb{C}$. Then we have*

$$\left(1 - t^{mr/d}\right)^d = \prod_{\zeta \in \mu_r} \left(1 - (\zeta t)^m\right). \tag{42}$$

PROOF. In $\mathbb{C}[X]$ we have the identity

$$(X^{r/d} - 1)^d = \prod_{\zeta \in \mu_r} (X - \zeta^m) : \tag{43}$$

indeed, both sides are monic polynomials whose roots in $\mathbb{C}$ are the $\frac{r}{d}$th roots of unity, each root appearing with multiplicity d. Substituting $X = t^{-m}$ in (43) and multiplying by t^{mr} gives the result. □

PROPOSITION 5.15. *Let $K/\mathbb{F}_q$ be a function field, let $r \in \mathbb{Z}^+$, let $Z(t)$ be the zeta function of $K/\mathbb{F}_q$ and let $Z_r(t)$ be the zeta function of $K_r/\mathbb{F}_{q^r}$. Then we have*

$$Z_r(t^r) = \prod_{\zeta \in \mu_r} Z(\zeta t). \tag{44}$$

PROOF. We have

$$Z_r(t^r) = \prod_{P \in \Sigma(K/\mathbb{F}_q)} \prod_{P' | P} \left(1 - t^{r \deg P'}\right)^{-1}.$$

Fix $P \in \Sigma(K/\mathbb{F}_q)$, and put $m \coloneqq \deg P$, $d \coloneqq \gcd(r, m)$. Then using Lemmas 5.4 and 5.14 we get

$$\prod_{P' | P} \left(1 - t^{r \deg P'}\right)^{-1} = \left(1 - t^{rm/d}\right)^{-d} = \prod_{\zeta \in \mu_r} \left(1 - (\zeta t)^m\right)^{-1}.$$

So

$$Z_r(t^r) = \prod_{\zeta \in \mu_r} \prod_{P \in \Sigma(K/\mathbb{F}_q)} \left(1 - (\zeta t)^{\deg P}\right)^{-1} = \prod_{\zeta \in \mu_r} Z(\zeta t). \qquad \square$$

THEOREM 5.16 (F.K. Schmidt). *For a function field $K/\mathbb{F}_q$, we have $\delta = 1$.*

PROOF. Let $\zeta \in \mu_\delta$. Then for all $P \in \Sigma(K/\mathbb{F}_q)$ we have $\delta \mid \deg P$, so

$$Z(\zeta t) = \prod_{P \in \Sigma(K/\mathbb{F}_q)} \left(1 - (\zeta t)^{\deg P}\right)^{-1} = \prod_{P \in \Sigma(K/\mathbb{F}_q)} \left(1 - t^{\deg P}\right)^{-1} = Z(t).$$

Thus by Proposition 5.15 we have

$$Z_\delta(t^\delta) = \prod_{\zeta \in \mu_\delta} Z(\zeta t) = Z(t)^\delta.$$

Proposition 5.6 implies that $Z(t)$ and $Z_\delta(t)$ have simple poles at $t = 1$. It follows that $Z(t)^\delta$ has a pole of order δ at $t = 1$. On the other hand, since $\operatorname{ord}_{t-1}(t^\delta) = 0$, the function $Z_\delta(t^\delta)$ has a simple pole of order 1 at $t = 1$, so we have $\delta = 1$. $\square$

COROLLARY 5.17. *Let $K/\mathbb{F}_q$ be a genus zero function field. Then:*

a) *The field K is rational: $K \cong_{\mathbb{F}_q} \mathbb{F}_q(t)$.*

b) *We have*

$$Z(t) = \frac{1}{(1-t)(1-qt)}.$$

PROOF. a) This follows from Schmidt's Theorem and Exercise 2.17d).
b) This follows from Schmidt's Theorem and Proposition 5.6a). $\square$

Let us record the simplification we get in Proposition 5.6b) by taking $\delta = 1$.

COROLLARY 5.18. *Let $K/\mathbb{F}_q$ be a function field of genus $g \geq 1$. Then*

$$Z(t) = F(t) + G(t),$$

where

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg C \leq 2g-2} q^{\ell(C)} t^{\deg C}$$

and

$$G(t) = \frac{h}{q-1} \left(\frac{q^g t^{2g-1}}{1-qt} - \frac{1}{1-t} \right).$$

6. The Functional Equation

THEOREM 5.19 (Functional Equation). *Let $K/\mathbb{F}_q$ be a function field of genus g. Then we have*

$$Z(t) = q^{g-1}t^{2g-2}Z(\frac{1}{qt}). \tag{45}$$

PROOF. If $g = 0$ then (45) follows from Corollary 5.17b) by straightforward calculation, so suppose $g \geq 1$. Then the matter of it is as follows: with $Z(t) = F(t) + G(t)$ as in Corollary 5.18, we will show that the functional equations hold separately for $F(t)$ and $G(t)$. For $G(t)$ this is again a straightforward calculation, whereas for $F(t)$ the symmetry so expressed comes by applying the Riemann-Roch Theorem. Here we go:

Let $\mathcal{K} \in \operatorname{Div} K$ be a canonical divisor. Observe that since $\deg \mathcal{K} = 2g - 2$, as C runs through all divisor classes on K of degree $0 \leq d \leq 2g - 2$ so does $\mathcal{K} - C$, so

$$(q-1)F(\frac{1}{qt}) = \sum_{0\leq \deg C\leq 2g-2} q^{\ell(C)}\left(\frac{1}{qt}\right)^{\deg C} = \sum_{0\leq \deg C\leq 2g-2} q^{\ell(\mathcal{K}-C)}\left(\frac{1}{qt}\right)^{\deg \mathcal{K}-C}.$$

Now, using Riemann-Roch we have

$$\begin{aligned}(q-1)F(t) &= \sum_{0\leq \deg C\leq 2g-2} q^{\ell(C)}t^{\deg C}\\ &= q^{g-1}t^{2g-2}\sum_{0\leq \deg C\leq 2g-2} q^{\deg C-(2g-2)+\ell(\mathcal{K}-C)}t^{\deg C-(2g-2)}\\ &= q^{g-1}t^{2g-2}\sum_{0\leq \deg C\leq 2g-2} q^{\ell(\mathcal{K}-C)}\left(\frac{1}{qt}\right)^{\deg(\mathcal{K}-C)}\\ &= q^{g-1}t^{2g-2}(q-1)F(\frac{1}{qt}).\end{aligned}$$

On the other hand, we have

$$\begin{aligned}q^{g-1}t^{2g-2}G(\frac{1}{qt}) &= \frac{hq^{g-1}t^{2g-2}}{q-1}\left(q^g\left(\frac{1}{qt}\right)^{2g-1}\frac{1}{1-q\left(\frac{1}{qt}\right)} - \frac{1}{1-\frac{1}{qt}}\right)\\ &= \frac{h}{q-1}\left(\frac{-1}{1-t} + \frac{q^gt^{2g-1}}{1-qt}\right) = G(t).\end{aligned}$$

□

7. The L-Polynomial

The following definition extracts the crucial information from the Hasse-Weil zeta function. For a function field $K/\mathbb{F}_q$, the **L-polynomial** is

$$L(t) \coloneqq (1-t)(1-qt)Z(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_nt^n.$$

It is immediate from Proposition 5.6 and Schmidt's Theorem that $L(t)$ is a polynomial of degree at most $2g$.

EXERCISE 5.5. *Show that $\mathbb{Z}[[t]] \cap \mathbb{C}[t] = \mathbb{Z}[t]$.*

It follows that the L-polynomial $L(t)$ has coefficients in $\mathbb{Z}$.

THEOREM 5.20. *Let $K/\mathbb{F}_q$ be a function field.*

a) *We have* $\deg L = 2g$.
b) *We have* $L(1) = h$, *the class number of* K.
c) *We have* $L(t) = q^g t^{2g} L(\frac{1}{qt})$.
d) *Write* $L(t) = a_0 + a_1 t + \ldots + a_{2g} t^{2g}$. *Then:*
   (i) *We have* $a_0 = 1$ *and* $a_{2g} = q^g$.
   (ii) *For* $0 \leq i \leq g$, *we have*

$$a_{2g-i} = q^{g-i} a_i. \tag{46}$$

   (iii) *We have*

$$a_1 = \#\Sigma_1(K/\mathbb{F}_q) - (q+1). \tag{47}$$

e) *Let* $L(t) = \prod_{i=1}^{2g}(1-\alpha_i t) \in \mathbb{C}[t]$. *Then the complex numbers* $\alpha_1, \ldots, \alpha_{2g}$ *are algebraic integers, and they can be ordered so that we have* $\alpha_i \alpha_{g+i} = q$ *for all* $1 \leq i \leq g$.
f) *Let* $L_r(t) = (1-t)(1-q^r t)Z_r(t)$ *be the L-polynomial of* K_r. *Then we have*

$$L_r(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t)\,. \tag{48}$$

PROOF. When $g = 0$ we have that $L(t) = 1$ (constant polynomial), and all of the assertions are trivial. Henceforth we assume $g \geq 1$.
a) This will follow from part d), since $a_{2g} = q^g \neq 0$.
b) Using Corollary 5.18 we get

$$L(t) = (1-t)(1-qt)F(t) + \frac{h}{q-1}\left(q^g t^{2g-2}(1-t) - (1-qt)\right),$$

so indeed $L(1) = h$.
c) Using Theorem 5.19 we get

$$q^g t^{2g} L(\frac{1}{qt}) = q^g t^{2g}(1-\frac{1}{qt})(1-\frac{1}{t})Z(\frac{1}{qt}) = q^{g-1}t^{2g-2}(1-t)(1-qt)Z(\frac{1}{qt})$$
$$= (1-qt)(1-t)Z(t) = L(t).$$

d) Using part c), we get

$$L(t) = q^g t^{2g} L(\frac{1}{qt}) = \frac{a_{2g}}{q^g} + \frac{a_{2g-1}}{q^{g-1}} t + \ldots + q^g a_0 t^{2g}.$$

Thus for $0 \leq i \leq g$ we get $a_{2g-i} = q^{g-i} a_i$, establishing (46). Writing out

$$L(t) = a_0 + a_1 t + \ldots + a_{2g} t^{2g} = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n$$

$$= (1-(q+1)t+qt^2)(1 + A_1 t + A_2 t^2 + \ldots) = 1 + (A_1 - (q+1))t + \ldots$$

and equating the coefficients of t^0 and t^1 we get

$$a_0 = 1,\ a_1 = A_1 - (q+1) = \#\Sigma_1(K/\mathbb{F}_q) - (q+1).$$

Taking $i = 0$ in (46) we get $a_{2g} = q^g a_0 = q^g$, completing the proof of part d).
e) Consider the polynomial

$$L^{\perp}(t) \coloneqq t^{2g} L(1/t) = t^{2g} + a_1 t^{2g-1} + \ldots + q^g.$$

Since $L^\perp(t)$ is monic with coefficients in $\mathbb{Z}$ and nonzero constant term, its roots in $\mathbb{C}$ are algebraic integers. If we write

$$L^\perp(t) = \prod_{i=1}^{2g}(t - \alpha_i),$$

then

$$L(t) = t^{2g}L^\perp(1/t) = \prod_{i=1}^{2g}(1 - \alpha_i t).$$

So for all $1 \leq i \leq 2g$ we have $L(\alpha^{-1}) = 0$ and $\prod_{i=1}^{2g} \alpha_i = q^g$. Making the substitution $t = qu$ and using part c), we get

$$\prod_{i=1}^{2g}(t - \alpha_i) = t^{2g}L(1/t) = q^{2g}u^{2g}L(\frac{1}{qu})$$

$$= q^g L(u) = q^g \prod_{i=1}^{2g}(1 - \alpha_i u) = q^g \prod_{i=1}^{2g}(1 - \frac{\alpha_i}{q}t)$$

$$= q^g \left(\prod_{j=1}^{2g} \frac{\alpha_j}{q}\right)\left(\prod_{i=1}^{2g} t - \frac{q}{\alpha_i}\right) = \prod_{j=1}^{2g}(t - \frac{q}{\alpha_j}).$$

This is close to what we want, but need a bit more care. Consider the involution $\alpha \mapsto \frac{q}{\alpha}$ on $\mathbb{C}^\times$. The above calculation shows that the multiset $\alpha_1, \ldots, \alpha_{2g}$ is stable under this involution. However, this involution has two fixed points, $\sqrt{q}$ and $-\sqrt{q}$. If we group the roots into k pairs of nonfixed points $\alpha_i \neq \frac{q}{\alpha_i}$, m elements $\sqrt{q}$ and n elements $-\sqrt{q}$, then we have

$$2k + m + n = 2g,$$

so $m + n$ is even. Also the product of all the roots is

$$q^g = q^k q^{m/2}(-\sqrt{q})^n = (-1)^n q^{k+m/2+n/2} = (-1)^n q^g,$$

which shows that n is even and thus also m is even. Part e) now follows.
f) Using Proposition 5.15 we get

$$L_r(t^r) = (1 - t^r)(1 - q^r t^r)Z_r(t_r) = (1 - t^r)(1 - q^r t^r) \prod_{\zeta \in \mu_r} Z(\zeta t)$$

$$= (1 - t^r)(1 - q^r t^r) \prod_{\zeta \in \mu_r} \frac{L(\zeta t)}{(1 - \zeta t)(1 - q\zeta t)} = \prod_{\zeta \in \mu_r} L(\zeta t)$$

$$= \prod_{i=1}^{2g} \prod_{\zeta \in \mu_r} (1 - \alpha_i \zeta t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t^r)\,.$$

It follows that

$$L_r(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t)\,.$$

completing the proof of part f) and thus of the result. □

Whereas the definition of the zeta function uses "infinitely many pieces of information" about K, namely the number of effective degree n divisors for all n, the fact that it is a rational function of t shows that it really only depends on "finitely many pieces of information." The L-polynomial makes this precise: since it is a polynomial of degree $2g$, knowing the $2g+1$ coefficients $a_0, \ldots, a_{2g}$ determines $L(t)$ and thus also $Z(t)$. As the rest of Theorem 5.20 shows, there is a symmetry in play – coming from the functional equation for the zeta function, which in turn comees from the Riemann-Roch Theorem – so that in fact one needs only to determine the g pieces of information $a_1, \ldots, a_g$ in order to determine $L(t)$ and thus $Z(t)$. (If one didn't know better, it would be a good idea to search for further relations among the coefficients of $L(t)$, but it turns out that there are no more known relations of the above simple kind.)

Moreover, from (47) we see that knowing a_1 is equivalent to knowing the number of degree 1 places of K. Knowing the number of degree d places for $1 \leq d \leq n$ is equivalent to knowing the numbers $A_0, \ldots, A_n$. This suggests that we should look for formulas for $a_1, a_2, \ldots, a_g$ in terms of $\#\Sigma_1(K_r/\mathbb{F}_{q^r})$ for $1 \leq r \leq g$.

COROLLARY 5.21. *Let $K/\mathbb{F}_q$ be a function field of genus g, and let $\alpha_1, \ldots, \alpha_{2g}$ be the reciprocal roots of $L(t)$. Then for all $r \in \mathbb{Z}^+$ we have*

$$\#\Sigma_1(K_r/\mathbb{F}_{q^r}) = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r. \tag{49}$$

PROOF. By (47) we have

$$\#\Sigma_1(K_r/\mathbb{F}_{q^r}) = q^r + 1 + a_{1,r},$$

where $a_{1,r}$ is the coefficient of t in the L-polynomial $L_r(t)$ of K_r. By (48) we have

$$L_r(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t),$$

so the coefficient $a_{1,r}$ of t in $L_r(t)$ is $-\sum_{i=}^{2g} \alpha_i^r$. The result follows. □

Conversely:

COROLLARY 5.22. *Let $K/\mathbb{F}_q$ be a function field, with L-polynomial $L(t) \in \mathbb{Z}[t]$. For $r \in \mathbb{Z}^+$, put*

$$S_r := \#\Sigma_1(K_r/\mathbb{F}_{q^r}) - (q^r + 1).$$

a) *We have $\frac{L'(t)}{L(t)} = \sum_{r=1}^{\infty} S_r t^{r-1}$.*

b) *For all $1 \leq i \leq g$ we have*

$$i a_i = S_i a_0 + S_{i-1} a_1 + \ldots + S_1 a_{i-1}. \tag{50}$$

PROOF. a) Since $L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t)$, by logarithmically differentiating and then applying Corollary 5.21, we get

$$\frac{L'(t)}{L(t)} = \sum_{i=1}^{2g} \frac{-\alpha_i}{1 - \alpha_i t} = \sum_{i=1}^{2g} (-\alpha_i) \sum_{r=0}^{\infty} (\alpha_i t)^r$$

$$= \sum_{r=1}^{\infty} \left(\sum_{i=1}^{2g} -\alpha_i^r \right) t^{r-1} = \sum_{r=1}^{\infty} S_r t^{r-1}.$$

b) Equating coefficients in $L'(t) = L(t) \sum_{r=1}^{\infty} S_r t^{r-1}$ gives (50). □

Corollary 5.22 shows how to compute $Z(t)$ given $\#\Sigma_1(K_r/\mathbb{F}_{q^r})$ for $1 \leq r \leq g$.

EXERCISE 5.6. *Let $K/\mathbb{F}_q$ be a function field of genus 1.*

a) *Show that we have*
$$Z(t) = \frac{1 - at + qt^2}{(1-t)(1-qt)},$$
where $a = q + 1 - \#\Sigma_1(K/\mathbb{F}_q)$.

b) *Let $L(t) = (1 - \alpha_1 t)(1 - \alpha_2 t)$. Show that $a = \alpha_1 + \alpha_2$ and that for all $r \in \mathbb{Z}^+$ we have*
$$\Sigma_1(K_r/\mathbb{F}_{q^r}) = q^r + 1 - \alpha_1^r - \frac{q^r}{\alpha_1^r}.$$
This means: for an elliptic curve $E_{/\mathbb{F}_q}$, if one knows $\#E(\mathbb{F}_q)$, then one knows $\#E(\mathbb{F}_{q^r})$ for all $r \geq 1$.

c) *Suppose $a = 0$. Show:*
   (i) *If r is odd, then $\#\Sigma_1(K_r/\mathbb{F}_{q^r}) = q^r + 1$.*
   (ii) *If $r \equiv 2 \pmod 4$, then $\Sigma_1(K_r/\mathbb{F}_{q^r}) = (q^{r/2} + 1)^2$.*
   (iii) *If $4 \mid r$, then $\Sigma_1(K_r/\mathbb{F}_{q^r}) = (q^{r/2} - 1)^2$.*

8. The Riemann Hypothesis

The following result of Weil and its corollary is probably the single most important result on alegbraic function fields over a finite constant field.

THEOREM 5.23 (Riemann Hypothesis for Curves over a Finite Field). *Let $K/\mathbb{F}_q$ be a function field of genus g, with L-polynomial $L(t) = \prod_{i=1}^{2g}(1 - \omega_i t)$. Then for all $1 \leq i \leq 2g$ we have $|\alpha_i| = \sqrt{q}$.*

It does not seem to be an exaggeration to say that *en route* proving Theorem 5.23 Weil laid the foundations for modern algebraic geometry. His proof uses intersection theory on algebraic surfaces. Later, more elementary proofs were given by Stepanov and Bombieri. We will give an adaptation of these proofs following Stichtenoth. As one might expect of an elementary proof of a deep and important result, it is not super quick. We will discuss the proof in the following section.

9. Bounds on $\#\Sigma_1(K/\mathbb{F}_q)$

The following is an immediate – and crucial! – consequence of Theorem 5.23.

COROLLARY 5.24 (Weil). *Let $K/\mathbb{F}_q$ be a function field of genus g. Then*
$$|\Sigma_1(K/\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}. \tag{51}$$

PROOF. By (49) and Theorem 5.23 we have
$$|\#\Sigma_1(K/\mathbb{F}_q) - (q+1)| = |\sum_{i=1}^{2g} \alpha_i| \leq 2g\sqrt{q}. \qquad \square$$

Next we want to discuss certain elementary improvements on the Weil bound: by this we mean that the proofs will make use of the Riemann Hypothesis but not its proof. In order to keep track of these bounds it seems helpful to introduce a quantiy that we will study more deeply later on. The basic philosophy here is that the Weil bound tends to be sharp if one fixes g and sends q to ∞. This is a natural

setup for instance, to look at reductions modulo primes of a fixed curve of genus g defined over a global field. On the other hand, when q is fixed and we send g to infinity, the Weil bound is still contentful but seems far from optimal. To study that we intrduce the quantiies $M_q(g)$ and $A(q)$. We define $M_q(g)$ to be the maximum number of degree one places of a genus g function field over $\mathbb{F}_q$, and we define

$$A(q) \coloneqq \limsup_{g\to\infty} \frac{M_q(g)}{g}.$$

In other words, for each $\epsilon > 0$, for all sufficiently large g we have

$$M_q(g) \leq (A(q) + \epsilon)g,$$

and $A(q)$ is the smallest real number for which this holds. The Weil bounds then give that for all q,

$$A(q) \leq 2\sqrt{q}.$$

EXAMPLE 5.3. *Mention results from p. 260 of Serre's article.*

Serre gave an improvement on the Weil bound whenever q is not a square. To motivate it, we observe that if q is not a square, then it is impossible for the Weil bound to be sharp – i.e., equality cannot occur in (51) because $2g\sqrt{q}$ is not an integer. So we can immediately improve the Weil bound to

$$|\Sigma_1(K/\mathbb{F}_q) - (q+1)| \leq \lfloor 2g\sqrt{q} \rfloor.$$

However this does not yield any improvement on $A(q)$, whereas the following does.

COROLLARY 5.25 (Serre Bound). *Let $K/\mathbb{F}_q$ be a function field of genus g.*

a) *We have*

$$|\#\Sigma_1(K/\mathbb{F}_q) - (q+1)| \leq g\lfloor 2\sqrt{q} \rfloor. \tag{52}$$

b) *It follows that $A(q) \leq \lfloor 2\sqrt{q} \rfloor$.*

PROOF. a) Of course we may assume that $g \geq 1$. Let $L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$. We may order the reciprocal roots α_i such that $\alpha_i\alpha_{g+i} = q$ and, by the Riemann Hypothesis, we have $|\alpha_i| = \sqrt{q}$ for all $1 \leq i \leq 2g$, and it follows that for all $1 \leq i \leq g$ we have

$$\overline{\alpha_i} = q\alpha_i^{-1} = \alpha_{g+i}.$$

For $1 \leq i \leq g$, we put

$$\gamma_i \coloneqq \alpha_i + \overline{\alpha_i} + \lfloor 2\sqrt{q} \rfloor + 1,$$

$$\delta_i \coloneqq -(\alpha_i + \overline{\alpha_i}) + \lfloor 2\sqrt{q} \rfloor + 1.$$

Then the γ_i and δ_i are real algebraic integers, and the Riemann Hypothesis implies that they are positive. Because $L^\perp(t) = \prod_{i=1}^{2g}(t - \alpha_i) \in \mathbb{Z}[t]$, every field embedding $\sigma : \mathbb{Q}(\alpha_1, \ldots, \alpha_{2g}) \hookrightarrow \mathbb{C}$ preserves the multiset $\alpha_1, \ldots, \alpha_{2g}$. If $\sigma(\alpha_i) = \alpha_j$, then

$$\sigma(\overline{\alpha_i}) = \sigma(\frac{q}{\alpha_i}) = \frac{q}{\sigma(\alpha_i}) = \overline{\sigma(\alpha_i)} = \overline{\alpha_j},$$

so σ permutes the multisets $\{\{\gamma_1, \ldots, \gamma_g\}\}$ and $\{\{\delta_1, \ldots, \delta_g\}\}$ as well. Put

$$\gamma \coloneqq \prod_{i=1}^{g} \gamma_i,\ \delta \coloneqq \prod_{i=1}^{g} \delta_i.$$

Then γ and δ are positive algebraic integers that are preserved by every field embedding $\sigma : \mathbb{Q}(\alpha_1, \ldots, \alpha_{2g}) \hookrightarrow \mathbb{C}$, so they are positive integers. The Arithmetic-Geometric Mean Inequality gives

$$\frac{1}{g}\sum_{i=1}^{g}\gamma_i \geq \left(\prod_{i=1}^{g}\gamma_i\right)^{1/g} \geq 1,$$

so

$$g \leq \sum_{i=1}^{g}\gamma_i = \sum_{i=1}^{g}(\alpha_i + \overline{\alpha_i}) + g\lfloor 2\sqrt{q}\rfloor + g = \sum_{i=1}^{2g}\alpha_i + g\lfloor 2\sqrt{q}\rfloor + g,$$

or equivalently

$$-\sum_{i=1}^{2g}\alpha_i \leq g\lfloor 2\sqrt{q}\rfloor.$$

The same argument with the δ_i's yields

$$\sum_{i=1}^{2g}\alpha_i \leq g\lfloor 2\sqrt{q}\rfloor,$$

so we get

$$|\sum_{i=1}^{2g}\alpha_i| \leq g\lfloor 2\sqrt{q}\rfloor. \tag{53}$$

Since by (49) we have

$$|\#\Sigma_1(K/\mathbb{F}_q) - (q+1)| = |\sum_{i=1}^{2g}\alpha_i|,$$

part a) follows. Part b) is an immediate consequence of part a). □

For instance, when $q = 2$ the Weil bounds imply that

$$\#\Sigma_1(K/\mathbb{F}_2) \leq 2.82842\ldots g + 3,\ A_2(2) \leq 2.82842\ldots,$$

whereas the Serre bounds imply

$$\#\Sigma_1(K/\mathbb{F}_2) \leq 2g + 3,\ A_2(2) \leq 2.$$

Recall that for $r \in \mathbb{Z}^+$, we put $N_r \coloneqq \#\Sigma_1(K_r/\mathbb{F}_{q^r})$ and that for $m \mid n$ we have $N_m \leq N_r$ (Corollary 5.5). In particular the fact that for all $r \geq 1$ we have

$$N_1 \leq N_r \leq q^r + 1 + g\lfloor 2q^{r/2}\rfloor$$

has the potential to give further information. This is indeed the case. We begin with a simple application of this idea, due to Ihara.

THEOREM 5.26 (Ihara Bound [**Ih81**]). *Let $K/\mathbb{F}_q$ be a function field of genus $g \geq 1$.*

a) *We have*

$$\#\Sigma_1(K/\mathbb{F}_q) \leq \frac{1}{2}\left(\sqrt{(8q+1)g^2 + (4q^2-4q)g} - (g-2q-2)\right). \tag{54}$$

b) *It follows that $A(q) \leq \frac{1}{2}\left(\sqrt{8q+1}-1\right)$.*

PROOF. a) As usual, we write $L(t) = \prod_{i=1}^{2g}(1-\alpha_i t)$. For $1 \leq i \leq g$, let $\omega_i := \alpha_i + \overline{\alpha_i}$. The ω_i's are real numbers, so applying Cauchy-Schwarz in $\mathbb{R}^g$ with $v = (1, 1, \ldots, 1)$ and $w = (\omega_1, \ldots, \omega_g)$ we have

$$\left(\sum_{i=1}^{g} \omega_i\right)^2 \leq g \sum_{i=1}^{g} \omega_i^2 = g \sum_{i=1}^{2g} \alpha_i^2 + 2qg^2.$$

So

$$q + 1 - \sum_{i=1}^{g} \omega_i = N_1 \leq N_2 = q^2 + 1 - \sum_{i=1}^{2g} \alpha_i^2 = q^2 + 1 + 2qg - \frac{1}{g}\left(\sum_{i=1}^{g} \omega_i\right)^2$$

$$= q^2 + 1 + 2qg - \frac{(q+1-N_1)^2}{g}.$$

We leave it to the reader to solve this quadratic inequality in N_1 to get (13), completing the proof of part a). Part b) follows immediately. □

Thus Ihara's Bound gives

$$A(2) \leq 1.56155281281,$$

which is progress over the bounds of Weil and Serre. However Example 5.3 suggests that in fact $A(2) < 1$. In fact this is true:

THEOREM 5.27 (Drinfeld-Vlădut Bound). *We have*

$$A(q) := \limsup_{g \to \infty} \leq \sqrt{q} - 1. \tag{55}$$

PROOF. Once again write $L(t) = \prod_{i=1}^{2g}(1-\alpha_i t)$ such that $\alpha_{g+i} = \overline{\alpha_i}$ for all $1 \leq i \leq g$. For all $r \in \mathbb{Z}^+$ we have

$$N_r = q^r + 1 - \sum_{i=1}^{g} (\alpha_i^r + \overline{\alpha_i}^r).$$

For $1 \leq i \leq g$, put $\theta_i := \alpha_i q^{-1/2}$, so $|\theta_i| = 1$ for all $1 \leq i \leq g$. For $r \in \mathbb{Z}^+$ we have

$$0 \leq \sum_{i=1}^{g} |1 + \theta_i + \ldots + \theta_i^r|^2 = \sum_{i=1}^{g} \sum_{k=0}^{r} \theta_i^k \sum_{k=0}^{r} \overline{\theta_i}^k.$$

Moreover we have

$$(1 + \theta_i + \ldots + \theta_i^r)(1 + \overline{\theta_i} + \ldots + \overline{\theta_i}^r) = \sum_{k=1}^{r} (r+1-k)(\theta_i^k + \overline{\theta_i}^k) + (r+1).$$

Summing over i gives

$$0 \leq g(r+1) + \sum_{k=1}^{r} (r+1-k) \sum_{i=1}^{g} (\theta_i^k + \overline{\theta_i}^k) = g(r+1) + \sum_{k=1}^{r} (r+1-k) \frac{q^k + 1 - N_k}{q^{k/2}}$$

$$\leq g(r+1) + \sum_{k=1}^{r} (r+1-k) \frac{q^k + 1 - N_1}{q^{k/2}}.$$

Rearranging, we get that

$$N \leq 1 + \frac{g(r+1) + \sum_{k=1}^{r} (r+1-k) q^{k/2}}{\sum_{k=1}^{r} (r+1-k) q^{-k/k2}}.$$

Thus for all $r \in \mathbb{Z}^+$ we have

$$A(q) = \limsup_{g\to\infty} \frac{M_q(g)}{g} \leq \frac{r+1}{\sum_{k=1}^r (r+1-k)q^{-k/2}}$$
$$= \frac{1+\frac{1}{r}}{\sum_{k=1}^r q^{-k/2} + \frac{1}{r}\sum_{k=1}^r (1-k)q^{-k/2}}.$$

Since this holds for all r, we may take the limit as $r \to \infty$. Since $\sum_{k=1}^\infty (1-k)q^{-k/2}$ is absolutely convergent, we have $\lim_{r\to\infty} \sum_{k=1}^\infty (1-k)q^{-k/2} = 0$ and thus

$$A(q) \leq \frac{1}{\sum_{k=1}^\infty q^{-k/2}} = \left(\frac{q^{-1/2}}{1-q^{-1/2}}\right)^{-1} = \sqrt{q} - 1. \qquad \square$$

The bound (55) gives

$$A(2) \leq 0.414213,$$

a significant improvement over the previous bounds. Asympotically in q, the Drinfeld-Vlădut Bound improves on Ihara's bound by a factor of $\sqrt{2}$. Later we will see that for all prime powers q, $A(q^2) = \sqrt{q} - 1$, so the Drinfeld-Vlădut Bound is an equality on squares. The precise value of $A(q)$ is not known for any nonsquare q.

These bounds give rise to a concrete and interesting classification problem: for a natural number g and a prime power q, put put

$$\mathcal{S}_q(g) \coloneqq \{n \in \mathbb{N} \mid \text{ There is a genus } g \text{ function field } K/\mathbb{F}_q \text{ with } \#\Sigma_1(K/\mathbb{F}_q) = n\}.$$

If we were in a position to determine $\mathcal{S}_q(g)$ for all g and q, then that would be that. However, we are quite far from that, so it is also interesting to consider other quantities, such as the maximum value $M_q(g)$ of $\mathcal{S}_q(g)$ (already defined above), the minimum value $m_q(g)$ of $\mathcal{S}_q(g)$, whether $0 \in \mathcal{S}_q(g)$, whether $q+1+2g\sqrt{q} \in \mathcal{S}_q(g)$, and so forth.

Let me add an invariant of my own: for a function field K over an arbitrary constant field k, let $I^+(K)$ be the least positive degree of an *effective* divisor on K. We call $I^+(K)$ the **effective index**.

Exercise 5.7. *Let K/k be a function field.*

a) *Show: $I^+(K)$ is the least integer r such that K has a place of degree r.*
b) *Show: $I(K) \mid I^+(K)$.*

We say a function field is **pointless** if $\Sigma_1(K/k) = \varnothing$. Equivalently, a function field is pointless if $I^+(K) \geq 2$, and thus $I^+(K)$ is a measure of "how pointless" the function field K/k is. So is the index I, but in a looser way: by Schmidt's Theorem, every function field over a finite field has index 1, but we will see that there are pointless function fields over $\mathbb{F}_q$. Notice also that $m_q(g) = 0$ iff there is a pointless function field of genus g over $\mathbb{F}_q$.

What is known about these quantities? Let us organize our answers by the genus.

Of course we know that $\mathcal{S}_q(0) = \{q+1\}$ for all q: by Corollary 5.17a), the only genus 0 function field over $\mathbb{F}_q$ is $\mathbb{F}_q(t)$.

The case of genus one is also completely known. First, we have the following important result.

THEOREM 5.28. *Every genus one function field $K/\mathbb{F}_q$ has $\Sigma_1(K/\mathbb{F}_q) \neq \varnothing$ and thus is an elliptic function field.*

PROOF. In genus one the Weil Bounds give

$$\#\Sigma_1(K/\mathbb{F}_q) \geq q + 1 - 2\sqrt{q} = (\sqrt{q} - 1)^2 > 0. \qquad \square$$

The set $\mathcal{S}_q(1)$ was determined by Waterhouse, with important special cases due to Hasse and Deuring.

THEOREM 5.29 (Waterhouse). *Let $q = p^f$ be a prime power, and let $K/\mathbb{F}_q$ be an elliptic function field with L-polynomial $L(t) = 1 - at + qt^2 = (1 - \alpha t)(1 - \overline{\alpha} t)$ and $\#\Sigma_1(K/\mathbb{F}_q) = a$. Among integers a with $|a| \leq 2\sqrt{q}$, the ones that occur – i.e., for some elliptic function function field $K/\mathbb{F}_q$ – are precisely as folows:*

(i) *If $\gcd(a, p) = 1$, then a occurs.*
(ii) *If f is even, then $a = \pm 2\sqrt{q}$ occurs.*
(iii) *If f is even and $p \not\equiv 1 \pmod 3$, then $a = \pm\sqrt{q}$ occurs.*
(iv) *If f is odd and $p \leq 3$, then $a = \pm p^{\frac{f+1}{2}}$.*
(v) *If f is odd, then $a = 0$ occurs.*
v) *If f is even and $p \not\equiv 1 \pmod 4$, then $a = 0$ occurs.*

PROOF. See [**Wa69**, Thm. 4.1]. This paper is the content of Waterhouse's 1968 PhD thesis, under Tate. It is an early – and strikingly beautiful – application of Honda-Tate's characterization of the isogeny category of abelian varieties over finite fields in terms of purely algebraic number theoretic data ("Weil q-numbers"). $\square$

Recall that for elliptic function fields we have $N_1 = h$, so Waterhouse's Theorem is equally well telling us the class numbers of elliptic function fields over $\mathbb{F}_q$. So this yields a solution of the class number one problem in this case:

EXERCISE 5.8. *Deduce from the Hasse-Deuring-Waterhouse Theorem that for a prime power q, the following are equivalent:*

(i) *There is a genus one function field $K/\mathbb{F}_q$ with class number 1.*
(ii) *We have $q \in \{2, 3, 4\}$.*

The class number perspective seems a bit richer, because $\mathrm{Cl}^0 K$ is a finite commutative group, and Waterhouse's Theorem has determined its possible size in the genus one case. But what about the group structure itself? The possible group structures of elliptic function fields over $\mathbb{F}_q$ were determined later by Rück [**Rü90**].

Already I believe that the sets $\mathcal{S}_q(2)$ are not known for all prime powers q, although much is known.

EXERCISE 5.9. *Show that $m_q(2) \geq 1$ for all $q > 13$.*

In fact Stark showed that also $m_{13}(2) \geq 1$ [**St73**].

Serre determined $M_q(2)$ for all q.

THEOREM 5.30 (Serre). *Let q be a prime power.*

a) *Suppose q is a square.*

(i) *We have* $M_2(4) = 10$.
(ii) *We have* $M_2(9) = 20$.
(iii) *For all* $q > 9$, *we have* $M_2(q) = q + 1 + 4\sqrt{q}$.
b) *Suppose that* q *is not a square* ***COMPLETE ME!***.

PROOF. See [**Se83.2**, Thms. 3 and 4]. □

THEOREM 5.31 (Lauter [**La00**]). *We have* $14 \notin \mathcal{S}_3(5)$.

THEOREM 5.32 (Savitt [**Sa03**]). *We have* $M_8(4) = 25$.

9.1. Explicit Formulas. The following approach is due to Serre. Keeping our usual notation, for $1 \leq i \leq 2g$ we put

$$\theta_i := \alpha_i/\sqrt{q},$$

so $|\theta_i|$ lies on the unit circle $S^1 \subset \mathbb{C}$, and we may order the θ_i's such that $\theta_{g+i} = \overline{\theta_i} = \theta_i^{-1}$. Then (49) gives

$$N_r q^{-r/2} = q^{r/2} + q^{-r/2} - \sum_{i=1}^{g} \theta_i^r + \theta_i^{-r}. \tag{56}$$

For a sequence $\{c_n\}_{n=1}^{\infty}$ of real numbers and $m \in \mathbb{Z}^+$ we put

$$\lambda_m(t) := \sum_{r=1}^{m} c_r t^r \in \mathbb{R}[t],$$

$$f_m(t) := 1 + \lambda_m(t) + \lambda_m(t^{-1}) \in \mathbb{R}[t, t^{-1}].$$

Notice that if $z \in S^1$ we have $f_m(z) = 1 + 2\Re(\lambda_m(z)) \in \mathbb{R}$. Summing (56) over $1 \leq r \leq m$ gives

$$N_1\lambda_m(q^{-1/2}) = \lambda_m(q^{1/2}) + \lambda_m(q^{-1/2}) + g - \sum_{i=1}^{g} f_m(\theta_i) - \sum_{r=1}^{m}(N_r - N_1)c_r q^{-r/2}. \tag{57}$$

PROPOSITION 5.33 (Serre's Explicit Formulas). *Suppose* $c_1, \ldots, c_m \in \mathbb{R}$ *satisfy:*

(i) *Each* c_r *is non-negative, and at least one is strictly positive.*
(ii) *For all* $z \in S^1$ *we have* $f_m(t) \geq 0$.

Then

$$N_1 = \#\Sigma_1(K/\mathbb{F}_q) \leq \frac{g + \lambda_m(q^{1/2})}{\lambda_m(q^{-1/2})} + 1. \tag{58}$$

PROOF. We have $N_1 \leq N_r$ for all r. So the term $-\sum_{r=1}^{m}(N_r - N_1)c_r q^{-r/2}$ in (57 is not positive. Using this and (ii) we get

(59)

$$N_1\lambda_m(q^{-1/2}) \leq \lambda_m(q^{1/2}) + \lambda_m(q^{-1/2}) + g - \sum_{i=1}^{g} f_m(\theta_i) \leq \lambda_m(q^{1/2}) + \lambda_m(q^{-1/2}) + g.$$

By (i) we have that $\lambda_m(q^{-1/2}) > 0$, so dividing (59) by $\lambda_m(q^{-1/2})$ gives (58). □

10. Proof of the Riemann Hypothesis

A proof was not given in the course and will not be given in these notes. In [**St**, §5.2], Stichtenoth gives a proof following Stepanov and Bombieri. Such elementary arguments are very impressive, but they are more useful to specialists in other areas of mathematics. For a student of arithmetic geometry it would be better to learn some basics of the theory of algebraic surfaces necessary to understand Weil's original proof. A very attractive exposition of this proof appears in [**Mi15**] – a long article, but even after spending several pages discussing history and overview, the proof of the Riemann hypothesis is completed on page 10. Indeed, Milne's exposition is written so as to be accessible to those with very little background in algebraic surfaces and can serve as a good motivation to learn that material.

The Hasse-Weil zeta function is defined not just for curves over a finite field but for any variety over a finite field, and the Riemann hypothesis in this much greater level of generality is a celebrated result of Deligne. As it happens, in Fall 2020 when I was (first?) teaching this course on curves, there was a concurrent course at UGA taught by Daniel Litt, in which Deligne's Theorem was proved.

There is however a more modern approach to the Riemann hypothesis for curves over a finite field from an elementary function field perspective, due to Stöhr-Voloch [**SV86**]. They get a proof that is significantly shorter than the one of Bombieri/Stepanov/Stichtenoth by first developing (in a novel way) the theory of Weierstrass points on curves over finite fields. This Stohr-Voloch theory has other applications and potential applications, so this seems to be the best proof to present in such a course. We did not have time to develop this in the course, and thus is does not (yet?) appear in these notes, but for instance this is the approach to the Riemann Hypothesis taken in Goldschmidt's text [**G**, §5.3].

11. Applications of RH II: Class Numbers

Recall that the class number h of a function field $K/\mathbb{F}_q$ is the cardinality h of the finite group $\mathrm{Cl}^0 K$. By Theorem 5.20b), we have

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

and thus using the Riemann Hypothesis – $|\alpha_i| = \sqrt{q}$ for all i – we have that $\sqrt{q} - 1 \leq |\alpha_i - 1| \leq \sqrt{q} + 1$ for all i, so

$$(\sqrt{q} - 1)^{2g} \leq h \leq (\sqrt{q} + 1)^{2g}.$$

Following Serre – and now also Aubry, Haloui and Lachaud – we can get a small improvement.

LEMMA 5.34. *Let $c_1, \ldots, c_n \in [0, \infty)$, and put*

$$F(t) := \prod_{i=1}^{n} (t + c_i) \in \mathbb{R}[t].$$

If $x \geq 0$ and $0 \leq c \leq (c_1 \cdots c_n)^{1/n}$, then we have

$$F(x) \geq (x + c)^n. \tag{60}$$

PROOF. Step 1: We claim that for $x_1, \dots, x_n, y_1, \dots, y_n \geq 0$, we have

$$\prod_{i=1}^{n} x_i^{1/n} + \prod_{i=1}^{n} y_i^{1/n} \leq \left(\prod_{i=1}^{n} (x_i + y_i) \right)^{1/n}. \tag{61}$$

Indeed this holds easily if any x_i or y_i is zero, so we may assume that all are strictly positive. By two applications of the Arithmetic Geometric Mean Inequality we get

$$\left(\prod_{i=1}^{n} \frac{x_i}{x_i + y_i} \right)^{1/n} \leq \frac{1}{n} \sum_{i=1}^{n} \frac{x_i}{x_i + y_i},$$

$$\left(\prod_{i=1}^{n} \frac{y_i}{x_i + y_i} \right)^{1/n} \leq \frac{1}{n} \sum_{i=1}^{n} \frac{y_i}{x_i + y_i}.$$

Adding the two inequalities and clearing denominators yields (61).
Step 2: Using (61) we get

$$x + c \leq \prod_{i=1}^{n} x^{1/n} + \prod_{i=1}^{n} c_i^{1/n} \leq \left(\prod_{i=1}^{n} (x + c_i) \right)^{1/n} = F(x)^{1/n}. \qquad \square$$

COROLLARY 5.35 (Serre-Aubry-Haloui-Lachaud). *If $K/\mathbb{F}_q$ is a function field of genus g, with class number $h = \# \operatorname{Cl}^0 K$, then we have*

$$(\sqrt{q} - 1)^{2g} \leq (q + 1 - \lfloor 2\sqrt{q} \rfloor)^g \leq h \leq \lfloor (\sqrt{q} + 1)^2 \rfloor^g = (q + 1 + \lfloor 2\sqrt{q} \rfloor)^g. \tag{62}$$

PROOF. Let $L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t)$ be the L-polynomial of $K/\mathbb{F}_q$. By Theorem 5.20b) we have

$$h = L(1) = \prod_{i=1}^{2g} (1 - \alpha_i).$$

For $1 \leq i \leq g$, put $\omega_i \coloneqq \alpha_i + \overline{\alpha_i} = \alpha_i + \alpha_{g+i}$; by the Riemann Hypothesis we have

$$\forall 1 \leq i \leq g,\ q + 1 - \omega_i \geq q + 1 - 2\sqrt{q} = (\sqrt{q} - 1)^2 > 0.$$

By (53) we have

$$\frac{1}{g} \left| \sum_{i=1}^{g} \omega_i \right| \leq \lfloor 2\sqrt{q} \rfloor.$$

Using this and the Arithmetic-Geometric Mean Inequality we get

$$h = \prod_{i=1}^{2g} (1 - \alpha_i) = \prod_{i=1}^{g} (q + 1 - \omega_i) \leq \left(\frac{1}{g} (q + 1 - \omega_i) \right)^g$$

$$= \left(q + 1 - \frac{1}{g} \sum_{i=1}^{g} \omega_i \right)^g \leq (q + 1 + \lfloor 2\sqrt{q} \rfloor)^g = \lfloor (\sqrt{q} + 1)^2 \rfloor^g.$$

For the lower bound, put

$$F(t) \coloneqq \prod_{i=1}^{g} (t + \lfloor 2\sqrt{q} \rfloor + 1 - \omega_i)$$

and for $1 \leq i \leq g$, put $c_i := \lfloor 2\sqrt{q} \rfloor + 1 - \omega_i$. Since $\omega_i \leq |\omega_i| \leq 2\sqrt{q} < \lfloor 2\sqrt{q} \rfloor + 1$, we have $c_i > 0$. Put

$$\gamma := \left(\prod_{i=1}^{g} \lfloor 2\sqrt{q} \rfloor + 1 - \omega_i \right)^{1/g} = \left(\prod_{i=1}^{g} c_i \right)^{1/g} > 0.$$

Then γ^g is a positive real number, an algebraic integer, and invariant under the action of $\mathfrak{g}_{\mathbb{Q}}$, so $\gamma^g \in \mathbb{Z}^+$ and thus $\gamma \geq 1$. So we may apply Lemma 5.34 with $n = g$, $c = 1$ and $x = q - \lfloor 2\sqrt{q} \rfloor$, getting

$$h = \prod_{i=1}^{g} (q + 1 - \omega_i) = F(q - \lfloor 2\sqrt{q} \rfloor) \geq (q + 1 - \lfloor 2\sqrt{q} \rfloor)^g. \qquad \square$$

Let us consider the lower bound $h \geq (q + 1 - \lfloor 2\sqrt{q} \rfloor)^g \geq (\sqrt{q} - 1)^{2g}$. We have $\sqrt{q} - 1 > 1$ iff $q > 4$, so even the weaker bound shows that for all $q \geq 5$ we have

$$h \geq (\sqrt{q} - 1)^{2g} \geq 1.236^{2g},$$

so the class number grows exponentially in g, uniformly across all $q \geq 5$. Unfortunately for $q \leq 4$ even the improved lower bound of (62) yields only the completely useless result that $h \geq 1$. So we supplement it with the following lower bound.

THEOREM 5.36. *Let $K/\mathbb{F}_q$ be a function field of genus $g \geq 1$. Then we have*

$$h \geq \frac{q-1}{2} \frac{q^{2g} + 1 - 2gq^g}{g(q^{g+1} - 1)}.$$

PROOF. The number A_{2g} of effective degree $2g$ divisors on K is $\frac{h(q^{g+1}-1)}{q-1}$ (Lemma 5.3c)).

Let $K_{2g} = K \otimes_{\mathbb{F}_q} \mathbb{F}_{q^{2g}}$. Let $Q \in \Sigma_1(K_{2g}/\mathbb{F}_{q^{2g}})$ be a degree one place. Let $P = Q \cap K$ be the place of K that Q lies over. If $\mathbb{F}_q(P)$ and $\mathbb{F}_{q^{2g}}(Q)$ are the residue fields, then we know that $\mathbb{F}_{q^{2g}}(Q) = \mathbb{F}_{q^{2g}}$ and

$$\mathbb{F}_q \subset \mathbb{F}_q(P) = \mathbb{F}_{q^{\deg P}} \subset \mathbb{F}_{q^{2g}}(Q) = \mathbb{F}_{q^{2g}},$$

so we have $\deg P \mid 2g$. Therefore $\frac{2g}{\deg P} P$ is an effective divisor on K of degree $2g$. This defines a mapping from $\Sigma_1(K_{2g}/\mathbb{F}_{q^{2g}})$ into the set of effective divisors on K of degree $2g$, in which each fiber has cardinality at most $2g$, since that is an upper bound for the number of places Q lying over a given place P. So we get

$$\frac{\#\Sigma_1(K_{2g})/\mathbb{F}_{q^{2g}}}{2g} \leq A_{2g} = h \frac{q^{g+1} - 1}{q - 1}.$$

Rearranging and using the Weil Bound on $N_{2g} = \#\Sigma_1(K_{2g}/\mathbb{F}_{q^2 g})$, we get

$$h \geq \frac{q^{2g} + 1 - 2gq^g}{2g} \frac{q-1}{q^{g+1} - 1} = \frac{q-1}{2} \frac{q^{2g} + 1 - 2gq^g}{g(q^{g+1} - 1)}. \qquad \square$$

EXERCISE 5.10. *Let $K/\mathbb{F}_q$ be a function field of genus $g \geq 1$.*

a) *Show:*

$$h \geq \frac{q-1}{2} \left(\frac{q^{g-1}}{g} - \frac{2}{q} \right).$$

b) *Fix any $a \in (0, 2)$. Let $\underline{h}(g)$ be the minimum class number of a genus g function field over any finite field. Show: as $g \to \infty$ we have $\underline{h}(g) \gg a^g$.*

c) *Deduce: for any $H \in \mathbb{Z}^+$, there are only finitely many pairs (q, g) with q a prime power and $g \in \mathbb{Z}^+$ for which there is a genus g function field $K/\mathbb{F}_q$ with class number at most H.*

EXERCISE 5.11. *Let $K/\mathbb{F}_q$ be a function field of genus $g \geq 1$. Let $h := \# \mathrm{Cl}^0 K$ be its class number.*

a) *Show: If $h = 1$, then $q \leq 4$.*
b) *Show: if $h = 1$ and $q = 4$ then $g = 1$.*
c) *Show: if $h = 1$ and $q = 3$, then $g \leq 2$.*
d) *Show: if $h = 1$ and $q = 2$, then $g \leq 4$.*

EXERCISE 5.12. *Let $K/\mathbb{F}_q$ be a genus one function field.*

a) *Recall that in Exercise 5.8 we used Waterhouse's Theorem (Theorem 5.29) to show that if $q \in \{2, 3, 4\}$ there is an elliptic function field $K/\mathbb{F}_q$ with class number 1.*
b) *Show (by enumerating all elliptic curves over $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_4$, presumably) that for each of $q \in \{2, 3, 4\}$ there is a **unique** (up to isomorphism) elliptic function field $K/\mathbb{F}_q$ with class number 1.*

EXERCISE 5.13. *Show that each of the following function fields has class number one. In each case we list q and the genus g and give a geometrically irreducible defining polynomial $f(x, y)$. (Suggestion: count points to compute $N_1, \ldots, N_g$, and thereby compute the zeta function.)*

a) $(q, g) = (2, 2)$, $f(x, y) = y^2 + y - x^5 - x^3 - 1$.
b) $(q, g) = (2, 2)$, $f(x, y) = y^2 + y - \frac{x^3+x^2+1}{x^3+x+1}$.
c) $(q, g) = (2, 3)$, $f(x, y) = y^4 + xy^3 - (x^2 + x)y^2 - (x^3 + 1)y - (x^4 + x + 1)$.
d) $(q, g) = (2, 3)$, $f(x, y) = y^2 + (x^3 + x + 1)y + (x^4 + x + 1)$.
e) $(q, g) = (2, 4)$, $f(x, y) =$

$$y^5+y^3+y^2(x^3+x^2+x)+y\frac{x^7+x^5+x^4+x^3+x}{x^4+x+1}+\frac{x^{13}+x^{12}+x^8+x^6+x^2+x+1}{(x^4+x+1)^2}.$$

It turns out that I have now shown you all function fields over finite fields of positive genus and class number one. There are precisely eight of them, of which three are elliptic. The five non-elliptic ones all occur over $\mathbb{F}_2$: in particular, whereas in Exercise 5.11 we did not rule out the possibility of a genus 2 function field over $\mathbb{F}_3$ with class number one, in fact there is no such field. Every other possibility permitted by Exercise 5.11 turns out to arise.

This solution of the **class number one problem** for function fields has a slightly curious history. The case of hyperelliptic function fields with a degree one place was resolved by MacRae [**Ma71**]. In [**MQ72**] Madan and Queen completed the hyperelliptic case and also eliminate the possibility of $(q, g) = (3, 2)$ [**MQ72**, Thm. 2.(i)] – the proof of this uses no tools other than what we have developed, but the analysis is rather intricate. Moreover they give a complete classification of class number one fields with $q = 2$ and $g \in \{2, 3\}$. For $q = 2$ and $g = 4$, they show that a class number one field has no place of degree less than 4 and exactly one place of degree 4. In the followup paper [**LMR75**] they eliminate the case of such a class number one function field with $q = 2$ and $g = 4$ and thus claim that there are precisely seven class number one function fields over finite fields of positive genus.

However, as Exercise 5.13e) shows, this last conclusion is false. This was not realized for a long time, until Stirpe explicitly constructed a class number one function field with $q = 2$ and $g = 4$ [**St14**]. He did not show at this time that this was the only such function field, but soon after this was shown with Mercuri [**MS15**] and, independently, by Shen-Shi [**SS15**].

Using methods very similar to those above, Villa Salvador [**VS**] records the following limitations on the class number h problem.

THEOREM 5.37 (Villa Salvador). *Let $K/\mathbb{F}_q$ be a function field of genus $g \geq 1$ and class number h.*

a) *If $h = 2$ then $q \leq 4$. Moreover, if $q = 4$ then $g = 1$. If $q = 3$, then $g \leq 2$. If $q = 2$, then $g \leq 5$.*
b) *If $h = 3$, then $q \leq 7$ and $g \leq 6$.*
c) *If $h = 4$, then $q \leq 8$ and $g \leq 6$.*
d) *If $h = 5$, then $q \leq 9$ and $g \leq 7$.*
e) *If $h = 6$, then $q \leq 11$ and $g \geq 7$.*
f) *If $h = 7$, then $q \leq 13$ and $g \leq 8$.*
g) *If $h = 8$, then $q \leq 13$ and $g \leq 8$.*
h) *If $h = 9$, then $q \leq 16$ and $g \leq 8$.*
i) *If $h = 10$, then $q \leq 17$ and $g \leq 8$.*

But so far as I know already the complete classification remains open in class number 2. Perhaps you would like to look into it! (If so: please work carefully...)

12. Pointless Function Fields

EXERCISE 5.14. *Let $K/\mathbb{F}_q$ be a function field of genus g. We say that K is **pointless** if $\Sigma_1(K/\mathbb{F}_q) = \varnothing$.*

a) *Show: if K is pointless then $q \leq (g + \sqrt{g^2 - 1})^2 < 4g^2 - 1$.*
b) *Show: if K is pointless, then $g \geq 2$.*
c) *Show: if $g = 2$ and K is pointless, then $q \leq 13$.*
d) *Let $f := y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + 1 \in \mathbb{F}_2[x, y]$. Show that f is geometrically irreducible and that K_f (the fraction field of $\mathbb{F}_2[x, y]/(f)$) defines a pointless function field of genus 2 over $\mathbb{F}_2$.*
e) *Let $f := y^2 - (2x^6 + x^5 + x^4 + x^3 + x + 2) \in \mathbb{F}_3[x, y]$. The polynomal f is geometrically irreducible. Show that K_f (the fraction field of $\mathbb{F}_3[x, y]/(f)$) defines a pointless function field of genus 2 over $\mathbb{F}_3$.*
f) *Show that up to isomorphism, the function field of part d) is the unique pointless function field over $\mathbb{F}_3$.*

Recall that the effective index $I^+(K)$ of a function field K/k is the least positive degree of an effective divisor on K; equivalently, it is the least degree of a place $P \in \Sigma(K/k)$.

EXERCISE 5.15. *Let $K/\mathbb{F}_q$ be a function field of genus g. Show:*

$$I^+(K) \leq 2\log_q(g) + 1 + \log_q(4).$$

It is interesting to ask how large the effective index can be compared to q and g. One way to study this is to fix q and define the quantity

$$\mathcal{C}(q) \coloneqq \limsup_{g\to\infty} \frac{\max\{I^+(K) \mid K/\mathbb{F}_q \text{ is a function field of genus } g\}}{\log_q(g)}.$$

Exercise 5.15 shows that for each prime power q we have

$$\mathcal{C}(q) \leq 2.$$

In my 2003 thesis, I used the family of Shimura curves $X_1^D(N)_{/\mathbb{F}_q}$ to show that for each prime power q, we have $\mathcal{C}(q) \geq \frac{1}{2}$. Around the same time, Noam Elkies and I improved this result by showing that for each fixed prime p there is a constant $C_p > 0$ such that for all $n \in \mathbb{Z}^+$ there is a function field $K_n/\mathbb{F}_p$ with genus $g \geq C_p n p^n$ such that $I^+(K_n) \geq n$. In the proof we used Igusa-Shimura curves – i.e., Shimura curves with level p structure in characteristic p – which have a small, but positive, number of places of small degree, and then an elementary argument that passes to a covering curve to "kill" these points while increasing the genus in a controllable way. As I remember it, just as we had decided to write the results up formally we realized that the covering argument would work almost as well when starting with any base function field – e.g. $\mathbb{F}_q(t)$ – to kill places of small degree, so the fact that the argument was "'not really about Shimura curves" (the subject of my PhD thesis) was somewhat deflating, which may be the reason we never published it.[1]

Exercise 5.16. *Deduce from this result of Clark-Elkies that for each prime power q we have*

$$\mathcal{C}(q) \geq 1.$$

In his thesis work, Claudio Stirpe found a totally different approach (using class field theory in the function field case) that improves the Clark-Elkies bound (though not enough to improve the bound on $\mathcal{C}(q)$).

Theorem 5.38 (Stirpe [**St13**]). *For each prime number p there is a constant $C_p > 0$ such that: for all powers q of p and all $n \in \mathbb{Z}^+$ there is a function field $K/\mathbb{F}_q$ of genus $g \leq C_p q^n$ with $I^+(K) \geq n$.*

In summary, what we have known for some time is

$$1 \leq \mathcal{C}(q) \leq 2.$$

It seems intriguing to ask where in this interval the truth lies.

13. Maximal Function Fields

A function field $K/\mathbb{F}_q$ is **maximal** if it has the largest number of degree one places permitted by the Weil bound:

$$\#\Sigma_1(K/\mathbb{F}_q) = q + 1 + 2g\sqrt{g}.$$

Thus maximal function fields can only exist if $g = 0$ (a trivial case) or q is a square. The following result of Ihara gives further restrictions.

[1] As a graduate student and a new PhD I had much less clarity as to what was worth publishing than I do today. If the work had been done, say, while I was a tenure track assistant professor I would certainly have tried to publish it and I am pretty sure I would have succeeded.

THEOREM 5.39 (Ihara [**Ih81**]). *If $K/\mathbb{F}_{q^2}$ is a maximal function field of genus g, then*

$$g \leq \frac{q^2-q}{2}. \tag{63}$$

PROOF. Ihara's bound gives

$$N_1 \leq \frac{1}{2}\left(\sqrt{(8q^2+1)g^2+(4q^4-4q^2)g}-(g-2q^2-2)\right),$$

so if K is maximal then we have

$$N_1 = q^2+1+2gq \leq \frac{1}{2}\left(\sqrt{(8q^2+1)g^2+(4q^4-4q^2)g}-(g-2q^2-2)\right). \tag{64}$$

I leave it to you to check that (64) implies $g \leq \frac{q^2-q}{2}$. □

EXERCISE 5.17. a) *Show $f := y^2+y-x^3 \in \mathbb{F}_4[x,y]$ defines an elliptic function field K over $\mathbb{F}_4$ with $N_1 = \Sigma_1(K/\mathbb{F}_4) = 9$.*

b) *Show that the function field of part a) is, up to isomorphism, the unique maximal function field $K/\mathbb{F}_4$ of positive genus.*

Remarkably, the bound (63) can be met for all prime powers q: indeed the function field A_q of Example 6.1 has genus $\frac{q^2-q}{2}$ and $q^3+1 = q^2+1+2\left(\frac{q^2-q}{2}\right)q$ degree 1 places, as does the function field H_q of Example 6.2. Have we really found two different function fields meeting Ihara's bound? Indeed not:

LEMMA 5.40. *The function fields $A_q/\mathbb{F}_{q^2}$ and $H_q/\mathbb{F}_{q^2}$ are isomorphic.*

PROOF. This is done by explicit changes of variable in [**St**, pp. 234-235]. □

The calculation of [**St**, pp. 234-235] is very elementary but not very enlightening. We should however cast no aspersions at Stichtenoth: thanks to him and Rück we have the following striking result.

THEOREM 5.41 (Rück-Stichtenoth [**RS94**]). *Let $K/\mathbb{F}_{q^2}$ be a maximal function field of genus $\frac{q^2-q}{2}$. Then K is isomorphic, as an $\mathbb{F}_{q^2}$-algebra, to the Hermitian function field A_q.*

The following results explain how one can use the Hermitian function field $A_q/\mathbb{F}_{q^2}$ to generate (well, finitely) many other maximal function fields over $\mathbb{F}_{q^2}$.

PROPOSITION 5.42. *Let $K/\mathbb{F}_{q^2}$ be a maximal function field of genus g. Then its zeta function is*

$$Z(t) = \frac{(1+qt)^{2g}}{(1-t)(1-qt)}.$$

PROOF. Let $L(t)$ be the L-polynomial of K. It suffices to show that

$$L(t) = \prod_{i=1}^{2g}(1-\alpha_i t) = (1+qt)^{2g},$$

or in other words that we have $\alpha_i = -q$ for all $1 \leq i \leq 2g$. By (49) we have

$$q^2+1+2gq = q^2+1-\sum_{i=1}^{2g}\alpha_i,$$

so

$$\sum_{i=1}^{2} g\alpha_i = -2gq.$$

Moreover the Riemann Hypothesis gives $|\alpha_i| = q$ for all i, and it follows that $\alpha_i = -q$ for all i. □

EXERCISE 5.18. *Let $K/\mathbb{F}_q$ be a maximal function field. For $r \in \mathbb{Z}^+$, let $K_r/\mathbb{F}_{q^r}$ be the degree r constant field extension.*

a) *Show: if r is odd, then $K_r/\mathbb{F}_{q^r}$ is maximal.*
b) *Show: if r is even, then $K_r/\mathbb{F}_{q^r}$ is minimal.*

THEOREM 5.43. a) *(Kleiman) Let $K/\mathbb{F}_q \subset L/\mathbb{F}_q$ be a finite extension of function fields over $\mathbb{F}_q$. Let L_K and L_L be the L-polynomials of K and L respectively. Then we have*

$$L_K(t) \mid L_L(t).$$

b) *(Serre) If $L/\mathbb{F}_q$ is a maximal function field, then so is $K/\mathbb{F}_q$.*

PROOF. a) This follows from the properties of the ℓ-adic cohomology groups that can be used to define and study the zeta function: see [**Kl68**, Prop. 1.2.4]. Alas, I am not aware of a proof from the function field perspective.
b) If L has genus zero, this follows from Lüroth's Theorem, so assume that the genus is at least one. Then since $L/\mathbb{F}_q$ is maximal, we have that q is a square, and by Proposition 5.42 each of the reciprocal roots of $L_L(t)$ is $-\sqrt{q}$. By part a), each of the reciprocal roots of $L_K(t)$ is $-\sqrt{q}$, which by Proposition 5.42 again implies that $K/\mathbb{F}_q$ is maximal. □

Let

$$G_q := \mathrm{Aut}(A_q/\mathbb{F}_{q^2})$$

be the group of all automorphisms of A_q that fix $\mathbb{F}_{q^2}$ pointwise. Like every function field over a finite field, the group G_q is finite. It is, however, extraordinarily large.

THEOREM 5.44. *We have $G_q \cong \mathrm{PGU}_3(\mathbb{F}_{q^2})$, a group of order $q^3(q^2-1)(q^3+1)$.*

EXERCISE 5.19. *Let g_q be the genus of the curve A_q. Show:*

$$\#G_q > 16g_q^4.$$

CHAPTER 6

Examples

1. Hyperelliptic Function Fields

A function field L/k is **hyperelliptic** if there is $f \in L \setminus k$ of degree 2: that is

$$2 = \deg(f)_+ = \deg(f)_- = [L : k(f)].$$

Thus a hyperelliptic function field is a quadratic extension of a rational function field $K \coloneqq k(x)$.

Until further notice we will assume that the characteristic of k is different from 2. Then we have

$$L = k(x(\sqrt{f})$$

for some $f \in k(x)^\times$. If $f \in k$, then $L = k(\sqrt{f})(x)$ has constant subfield $k(\sqrt{f}) \supsetneq k$, so this case is excluded by our running assumption that we consider only function fields with $\kappa(K) = k$. So we have $f \in L \setminus k$ and thus

$$f = \alpha \frac{p_1^{a_1} \cdots p_r^{a_r}}{q_1^{b_1} \cdots q_s^{b_s}}$$

with $\alpha \in k^\times$, $p_1, \ldots, p_r, q_1, \ldots, q_s \in k[x]$ pairwise distinct monic irreducible polynomials and $a_1, \ldots, a_r, b_1, \ldots, b_s \in \mathbb{Z}^+$. As usual for quadratic field extensions, the field $k(x)(\sqrt{f})$ depends only on the square class of f, so we may multiply by $q_1^{2b_1} \cdots q_r^{2b_s}$ to clear denominators and then repeatedly divide by squares of irreducible factors to get

$$f = \alpha p_1 \cdots p_r,\ \alpha \in k^\times,\ p_1, \ldots, p_r \in k[x] \text{ distinct monic irreducible polynomials.}$$

Thus f is separable: there are distinct $r_1, \ldots, r_d \in \overline{k}$ such that

$$f = \alpha(x - r_1) \cdots (x - r_d).$$

Since $v_{x-r_i}(f) = 1$ for all i, f is not a square in $\overline{k}(x)$ and thus

$$P(x, y) \coloneqq y^2 - f(x) \in k[x, y]$$

is geometrically irreducible and

$$L = k(x, y) = k(x, \sqrt{f})$$

is a regular function field.

PROPOSITION 6.1. *Let $L = k(x, y) = k(x, \sqrt{f})$ be a hyperelliptic function field.*

a) *The ring $k[X, Y]/(Y^2 - f(X))$ is an affine Dedekind domain in L.*
b) *The integral closure of $k[x]$ in L is $k[x, y] \cong k[X, Y]/(Y^2 - f(X))$.*

c) *Let S_∞ be the set of places $Q \in \Sigma(L/k)$ such that $Q \cap k(x) = \infty \in \Sigma(k(x)/k)$. Then*

$$k[x,y] = R^{S_\infty}.$$

PROOF. a) Let $P(x,y) := y^2 - f(x) \in k[x,y]$ and let $(a,b) \in \overline{k}^2$. Then $\frac{\partial P}{\partial x}(a,b) = -f'(a)$ and $\frac{\partial P}{\partial y}(a,b) = 2b = 2\sqrt{f(a)}$. Since the characteristic of k is different from 2, if both partial derivatives are zero, then we have $f(a) = f'(a) = 0$, contradicting the separability of a. Therefore the affine domain $k[x,y] \cong k[X,Y]/(Y^2 - f(X))$ is a Dedekind domain by Theorem 1.13.
b) The element y satisfies the monic polynomial $t^2 - f(x) \in k[x]$, so $k[x,y]$ is integral over $k[x]$. By part a), the domain $k[x,y]$ is integrally closed.
c) Since $k \subset k[x,y] \subset L$ and $k[x,y]$ is integrally closed, we have that $k[x,y]$ is the intersection of all $k[x,y]$-regular valuation rings. If $Q \notin S_\infty$ then $v_Q(x) \geq 0$ so $x \in R_Q$, and since R_Q is integrally closed also $k[x,y] \subset R_Q$. If $Q \in S_\infty$ then $v_Q(x) < 0$ so $x \notin R_Q$ and thus R_Q is not $k[x,y]$-regular. □

Proposition 6.1 allows us to determine how places $P \neq \infty \in \Sigma(k(x)/k)$ split in L. For now we restrict to degree 1 places $x - a$ for $a \in k$.

We call a version of the NTI approach to splitting of primes in extensions of Dedekind domains: let A be a Dedekind domain with fraction field K, let L/K be a finite degree field extension, and let B be the integral closure of A in L (a Dedekind domain), and let $\mathfrak{p} \in \operatorname{MaxSpec} A$. Then the prime ideals $\mathcal{P}$ of B lying over $\mathfrak{p}$ correspond to the prime ideals of the quotient ring $B/\mathfrak{p}B$. Any quotient of a Dedekind domain modulo a nonzero ideal is an Artinian ring, hence $B/\mathfrak{p}B$ decomposes as $\prod_{i=1}^r \mathfrak{r}_i$, where $\mathfrak{r}_i$ is Artinian local with maximal ideal $\mathfrak{m}_i$. Then:

• We have that r is the number of prime ideals of B lying over $\mathfrak{p}$; write them as $\mathcal{P}_1, \ldots, \mathcal{P}_r$.
• For all $1 \leq i \leq r$ we have that $e(\mathcal{P}_i|\mathfrak{p})$ is the least $e \in \mathbb{Z}^+$ such that $\mathfrak{m}_i^e = (0)$.
• For all $1 \leq i \leq r$, we have that $f(\mathcal{P}_i|\mathfrak{p}) = [\mathfrak{r}_i/\mathfrak{m}_i : A/\mathfrak{p}]$.

In our case we have $A = k[x]$, $K = k(x)$, $B = k[x,y]$, $L = k(x,y)$ and $\mathfrak{p} = (x-a)$, so we consider the ring

$$B/\mathfrak{p}B \cong k[X,Y]/(Y^2 - f(X), X - a) \cong k[Y]/(Y^2 - f(a)).$$

Thus:
• If $f(a) \in k^{\times 2}$, then $B/\mathfrak{p}B \cong k \times k$, so v_{x-a} splits into two places, each with residue field k.
• If $f(a) = 0$, then $B/\mathfrak{p}B \cong k[Y]/(Y^2)$, which is an Artinian local ring with nilpotency index $e = 2$, so v_{x-a} ramifies.
• If $f(a)$ is not a square in k, then v_{x-a} is inert: there is a single place $Q \mid (x-a)$ with residue field $k(\sqrt{f(a)})$.

The question now becomes: how does $\infty \in \Sigma(k(x)/k)$ split in L?

We will answer this twice, first using the machinery we've developed and second using the theory theory of completions of discretely valued fields.

Case 1: Suppose that f has even degree: then there is $g \in \mathbb{N}$ such that

$$f(x) = a_{2g+2}x^{2g+2} + \ldots + a_1x + a_0,\ a_i \in k,\ a_{2g+2} \neq 0. \tag{65}$$

Now we have

$$L = k(x,y) = k(\frac{y}{x^{g+1}}, \frac{1}{X})$$

and dividing (65) by x^{2g+2} gives

$$\left(\frac{y}{x^{g+1}}\right)^2 = a_{2g+2} + a_{2g+1}(1/x) + \ldots + a_0\left(\frac{1}{x^{2g+2}}\right) =: f^\perp(1/x) \in k[1/x].$$

Using $x^{2g+2}f^\perp(1/x) = f(x)$, one sees easily that he nonzero roots of $f^\perp$ in $\overline{k}$ are the reciprocals of the nonzero roots of f in k. Moreover $f^\perp(0) = a_{2g+2} \neq 0$. Thus $f^\perp(x) \in k[x]$ is separable, so the ring

$$k[\frac{1}{x}, \frac{y}{x^{g+1}}] \cong k[X,Y]/(Y^2 - f^\perp(X))$$

is the integral closure of $k[1/x]$ in L. Let S_0 be the set of places of L lying over $(x-0)$ in $\Sigma(k(x)/k)$. Then Proposition 6.1 gives

$$k[\frac{1}{x}, \frac{y}{x^{g+1}}] = R^{S_0},$$

and we can apply the above analysis to determine how ∞ splits in L. We get:

• If $f^\perp(0) = a_{2g+2} \in k^{\times 2}$, then there are two degree 1 places of L lying over ∞.
• if $f^\perp(0) = a_{2g+2} \notin k^{\times 2}$, then there is a one degree 2 place of L lying over ∞, with residue field $k(\sqrt{a_{2g+2}})$.

Case 2: Suppose that f has odd degree: then there is $g \in \mathbb{N}$ such that

$$f(x) = a_{2g+1}x^{2g+1} + \ldots + a_1x + a_0,\ a_i \in k,\ a_{2g+1} \neq 0. \tag{66}$$

As above we divide (66) by x^{2g+2}, getting

$$\left(\frac{y}{x^{g+1}}\right)^2 = a_{2g+1}(1/x) + \ldots + a_0\left(\frac{1}{x^{2g+2}}\right) =: f^\perp(1/x) \in k[1/x].$$

Using $x^{2g+2}f^\perp(1/x) = f(x)$ we see as above that the nonzero roots of $f^\perp$ in $\overline{k}$ have multiplicity 1. This time $f^\perp$ has zero constant term so does have 0 as a root, but because $a_{2g+1} \neq 0$ it is a simple root, so again $f^\perp(x) \in k[x]$ is separable, so once again we have

$$R^{S_0} = k[\frac{1}{x}, \frac{y}{x^{g+1}}] \cong k[X,Y]/(Y^2 - f^\perp(X))$$

is the integral closure of $k[\frac{1}{x}]$ in L. Since $f\perp(0) = 0$, it follows that ∞ ramifies in L.

Next we give an "NTII" approach. For this, we recall the following fact (cf. [**NTII**, Thm. 1.64] and the surrounding material): if v is a rank one valuation on a field K and L/K is a finite degree field extension, then there is always at least one extension of v to a valuation on L and only finitely many extensions: let them be $w_1, \ldots, w_r$.

Let $\hat{K}$ be the completion of K with respect to v. For each $1 \leq i \leq r$, let $\hat{L}_i$ be the completion of L with respect to w_i. Then we have a $\hat{K}$-algebra homomorphism

$$\Phi : L \otimes_K \hat{K} \to \prod_{i=1}^{r} \hat{L}_i, \ \sum x_j \otimes y_j \mapsto \sum_j \iota_i(x)y.$$

Moreover the map Φ is surjective, and its kernel is the (nil = Jacobson) radical of the Artinian ring $L \otimes_K \hat{K}$. So if $\mathrm{MaxSpec}(L \otimes_K \hat{K}) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$, then Φ may be identified with the CRT homomorphism

$$L \otimes_K \hat{K} \to \prod_{I=1}^{r} (L \otimes_K \hat{K})/\mathfrak{m}_i.$$

If L/K is separable, then Φ is a homomorphism. Moreover, the ramification index $e_i = e(w_i|v)$ is the ramification index of $\hat{L}_i/\hat{K}$, i.e., the index of $v(\hat{K}^\times)$ in $w_i(\hat{L})^\times$, and the residual degree $f_i = f(w_i/v)$ is the degree of the residual extension l_i/k.

In our case we take v_∞ on $K = k(x)$ and $L = k(x, y) = k(x, \sqrt{f})$. By Proposition 1.16, we have $\hat{K} = k((1/x))$. So

$$\hat{K} \otimes_K L = \hat{K} \otimes_{k(x)} k(x)[y]/(y^2 - f(x)) = \hat{K}[y]/(y^2 - f),$$

and we have essentially reduced to the question of how the polynomial $y^2 - f(x)$, which is irreducible in $k(x)[y]$, factors in $k((1/x))[y]$, which in turn reduces to squares in complete discretely valued fields. The following result is an easy consequence of the structure theory of such fields.

EXERCISE 6.1. *Let (K, v) be a complete, discretely valued field with uniformizer π and residue field k, which we assume to have characteristic different from 2.*

a) *For $x \in K^\times$, show: $x \in K^\times$ iff $v(x)$ is even and $\frac{x}{\pi^{v(x)}} \pmod{(\pi)} \in k^{\times 2}$.*
b) *If $x \in K^\times \setminus K^{\times 2}$, then $K(\sqrt{x})/K$ is ramified iff $v(x)$ is odd. If $v(x)$ is even then residue field of $K(\sqrt{x})$ is $k(\sqrt{\overline{x}})$, where $\overline{x} = x \pmod{(\pi)}$.*

Now we place ourselves in **Case 1**, where $f = a_{2g+2}x^{2g+2} + \ldots + a_1 x + a_0$. Then $v(f) = v_\infty(f) = -(2g + 2)$ is even. We take $\pi = \frac{1}{x}$ as our uniformizer for $\hat{K} = k((1/x))$. Then

$$\frac{x}{\pi^{v(f)}} = \frac{f}{x^{2g+2}} = a_{2g+2} + a_{2g+1}(1/x) + \ldots + a_0 \left(\frac{1}{x}\right)^{2g+2}.$$

It follows that the image of this element in the residue field is a_0. So by the exercise, we get that if $a_{2g+2} \in k^{\times 2}$, then $y^2 - f$ splits into distinct linear factors in $\hat{K}[y]$, so $\hat{K} \otimes_K L \cong \hat{K} \times \hat{K}$: the place ∞ splits into two degree 1 places in L. If $a_{2g+2} \notin k^{\times 2}$, then $y^2 - f$ remains irreducible over $\hat{K}[y]$, so $\hat{K} \otimes_K L = \hat{K}(\sqrt{f})$, an unramified quadratic extension of $\hat{K}$ with residue field $k(\sqrt{a_{2g+2}})$. Thus there is a unique place of L lying over ∞, which has residue field $k(\sqrt{a_{2g+2}})$.

And finally, we again place ourselves in **Case 2**, where $f = a_{2g+1}x^{2g+1} + \ldots + a_0$. Then $v(f) = v_\infty(f) = -(2g + 1)$ is odd, so $y^2 - f$ remains irreducible over $\hat{K}[y]$ and the quadratic field extension $\hat{K} \otimes_K L = \hat{K}(\sqrt{f})$ is ramified, which means that there is a unique place P of L lying over ∞, which has $e(P|\infty) = 2$ and $f(P|\infty) = 1$.

To summarize, we have proved the following result twice.

THEOREM 6.2. *Let k be a field of characteristic 2, and let L/k be a function field that is a quadratic extension of a subfield $k(x)$. There is a separable polynomial $f \in k[x]$ such that $L = k(x, \sqrt{f}) = k(x, y)$ is the fraction field of $k[X, Y]/(Y^2 - f(X))$. Moreover:*

a) *If f has even degree $2g+2$ and the leading coefficient a_{2g+2} is a square in k, then there are two places $\tilde{\infty}_1, \tilde{\infty}_2 \in \Sigma(L/k)$ lying over $\infty \in \Sigma(k(x)/k)$, each with residue field k. There is no ramification over ∞.*
b) *If f has even degree $2g+2$ and the leading coefficient a_{2g+2} is not a square in k, then there is a unique place $\tilde{\infty} \in \Sigma(L/k)$ lying over $\infty \in \Sigma(k(x)/k)$, with residue field $k(\sqrt{a_{2g+2}})$. There is no ramification over ∞.*
c) *If f has odd degree $2g+1$, then there is a unique place $\tilde{\infty} \in \Sigma(L/k)$ lying over $\infty \in \Sigma(k(x)/k)$ with residue field k. We have $e(\tilde{\infty}|\infty) = 2$.*

EXERCISE 6.2. *Suppose k is algebraically closed. Let L/k be a hyperelliptic function field with separable defining polynomial $f = \alpha \prod_{i=1}^{d}(x - r_i) \in k[x]$: thus, as above, L is the fraction field of $k[X, Y]/(Y^2 - f(X))$.*

a) *Suppose that f has even degree $2g + 2$. Show: none of the Weierstrass points of L lie over the point $\infty \in \Sigma(k(x)/k)$ and in the affine coordinate chart $k[x, y]$, are precisely the maximal ideals corresponding to the points $(r_i, 0) \in k^2$.*
b) *Suppose that f has odd degree $2g+1$: Show: the unique place P_∞ of L lying over $\infty \in \Sigma(k(x)/k)$ is a Weierstrass point, and the other Weierstrass points are, as above, the places corresponding to the points $(r_i, 0) \in k^2$.*

2. Superelliptic Function Fields

A **superelliptic function field** is a Kummer extension of a rational function field. We begin with the following useful genus formula.

THEOREM 6.3. *Let $n \geq 2$, and let k be a field of characteristic not dividing n. Let $f = a \prod_{i=1}^{r} p_i^{n_i} \in k[t]$, where $r \geq 1$, $p_1, \ldots, p_r$ are distinct monic irreducible polynomials and $n_i \in \mathbb{Z}^+$ is such that $\gcd(n, n_i) = 1$ for all $1 \leq i \leq r$. Put $K = k(x)$ and*

$$L \coloneqq K(f^{1/n}).$$

a) *The function field L/k is regular. The extension L/K is cyclic iff k contains a primitive nth root of unity.*
b) *Let $P_1, \ldots, P_r$ be the places of $k(x)$ corresponding to the irreducible polynomials $p_1, \ldots, p_r$. Then for all $1 \leq i \leq r$ we have that P_i is totally ramified in L. Put*

$$d \coloneqq \gcd(n, \deg(f).$$

Then every place $Q_\infty \mid P_\infty$ has $e(Q_\infty|P_\infty) = \frac{n}{d}$. Every place $P \notin \{P_1, \ldots, P_r, P_\infty\}$ is unramified in L.
c) *We have*

$$g_L = \frac{n-1}{2}\left(-1 + \sum_{i=1}^{r} \deg p_i\right) - \frac{d-1}{2}.$$

PROOF. This follows immediately by applying Corollary 3.29. □

Theorem 6.3 gives us a large supply of Kummer extensions of $k(x)$, but not all of them:

EXERCISE 6.3. *Suppose that k contains a primitive nth root of unity.*

a) *Suppose that n is a prime number. Show that every degree n Kummer extension of $k(x)$ is of the form considered in Theorem 6.3.*
b) *Suppose that $n = \ell^A$ is a prime power and k is algebraically closed. Show that every degree n Kummer extension of $k(x)$ is of the form considered in Theorem 6.3.*
c) *Suppose that n is not a prime power and k is algebraically closed. Show that there are degree n Kummer extensions of $k(x)$ that are not totally ramified above any $P \in \Sigma(K/k)$.*

On the other hand, in some ways it is nice to focus on a somewhat smaller class of extensions.

LEMMA 6.4. *With notation as in Theorem 6.3, suppose that $n_i = 1$ for all $1 \leq i \leq r$. Show that the integral closure of $k[x]$ in L is $k[x,y]/(y^n - f)$. Show that the converse holds if k is perfect.*

EXERCISE 6.4. *Let $m, n \in \mathbb{Z}^+$ be such that the characteristic of k does not divide mn. Let $b, c \in k^\times$ be distinct elements. Put $K = k(x)$,*

$$f(x) = \frac{x^m - b}{x^m - c}, \ L = K(f^{1/n}).$$

Show:

$$g_L = (m-1)(n-1).$$

EXERCISE 6.5. *Let $m, n \in \mathbb{Z}^+$ be such that the characteristic of k does not divide mn. Let $a, b, c \in k^\times$.*

a) *Show that the function field K_f associated to the polynomial $f = ax^m + b^n - c$ is regular of genus $\frac{(m-1)(n-1)+1-\gcd(m,n)}{2}$. When $m = n$ we get*

$$g_{K_f} = \frac{(n-1)(n-2)}{2}.$$

*These function fields are of **Fermat type**.*
b) *Show: if k is algebraically closed then two Fermat type function fields are isomorphic iff they have the same genus.*

3. Generalized Artin-Schreier Extensions

Let k be a perfect field of characteristic $p > 0$. Following Stichtenoth [**St**, Prop. 6.4.1] we discuss a class of coverings of $L/k(x)$ that are "Artin-Schreier like": they are finite Galois with Galois group an elementary commutative p-group and they are unramified away from ∞.

THEOREM 6.5. *Let k be a perfect field of characteristic $p > 0$. Let $K = k(x)$. Let $q = p^s$ for some $s \in \mathbb{Z}^+$. Let $\mu \in k^\times$ and suppose that the polynomial $t^q + \mu t$ splits over k. Let $f \in k[x]$ have degree M with $p \nmid M$. Then:*

a) *The polynomial*

$$P(x,y) \coloneqq y^q + \mu y - f(x) \in k[x,y]$$

is geometrically irreducible, so

$$L \coloneqq \mathrm{ff}(k[x,y]/(P))$$

is a regular function field over k.

b) *We have $[L:K] = q$.*

c) *Let*

$$A \coloneqq \{\gamma \in k \mid \gamma^q + \mu\gamma = 0\}.$$

Then A is an order q subgroup of $(k,+)$. For all $\sigma \in \mathrm{Aut}(L/K)$, there is a unique $\gamma(\sigma(\in A$ such that $\sigma(y) = y + \gamma(\sigma)$, and the map $\sigma \mapsto \gamma(\sigma)$ gives an isomorphism

$$\mathrm{Aut}(L/K) \xrightarrow{\sim} A.$$

d) *No finite place of K ramifies in L, while the infinite place P_∞ is totally ramified. If $\tilde{P}_\infty$ denotes the unique place of L lying over P_∞ then we have*

$$d(\tilde{P}_\infty | P_\infty) = (q-1)(M+1).$$

e) *We have*

$$g_L = \frac{(q-1)(M-1)}{2}.$$

Exercise 6.6. *Prove Theorem 6.5.*

Exercise 6.7. *Let q be a power of the prime number p, and let k be a field of characteristic p. For a positive integer n not divisible by p, we denote by μ_n the group of nth roots of unity in an algebraic closure $\overline{k}$ of k.*

a) *Show: the polynomial $t^q - t$ splits in k iff $\mu_{q-1} \subset k$.*

b) *Suppose $p = 2$. Show: $t^q + t$ splits in k iff $\mu_{q-1} \subset k$.*

c) *Suppose $p > 2$. Show: $t^q + t$ splits in k iff $\mu_{2q-2} \subset k$, hence in particular if $\mathbb{F}_{q^2} \subset k$.*

Exercise 6.8. *Let q be a a power of the prime number p.*

a) *Consider the map $[q+1] : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ given by $x \mapsto x^{q+1}$. Show that it is a group homomorphism with image $\mathbb{F}_q^\times$.*

b) *Let $\tau : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ be the map $y^q + y$, and put $A \coloneqq \{a \in \mathbb{F}_{q^2} \mid a^q + a = 0\}$. Either by identifying τ as a trace map or otherwise, show that τ is a homomorphism of additive groups, with kernel A and image $\mathbb{F}_q$.*

Example 6.1. *For any prime power $q = p^s$, we consider the function field A_q attached to the polynomial $y^q + y - x^{q+1}$. This is an instance of Theorem 6.5 with $\mu = 1$ and $M = q+1$, and therefore $A_q/\mathbb{F}_{q^2}$ is regular of genus*

$$g_{A_q} = \frac{q(q-1)}{2}.$$

Theorem 6.6. *We have $\#\Sigma_1(A_q/\mathbb{F}_{q^2}) = q^3 + 1$.*

Proof. Consider

$$B \coloneqq \mathbb{F}_{q^2}[X,Y]/(P(X,Y)),\ P(X,Y) = Y^q + Y - X^{q+1}.$$

Since $\frac{dP}{dy} \equiv 1$, by Theorem 1.13 is a Dedekind domain, and therefore it is the ring of all functions on A_q regular away from the place $\tilde{P}_\infty$ lying over P_∞ of $K = \mathbb{F}_{q^2}(x)$. So the degree 1 places of A_q not lying over P_∞ correspond to elements of

$$V \coloneqq \{(a,b) \in \mathbb{F}_{q^2}^2 \mid b^q + b = a^{q+1}.$$

If $a = 0$, then $(a,b) \in V$ iff $b \in A$ (notation as in the previous exercise), hence there are q such points.

If $a \in \mathbb{F}_q^\times$, then by the previous exercise $a^{q+1} \in \mathbb{F}_q^\times$ and it follows that there is $b \in \mathbb{F}_{q^2}$ such that $b^q + b = a^{q+1}$. The collection of such b forms a nonempty fiber of a group homomorphism hence is a coset of the kernel A, so there are values of b such that $(ab,) \in \mathbb{F}_{q^2}$.

Since P_∞ has residue field $\mathbb{F}_{q^2}$ and $A_q/\mathbb{F}_{q^2}(x)$ is totally ramified over P_∞, the point $\tilde{P}_\infty$ is the unique place of A_q lying over P_∞ and has degree 1.

In total we get $q + (q^2-1)q + 1 = q^3 + 1$ degree 1 places of A_q. □

4. Hermitian Function Fields

Let q be a prime power. For a field $k \supset \mathbb{F}_q$ and $a, b, c \in \mathbb{F}_q^\times$, we consider the Fermat type function field $k(x,y)$ attached to the polynomial

$$f(x,y) = ax^{q+1} + by^{q+1} - c.$$

EXERCISE 6.9. *Suppose that $k \supset \mathbb{F}_{q^2}$. Show that any two function fields of the above form are isomorphic. (Hint: show that every element of $\mathbb{F}_q$ is of the form a^{q+1} for some $a \in \mathbb{F}_{q^2}$.)*

EXAMPLE 6.2. *We define the **Hermitian function field** $H_q/\mathbb{F}_{q^2}$ to be the function field $\mathbb{F}_{q^2}(x,y)$ where $y^{q+1} = x^{q+1} - 1$. By Exercise 6.5 the Hermitian function field H_q is regular of genus $\frac{q(q-1)}{2}$.*

THEOREM 6.7. *Let q be a prime power. Then we have*

$$\#\Sigma_1(H_q/\mathbb{F}_{q^2}) = q^3 + 1.$$

PROOF. The polynomial $x^{q+1} - 1$ is separable, so by Lemma 6.4 we have that $A \coloneqq k[x,y]/(y^{q+1} - x^{q+1} + 1)$ is a Dedekind domain and is thus indeed the holomorphy ring of all functions in H_q regular away from the places lying over P_∞.

Every degree 1 place of H_q lies over a degree 1 place of $\mathbb{F}_{q^2}(x)$. For a finite place P_a corresponding to the polynomial $x - a$, the degree 1 places on H_q lying over P_a correspond to the maximal ideals of A lying over $x - a$, which in turn corresponds to pairs $(a,b) \in \mathbb{F}_{q^2}^2$ such that $b^{q+1} = a^{q+1} - 1$.

Case 1: If $a^{q+1} = 1$, then the unique such b is $b = 0$. Since $\mathbb{F}_{q^2}^\times$ is cyclic of order $q^2 - 1$ and $q - 1 \mid q^2 - 1$, there are precisely $q + 1$ such $a \in \mathbb{F}_{q^2}$, which thus gives rise to $q + 1$ degree 1 places altogether.

Case 2: For all $a \in \mathbb{F}_{q^2}$ we have $a^{q+1} \in \mathbb{F}_q$: this is clear if $a = 0$; otherwise we have $1 = a^{q^2-1} = (a^{q+1})^{q-1}$, so a^{q-1} is a $(q-1)$st root of unity, hence lies in $\mathbb{F}_q$. As mentioned above, every element of $\mathbb{F}_q$ is the $(q+1)$st power of some element of $\mathbb{F}_{q^2}$, and since $\mathbb{F}_{q^2}$ contains the $q+1$st roots of unity, this means that for every $a \in \mathbb{F}_{q^2}$ such that $a^{q+1} \neq 1$ there are $q + 1$ elements $b \in \mathbb{F}_{q^2}$ such that $b^{q+1} = a^{q+1} - 1$. This contributes $(q^2 - q - 1)(q + 1)$ degree 1 places.

Case 3: Consider now the point P_∞. Its splitting in H_q is controlled by the algebra

$$\hat{K}_{P_\infty} \otimes_K H_q = \mathbb{F}_{q^2}((1/x))[t]/(t^{q+1} - x^{q+1} + 1).$$

We claim that $\theta := x^{q+1} - 1$ is a $(q+1)$st power in $\mathbb{F}_{q^2}((1/x))$ hence the polynomial $t^{q+1} - x^{q+1} + 1$ splits completely, which means that all places of H_q lying over P_∞ have degree 1. Indeed we need the valuation to be a multiple of $q+1$ and for $\frac{\theta}{(1/x)^{v(\theta)}}$ to reduce to a $(q+1)$st power in the residue field $\mathbb{F}_{q^2}$. The valuation of $\theta = x^{q+1} - 1$ is the negative of its degree, hence $-(q+1)$, and

$$\frac{\theta}{(1/x)^{-q-1}} = 1 - (1/x)^{q+1},$$

which reduces to 1, which is indeed a perfect $(q+1)$st power! This shows that there are $q+1$ degree 1 places lying over P_∞.
All in all, the number of degree 1 places is

$$(q+1) + (q^2 - q - 1)(q+1) + (q+1) = (q^2 - q + 1)(q+1) = q^3 + 1. \qquad \square$$

Bibliography

[Ac79] R.D.M. Accola, *On Castelnuovo's inequality for algebraic curves. I.* Trans. Amer. Math. Soc. 251 (1979), 357–373.

[ACGH] E. Arbarello, M. Cornalba, P.A. Griffiths and J. Harris, *Geometry of algebraic curves.* Vol. I. Grundlehren der Mathematischen Wissenschaften 267. Springer-Verlag, New York, 1985.

[AHL12] Y. Aubry, S. Haloui and G. Lachaud, *On the number of points on abelian and Jacobian varieties over finite fields.* Acta Arith. 160 (2013), 201–241.

[Ba00] M.H. Baker, *Cartier points on curves.* Internat. Math. Res. Notices 2000, 353–370.

[Be09] P. Beelen, *A generalization of Baker's theorem.* Finite Fields Appl. 15 (2009), 558–568.

[BG13] R. Becker and D. Glass, *Pointless hyperelliptic curves.* Finite Fields Appl. 21 (2013), 50-57.

[BGKM20] D. Bartolo, M. Giulietti, M. Kawakita and M. Montanucci, *New examples of maximal curves with low genus.* Finite Fields Appl. 68 (2020), 101744, 32 pp.

[CA] P.L. Clark, *Commutative Algebra.* `http://math.uga.edu/~pete/integral2015.pdf`

[CE59] E.D. Cashwell and C.J. Everett, *The ring of number-theoretic functions.* Pacific J. Math. 9 (1959), 975–985.

[CG72] C.H. Clemens and P.A. Griffiths, *The intermediate Jacobian of the cubic threefold.* Ann. of Math. (2) 95 (1972), 281–356.

[Cl04] P.L. Clark, *There are genus one curves of every index over every number field.* J. Reine Angew. Math. 594 (2006), 201–206.

[Cl12] P.L. Clark, *Covering numbers in linear algebra.* Amer. Math. Monthly 119 (2012), 65-–67.

[Ei] D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry.* Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.

[FGT97] R. Fuhrmann, A. Garcia and F. Torres, *On maximal curves.* J. Number Theory 67 (1997), 29–51.

[FT] P.L. Clark, *Field Theory.* `http://math.uga.edu/~pete/FieldTheory.pdf`

[G] D.M. Goldschmidt, *Algebraic functions and projective curves.* Graduate Texts in Mathematics, 215. Springer-Verlag, New York, 2003.

[GSX00] A. Garcia, H. Stichtenoth and C.-P. Xing, *On subfields of the Hermitian function field.* Compositio Math. 120 (2000), 137–170.

[He] R. Hartshorne, *Algebraic geometry.* Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[Hi] D. Harari, *Galois Cohomology and Class Field Theory.* Springer, 2017.

[Ha05] T. Hasegawa, *On the number of places of function fields and congruence zeta functions.* Nihonkai Math. J. 16 (2005), 77–84.

[HKT] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic curves over a finite field.* Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008.

[HS13] L.L. Hall-Seelig, *New lower bounds for the Ihara function A(q) for small primes.* J. Number Theory 133 (2013), 3319–3324.

[Ih81] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields.* J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28 (1981), 721–724.

[Kl68] S.L. Kleiman, *Algebraic cycles and the Weil conjectures.* Dix exposés sur la cohomologie des schémas, 359–386, Adv. Stud. Pure Math., 3, North-Holland, Amsterdam, 1968.

[KT02] G Korchmáros and F. Torres, *On the genus of a maximal curve.* Math. Ann. 323 (2002), 589–608.

[La00] K. Lauter, *Non-existence of a curve over $\mathbb{F}_3$ of genus 5 with 14 rational points.* Proc. Amer. Math. Soc. 128 (2000), 369–374.

[Li] Q. Liu, *Algebraic geometry and arithmetic curves.* Translated from the French by Reinie Erné. Oxford Graduate Texts in Mathematics, 6. Oxford Science Publications. Oxford University Press, Oxford, 2002.

[Lo] D. Lorenzini, *An invitation to arithmetic geometry.* Graduate Studies in Mathematics, 9. American Mathematical Society, Providence, RI, 1996.

[LMR75] J. Leitzel, M. Madan, C. Queen, *Algebraic function fields with small class number.* J. Number Theory 7 (1975), 11–27.

[LV00] G. Lachaud and S. Vlădut, *Gauss problem for function fields.* J. Number Theory 85 (2000), 109–129.

[Ma71] R.E. MacRae, *On unique factorization in certain rings of algebraic functions.* J. Algebra 17 (1971), 243–261.

[Mi15] J.S. Milne, *The Riemann Hypothesis over Finite Fields. From Weil to the Present Day.* `https://arxiv.org/pdf/1509.00797.pdf`

[MN02] E. Nart and D. Maisner, *Abelian surfaces over finite fields as Jacobians.* With an appendix by Everett W. Howe. Experiment. Math. 11 (2002), 321–337.

[MQ72] M.L. Madan and C.S. Queen, *Algebraic function fields of class number one.* Acta Arith. 20 (1972), 423–432.

[MS15] P. Mercuri and C. Stirpe, *Classification of algebraic function fields with class number one.* J. Number Theory 154 (2015), 365–374.

[MT10] S. Meagher and J. Top, *Twists of genus three curves over finite fields.* Finite Fields Appl. 16 (2010), 347–368.

[NTII] P.L. Clark, *Algebraic Number Theory II: Valuations, Local Fields and Adeles.* `http://math.uga.edu/~pete/8410FULL.pdf`

[Po07] B. Poonen, *Gonality of modular curves in characteristic p.* Math. Res. Lett. 14 (2007), 691–701.

[Po17] I. Pogildiakov, *On the linear bounds on genera of pointless hyperelliptic curves.* `https://arxiv.org/abs/1703.08312`

[Ro] M. Rosen, *Number theory in function fields.* Graduate Texts in Mathematics, 210. Springer-Verlag, New York, 2002.

[Ro73] M. Rosen, *S-units and S-class group in algebraic function fields.* J. Algebra 26 (1973), 98–108.

[Ro76] M. Rosen, *Elliptic curves and Dedekind domains.* Proc. Amer. Math. Soc. 57 (1976), 197–201.

[Rü90] H.G. Rück, *A note on elliptic curves over finite fields.* Math. Comp. 49 (1987), 301–304.

[RS94] H.-G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields.* J. Reine Angew. Math. 457 (1994), 185–188.

[RX18] J. Roé and X. Xarles, *Galois descent for the gonality of curves.* Math. Res. Lett. 25 (2018), 1567–1589.

[S] J.-P. Serre, *Algebraic groups and class fields.* Translated from the French. Graduate Texts in Mathematics, 117. Springer-Verlag, New York, 1988.

[Sa03] D. Savitt, *The maximum number of points on a curve of genus 4 over $\mathbb{F}_8$ is 25.* With an appendix by Kristin Lauter. Canad. J. Math. 55 (2003), 331–352.

[Se83.1] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini.* C. R. Acad. Sci. Paris Sér. I Math. 296 (1983), 397–402.

[Se83.2] J.-P. Serre, *Nombres de points des courbes algébriques sur $\mathbb{F}_q$.* Seminar on number theory, 1982-1983 (Talence, 1982/1983), Exp. No. 22, 8 pp., Univ. Bordeaux I, Talence, 1983.

[Si] J.H. Silverman, *The arithmetic of elliptic curves.* Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

[SS15] Q. Shen and S. Shi, *Function fields of class number one.* J. Number Theory 154 (2015), 375–379.

[St] H. Stichtenoth, *Algebraic function fields and codes.* Second edition. Graduate Texts in Mathematics, 254. Springer-Verlag, Berlin, 2009.

[St73] H. Stark, *On the Riemann hypothesis in hyperelliptic function fields.* In Analytic Number Theory, Proceedings of Symposia in Pure Mathematics, Vol. XXIV, pp. 285–302, American Mathematical Society, Providence, RI, 1973.

[St11] H. Stichtenoth, *Curves with a prescribed number of rational points.* Finite Fields Appl. 17 (2011), 552–559.

[St13] C. Stirpe, *An upper bound for the minimum genus of a curve without points of small degree.* Acta Arith. 160 (2013), 115–128.

[St14] C. Stirpe, *A counterexample to 'Algebraic function fields with small class number'.* J. Number Theory 143 (2014), 402–404.

[SV86] K.-O. Stöhr and J.F. Voloch, *Weierstrass points and curves over finite fields.* Proc. London Math. Soc. 52 (1986), 1–19.

[Su.5] A Sutherland, `https://math.mit.edu/classes/18.785/2016fa/LectureNotes5.pdf`

[Su.12] A. Sutherland, `https://math.mit.edu/classes/18.785/2016fa/LectureNotes12.pdf`

[Ta52] J. Tate, *Genus change in inseparable extensions of function fields.* Proc. Amer. Math. Soc. 3 (1952), 40–406.

[Tr88] H.F. Trotter, *An overlooked example of nonunique factorization.* Amer. Math. Monthly 95 (1988), 339–342.

[TVZ82] M.A. Tsfasman, S.G. Vlăduts and T. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound.* Math. Nachr. 109 (1982), 21–28.

[VS] G.D. Villa Salvador, *Topics in the theory of algebraic function fields.* Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 2006.

[Vo05] J. Voight, *Curves over finite fields with many points: an introduction.* Computational aspects of algebraic curves, 124–144, Lecture Notes Ser. Comput., 13, World Sci. Publ., Hackensack, NJ, 2005.

[Wa69] W.C. Waterhouse, *Abelian varieties over finite fields.* Ann. Sci. École Norm. Sup. (4) 2 (1969), 521–560.

[WS10] Q. Wu and R. Scheidler, *The ramification groups and different of a compositum of Artin-Schreier extensions.* Int. J. Number Theory 6 (2010), 1541–1564.

[Ye07] S. Yekhanin, *A note on plane pointless curves.* Finite Fields Appl. 13 (2007), 418–422.

[Za58] O. Zariski, *On Castelnuovo's criterion of rationality $p_a = P_2 = 0$ of an algebraic surface.* Illinois J. Math. 2 (1958), 303–315.