Brown Universty

Honors Thesis

Hermite's Theorem for Function Fields

Author:
Zev Chonoles

Advisor:
Prof. Michael Rosen

Submitted:
May 3, 2012

Acknowledgements

I am forever indebted to Professor Glenn Stevens and everyone else at the PROMYS program, without whose patience and encouragement I would not be doing mathematics today. I also express my deepest thanks to my professors at Brown, all of whom have made my time here immensely enjoyable and educational; and in particular, to Professor Mike Rosen, who proposed this problem for my thesis and who has been a superb mentor. Most of all, I thank my father for imbuing me with his intellectual curiosity and love of mathematics, and for paying my tuition.

Abstract

Hermite's theorem states that there are only finitely many number fields with bounded discriminant. In this work, we investigate an analog of Hermite's theorem for function fields: there are only finitely many separable function fields with bounded degree and discriminant. We prove this in the case that the function fields are unramified at ∞. Although Hermite's theorem for function fields is known through other methods, we used an adaptation of a classical technique from the theory of number fields, namely that of "geometry of numbers". We expect that the generalization we construct here can, with a few modifications, serve to extend any "geometry of numbers" argument to function fields.

Contents

1 Preliminaries

We assume the reader is familiar with basic defintions and properties of algebraic number theory, as well as basic point-set topology and measure theory. Recommended references for algebraic number theory include [Neu99] and [Lan86]; for topology, [Mun00]; and for measure theory, [Fol99].

1.1 Geometry of numbers

Definition. A *lattice* in $\mathbb{R}^n$ is a subgroup $\mathcal{L}$ of $\mathbb{R}^n$ of the form

$$\mathcal{L} = \{a_1v_1 + \cdots + a_nv_n \mid a_i \in \mathbb{Z}\}$$

where $\{v_1, \ldots, v_n\}$ is a basis for $\mathbb{R}^n$. The *fundamental domain* of $\mathcal{L}$ is

$$D_{\mathcal{L}} = \{a_1v_1 + \cdots + a_nv_n \mid a_i \in [0, 1)\}$$

and the *volume* of $\mathcal{L}$ is

$$\mathrm{vol}(\mathcal{L}) = m(D_{\mathcal{L}})$$

where m is the Lebesgue measure.

Minkowski's Theorem. *Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice, and let $K \subseteq \mathbb{R}^n$ be convex and centrally symmetric. If $m(K) > 2^n \mathrm{vol}(\mathcal{L})$, then $K \cap \mathcal{L} \supsetneq \{0\}$.*

This theorem has surprising applications to algebraic number theory. The most well-known is

Minkowski's Bound. *Let K be a number field of degree n with discriminant $\mathfrak{d}_K$. Let r_2 be the number of conjugate pairs of complex embeddings of K. Then any class in Cl_K, the ideal class group of K, has a representative I which is an integral ideal of $\mathcal{O}_K$ and which has*

$$N(I) = |\mathcal{O}_K/I| \leq \sqrt{|\mathfrak{d}_K|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}.$$

However, the one being generalized in this work is

Hermite's Theorem. *For any $N \in \mathbb{N}$, there are only finitely many number fields K with $|\mathfrak{d}_K| < N$.*

See [Neu99] and [Lan86] for proofs.

1.2 Measure theory

We assume the reader is familiar with the notions of and basic results concerning σ-algebras and measures. A good reference for this topic is [Fol99]. We introduce some definitions and results the reader may not be familiar with.

Definition. Given two measure spaces $(X, \mathcal{M}, \mu)$ and $(Y, \mathcal{N}, \nu)$, the *product σ-algebra* $\mathcal{M} \otimes \mathcal{N}$ on $X \times Y$ is the σ-algebra generated by $\{A \times B \mid A \in \mathcal{M}, B \in \mathcal{N}\}$. When μ and ν are σ-finite (which all measure spaces appearing in this work are), the product measure $\mu \times \nu$ is the unique measure on $\mathcal{M} \otimes \mathcal{N}$ such that $(\mu \times \nu)(A \times B) = \mu(A)\nu(B)$ for all $A \in \mathcal{M}, B \in \mathcal{N}$.

Definition. Given a locally compact Hausdorff topological space X, a *Radon measure* on X is a Borel measure μ on X with the property that $\mu(K) < \infty$ for every compact $K \subseteq X$, that

$$\mu(E) = \sup\{\mu(K) \mid \text{compact } K \subseteq A\}$$

for all open $E \subseteq X$, and that

$$\mu(E) = \inf\{\mu(U) \mid \text{open } U \supseteq E\}$$

for all Borel $E \subseteq X$.

Definition. Let G be a locally compact topological group. A *left Haar measure* on G is a non-zero Radon measure μ on G with the property that $\mu(xE) = \mu(E)$ for every Borel set $E \subseteq G$ and $x \in G$.

It is a fundamental result of harmonic analysis that on any locally compact group there exists a left Haar measure, which is unique up to a multiplicative constant. Precisely,

Proposition 1 ([Fol95], Theorems 2.10 and 2.20)**.** *There exists a left Haar measure on any locally compact group G. If λ and μ are any two left Haar measures on G, then there exists some $c > 0$ such that $\lambda = c\mu$.*

2 Results

Throughout, let $\mathbb{F}_q$ be a fixed finite field of cardinality q, let $k = \mathbb{F}_q(T)$, and let $A = \mathbb{F}_q[T] \subset k$.

Let ∞ be the infinite place of k.

The completion of k with respect to $|\cdot|_\infty$ is $k_\infty = \mathbb{F}_q((\frac{1}{T}))$.

The ring of integers of k_∞ is $\mathcal{O}_\infty = \mathbb{F}_q[[\frac{1}{T}]] \subset k_\infty$.

The unique maximal ideal of $\mathcal{O}_\infty$ is $\mathfrak{m}_\infty = (\frac{1}{T}) \subset \mathcal{O}_\infty$.

The residue field of k_∞ is $\kappa_\infty = \mathcal{O}_\infty/\mathfrak{m}_\infty \cong \mathbb{F}_q$.

2.1 Minkowski's theorem for function fields

The field k_∞, being the completion of k with respect to $|\cdot|_\infty$, is of course complete, and has finite residue field κ_∞. By ([Ser79], Ch. II, Prop. 1), this implies that k_∞ is locally compact. By Proposition 1, this implies that there is a left Haar measure on k_∞ which is unique up to a multiplicative constant.

The set $\mathfrak{m}_\infty$ is closed in the topology induced by $|\cdot|_\infty$, so it is a Borel set, and therefore measureable under a Haar measure.

Let ν be the unique Haar measure on k_∞ such that $\nu(\mathfrak{m}_\infty) = 1$.

Let μ be the product measure ν^n on $V = k_\infty^n$. The group V is locally compact and μ is a Haar measure, so μ is the unique Haar measure on V such that

$$\mu(\mathfrak{m}_\infty^n) = \nu(\mathfrak{m}_\infty)^n = 1^n = 1.$$

Definition. An *A-lattice* in V is a sub-A-module $\mathcal{L}$ of V of the form

$$\mathcal{L} = \{a_1 v_1 + \cdots + a_n v_n \in V \mid a_i \in A\}$$

where $\{v_1, \dots, v_n\}$ is a k_∞-basis for V.

Any $a \in k_\infty$ can be uniquely expressed in the form $f + g$, where $f \in A$ and $g \in \mathfrak{m}_\infty$. Therefore, if $\mathcal{L} \subset V$ is the A-lattice in V spanned by $\{v_1, \dots, v_n\}$, any $v \in V$ can be uniquely expressed as

$$v = \sum_{j=1}^n f_j v_j + \sum_{j=1}^n g_j v_j$$

where $f_j \in A, g_j \in \mathfrak{m}_\infty$. In other words, we have that $V = \mathcal{L} \oplus D_\mathcal{L}$, where

$$D_\mathcal{L} = \bigoplus_{j=1}^n \mathfrak{m}_\infty v_j = \{a_1 v_1 + \cdots + a_n v_n \mid a_i \in \mathfrak{m}_\infty\} \subset V.$$

Thus $D_\mathcal{L}$ is a fundamental domain for $\mathcal{L}$. Define $\mathrm{vol}(\mathcal{L})$ by

$$\mathrm{vol}(\mathcal{L}) = \mu(D_\mathcal{L}).$$

Let $\mathcal{E} \subset V$ be the A-lattice spanned by the standard basis $\{e_1, \dots, e_n\}$ of V, and define a_{ij} by $v_i = \sum_{j=1}^n a_{ij} e_j$. Then $D_\mathcal{L} = M_\mathcal{L}(D_\mathcal{E})$, where $M_\mathcal{L} = (a_{ij}) \in \mathrm{GL}(V)$.

Lemma 1. *For any $b \in k_\infty^\times$, $\nu(b \cdot \mathfrak{m}_\infty) = |b|_\infty$.*

Proof. For any $n \in \mathbb{Z}$, we have that $\mathfrak{m}_\infty^n$ is the disjoint union of the q cosets of $\mathfrak{m}_\infty^{n+1}$,

$$\mathfrak{m}_\infty^n = \bigcup_{a \in \mathbb{F}_q} a \left(\tfrac{1}{T}\right)^n + \mathfrak{m}_\infty^{n+1},$$

which implies that

$$\nu(\mathfrak{m}_\infty^n) = \sum_{a \in \mathbb{F}_q} \nu \left(a \left(\tfrac{1}{T}\right)^n + \mathfrak{m}_\infty^{n+1}\right) = q\nu(\mathfrak{m}_\infty^{n+1})$$

because ν, being a Haar measure, is translation invariant. Because $\nu(\mathfrak{m}_\infty) = 1$ we have that

$$\nu(\mathfrak{m}_\infty^{n+1}) = q^{-n}\nu(\mathfrak{m}_\infty) = q^{-n}.$$

Any $b \in k_\infty^\times$ can be written as $u(\frac{1}{T})^n$ for some $n \in \mathbb{Z}$ and $u \in \mathcal{O}_\infty^\times$, and by definition $|b|_\infty = q^{-n}$. Because $b \cdot \mathfrak{m}_\infty = \mathfrak{m}^{n+1}$, we have that

$$\nu(b \cdot \mathfrak{m}_\infty) = \nu(\mathfrak{m}_\infty^{n+1}) = q^{-n} = |b|_\infty.$$

$\square$

Proposition 2. *Let $\mathcal{L} \subset V$ be the A-lattice spanned by $\{v_1, \ldots, v_n\}$, where $v_i = \sum_{j=1}^n a_{ij} e_j$. Then*

$$\mathrm{vol}(\mathcal{L}) = |\det(a_{ij})|_\infty.$$

Proof. We will prove that for any $M \in \mathrm{GL}(V)$ and measurable $S \subseteq V$,

$$\mu(M(S)) = |\det(M)|_\infty \mu(S).$$

The result will then follow because $D_{\mathcal{L}} = M_{\mathcal{L}}(D_{\mathcal{E}})$ and $\mu(D_{\mathcal{E}}) = 1$. It suffices to prove this is true for elementary matrices, because they generate $\mathrm{GL}(V)$ and the determinant is multiplicative.

Row-multiplying transformations.

Given any $b \in k_\infty^\times$ and $1 \leq h \leq n$, let $M = (a_{ij}) \in \mathrm{GL}(V)$ where $a_{hh} = b$, $a_{ii} = 1$ for $i \neq h$, and $a_{ij} = 0$ otherwise. Applying this matrix to a vector multiplies the hth coordinate by b and preserves the other coordinates. Note that $|\det(M)|_\infty = |b|_\infty$.

Define the Borel measure μ_M on V by $\mu_M(S) = \mu(M(S))$ (because M^{-1} is linear, and therefore continuous, we know that $M(S)$ is Borel whenever S is). It is easy to see that μ_M is a Haar measure on V because μ is. Therefore, by Proposition 1, $\mu_M = c\mu$ for some $c \in \mathbb{R}$. We can find c by looking at $D_{\mathcal{E}}$:

$$\begin{aligned}\mu_M(D_{\mathcal{E}}) &= \mu(M(D_{\mathcal{E}})) = \mu\left(\mathfrak{m}_\infty e_1 \oplus \cdots \oplus b \cdot \mathfrak{m}_\infty e_h \oplus \cdots \oplus \mathfrak{m}_\infty e_n\right) \\ &= \nu(\mathfrak{m}_\infty) \cdots \nu(b\mathfrak{m}_\infty) \cdots \nu(\mathfrak{m}_\infty) = 1 \cdots |b|_\infty \cdots 1 = |b|_\infty = |b|_\infty \mu(D_{\mathcal{E}}),\end{aligned}$$

so that $c = |b|_\infty = |\det(M)|_\infty$. Thus $\mu_M = |\det(M)|_\infty \mu$.

Row-switching transformations.

Given any distinct $1 \leq g, h \leq n$, let $M = (a_{ij}) \in \mathrm{GL}(V)$ where $a_{gh} = 1$, $a_{hg} = 1$, $a_{ii} = 1$ for $i \neq g, h$, and $a_{ij} = 0$ otherwise. Applying this matrix to a vector interchanges the gth and hth coordinates and preserves the other coordinates. Note that $|\det(M)|_\infty = |1|_\infty = 1$.

Define the measure μ_M on V by $\mu_M(S) = \mu(M(S))$. Because μ_M is a Haar measure on V, $\mu_M = c\mu$ for some $c \in \mathbb{R}$. We have that

$$\mu_M(D_{\mathcal{E}}) = \mu(M(D_{\mathcal{E}})) = \mu\left(\mathfrak{m}_\infty e_1 \oplus \cdots \oplus \mathfrak{m}_\infty e_h \oplus \cdots \oplus \mathfrak{m}_\infty e_g \oplus \cdots \oplus \mathfrak{m}_\infty e_n\right)$$

$$= \nu(\mathfrak{m}_\infty)\cdots\nu(\mathfrak{m}_\infty)\cdots\nu(\mathfrak{m}_\infty) = 1\cdots 1 = 1 = \mu(D_{\mathcal{E}}),$$

so that $c = 1 = |\det(M)|_\infty$. Thus $\mu_M = |\det(M)|_\infty \mu$.

Row-addition transformations.

Let $M = (a_{ij}) \in \mathrm{GL}(V)$ where $a_{ii} = 1$ for all i, $a_{12} = 1$, and $a_{ij} = 0$ otherwise. Applying this matrix to a vector adds the second coordinate to the first coordinate, and preserves the other coordinates. It suffices to consider M, because all other row-addition transformations can be generated by this one and combinations of row-switching and row-multiplying transformations.

Define the measure μ_M on V by $\mu_M(S) = \mu(M(S))$. Because μ_M is a Haar measure on V, $\mu_M = c\mu$ for some $c \in \mathbb{R}$. We have that

$$M(D_{\mathcal{E}}) = \mathfrak{m}_\infty e_1 \oplus \mathfrak{m}_\infty(e_1 + e_2) \oplus \cdots \oplus \mathfrak{m}_\infty e_n = \{(a_1 + a_2, a_2, \ldots, a_n) \mid a_i \in \mathfrak{m}_\infty\} \subseteq D_{\mathcal{E}}$$

because $\mathfrak{m}_\infty$ is an ideal. This implies that $D_{\mathcal{E}} \subseteq M^{-1}(D_{\mathcal{E}})$. Now note that $M^{-1} = (b_{ij})$ where $b_{ii} = 1$ for all i, $b_{12} = -1$, and $b_{ij} = 0$ otherwise, so that

$$M^{-1}(D_{\mathcal{E}}) = \mathfrak{m}_\infty e_1 \oplus \mathfrak{m}_\infty(e_1 - e_2) \oplus \cdots \oplus \mathfrak{m}_\infty e_n = \{(a_1 - a_2, a_2, \ldots, a_n) \mid a_i \in \mathfrak{m}_\infty\} \subseteq D_{\mathcal{E}}$$

again because $\mathfrak{m}_\infty$ is an ideal. Thus $M^{-1}(D_{\mathcal{E}}) = D_{\mathcal{E}} = M(D_{\mathcal{E}})$, and thus $\mu_M(D_{\mathcal{E}}) = \mu(D_{\mathcal{E}}) = 1$. Therefore we have that $c = 1$, and thus $\mu_M = |\det(M)|_\infty \mu$. $\square$

The following theorem is our analog of Minkowski's theorem.

Theorem 1. *Let $\mathcal{L} \subset V$ be an A-lattice, and let $C \subseteq V$ be a μ-measurable set which is closed under subtraction. If $\mu(C) > \mathrm{vol}(\mathcal{L})$, then C contains a non-zero element of $\mathcal{L}$.*

Proof. Because

$$V = \bigcup_{\lambda \in \mathcal{L}} (\lambda + D_{\mathcal{L}}),$$

we have that

$$C = \bigcup_{\lambda \in \mathcal{L}} \big((\lambda + D_{\mathcal{L}}) \cap C\big).$$

Note that the sets $\lambda + D_{\mathcal{L}}$ are disjoint, and that the lattice $\mathcal{L}$ is countable because A is countable. Therefore

$$\mu(C) = \sum_{\lambda \in \mathcal{L}} \mu\big((\lambda + D_{\mathcal{L}}) \cap C\big).$$

For any $\lambda \in \mathcal{L}$, we have that

$$\big(\lambda + D_{\mathcal{L}}\big) \cap C = \lambda + (-\lambda) + \big((\lambda + D_{\mathcal{L}}) \cap C\big) = \lambda + \big(D_{\mathcal{L}} \cap (-\lambda + C)\big).$$

Because μ is a left Haar measure on the abelian group V, it is left-translation invariant, so that

$$\mu\big((\lambda + D_{\mathcal{L}}) \cap C\big) = \mu\big(\lambda + (D_{\mathcal{L}} \cap (-\lambda + C))\big) = \mu\big(D_{\mathcal{L}} \cap (-\lambda + C)\big).$$

Thus,

$$\mu(C) = \sum_{\lambda \in \mathcal{L}} \mu\big(D_{\mathcal{L}} \cap (-\lambda + C)\big).$$

The sets $D_{\mathcal{L}} \cap (-\lambda + C)$ cannot all be disjoint, because otherwise

$$\mu(C) = \sum_{\lambda \in \mathcal{L}} \mu\big(D_{\mathcal{L}} \cap (-\lambda + C)\big) \leq \mu(D_{\mathcal{L}}) = \mathrm{vol}(\mathcal{L}),$$

contradicting our assumption that $\mu(C) > \mathrm{vol}(\mathcal{L})$. Thus, there exist $c_1, c_2 \in C$ and distinct $\lambda_1, \lambda_2 \in \mathcal{L}$ such that $c_1 - \lambda_1 = c_2 - \lambda_2$. Thus $\lambda_2 - \lambda_1 \in \mathcal{L}$ is non-zero, and $\lambda_2 - \lambda_1 = c_2 - c_1 \in C$ because C is closed under subtraction. $\square$

2.2 Extensions of the absolute value ∞ in a Galois extension K/k

Let K be a finite Galois extension of k. Let $n = [K : k]$ and $G = \mathrm{Gal}(K/k)$.

Fix an algebraic closure k_∞^{alg} of k_∞. There is a unique absolute value w on k_∞^{alg} that extends the absolute value ∞ on k_∞ ([Neu99], Ch. II, Theorem 4.8).

Choose a k-embedding $\rho : K \to k_\infty^{\mathrm{alg}}$. Pulling back the absolute value w via ρ, we obtain an absolute value on K which will also be denoted w. Thus, $|\alpha|_w = |\rho(\alpha)|_w$ for $\alpha \in K$.

Let $M = \rho(K)$. Clearly, M/k is also Galois, with $n = [M : k]$. Letting $\mathcal{G} = \mathrm{Gal}(M/k)$, there is an isomorphism $r : G \to \mathcal{G}$ given by $r(\sigma) = \rho \circ \sigma \circ \rho^{-1}$.

Let $L = k_\infty M$. Because M/k is Galois, L/k_∞ is also Galois, with an isomorphism

$$\mathrm{Gal}(L/k_\infty) \to \mathrm{Gal}(M/M \cap k_\infty)$$

given by restriction to M ([Lan02], Ch. VI, Theorem 1.12).

Let $E = \rho^{-1}(M \cap k_\infty)$, and let $f = [K : E] = [M : M \cap k_\infty]$. Let $t = \frac{n}{f} = [E : k]$.

Here is a diagram of our situation:

$$\begin{tikzcd}
 & & & k_\infty^{\mathrm{alg}} \arrow[d, dash] & \\
 & & & L \arrow[dl, dash] \arrow[dr, dash, "f"] & \\
K \arrow[rr, "\rho"] \arrow[dr, dash, "f"'] & & M \arrow[dr, dash, "f"] & & k_\infty \arrow[dl, dash] \\
 & E \arrow[rr] \arrow[drr, dash, "t"'] & & M \cap k_\infty \arrow[d, dash, "t"] & \\
 & & & k &
\end{tikzcd}$$

By ([Neu99], Ch. II, Theorem 8.1), we have

Proposition 3.

(i) *Every extension of the absolute value ∞ to K arises as the restriction of w by some k-embedding $\phi : K \to k_\infty^{\mathrm{alg}}$.*

(ii) *The two extensions of the absolute value ∞ to K induced by $\phi : K \to k_\infty^{\mathrm{alg}}$ and $\phi' : K \to k_\infty^{\mathrm{alg}}$ are equal if and only if $\phi' = \psi \circ \phi$ for some $\psi \in \mathrm{Gal}(k_\infty^{\mathrm{alg}}/k_\infty)$.*

Because $[K : k] = n$ and k_∞^{alg} is an algebraically closed field containing k, we know that there exist n distinct k-embeddings $K \to k_\infty^{\mathrm{alg}}$. These are precisely the maps $\rho \circ \sigma$ for $\sigma \in \mathrm{Gal}(K/k)$, as any such map is a k-embedding of K into k_∞^{alg}, and all n of them are distinct because ρ is injective and hence

$\rho \circ \sigma = \rho \circ \tau$ implies $\sigma = \tau$. This demonstrates the fact that every k-embedding of K in k_∞^{alg} has the same image, namely $M = \rho(K)$ (this is a general property of normal extensions).

Let $(\rho \circ \sigma) : K \to k_\infty^{\mathrm{alg}}$ be a k-embedding. We want to determine which k-embeddings $\rho \circ \tau$ occur as $\psi \circ \rho \circ \sigma$ for some $\psi \in \mathrm{Gal}(k_\infty^{\mathrm{alg}}/k_\infty)$. The only aspect of ψ that might affect where elements of K are sent is $\psi|_M \in \mathrm{Gal}(M/M \cap k_\infty)$, because $M = (\rho \circ \sigma)(K)$. Thus, there are at most $f = |\,\mathrm{Gal}(M/M \cap k_\infty)|$ embeddings that can be obtained this way. On the other hand, any element of $\mathrm{Gal}(M/M \cap k_\infty)$ extends (uniquely) to an element of $\mathrm{Gal}(L/k_\infty)$, via the inverse of the isomorphism between those two groups mentioned earlier, and any element of $\mathrm{Gal}(L/k_\infty)$ extends (non-uniquely) to an element of $\mathrm{Gal}(k_\infty^{\mathrm{alg}}/k_\infty)$. Each element of $\mathrm{Gal}(M/M \cap k_\infty)$ acts differently on M, and they can all be realized as $\psi|_M$ for some $\psi \in \mathrm{Gal}(k_\infty^{\mathrm{alg}}/k_\infty)$. Thus, there are precisely f k-embeddings which are conjugate to $\rho \circ \sigma$, those of the form $\widehat{\theta} \circ \rho \circ \sigma$ where $\theta \in \mathrm{Gal}(M/M \cap k_\infty)$ and $\widehat{\theta}$ is any extension of θ to $\mathrm{Gal}(k_\infty^{\mathrm{alg}}/k_\infty)$.

Pulling this back by ρ, we obtain an equivalent statement: there are f k-embeddings which are conjugate to $\rho \circ \sigma$, those of the form $\rho \circ (\eta \circ \sigma)$ where $\eta \in \mathrm{Gal}(K/E)$. This is because $r(\mathrm{Gal}(K/E)) = \mathrm{Gal}(M/M \cap k_\infty)$ and, for the $\eta \in G$ such that $\eta = \rho^{-1} \circ \theta \circ \rho = r^{-1}(\theta)$,

$$\widehat{\theta} \circ \rho \circ \sigma = (\widehat{\rho \circ \eta \circ \rho^{-1}}) \circ \rho \circ \sigma = \rho \circ \eta \circ \sigma.$$

(the extension $\widehat{\theta}$ chosen doesn't matter, as the image in k_∞^{alg} of every element of K is already determined).

Fix coset representatives $\sigma_1 = \mathrm{id}_K, \ldots, \sigma_t$ of $\mathrm{Gal}(K/E) \subseteq G$. Let $\rho_i = \rho \circ \sigma_i$. By Proposition 3 and our observations above, we conclude that there are t extensions of the absolute value ∞ to K, each of which is induced by pulling back the absolute value w on k_∞^{alg} via one of the ρ_i.

2.3 Existence of a normal basis for L/k_∞ having absolute value 1

We keep the notation of section 2.2. Thus, by assumption, K/k is unramified at ∞. By ([CF10], Ch. 1, §5, corollary to Proposition 2), this implies that L/k_∞ is unramified.

Applying ([Wei98], Ch. 3, Proposition 3-2-12.ii),

Proposition 4. *As extensions of $k_\infty = \mathbb{F}_q(\!(\frac{1}{T})\!)$, we have $L \cong \mathbb{F}_{q^f}(\!(\frac{1}{T})\!)$.*

The unique subfield of L which is isomorphic to $\mathbb{F}_{q^f}$ is simply the maximal subfield of L algebraic over $\mathbb{F}_q$. We now identify it with $\mathbb{F}_{q^f}$. Proposition 4 clearly implies that

$$\mathrm{Gal}(L/k_\infty) \cong \mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q) = \{\mathrm{id}_L, \varphi, \ldots \varphi^{f-1}\}.$$

Theorem 2. *There is a normal basis $\{\gamma_1, \ldots, \gamma_f\}$ for L/k_∞ such that $|\gamma_i|_w = 1$ for all i.*

Proof. Taking an $\alpha \in \mathbb{F}_{q^f} \subset L$ such that $\mathbb{F}_{q^f} = \mathbb{F}_q(\alpha)$, we have that $\{\alpha, \varphi(\alpha), \ldots, \varphi^{f-1}(\alpha)\}$ is a normal basis for $\mathbb{F}_{q^f}/\mathbb{F}_q$, and hence it is also a normal basis for L/k_∞. For notational clarity, we let $\gamma_i = \varphi^{i-1}(\alpha) = \alpha^{q^{i-1}}$. Thus, $\varphi \in \mathrm{Gal}(L/k_\infty)$ acts on L by

$$\varphi(c_1\gamma_1 + \cdots + c_n\gamma_n) = c_1\gamma_2 + \cdots + c_n\gamma_1$$

where the $c_i \in k_\infty$. Finally, the fact that $\alpha \in \mathcal{O}_L^\times$ implies that $|\gamma_i|_w = |\alpha|_w^{q^{i-1}} = 1$ for all i. □

Note that our conclusions from the end of section 2.2, combined with the observations above, imply that the n k-embeddings of K in k_∞^{alg} can be realized as $\varphi^j \circ \rho_i$, for $1 \leq i \leq t$ and $1 \leq j \leq f$.

Considering L as a k_∞-vector space, define $\lambda_j : L \to k_\infty$ to be projection on the basis element γ_j.

2.4 The Minkowski lattice of a Galois extension K/k

Consider the map $\Lambda : \mathcal{O}_K \to k_\infty^n$, defined as the composition of the following sequence of maps:

$$\mathcal{O}_K \hookrightarrow K \xrightarrow{(\rho_i)} \bigoplus_{i=1}^{t} L \xrightarrow{(\lambda_{ij})} k_\infty^n$$

where λ_{ij} denotes the map λ_j from the ith direct summand L.

Let $\{\beta_1, \ldots, \beta_n\}$ be an integral basis for $\mathcal{O}_K$ over A. Certainly, $\{\beta_1, \ldots, \beta_n\}$ is also a k-basis for K, so $\mathcal{O}_K$ forms an A-lattice in K. Let $\mathcal{L} = \Lambda(\mathcal{O}_K) \subset k_\infty^n$ be the A-lattice spanned by $\{\Lambda(\beta_1), \ldots, \Lambda(\beta_n)\}$, and consider the matrix

$$M = (\Lambda(\beta_1) \mid \cdots \mid \Lambda(\beta_n)) = \begin{pmatrix} \lambda_{11}(\rho_1(\beta_1)) & \lambda_{11}(\rho_1(\beta_2)) & \cdots & \lambda_{11}(\rho_1(\beta_n)) \\ \vdots & \vdots & & \vdots \\ \lambda_{1f}(\rho_1(\beta_1)) & \lambda_{1f}(\rho_1(\beta_2)) & \cdots & \lambda_{1f}(\rho_1(\beta_n)) \\ \lambda_{21}(\rho_2(\beta_1)) & \lambda_{21}(\rho_2(\beta_2)) & \cdots & \lambda_{21}(\rho_2(\beta_n)) \\ \vdots & \vdots & & \vdots \\ \lambda_{2f}(\rho_2(\beta_1)) & \lambda_{2f}(\rho_2(\beta_2)) & \cdots & \lambda_{2f}(\rho_2(\beta_n)) \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{t1}(\rho_t(\beta_1)) & \lambda_{t1}(\rho_t(\beta_2)) & \cdots & \lambda_{t1}(\rho_t(\beta_n)) \\ \vdots & \vdots & & \vdots \\ \lambda_{tf}(\rho_t(\beta_1)) & \lambda_{tf}(\rho_t(\beta_2)) & \cdots & \lambda_{tf}(\rho_t(\beta_n)) \end{pmatrix}$$

so that by Proposition 2, $\mathrm{vol}(\mathcal{L}) = |\det(M)|_\infty$. Note that $M \in \mathrm{GL}_n(k_\infty) \subset M_{n\times n}(k_\infty^{\mathrm{alg}})$.

Theorem 3. *With all notation as above,* $\mathrm{vol}(\mathcal{L}) = \sqrt{|\mathfrak{d}_{K/k}|_\infty}$.

Proof. Let $T \in M_{n\times n}(k_\infty^{\mathrm{alg}})$ be the matrix

$$T = \begin{pmatrix} \begin{matrix} \gamma_1 & \gamma_2 & \cdots & \gamma_f \\ \gamma_2 & \gamma_3 & \cdots & \gamma_1 \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_f & \gamma_1 & \cdots & \gamma_{f-1} \end{matrix} & & & \\ & \begin{matrix} \gamma_1 & \gamma_2 & \cdots & \gamma_f \\ \gamma_2 & \gamma_3 & \cdots & \gamma_1 \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_f & \gamma_1 & \cdots & \gamma_{f-1} \end{matrix} & & \\ & & \ddots & \\ & & & \begin{matrix} \gamma_1 & \gamma_2 & \cdots & \gamma_f \\ \gamma_2 & \gamma_3 & \cdots & \gamma_1 \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_f & \gamma_1 & \cdots & \gamma_{f-1} \end{matrix} \end{pmatrix}$$

Let $i = (a-1)f + b$ for $1 \le a \le t$ and $1 \le b \le f$. Then the inner product of the ith row of T with the jth column of M, which is just the ijth entry of TM, is

$$0+0+\cdots+0+\gamma_b\lambda_{a1}(\rho_a(\beta_j))+\gamma_{b+1}\lambda_{a2}(\rho_a(\beta_j))+\cdots+\gamma_{b-1}\lambda_{af}(\rho_a(\beta_j))+0+\cdots+0$$
$$=\varphi^{b-1}\big[\gamma_1\lambda_1(\rho_a(\beta_j))+\gamma_2\lambda_2(\rho_a(\beta_j))+\cdots+\gamma_f\lambda_f(\rho_a(\beta_j))\big]=\varphi^{b-1}(\rho_a(\beta_j)).$$

Thus, the matrix TM is just

$$\begin{pmatrix} \rho_1(\beta_1) & \rho_1(\beta_2) & \cdots & \rho_1(\beta_n) \\ (\varphi\circ\rho_1)(\beta_1) & (\varphi\circ\rho_1)(\beta_2) & \cdots & (\varphi\circ\rho_1)(\beta_n) \\ \vdots & \vdots & & \vdots \\ (\varphi^{f-1}\circ\rho_1)(\beta_1) & (\varphi^{f-1}\circ\rho_1)(\beta_2) & \cdots & (\varphi^{f-1}\circ\rho_1)(\beta_n) \\ \rho_2(\beta_1) & \rho_2(\beta_2) & \cdots & \rho_2(\beta_n) \\ \vdots & \vdots & & \vdots \\ (\varphi^{f-1}\circ\rho_t)(\beta_1) & (\varphi^{f-1}\circ\rho_t)(\beta_2) & \cdots & (\varphi^{f-1}\circ\rho_t)(\beta_n) \end{pmatrix}$$

which, up to a reordering of the rows (which doesn't change the absolute value of the determinant), is

$$\begin{pmatrix} \rho_1(\beta_1) & \rho_1(\beta_2) & \cdots & \rho_1(\beta_n) \\ \rho_2(\beta_1) & \rho_2(\beta_2) & \cdots & \rho_2(\beta_n) \\ \vdots & \vdots & & \vdots \\ \rho_n(\beta_1) & \rho_n(\beta_2) & \cdots & \rho_n(\beta_n) \end{pmatrix}.$$

Thus

$$\det(T)\det(M)=\det(TM)=\pm\det\begin{pmatrix} \rho_1(\beta_1) & \rho_1(\beta_2) & \cdots & \rho_1(\beta_n) \\ \rho_2(\beta_1) & \rho_2(\beta_2) & \cdots & \rho_2(\beta_n) \\ \vdots & \vdots & & \vdots \\ \rho_n(\beta_1) & \rho_n(\beta_2) & \cdots & \rho_n(\beta_n) \end{pmatrix}$$

so by the definition of the discriminant,

$$|\det(T)|_w\cdot|\det(M)|_w=|\det(T)|_w\cdot|\det(M)|_\infty=|\det(\rho_i(\beta_j))|_\infty=\sqrt{|\mathfrak{d}_{K/k}|_\infty}$$

where we have used the fact that w extends ∞. Now note that

$$\det(T)=\det\begin{pmatrix} \gamma_1 & \gamma_2 & \cdots & \gamma_f \\ \gamma_2 & \gamma_3 & \cdots & \gamma_1 \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_f & \gamma_1 & \cdots & \gamma_{f-1} \end{pmatrix}^n$$

will lie in $\mathbb{F}_{q^f}$ because all of the $\gamma_i\in\mathbb{F}_{q^f}$. We know that $\mathfrak{d}_{K/k}\neq 0$ for any function field K, so that

$$|\det(T)|_w\cdot|\det(M)|_\infty=\sqrt{|\mathfrak{d}_{K/k}|_\infty}\neq 0,$$

hence $|\det(T)|_w\neq 0$, and therefore $\det(T)\neq 0$. This implies that $\det(T)\in\mathcal{O}_L^\times$, and therefore $|\det(T)|_w=1$. Thus, we have shown that

$$\mathrm{vol}(\mathcal{L})=|\det(M)|_\infty=\sqrt{|\mathfrak{d}_{K/k}|_\infty}.$$

□

2.5 Hermite's theorem for function fields unramified at ∞

Main Result. *There are only finitely many separable extensions K/k of bounded degree and discriminant that are unramified at ∞. More precisely, for any $n, b \in \mathbb{N}$, there are (up to k-isomorphism) only finitely many separable extensions K/k that are unramified at ∞ with $[K : k] \leq n$ and $|\mathfrak{d}_K|_\infty \leq b$.*

Proof. Our approach is to reduce the problem to the case when K/k is Galois, and then use our earlier results for that case.

Reduction to the case of Galois K/k

The following is a well-known result about the different of an extension.

Proposition 5 (Prop. 2.4 and Theorem 2.5 in Chapter 2 of Neukirch, p.197-198)**.**

Let A be a Dedekind domain with field of fractions K, let L be a finite separable extension of K, and let B be the integral closure of A in L. Assume that all residue field extensions $\kappa(\mathfrak{P})/\kappa(P)$ of B/A are separable. For any $\alpha \in B$ such that $L = K(\alpha)$, $f'(\alpha) \in \mathfrak{D}_{B/A}$ where $f \in A[x]$ is the minimal polynomial for α over A. Furthermore, if $B = A[\alpha]$, then $\mathfrak{D}_{B/A} = (f'(\alpha))$.

We will use it to prove the following general theorem:

Theorem 4. *Let A be a Dedekind domain, and F its field of fractions. Let K_1 and K_2 be two finite separable extensions of F contained in some common algebraic closure of F, and let $L = K_1K_2$ be their compositum. Let B_1, B_2, C be the integral closures of A in K_1, K_2, L respectively. Assume that all residue field extensions of C/A are separable. Then*

$$(\mathfrak{D}_{B_1/A}C)(\mathfrak{D}_{B_2/A}C) \subseteq \mathfrak{D}_{C/A}.$$

Proof. We first reduce to the case that A is a discrete valuation ring. Using unique factorization of ideals, but grouping the primes of C according to the prime P of A they lie over, we see that

$$(\mathfrak{D}_{B_1/A}C)(\mathfrak{D}_{B_2/A}C) \subseteq \mathfrak{D}_{C/A}$$

if and only if, for every non-zero prime P of A,

$$S^{-1}(\mathfrak{D}_{B_1/A}C)S^{-1}(\mathfrak{D}_{B_2/A}C) \subseteq S^{-1}\mathfrak{D}_{C/A}$$

where $S = A \setminus P$. Applying Prop. 2.2ii of Chapter 2 of Neukirch (p. 195), as well as simple facts about localization and extension of ideals, we can re-express this as

$$(\mathfrak{D}_{S^{-1}B_1/S^{-1}A}S^{-1}C)(\mathfrak{D}_{S^{-1}B_2/S^{-1}A}S^{-1}C) \subseteq \mathfrak{D}_{S^{-1}C/S^{-1}A}.$$

For any prime $P \subseteq A$, the ring $S^{-1}A = A_P$ is a discrete valuation domain with field of fractions F, and $S^{-1}B_1, S^{-1}B_2, S^{-1}C$ are the integral closures of $S^{-1}A$ in K_1, K_2, L respectively (Corollary to Proposition 8 in Chapter 1 of Lang's ANT, p.8). The residue field extensions of $S^{-1}C/S^{-1}A$ are separable because they are just those residue field extensions of C/A occurring over P. Thus, to prove the theorem is true, it suffices to prove it in the case that A is a discrete valuation ring.

We will now reduce further to the case that A is a complete discrete valuation ring. Suppose that A is a discrete valuation ring, with P its prime ideal. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$ be the non-zero primes of C, each of which necessarily lies over P. Given a non-zero ideal $I \subseteq C$, let $v_j(I)$ be the exponent of $\mathfrak{P}_j$ occurring in the factorization of I, and let

$$e_{j1} = v_j(\mathfrak{D}_{B_1/A}C), \quad e_{j2} = v_j(\mathfrak{D}_{B_2/A}C), \quad h_j = v_j(\mathfrak{D}_{C/A}).$$

By unique factorization of ideals,

$$(\mathfrak{D}_{B_1/A}C)(\mathfrak{D}_{B_2/A}C) \subseteq \mathfrak{D}_{C/A}$$

if and only if, for every non-zero prime $\mathfrak{P}_j$ of C,

$$(\mathfrak{D}_{B_1/A}C_{\mathfrak{P}_j})(\mathfrak{D}_{B_2/A}C_{\mathfrak{P}_j}) = (\mathfrak{P}_jC_{\mathfrak{P}_j})^{e_{j1}}(\mathfrak{P}_jC_{\mathfrak{P}_j})^{e_{j2}} \subseteq (\mathfrak{P}_jC_{\mathfrak{P}_j})^{h_j} = \mathfrak{D}_{C/A}C_{\mathfrak{P}_j}$$

where $C_{\mathfrak{P}}$ is the localization of C at $\mathfrak{P}$ and $\mathfrak{P}C_{\mathfrak{P}}$ is its maximal ideal. If $\widehat{C_{\mathfrak{P}}}$ is the completion of the DVR $C_{\mathfrak{P}}$, then $\mathfrak{P}\widehat{C_{\mathfrak{P}}}$ is the maximal ideal of $\widehat{C_{\mathfrak{P}}}$, so in particular the exponents are not altered by extending ideals of $C_{\mathfrak{P}}$ to ideals of $\widehat{C_{\mathfrak{P}}}$. Thus,

$$(\mathfrak{P}_jC_{\mathfrak{P}_j})^{e_{j1}}(\mathfrak{P}_jC_{\mathfrak{P}_j})^{e_{j2}} \subseteq (\mathfrak{P}_jC_{\mathfrak{P}_j})^{h_j}$$

if and only if

$$(\mathfrak{P}_j\widehat{C_{\mathfrak{P}_j}})^{e_{j1}}(\mathfrak{P}_j\widehat{C_{\mathfrak{P}_j}})^{e_{j2}} \subseteq (\mathfrak{P}_j\widehat{C_{\mathfrak{P}_j}})^{h_j}.$$

Therefore,

$$(\mathfrak{D}_{B_1/A}C)(\mathfrak{D}_{B_2/A}C) \subseteq \mathfrak{D}_{C/A}$$

if and only if, for every non-zero prime $\mathfrak{P}_j$ of C,

$$(\mathfrak{D}_{B_1/A}\widehat{C_{\mathfrak{P}_j}})(\mathfrak{D}_{B_2/A}\widehat{C_{\mathfrak{P}_j}}) = (\mathfrak{P}_j\widehat{C_{\mathfrak{P}_j}})^{e_{j1}}(\mathfrak{P}_j\widehat{C_{\mathfrak{P}_j}})^{e_{j2}} \subseteq (\mathfrak{P}_j\widehat{C_{\mathfrak{P}_j}})^{h_j} = \mathfrak{D}_{C/A}\widehat{C_{\mathfrak{P}_j}}.$$

If $\mathfrak{p}_{j1} = B_1 \cap \mathfrak{P}_j$ and $\mathfrak{p}_{j2} = B_2 \cap \mathfrak{P}_j$, then there are natural inclusions of the localized rings

$$(B_1)_{\mathfrak{p}_{j1}} \hookrightarrow C_{\mathfrak{P}_j}, \;\; (B_2)_{\mathfrak{p}_{j2}} \hookrightarrow C_{\mathfrak{P}_j},$$

and hence the same is true for the completions,

$$\widehat{(B_1)_{\mathfrak{p}_{j1}}} \hookrightarrow \widehat{C_{\mathfrak{P}_j}}, \;\; \widehat{(B_2)_{\mathfrak{p}_{j2}}} \hookrightarrow \widehat{C_{\mathfrak{P}_j}}.$$

Clearly, we can extend an ideal of B_1 to an ideal of $\widehat{(B_1)_{\mathfrak{p}_{j1}}}$, then to an ideal of $\widehat{C_{\mathfrak{P}_j}}$, or just extend it directly to an ideal of $\widehat{C_{\mathfrak{P}_j}}$, and get the same result. Now applying Prop. 2.2iii of Chapter 2 of Neukirch (p. 195),

$$(\mathfrak{D}_{B_1/A}\widehat{C_{\mathfrak{P}_j}})(\mathfrak{D}_{B_2/A}\widehat{C_{\mathfrak{P}_j}}) \subseteq \mathfrak{D}_{C/A}\widehat{C_{\mathfrak{P}_j}}$$

if and only if

$$(\mathfrak{D}_{\widehat{(B_1)_{\mathfrak{p}_{j1}}}/\widehat{A_P}}\widehat{C_{\mathfrak{P}_j}})(\mathfrak{D}_{\widehat{(B_2)_{\mathfrak{p}_{j2}}}/\widehat{A_P}}\widehat{C_{\mathfrak{P}_j}}) \subseteq \mathfrak{D}_{\widehat{C_{\mathfrak{P}_j}}/\widehat{A_P}}.$$

Note that $\widehat{A_P}$ is a complete discrete valuation ring, with field of fractions $\widehat{F_P}$, that $\widehat{L_{\mathfrak{P}_j}}$ is a finite separable extension of $\widehat{F_P}$, and that $\widehat{(B_1)_{\mathfrak{p}_{j1}}}$, $\widehat{(B_2)_{\mathfrak{p}_{j2}}}$, and $\widehat{C_{\mathfrak{P}_j}}$ are the integral closures of $\widehat{A_P}$ in $\widehat{(K_1)_{\mathfrak{p}_{j1}}}$, $\widehat{(K_2)_{\mathfrak{p}_{j2}}}$, and $\widehat{L_{\mathfrak{P}_j}}$ respectively. The sole residue field extension of $\widehat{C_{\mathfrak{P}_j}}/\widehat{A_P}$ is

$$\kappa(\mathfrak{P}_j\widehat{C_{\mathfrak{P}_j}})/\kappa(P\widehat{A_P}) \cong \kappa(\mathfrak{P}_j)/\kappa(P),$$

which is separable because we assumed that all residue field extensions of C/A were separable. Thus, to prove the theorem is true, it suffices to prove it in the case that A is a complete discrete valuation ring.

So, now let A be a complete discrete valuation ring with field of fractions F (which implies that F is complete), and let K_1, K_2, L and B_1, B_2, C be as in the statement of the theorem. There is a unique extension to K_2 of the valuation on F, and K_2 is complete under this valuation (Theorem 4.8

of Chapter 2, Neukirch, p.131); B_2 is the corresponding valuation ring. By Prop. 3 in Chapter 3 of Lang's ANT, there is some $\theta \in B_2$ such that $B_2 = A[\theta]$ (we need the hypothesis that the residue field extension of B_2/A is separable to apply this result). Let $f \in A[x]$ be the minimal polynomial for θ over F. Then by the first cited proposition, $\mathfrak{D}_{B_2/A} = f'(\theta)B_2$. Because $K_2 = F(\theta)$, we also have that $L = K_1K_2 = K_1(\theta)$. Let $g \in K_1[x]$ be the minimal polynomial for θ over K_1. Then because $f(\theta) = 0$, we have that $f = gh$ for some $h \in K_1[x]$. Differentiating,

$$f'(\theta) = g'(\theta)h(\theta) + g(\theta)h'(\theta) = g'(\theta)h(\theta).$$

Thus

$$\mathfrak{D}_{B_2/A}C = f'(\theta)C \subseteq g'(\theta)C \subseteq \mathfrak{D}_{C/B_1}$$

and hence $\mathfrak{D}_{C/A} = \mathfrak{D}_{C/B_1}(\mathfrak{D}_{B_1/A}C) \supseteq (\mathfrak{D}_{B_2/A}C)(\mathfrak{D}_{B_1/A}C)$. □

We now need another well-known result, connecting the different and the discriminant:

Proposition 6 (Theorem 2.9 in Chapter 2 of Neukirch, p.201)**.**

Let A be a Dedekind domain with field of fractions K, let L be a finite separable extension of K, and let B be the integral closure of A in L. Assume that all residue field extensions of B/A are separable. The different $\mathfrak{D}_{B/A}$ and discriminant $\mathfrak{d}_{B/A}$ are related as follows:

$$\mathfrak{d}_{B/A} = N_K^L(\mathfrak{D}_{B/A}).$$

We can apply Theorem 4 to bound the discriminant of a finite separable extension K/F in terms of the discriminant of its Galois closure and certain degrees of field extensions:

Theorem 5. *Let A be a Dedekind domain with field of fractions F, let K be a finite separable extension of F, and let B be the integral closure of A in K. Assume that all residue fields of A are perfect. Let L be the Galois closure of K in some algebraic closure $\overline{F}$ of F, and let C be the integral closure of A in L. Then*

$$(\mathfrak{d}_{B/A})^{n\cdot[L:F]} \subseteq \mathfrak{d}_{C/A}$$

Proof. Let $M_1, \ldots, M_n$ be the (not necessarily distinct) embeddings of K in $\overline{F}$, so that $L = M_1 \cdots M_n$. Let R_i be the integral closure of A in M_i. Using Theorem 1 repeatedly, we have that

$$(\mathfrak{D}_{R_1/A}C) \cdots (\mathfrak{D}_{R_n/A}C) \subseteq \mathfrak{D}_{C/A}.$$

Applying the norm $N_F^L = N_F^{M_i} \circ N_{M_i}^L$, which is multiplicative, and using Corollary 1 to Proposition 21 in Chapter 1 of Lang's ANT (p.25) we have that

$$N_F^{M_1}((\mathfrak{D}_{R_1/A})^{[L:M_1]}) \cdots N_F^{M_n}((\mathfrak{D}_{R_n/A})^{[L:M_n]}) = (\mathfrak{d}_{R_1/A} \cdots \mathfrak{d}_{R_n/A})^{[L:F]} = (\mathfrak{d}_{B/A})^{n\cdot[L:F]} \subseteq \mathfrak{d}_{C/A}.$$

□

Now we can apply the above general results to our situation to obtain:

Corollary 1. *Let K be a finite separable extension of k of degree n, and let L be the Galois closure of K over k in k_∞^{alg}. Let $\mathcal{O}_K$ and $\mathcal{O}_L$ be the integral closures of A in K and L, respectively. Then*

$$|\mathfrak{d}_{L/k}|_\infty \leq (|\mathfrak{d}_{K/k}|_\infty)^{n\cdot(n!)}$$

where $\mathfrak{d}_{L/k} = \mathfrak{d}_{\mathcal{O}_L/A}$ and $\mathfrak{d}_{K/k} = \mathfrak{d}_{\mathcal{O}_K/A}$.

Proof. Because $[K : k] = n$ and L is the Galois closure of K, we have that $[L : k] \leq n!$. By the theorem, $(\mathfrak{d}_{K/k})^{n\cdot(n!)} \subseteq \mathfrak{d}_{L/k}$, and hence

$$|\mathfrak{d}_{L/k}|_\infty \leq (|\mathfrak{d}_{K/k}|_\infty)^{n\cdot(n!)}.$$

$\square$

Thus, given any finite separable extension K/k unramified at ∞ such that $[K : k] \leq n$ and $|\mathfrak{d}_{K/k}|_\infty \leq b$, the Galois closure L/k of K/k must have $[L : k] \leq n!$ and $|\mathfrak{d}_{L/k}|_\infty \leq b^{n\cdot(n!)}$. If we prove our main result for Galois extensions, then there are, up to k-isomorphism, only finitely many such fields L. Each of them has only finitely many intermediate fields, and K is of course isomorphic to one of the intermediate fields of one of the L's; thus, there are only finitely many k-isomorphism classes of separable extensions K/k unramified at ∞ such that $[K : k] \leq n$ and $|\mathfrak{d}_{K/k}|_\infty \leq b$. Thus, to prove our main result, it suffices to prove it in the case that K/k is Galois.

The case of Galois K/k

Now let K/k be a finite Galois extension in which ∞ is unramified, and let $n = [K : k]$. Let $G = \mathrm{Gal}(K/k)$. We consider again the map $\Lambda : \mathcal{O}_K \to k_\infty^n$ from section 2.4, defined as the composition of the following sequence of maps:

$$\mathcal{O}_K \hookrightarrow K \xrightarrow{(\rho_i)} \bigoplus_{i=1}^{t} L \xrightarrow{(\lambda_{ij})} k_\infty^n.$$

We showed that, for the A-lattice $\mathcal{L} = \Lambda(\mathcal{O}_K)$ in k_∞^n, we have $\mathrm{vol}(\mathcal{L}) = \sqrt{|\mathfrak{d}_{K/k}|_\infty}$.

Define $C \subset k_\infty^n$ to be

$$C = \left\{ (x_1, \ldots, x_n) \in k_\infty^n \;\middle|\; \begin{array}{c} |x_1|_\infty \leq q^n\sqrt{b}, \\ |x_i|_\infty \leq q^{-1} \text{ for } i = 2, \ldots, n \end{array} \right\}.$$

For any field K satisfying the assumptions of our theorem, we have that $\mu(C) = q\sqrt{b} > \sqrt{|\mathfrak{d}_{K/k}|_\infty}$, and C is closed under subtraction because the inequalities defining C simply make C into a direct sum of fractional ideals of $\mathcal{O}_\infty$.

By Theorem 1, our analog of Minkowski's Theorem, this means that there is a non-zero $\beta \in \mathcal{O}_K$ such that $\Lambda(\beta) \in C$, i.e.

$$|\lambda_{11}(\rho_1(\beta))|_\infty \leq q^n\sqrt{b}, \quad |\lambda_{ij}(\rho_i(\beta))|_\infty \leq q^{-1} \text{ otherwise.}$$

Because $\beta \in \mathcal{O}_K$, we have that $|\beta|_v \leq 1$ for all finite absolute values v. Therefore, by the product formula, we must have $\prod_{i=1}^{t} |\beta|_{w_i} \geq 1$ where the w_i are the infinite places obtained by pulling back w along the ρ_i. But $|\lambda_{ij}(\rho_i(\beta))|_\infty \leq q^{-1}$ for all $(i,j) \neq (1,1)$, so that for any $i \neq 1$ we have

$$|\beta|_{w_i} = |\rho_i(\beta)|_w = |\gamma_1\lambda_{i1}(\rho_i(\beta)) + \cdots + \gamma_f\lambda_{if}(\rho_i(\beta))|_w$$

$$\leq \max_{1\leq j\leq f} |\gamma_j|_w |\lambda_{ij}(\rho_i(\beta))|_w \leq \max_{1\leq j\leq f} 1 \cdot |\lambda_{ij}(\rho_i(\beta))|_w \leq q^{-1}.$$

Thus, the only way the product formula can be satisfied is if $|\beta|_{w_1} \geq 1$, and because

$$|\beta|_{w_1} \leq \{|\lambda_{11}(\rho_1(\beta))|_w, q^{-1}, \ldots, q^{-1}\}$$

we must have that $|\lambda_{11}(\rho_1(\beta))|_\infty \geq 1$.

We claim that $K = k(\beta)$. If this were not the case, then there would exist a $\sigma \neq \mathrm{id}_K \in G$ such that $\sigma(\beta) = \beta$. Because $\sigma \neq \mathrm{id}_L K$, we would have $\lambda_{11} \circ \rho_1 \circ \sigma \neq \lambda_{11} \circ \rho_1$, hence

$$|\lambda_{11}(\rho_1(\beta))|_\infty = |\lambda_{11}(\rho_1(\sigma(\beta)))|_\infty \leq q^{-1} < 1$$

which is a contradiction.

Now let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$ be the minimal polynomial for β over k. Its coefficients (up to sign) are the elementary symmetric polynomials in its n roots, that is, in the n different elements $(\varphi^j \circ \rho_i)(\beta)$. The fact that β is in the region C tells us that $|(\varphi^j \circ \rho_i)(\beta)|_w$ is bounded above, for all i and j, by a quantity that depends solely in terms of n and b (the bounds on the degree and discriminant, respectively); specifically,

$$|(\varphi^j \circ \rho_i)(\beta)|_w = |\gamma_j \lambda_{i1}(\rho_i(\beta)) + \gamma_{j+1}\lambda_{i2}(\rho_i(\beta)) + \cdots + \gamma_{j-1}\lambda_{if}(\rho_i(\beta))|_w$$

$$\leq \max_{1 \leq s \leq f} |\lambda_{is}(\rho_i(\beta))|_w \leq \begin{cases} q^{-1} & \text{if } i \neq 1, \\ q^n\sqrt{b} & \text{if } i = 1 \end{cases} \leq q^n\sqrt{b}.$$

Thus, the possible values of the quantities $|a_i|_\infty$ can also be bounded solely in terms of n and b. Because there are only finitely many elements of A of bounded degree, there are only finitely many possibilities for the minimal polynomial of β, and hence only finitely many possible k-isomorphism types of the field K. □

2.6 Counterexample when ∞ is not required to be unramified

By ([Sti09], Ch. 6, Proposition 6.4.1), for any $m \in \mathbb{N}$ the function field $K = k(x)$, where

$$x^q - x = T^{mq+1},$$

has $[K : k] = q$, and K is separable over $k = \mathbb{F}_q(T)$, and K is ramified only at ∞, so $|\mathfrak{d}_K|_\infty = 1$ is bounded; but there are infinitely many such fields.

3 Future Research

We have two ideas as to expand this approach to arbitrary finite separable function fields.

- Recall that one can extend the constant field of a function field K without changing the discriminant ([Ros02]), and that extending the constant field also reduces the degree of certain places in K ([Ros02]). We know that almost all places of K are unramified, so by extending the constant field of K sufficiently, we will eventually create a new extension $K\mathbb{F}_{q^n}/\mathbb{F}_{q^n}(T)$ with the same discriminant as $K/\mathbb{F}_q(T)$, and with an unramified place of degree 1. We can then make a change of variables to move that place to ∞, at which point we can finish with our results above.
- Perhaps we can allow bounded ramification at ∞, and solve the general problem by reducing the case when ∞ is ramified to a (hopefully) simpler special case, e.g. ∞ being totally ramified.

4 References

[CF10] J.W.S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, 2nd ed., London Mathematical Society, London, 2010.

[Fol95] Gerald B. Folland, *A Course in Abstract Harmonic Analysis*, CRC Press LLC, 1995.

[Fol99] ———, *Real Analysis: Modern Techniques and Their Applications*, 2nd ed., John Wiley & Sons, Inc., 1999.

[Gos98] David Goss, *Basic Structures of Function Field Arithmetic*, Springer-Verlag, Berlin, 1998.

[Lan86] Serge Lang, *Algebraic Number Theory*, Springer-Verlag, New York, 1986.

[Lan02] ———, *Algebra*, revised 3rd ed., Springer-Verlag, New York, 2002.

[Mun00] James Munkres, *Topology*, 2nd ed., Prentice Hall, Upper Saddle River, NJ, 2000.

[Neu99] Jürgen Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.

[Ros02] Michael Rosen, *Number Theory in Function Fields*, Springer-Verlag, New York, 2002.

[Ser79] Jean-Pierre Serre, *Local Fields*, Springer-Verlag, New York, 1979.

[Sti09] Henning Stichtenoth, *Algebraic Function Fields and Codes*, 2nd ed., Springer-Verlag, Berlin Heidelberg, 2009.

[Wei98] Edwin Weiss, *Algebraic Number Theory*, Dover Publications, Mineola, New York, 1998.