# The Riemann-Roch Theorem for Number Fields

Sam Mundy

Defended on 4/28/2015

## Introduction

It has long been understood that there are deep connections between algebraic number theory and algebraic geometry. This has been known since these fields were in their infancy.

In this paper, we expose some of these deep connections, particularly the ones appearing in the theory surrounding the Riemann-Roch theorem. This theorem (which we describe in Section 1) is an extremely fundamental result in algebraic geometry which describes certain spaces of functions on a given curve. In order to expose the connections between number theory and geometry, we describe generally the basics of algebraic number theory with an emphasis on its geometric aspects, and we specialize a little as well in order to describe an arithmetic analogue of the Riemann-Roch theorem. This theorem is what we will call the Riemann-Roch theorem for number fields, as in the title. In the second half of the paper, we also see analysis enter the picture in an interesting way. This will lead to a new proof of the Riemann-Roch theorem for number fields.

### Organization

First we should note that the entire paper at hand provides very few proofs because this theory, if developed in detail, could occupy many books. However, every result which is needed is stated fully, and all of the main definitions are given.

This being said, we begin with an overview of the theory of nonsingular projective curves. The reason for this is to have an organized description of the theory which we are trying to mimic. Next we enter the theory of algebraic numbers and describe the proof of the Riemann-Roch theorem for number fields. Then, since it will be beneficial to the later developments in this paper, we introduce the theory of function fields. In the generality of both number fields and function fields, we may then develop the local theory and the adelic (global) theory of these objects. The resulting situation is that we will have a plethora of locally compact abelian groups on our hands, and such groups have a rich analytic theory. Hence we review the Fourier analysis associated to locally compact abelian groups and apply it, as Tate did, to our number theory. This will lead to a different theorem which also deserves the name of Riemann-Roch, and we then apply this theorem to obtain a new proof the Riemann-Roch theorem for number fields, as mentioned above.

### Prerequisites and Conventions

Since this is an undergraduate thesis, we assume nothing beyond the following basic mathematics: Abstract algebra up through basic Galois theory; Real analysis through basic abstract measure theory; Basic topology, not including differential geometry or algebraic topology. However, the reader who is only familiar with these subjects will likely find this material to be extremely dense. Also, when it improves the exposition, we have not hesitated to include various comments which describe a more advanced theory for the sake of the reader who has the necessary background. We always preface these comments with the word "Remark". Conversely, remarks are reserved for this purpose.

### Acknowledgements

I would like to thank Alexandru Buium for his continuous support throughout my time as an undergraduate at UNM, and Anna Skripka for proofreading this thesis. I was supported by the NSF-MCTP DMS-0739417 grant, coordinated by Monika Nitsche.

### References

References for all material in this paper are given by section as follows.

1. Hartshorne [3], Shafarevich [13], Mumford [7].
2. Lang [4], Marcus [5], Neukirch [9].
3. Neukirch [9].
4. Rosen [11], Silverman [14].
5. Weil [15], Lang [4], Neukirch [9].
6. Weil [15], Lang [4].
7. Folland [2], Ramakrishnan and Valenza [10].

8, 9, 10. Tate's thesis in Cassels and Frohlich [1], Ramakrishnan and Valenza [10], Lang [4].

11. My paper on the arXiv [8].

# 1 The Geometry of Projective Curves

Classical abstract algebraic geometry is concerned with geometric objects which are locally given by solution sets of polynomial equations over a field which is algebraically closed (i.e., every nonconstant polynomial with coefficients in the field has a root in that field.) The reason one wants algebraic closure is given by the following theorem, which is false without that hypothesis.

**Theorem 1.1** (Hilbert's Nullstellensatz)**.** *Let $k$ be an algebraically closed field. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal in the ring of polynomials in $n$ variables over $k$. Consider the set $V(I)$ which, by definition, consists of all $n$-tuples in $k^n$ at which all polynomials in $I$ vanish simultaneously. Finally, let $J$ be the ideal of all polynomials which vanish on all points in $V(I)$. Then $J = \sqrt{I}$, where $\sqrt{I}$ denotes the radical of the ideal $I$.*

For the rest of this section, we fix an algebraically closed field $k$.

Let $\mathbb{A}^n$ denote the set $k^n$, which is the cartesian product of $k$ with itself $n$ times. This is called *affine $n$-space.* The definition of an *(affine) algebraic set* is any set of the form $V(I)$ as in the theorem, where $I$ is an ideal in a polynomial ring $k[x_1, \ldots, x_n]$ for some $n$. We can view an affine algebraic set as subset of $\mathbb{A}^n$. In fact, it turns out that the algebraic sets contained in $\mathbb{A}^n$ form the closed sets for a topology on $\mathbb{A}^n$, called the *Zariski topology,* which the algebraic sets themselves then inherit. Beware that this is a very strange topology, which, for instance, is almost never Hausdorff.

We can then define the notion of dimension as follows. First, we call a topological space irreducible if it cannot be decomposed into two disctinct closed subsets. The dimension of a topological space $X$ is then defined to be the length $d$ of the longest chain of irreducible closed subsets

$$\emptyset \subset X_1 \subset X_2 \subset \cdots \subset X_d,$$

each inclusion being proper. Notice that this is very similar to the definition of Krull dimension of a ring $R$, which is, by definition, the length of the longest chain of prime ideals in $R$. In fact, we have

**Proposition 1.2.** *Let $X$ be an algebriac set in $\mathbb{A}^n$, defined by an ideal $I$. Then the dimension of $X$ as a topological space is equal to the Krull dimension of the ring $k[x_1, \ldots, x_n]/I$.*

This is clarified by the following proposition, which is a consequence of the Nullstellensatz.

**Proposition 1.3.** *There are one-to-one correspondences, each given by $I \mapsto V(I)$, between the following:*

*(1) Radical ideals in $k[x_1, \ldots, x_n]$, and closed subsets of $\mathbb{A}^n$;*

*(2) Prime ideals in $k[x_1, \ldots, x_n]$, and irreducible closed subsets of $\mathbb{A}^n$;*

*(3) Maximal ideals in $k[x_1, \ldots, x_n]$, and points in $\mathbb{A}^n$.*

An algebraic set defined by a prime ideal is called an *affine variety.* Thus an affine variety is an irreducible algebraic set. A *quasi-affine variety* is an open subset of an affine variety. These varieties have more structure than just topology. We will now define certain functions on these sets.

Let $X \subset \mathbb{A}^n$ be a quasi-affine variety. A map $f : X \to k$ is called regular if it is locally the quotient of two polynomials. In more detail, this means that there exists an open cover (for the Zariski topology) $\{U\}$ of $X$ and polynomials $g_U, h_U \in k[x_1, \ldots, x_n]$ for each $U$, with $h_U$ not vanishing on $U$, such that $f = g_U/h_U$ on $U$. The set of regular functions on $X$ forms a ring denoted $\mathcal{O}(X)$.

Let $P \in X$ be a point. Then the *local ring at $P$,* denoted $\mathcal{O}_P$, is the ring of germs about $P$. In more detail, it is the ring of equivalence classes $\langle f, U\rangle$, where $f$ is regular on the open set $U$ which contains $P$, and the equivalence is given by $\langle f, U\rangle \sim \langle g, V\rangle$ if $f|_W = g|_W$ for some open subset $W \subset U \cap V$.

Now assume $X$ is irreducible. As a consequence of the definition of irreducibility, any two nonempty open subsets of $X$ have nonempty intersection. A *rational function* on $X$ then has almost the same definition as an element in the local ring: A rational function is an equivalence class $\langle f, U\rangle$, where $f$ is regular on the open set $U$ (not necessarily containing any specific point), and the equivalence is given by $\langle f, U\rangle \sim \langle g, V\rangle$ if $f|_W = g|_W$ for some open subset $W \subset U \cap V$. The rational functions form a field denoted $K(X)$, called the *function field* of $X$.

**Remark.** What is really going on here is that we have naturally a sheaf on $X$ which associates to each open subset of $X$ the regular functions on that subset. The local rings are the stalks. The function field does not have a purely sheaf-theoretic description, at least when $X$ is only viewed as a variety. However, scheme-theoretically, the points of $X$ form the closed points of an integral scheme, and the function field is the residue field at the generic point.

All of these functions have nice descriptions.

**Proposition 1.4.** *Let $X = V(I) \subset \mathbb{A}^n$ be an affine variety. Then:*

*(a) $\mathcal{O}(X) \cong k[x_1 \ldots, x_n]/I$;*

*(b) With this identification, let $P \in X$, let $\mathfrak{M}_P \subset k[x_1, \ldots, x_n]$ be the maximal ideal corresponding to $P$ as in Proposition 1.3, and let $\mathfrak{m}_P = \mathfrak{M}_P\mathcal{O}(X)$. Then $\mathcal{O}_P \cong \mathcal{O}(X)_{\mathfrak{m}_P}$, and so $\mathcal{O}_P$ is indeed local.*

*(c) $K(X) \cong \mathrm{Frac}(\mathcal{O}(X))$.*

Note that in (c) above, taking fraction fields makes sense because $\mathcal{O}(X)$ is an integral domain, i.e., $ab = 0$ implies $a = 0$ or $b = 0$ in $\mathcal{O}(X)$. Recall that the fraction field of an integral domain $A$ is just the field obatined by formally adjoining the multiplicative inverses of every nonzero element in $A$. Also, in (b) above, $\mathcal{O}(X)_{\mathfrak{m}_P}$ denotes the localization of $\mathcal{O}_X$ at the maximal ideal $\mathfrak{m}_P$, which we recall is just the ring obtained by formally adjoining the multiplicative inverses of all elements of $\mathcal{O}(X)$ not in $\mathfrak{m}_P$. Finally, in reference again to (b), we recall that a ring called is local whenever it has only one maximal ideal, and any localization of a ring at a prime ideal is local.

Now for most purposes, it turns out that affine varieties are not the right objects to consider. Technically, they fail to be proper (in a sense not to be explained here). So we define a new type of variety. First we need the following construction. Let $k^\times$ act on $k^{n+1}\backslash\{0\}$ by multiplication on each entry of a given tuple. We define the *projective space* $\mathbb{P}^n$ to be equal to $(k^{n+1}\backslash\{0\})/k^\times$. Thus it is the set of all $(n+1)$-tuples $(y_0, \ldots, y_n)$, with at least one component not zero, modulo scaling. One may also view it as the set of lines

in $\mathbb{A}^{n+1}$ passing through the origin.

For $0 \leq i \leq n$, let $H_i$ be the set of all points in $\mathbb{P}^n$ whose $i$th coordinate is 0. We view these as hyperplanes. Then $\mathbb{P}^n \backslash H_i$ is in bijection with $\mathbb{A}^n$. Thus $\mathbb{P}^n$ is the union (not disjoint) of $n+1$ copies of $\mathbb{A}^n$. The hyperplane $H_0$ is sometimes called the *hyperplane at infinity,* for the same reason a sphere is viewed as a plane with a point at infinity. We can also remove other hyperplanes, defined by equations $\sum_{i=0}^{n} a_i y_i = 0$, and get other copies of $\mathbb{A}^n$. These do just as well.

There are two ways to proceed in order to topologize $\mathbb{P}^n$ and put functions on its irreducible closed subsets. Either we can do everything locally in terms of the covering by copies of $\mathbb{A}^n$, or we could define the closed subsets to be zero loci of *homogeneous* polynomials in $k[y_0, \ldots, y_n]$. Both approaches are equivalent and both are necessary to develop the theory. However, we will mainly adhere to the first approach in our description of the theory, though we will take the second approach for the moment.

Now a homogeneous polynomial in $k[y_0, \ldots, y_n]$ is one which is invariant under scaling each variable by a nonzero element of $k$. Thus it is a polynomial all of whose monomials have the same total degree. Their zero sets in $k^{n+1}$ are invariant under scaling, and thus define subsets of $\mathbb{P}^n$. We take these to be the closed sets. It is the equivalent to take the open subsets of $\mathbb{P}^n$ to be unions of open sets in some copies of $\mathbb{A}^n$ which cover it.

Irreducible closed subsets of $\mathbb{P}^n$ are called *projective varieties,* and their open subsets are *quasi-projective varieties.* Quasi-projective varieties have regular functions defined the same way as affine varieties, but with homogeneous polynomials. Alternatively, a function is regular on a quasi-projective variety if it is regular on every quasi-affine subset. Then the local rings are defined the same way, and so are the function fields. These rings are all denoted in the same way as in the affine case.

**Proposition 1.5.** *Let $X$ be a projective variety. Then:*

*(a) $\mathcal{O}(X) \cong k$;*

*(b) Let $P \in X$ and $U \subset X$ be an open affine subset which contains $P$. Then the local ring of $X$ at $P$ is the local ring of $U$ at $P$;*

*(c) Let $U \subset X$ again be an open affine subset. Then $U$ is irreducible, its closure in $\mathbb{A}^n$ is an affine variety, and the function field of its closure is the function field of $X$.*

**Remark.** The fact that $\mathcal{O}(X) \cong k$ above may be surprising because it is so different from the affine case. Actually, this is no different than the situation in complex differential geometry. For instance, the global holomorphic functions on a compact Riemann surface are constant. The link between the theory of varieties over $\mathbb{C}$ and the theory of complex manifolds is deep, but we will not go into this here.

A morphism $\varphi : X \to Y$ between varieties (affine, quasi-affine, projective, or quasi-projective) is a map which is continuous and such that for any open subset $V$ of $Y$ and any regular function $f$ on $V$, $f \circ \varphi : \varphi^{-1}(V) \to k$ is regular. In particular, a morphism $X \to Y$ of affine varieties induces a homomorphism in the other direction $\mathcal{O}(Y) \to \mathcal{O}(X)$ on the rings of regular functions. In fact, we have

**Proposition 1.6.** *The category of affine varieties, with morphisms defined as above, is equivalent to the category of finitely generated integral domains over $k$ via taking the ring of regular functions.*

Note that we now have a notion of isomorphism; it is a morphism with a two-sided inverse. The last thing we should say about morphisms for now is the following.

**Proposition 1.7.** *Let $X$ be a variety.*

*(a) When $k$ is identified with $\mathbb{A}^1$ with its Zariski topology, then the regular functions $X \to k$ are precisely the morphisms $X \to \mathbb{A}^1$.*

*(b) For every rational function $f$ on $X$, there is a unique largest open subset $U \subset X$ on which $f$ can be defined such that $f$ is regular on $U$. Now view $\mathbb{P}^1 = \mathbb{A}^1 \cup H_0$ in our notation above, so that $H_0$ consists of one point, which we denote by $\infty$. If we declare $f$ to take on the value $\infty$ at the places where it is not defined, then $f$ is a morphism to $\mathbb{P}^1$. Conversely, all rational functions come from morphisms to $\mathbb{P}^1$.*

We now specialize to projective varieties of dimension 1, i.e., *curves,* because this theory is what will be mimicked in arithmetic. The Zariski topology on a curve is just the cofinite topology. It can be shown without too much effort that every curve has a cover consisting of exactly two open affine subsets. The compliment of one of these is a finite set, and should be thought of as "points at infinity" with respect to the open affine subset of which they are the compliment.

Let $X$ be a curve and $P \in X$. Let $\mathfrak{m}_P$ denote the maximal ideal in the local ring $\mathcal{O}_P$. It turns out that the residue field $\mathcal{O}_P/\mathfrak{m}_P$ is $k$. Then we define $X$ to be *nonsingular,* or *smooth,* at $P$ if $\mathfrak{m}_P/\mathfrak{m}_P^2$ is a one-dimensional $k$-vector space.

**Remark.** It happens that, given any point $P$ on a projective variety, the vector space $\mathfrak{m}_P/\mathfrak{m}_P^2$ is a good analogue of the cotangent space from differential geometry. One sees this during the development of the algebraic theory of differential forms. Nonsingularity in higher dimensions means that $\mathfrak{m}_P/\mathfrak{m}_P^2$ has dimension as a $k$-vector space the same as the dimension of the variety. Thus nonsingularity corresponds to the cotangent space having the right dimension.

Nonsingular curves appear in two other guises, both of which will inspire our developments in the sequel. The first is this.

**Proposition 1.8.** *There is an equivalence of categories between the category of nonsingular projective curves with non-constant morphisms of varieties, and the category of field extensions of $k$ of transcendence degree 1 with $k$-homomorphisms. The equivalence is given by taking function fields.*

The nonsingularity hypothesis is essential here. If a curve $X$ is singular, then its function field will be the function field of some nonsingular curve, which turns out to be obtainable from the curve $X$ by *resolving* its singularities, in manners which will not be touched upon here.

So we see that all of the information about a nonsingular curve is essentially contained in its function field. To make this more explicit, we describe the second guise in which nonsingular curves appear. Let $X$ be a nonsingular curve. First of all, one can show, using the nonsingularity hypothesis, that the local rings of $X$ are discrete valuation rings. This means they are local principal ideal domains. Also, their fields of fractions are $K(X)$. Thus a point gives rise to a discrete valuation ring with fraction field $K(X)$, and the next proposition shows that this process is reversible.

**Proposition 1.9.** *The points of a nonsingular curve $X$ are in bijection with the discrete valuation rings contained in $K(X)$ with fraction field $K(X)$.*

A morphism $X \to Y$ on this level would correspond to an inclusion of function fields $K(Y) \hookrightarrow K(X)$ as well as intersecting the discrete valuation rings of $K(Y)$ with $K(X)$ itself.

Now we come to divisors. We fix a nonsingular curve $X$. Denote by $\mathrm{Div}(X)$ the free abelian group on the points of $X$. The elements of $\mathrm{Div}(X)$ are called *divisors.* We think of a divisor $D$ as a sum of points with multiplicities, and we often write $D = \sum_{P \in X} n_P P$ where $n_P \in \mathbb{Z}$ and all but finitely many of the $n_P$ are zero.

Divisors may be thought of as a tool to examine the zeros and poles of rational functions. We can easily say what it means for a rational function on $X$ to vanish or to have a pole: When viewed as a morphism to $\mathbb{P}^1$, a rational function $f \in K(X)$ vanishes at $P$ if it takes the value $0 = \langle 1, 0 \rangle \in \mathbb{P}^1$ at $P$, and it has a pole at $P$ if it takes the value $\infty = \langle 0, 1 \rangle$ at $P$. Here, $\langle a, b \rangle$ is our notation for the class of the point $(a, b) \in k^2 \backslash 0$ modulo $k^\times$.

**Remark.** For a large class of varieties, or even for some schemes, this notion of divisor generalizes to what is called a *Weil divisor.* There is another notion of divisor, called a *Cartier divisor,* defined for an arbitrary scheme, which is not always equivalent to the notion of Weil divisor. However, one can show that the two notions coincide on a certain class of schemes. Now Cartier divisors show up in the theory of line bundles. In fact, the two theories are essentially equivalent. Thus, in nice cases, the theory of Weil divisors is, in some sense, equivalent to the theory of line bundles. We will not define line bundles here, but we will study the vector spaces $L(D)$ which turn out to be the spaces of global sections of certain line bundles arising from this theory.

Now it is not immediately clear what it should mean for a rational function to vanish to order $n$ or have a pole of order $n$. For this, we must examine the local rings of $X$. Let $f$ be a nonzero rational function which is regular at $P$. Then $f$ defines an element of the local ring $\mathcal{O}_P$. The function $f$ will vanish at $P$ if it is not invertible in $\mathcal{O}_P$, i.e., if it is in $\mathfrak{m}_P$. Now since $\mathcal{O}_P$ is a discrete valuation ring, $\mathfrak{m}_P$ is principal. Say it is generated by $\pi$. Then $f$ can be uniquely written as $f = u\pi^m$ where $m \geq 0$ is an integer and $u \in \mathcal{O}_P^\times$. The number $m$ is the order of vanishing of $f$, and it is denoted $v_P(f)$. It is independent of the choice of $\pi$.

If $f$ has a pole at $P$, then we apply this same process to $1/f$ and take the negative of the result to obtain the order of the pole.

**Proposition 1.10.** *The function $v_P$ is a well defined homomorphism $K(X)^\times \to \mathbb{Z}$ for all $P$. For any given $f \in K(X)^\times$, the number $v_P(f)$ is not zero for only finitely many points $P$.*

Let $f \in K(X)^\times$. Then we can define a divisor $\mathrm{div}(f) = \sum_{P \in X} v_P(f) P$. By the proposition, this is a well defined homomorphism $K(X)^\times \to \mathrm{Div}(X)$. We denote the image of div by $P(X)$ and call its elements *principal divisors.* Denote the group $\mathrm{Div}(X)/P(X)$ by $\mathrm{Cl}(X)$ and call this the *divisor class group.* Thus the divisor class group contains information about what combinations of zeros and poles rational functions are allowed to have. The next proposition will imply that this group is infinite, but we need to define

another homomorphism before stating it.

Let $D = \sum n_P P$ be a divisor. We define $\deg D$, called the *degree* of $D$, to be the integer $\sum n_P$. This defines a homomorphism $\mathrm{Div}(X) \to \mathbb{Z}$.

**Proposition 1.11.**

$$\deg \circ \operatorname{div} = 0.$$

Thus the degree factors through $\mathrm{Cl}(X)$. Since there exists divisors of all degrees, we have an exact sequence

$$0 \to \mathrm{Cl}^\circ(X) \to \mathrm{Cl}(X) \to \mathbb{Z} \to 0,$$

where $\mathrm{Cl}^\circ(X)$ denotes the divisor classes of degree zero. So $\mathrm{Cl}(X)$ is infinite. In fact, even the group $\mathrm{Cl}^\circ(X)$ is often highly nontrivial. We will remark on this later.

We are getting close to being able to state the Riemann-Roch theorem. Let $D = \sum n_P P$ be a divisor on $X$. We define the $k$-vector space

$$L(D) = \{f \in K(X)^\times \mid v_P(f) \geq -n_P \text{ for all } P \in X\} \cup \{0\}.$$

The dimension of this space turns out to be finite for all $D$, and is denoted $\ell(D)$. This number is called the *length* of $D$. It remains the same if we add to $D$ a principal divisor, i.e., $\ell$ is well defined on $\mathrm{Cl}(X)$.

**Theorem 1.12** (Riemann-Roch)**.** *Let $X$ be a nonsingular projective curve over $k$. There exists a divisor class $K$, depending only on $X$, such that for any divisor $D$, we have*

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

*where $g = \ell(K)$ is called the* genus *of $X$.*

This theorem is extremely deep, and it offers very useful information about the projective geometry of the curve $X$. The proof is very difficult. Hartshorne proves it in his text using methods from the cohomology of schemes. The main step is a deep theorem of Serre, which is often called Serre duality.

Weil's proof of this theorem uses his *répartitions,* or *adeles.* See Serre [12]. These are like the adeles we will encounter in number theory later.

**Remark.** Serre duality states, in the one-dimensional case, that there is a relation amongst cohomology groups,

$$H^1(X, \mathcal{L}(D)) = H^0(X, \mathcal{L}(D)^\vee \otimes \Omega_{X/k}),$$

where $\mathcal{L}(D)$ is the line bundle associated to the divisor $D$, $\Omega_{X/k}$ is the sheaf of differentials on $X$, and the check denotes the dual. The divisor class $K$ of the Riemann-Roch theorem is the one corresponding to the line bundle $\Omega_{X/k}$.

**Remark.** The group $\mathrm{Cl}^\circ(X)$ has a natural structure of abelian variety, and with this structure $\mathrm{Cl}^\circ(X)$ is called the *Jacobian* of $X$. Its dimension as a variety is equal to the genus of $X$.

## 2 Number Fields, Minkowski Theory

A *number field* is a finite field extension of the rationals $\mathbb{Q}$ (i.e., its degree over $\mathbb{Q}$, or its dimension as a $\mathbb{Q}$-vector space, is finite.) Its *degree* is its degree as an extension field of $\mathbb{Q}$. Just as a lot of information about $\mathbb{Q}$ is contained in its subring $\mathbb{Z}$, a number field has a canonical subring which contains a good deal of its information. It is constructed as follows.

Fix an arbitrary integral domain $A$. Let $K$ be its field of fractions, and let $L$ be an extension field of $K$. The main example to keep in mind is $A = \mathbb{Z}$, so that $K = \mathbb{Q}$ and $L$ is a therefore a number field. An element $\alpha \in L$ is called integral over $A$ if it is the root of a monic polynomial equation with coefficients in $A$,

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

with $c_i \in A$ for all $i$. The set of all elements of $L$ which are integral over $A$ forms a ring (which is not obvious) called *the integral closure of $A$ in $L$.* An integral domain is *integrally closed,* or is an *integrally closed domain,* if it is its own integral closure in its field of fractions.

**Definition 2.1.** Let $K$ be a number field of degree $n$. We define the subring $\mathcal{O}_K$ of $K$ to be the integral closure of $\mathbb{Z}$ in $K$, as in the previous paragraph. This is called the *ring of integers* in $K$.

The ring of integers in a number field should be viewed as analogous to the ring of regular functions on an open affine subset of a nonsingular curve, and the number field itself should be viewed as analogous to the function field of the curve. This analogy is extremely deep, and it is the main one which will be pursued in this paper.

**Example.** (0) Let $K = \mathbb{Q}$. Then $\mathcal{O}_K = \mathbb{Z}$. This is a standard exercise which we leave to the reader.

(1) Let $K$ be the number field $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$, where $i = \sqrt{-1}$. Then $\mathcal{O}_K = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. This can be seen by considering the field theoretic norm and trace (see Definition 2.6 later.) The point is that the norm and trace of any element in $\mathcal{O}_K$ is again in $\mathcal{O}_K$, but also in $\mathbb{Q}$, hence is in $\mathbb{Z}$. Thus if $a + bi \in \mathcal{O}_K$, then $\mathrm{Nm}(a+bi) = (a+bi)(a-bi) = a^2 + b^2$ and $\mathrm{Tr}(a+bi) = a+bi+a-bi = 2a$ are in $\mathbb{Z}$, from which one sees easily that $a, b \in \mathbb{Z}$.

(2) Now let $K = \mathbb{Q}(\sqrt{-3})$. Then $\mathbb{Z}[\sqrt{-3}] \subset \mathcal{O}_K$, but this inclusion is proper. In fact, $\mathcal{O}_K = \mathbb{Z}[\frac{1-\sqrt{-3}}{2}]$ (Note that $\alpha = \frac{1-\sqrt{-3}}{2}$ is a third root of unity and satisfies $\alpha^2 + \alpha + 1 = 0$.) So it is not always true that $\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$, even when $\alpha$ is integral.

Now $\mathbb{Z}$ is a principal ideal domain, and hence has unique prime factorization. It is an extremely important point that $\mathcal{O}_K$ very often does not have unique factorization. If it did, we would actually have on our hands an easy proof of Fermat's last theorem! See [6], Chapter 7, Section 1.2 for details.

To salvage the unique factorization property, one works with prime ideals instead of irreducible elements. In fact, it is convenient to introduce a more general type of ring which will have unique factorization into prime ideals.

A *Dedekind domain* is a noetherian integrally closed domain of Krull dimension 1. The

integers $\mathbb{Z}$ form a Dedekind domain, and the integral closure of a Dedekind domain in a finite extension of its field of fractions is again a Dedekind domain. Thus rings of integers $\mathcal{O}_K$ are Dedekind domains. Other examples are discrete valuation rings, and so the local rings of a nonsingular curve are Dedekind domains. Actually, localizations of Dedekind domains at their maximal (i.e., nonzero prime) ideals are discrete valuation rings, and so the localization of a ring of integers at a nonzero prime ideal is a discrete valuation ring. Thus we see some more similarities between rings of integers and rings of regular functions.

A *fractional ideal* in a Dedekind domain $A$ is an $A$-submodule $\mathfrak{a}$ of the fraction field $K$ of $A$ such that there exists an $\alpha \in A$ such that $\alpha\mathfrak{a} \subset A$, that is, $\alpha\mathfrak{a}$ is an ideal. Equivalently, it is a finitely generated $A$-submodule of $K$. We denote by $J(A)$ the set of all nonzero fractional ideals.

For two fractional ideals $\mathfrak{a}, \mathfrak{b}$, define their product to be the ideal generated by pairwise products of elements in $\mathfrak{a}$ and $\mathfrak{b}$:

$$\mathfrak{a}\mathfrak{b} = (\alpha\beta \mid \alpha \in \mathfrak{a}, \beta \in \mathfrak{b}).$$

The product of two fractional ideals is again a fractional ideal, and we have

**Theorem 2.2.** *Let $A$ be a Dedekind domain. Then the product above turns $J(A)$ into a group with identity $A$. The inverse is given by*

$$\mathfrak{a}^{-1} = \{\alpha \in K \mid \alpha\mathfrak{a} \subset A\}.$$

*The group $J(A)$ is free abelian on the nonzero prime ideals of $A$, and so every nonzero fractional ideal $\mathfrak{a}$ can be uniquely factored as*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}},$$

*where the product is over all nonzero prime ideals of $A$, and the $n_\mathfrak{p}$ are uniquely determined integers, almost all of which are zero. Moreover, all of the $n_\mathfrak{p}$ are positive if and only if $\mathfrak{a}$ is an ideal.*

Thus the group $J(\mathcal{O}_K)$ looks like a good analogue of the divisor group of a nonsingular curve, but actually it is only a good analogue of the divisor group on an open affine subset of a curve. For instance, the analogue of $\deg \circ \operatorname{div} = 0$ will not hold here. In the next section, we will introduce a better analogue of the divisor group.

**Remark.** It is true, however, that for a Dedekind domain $A$, the group of Weil divisors on $\operatorname{Spec} A$ and the group $J(A)$ are naturally isomorphic. But $\operatorname{Spec} \mathcal{O}_K$ is not a proper scheme. This is the problem. However, Arakelov theory makes a good attempt at overcoming this problem.

One can also define something which looks like the divisor class group as follows. Let $A$ be a Dedekind domain, and define $P(A)$ to be the set of all nonzero *principal* fractional ideals. These are the fractional ideals which are generated as $A$-modules by one element.

**Definition 2.3.** We define the *ideal class group* of a Dedekind domain $A$ to be $C(A) = J(A)/P(A)$, where $J(A)$ and $P(A)$ are as above.

The ideal class group naturally measures how close a Dedekind domain is to being a principal ideal domain. In fact, a Dedekind domain is principal if and only if it is a unique factorization domain, so this group actually measures the failure of unique factorization.

We move now to ramification theory. Let us simply call the nonzero prime ideals of a Dedekind domain "primes".

Let $A$ be a Dedekind domain with fraction field $K$, $L$ a finite extension of $K$, and $B$ the integral closure of $A$ in $L$. Let $\mathfrak{p}$ be a prime of $K$. Then a prime $\mathfrak{P}$ of $L$ is said to *lie over* $\mathfrak{p}$ if $\mathfrak{P} \cap A = \mathfrak{p}$.

When $\mathfrak{p}$ is a prime in $A$, we can form the ideal $\mathfrak{p}B$ and then factor it,

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

The factorization will contain all of the primes in $B$ which lie over $\mathfrak{p}$. The numbers $e_i$ are called the *ramification indices* of $\mathfrak{p}$. We always have $e_i \geq 1$, and if $e_i > 1$, we say $\mathfrak{P}_i$ is *ramified* and that $\mathfrak{p}$ *ramifies.*

When $K$ and $L$ are number fields and $A$ and $B$ are the respective rings of integers, this situation is analogous to a morphism of nonsingular curves $X \to Y$. In this case, $K$ is like $K(Y)$ and $L$ is like $K(X)$. The morphism is the same as intersecting the local rings of $K(X)$ with $K(Y)$. Here we are intersecting primes of $L$ with $\mathcal{O}_K$, but it is the same to intersect the localization of $\mathcal{O}_L$ at a prime $\mathfrak{P}$ with $K$. When this is done, we obtain a subring of $K$ which is equal to the localization of $\mathcal{O}_K$ at $\mathfrak{P} \cap \mathcal{O}_K$. There is also a notion of ramification in algebraic geometry, and it behaves well with this analogy, but we will not need it here.

Returning to our situation, we will also define another invariant of the extension of primes $\mathfrak{P}_i/\mathfrak{p}$. It is not hard to see that there is an inclusion of residue fields $A/\mathfrak{p} \hookrightarrow B/\mathfrak{P}_i$ (these are indeed fields because primes are maximal in Dedekind domains by definition). The degree of this field extension is finite and is denoted $f_i$. This is called the *inertia degree.*

**Theorem 2.4.** *Let $A$ be a Dedekind domain with fraction field $K$, $L$ a finite extension of $K$ of degree $n$, and $B$ the integral closure of $A$ in $L$. Let $\mathfrak{p}$ be a prime of $A$, factored in $B$ as*

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

*Then*

$$\sum_{i=1}^{r} e_i f_i = n.$$

*If $L/K$ is moreover Galois, then the Galois group $\mathrm{Gal}(L/K)$ permutes the primes above $\mathfrak{p}$ transitively. Consequently, all of the ramification indices are equal, to $e$, say, and all of the inertia degrees are equal, to $f$, say, and hence*

$$ref = n.$$

Now let $K$ be a number field of degree $n$. Its ring of integers $\mathcal{O}_K$ is a free abelian group of rank $n$, additively. We call a basis of $\mathcal{O}_K$ as a free abelian group an *integral basis.* Let $\bar{\mathbb{Q}}$ be a fixed algebraic closure of $\mathbb{Q}$, and view $K$ as a subfield of $\bar{\mathbb{Q}}$. Then there are exactly

$n$ homomorphisms of $K$ into $\bar{\mathbb{Q}}$. Denote them by $\tau_1, \ldots, \tau_n$. Let $\alpha_1, \ldots, \alpha_n$ be an integral basis. We form the matrix

$$A = \begin{bmatrix} \tau_1\alpha_1 & \tau_1\alpha_2 & \cdots & \tau_1\alpha_n \\ \tau_2\alpha_1 & \tau_2\alpha_2 & \cdots & \tau_2\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \tau_n\alpha_1 & \tau_n\alpha_2 & \cdots & \tau_n\alpha_n \end{bmatrix}.$$

Then we define $\Delta_K = \det A^2$.

**Definition 2.5.** The number $\Delta_K$ defined above is called the *discriminant* of the number field $K$.

It turns out that the discriminant of a number field is a nonzero integer which is independent of the choice of integral basis. It is a very important invariant of $K$.

When $L/K$ is an extension of number fields, there is a closely related invariant. To define it, we recall a definition from field theory.

**Definition 2.6.** Let $E/F$ be a finite separable extension of fields. Let $\sigma_1, \ldots, \sigma_n$ be all of the embeddings of $E$ into a separable algebraic closure $\bar{F}$ of $F$. Then the *trace* and *norm* of an element $\alpha \in E$ are respectively defined by

$$\mathrm{Tr}_{E/F}\,\alpha = \sum_{i=1}^{n} \sigma_i\alpha, \qquad \mathrm{Nm}_{E/F}\,\alpha = \prod_{i=1}^{n} \sigma_i\alpha.$$

Both are elements of $F$.

Now consider the set

$$\mathfrak{C}_{L/K} = \{\beta \in L \mid \mathrm{Tr}_{L/K}\,\beta \in \mathcal{O}_K\}.$$

This is a fractional ideal of $\mathcal{O}_L$, called *Dedekind's complimentary module.* We define

$$\mathfrak{D}_{L/K} = \mathfrak{C}_{L/K}^{-1}.$$

The fractional ideal $\mathfrak{D}_{L/K}$ is an ideal, called the *different* of $L/K$. We have the following theorem.

**Theorem 2.7.** *Let $L/K$ be an extension of number fields and let $\mathfrak{P}$ be a prime of $L$ (i.e., a prime of $\mathcal{O}_L$). Then $\mathfrak{P}$ is ramified if and only if it appears in the factorization of the different $\mathfrak{D}_{L/K}$. We also have*

$$|\mathcal{O}_K/\mathfrak{D}_{K/\mathbb{Q}}| = |\Delta_K|$$

*where $|\mathcal{O}_K/\mathfrak{D}_{K/\mathbb{Q}}|$ denotes the cardinality of the set $\mathcal{O}_K/\mathfrak{D}_{K/\mathbb{Q}}$. One can show that this implies that a prime of $\mathbb{Z}$ ramifies in $K$ if and only if it divides the discriminant of $K$.*

In particular, given any extension of number fields, there are only finitely many primes which ramify in that extension.

If $\mathfrak{a}$ is a nonzero ideal in $\mathcal{O}_K$, we denote by $\mathbb{N}\mathfrak{a}$ the order of the residue ring $\mathcal{O}_K/\mathfrak{a}$. One can show that this is always finite, and that it is multiplicative, i.e., $\mathbb{N}(\mathfrak{ab}) = \mathbb{N}\mathfrak{a}\mathbb{N}\mathfrak{b}$. Thus it extends to a homomorphism from the group of fractional ideals $J(\mathcal{O}_K)$ to $\mathbb{Q}^\times$, which will be important to us in the sequel.

**Definition 2.8.** The function $\mathbb{N} : J(\mathcal{O}_K) \to \mathbb{Q}^\times$ is the unique homomorphism such that $\mathbb{N}\mathfrak{a}$ is the cardinality of the ring $\mathcal{O}_K/\mathfrak{a}$ if $\mathfrak{a}$ is an ideal (that is, when $\mathfrak{a} \subset \mathcal{O}_K$).

We now begin to study Minkowski theory. The idea of this theory is to embed a number field $K$ of degree $n$ into $\mathbb{R}^n$ and study the geometry of this embedding. Let us explain this embedding now. By Galois theory, there are exactly $n$ embeddings of $K$ into any fixed algebraically closed field of characteristic 0. So write

$$\mathrm{Hom}(K, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \bar{\sigma}_{r+1}, \ldots, \sigma_{r+s}, \bar{\sigma}_{r+s}\},$$

where the notation is explained as follows. The first $r$ embeddings have image contained in $\mathbb{R}$, and they are called *real embeddings.* The last $2s$, called *complex embeddings,* intersect $\mathbb{C}\backslash\mathbb{R}$. Hence the complex embeddings come in complex conjugate pairs. By definition, $n = r + 2s$.

Consider the $\mathbb{R}$-vector space $\mathbb{R}^r \times \mathbb{C}^s$, which is isomorphic to $\mathbb{R}^n$. Define $i : K \to \mathbb{R}^n$ via the map $K \to \mathbb{R}^r \times \mathbb{C}^s$ given by

$$\alpha \mapsto (\sigma_1\alpha, \ldots, \sigma_{r+s}\alpha),$$

where we choose only one embedding from each pair of complex embeddings. This is an embedding because it is injective on each component.

A lattice in $\mathbb{R}^n$ is by definition a subgroup of $\mathbb{R}^n$ spanned as a free abelian group by a basis of $\mathbb{R}^n$. It is discrete in the euclidean topology. Let $\Lambda \subset \mathbb{R}^n$ be a lattice spanned by a basis $\lambda_1, \ldots, \lambda_n$. A *fundamental parallelepiped* of $\Lambda$ is a set of the form

$$F = \left\{ \sum_{i=1}^{n} a_i\lambda_i \;\middle|\; 0 \le a_i \le 1 \text{ for all } i \right\}.$$

A fundamental parallelepiped depends on a basis, but its volume (under the Lebesgue measure) does not.

**Proposition 2.9.** *Let $i : K \to \mathbb{R}^n$ be as above, and let $\mathfrak{a}$ be a nonzero fractional ideal of $\mathcal{O}_K$. Then $i(\mathfrak{a})$ is a lattice in $\mathbb{R}^n$ and the volume of any of its fundamental parallelepipeds is equal to $2^{-s}\sqrt{|\Delta_K|}\mathbb{N}\mathfrak{a}$, where, as before, $2s$ is the number of complex embeddings of $K$.*

**Example.** (1) Let $K = \mathbb{Q}(i)$, so that $\mathcal{O}_K = \mathbb{Z}[i]$. The field $\mathbb{Q}(i)$ has degree 2, so it has two embeddings into $\mathbb{C}$. One is the embedding sending $a + bi \in \mathbb{Q}(i)$ into the same thing, but with $a, b \in \mathbb{Q}$ viewed as real numbers, and the other is the conjugate of this embedding. To define the map $i$, we (arbitrarily) choose the former embedding, and this embeds $\mathbb{Z}[i]$ into the grid of numbers in $\mathbb{C}$ with integer real and imaginary parts.

(2) Let $K = \mathbb{Q}(\sqrt{2})$. One can show that $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. The field $K$ has two embeddings into $\mathbb{C}$ and they are both real. They are determined by sending $\sqrt{2} \in K$ into either $\sqrt{2} \in \mathbb{R}$ or $-\sqrt{2} \in \mathbb{R}$. Then, letting $\sigma_1$ be the first of these embeddings, and $\sigma_2$ the other, we see that $i(a + b\sqrt{2}) = (a + b\sqrt{2}, a - b\sqrt{2}) \in \mathbb{R}^2$. In particular, since $\{1, \sqrt{2}\}$ is an integral basis for the ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$, we find that the lattice $i(\mathcal{O}_K)$ is generated (as a free abelian group) by the vectors $(1, 1)$ and $(\sqrt{2}, -\sqrt{2})$.

**Definition 2.10.** For a number field $K$, let $h_K$ denote the order of the ideal class group $C(\mathcal{O}_K)$ of the ring of integers in $K$, defined in Definition 2.3. The number $h_K$ is called the *class number of* $K$.

One uses Minkowski theory to prove

**Theorem 2.11.** *The class number $h_K$ is finite.*

Thus rings of integers in a number field $K$ do not deviate too far from being unique factorization domains, in some sense.

Let us very briefly outline the proof of this fact. First one puts an explicit and uniform bound on the largest of the smallest nonzero element of a fractional ideal. More precisely, given a fractional ideal $\mathfrak{a}$, there is a nonzero element $\alpha \in \mathfrak{a}$ such that

$$|\operatorname{Nm}_{K/\mathbb{Q}} \alpha| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \mathbb{N}\mathfrak{a} \sqrt{|\Delta_K|},$$

where, recall, $n$ is the degree of $K$, $s$ is the number of complex embeddings, and $\Delta_K$ is the discriminant of $K$. To prove this, one must locate an element of small size in the lattice $i(\mathfrak{a})$. The ability to do this is furnished by

**Theorem 2.12** (Minkowski)**.** *Let $\Lambda$ be a lattice in $\mathbb{R}^n$ with fundamental parallelepiped $F$. Let $X \subset \mathbb{R}^n$ be a compact region which is convex (any two points in $X$ can be joined by a line segment in $X$) and symmetric about the origin ($x \in X$ implies $-x \in X$). If the volume of $X$ exceeds $2^n \operatorname{Vol}(F)$, then $X$ contains a nonzero lattice point.*

One then shows that the above bound implies that every ideal class has an integral (i.e., in $\mathcal{O}_K$) representative $\mathfrak{a}$ such that

$$\mathbb{N}\mathfrak{a} \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\Delta_K|}.$$

But it is easy to see that there are only finitely many primes in $\mathbb{Z}$ which lie under primes satisfying this, or any, bound. By unique factorization and the fact that the function $\mathbb{N}$ is multiplicative, this would complete the proof.

A nice consequence of this proof is that the first bound above implies that, since the norm of an integral ideal is always a positive integer,

$$\left(\frac{\pi}{4}\right)^s \frac{n^n}{n!} \leq \sqrt{|\Delta_K|}$$

One can show that the expression on the left is always larger than 1 for $n \geq 2$, so there are no unramified extensions of $\mathbb{Q}$!

Finally, we would like to describe a similar construction for $K^\times$. Write again

$$\operatorname{Hom}(K, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \bar{\sigma}_{r+1}, \ldots, \sigma_{r+s}, \bar{\sigma}_{r+s}\}.$$

Define a map $\log : K^\times \to \mathbb{R}^{r+s}$ via

$$\alpha \mapsto (\log|\sigma_1\alpha|, \ldots, \log|\sigma_{r+s}\alpha|),$$

where, again, we only choose one embedding from each pair of complex embeddings. Define the hyperplane $H \subset \mathbb{R}^{r+s}$ by the equation

$$x_1 + \cdots + x_r + 2x_{r+1} + \cdots + 2x_{r+s} = 0$$

where the $x_i$'s are the coordinates of $\mathbb{R}^{r+s}$. One can prove that the norm over $\mathbb{Q}$ of any element of $\mathcal{O}_K^\times$ is $\pm 1$. This implies that log takes $\mathcal{O}_K^\times$ into $H$. In fact,

**Theorem 2.13.** *The set* $\log(\mathcal{O}_K^\times)$ *forms a lattice in* $H$.

An immediate consequence is

**Theorem 2.14** (Dirichlet's Unit Theorem)**.** *The group* $\mathcal{O}_K^\times$ *is a finitely generated abelian group of rank* $r + s - 1$ *with torsion the roots of unity in* $K$.

In the next section, we will make a deeper study of the analogies between number fields and the function fields of nonsingular curves, and use Minkowski theory to outline the proof of the Riemann-Roch theorem for number fields.

# 3 The Riemann-Roch Theorem for Number Fields

Fix throughout this section a number field $K$ of degree $n$. There are $r$ real embeddings and $2s$ complex embeddings. The embedding $K \hookrightarrow \mathbb{R}^n$ is still denoted $i$, and $\mathbb{R}^n$ will be identified with $\mathbb{R}^r \times \mathbb{C}^s$. It will be convenient to give $\mathbb{C}$ twice the Lebesgue measure, so that the fundamental parallelepiped of $i(\mathcal{O}_K)$ gets measure exactly $\sqrt{|\Delta_K|}$, without the factor of $2^{-s}$ as before.

Now we have seen that the primes of a number field behave like the points on an open affine subset of a nonsingular curve. There is a very good idea about what the analogue of the points at infinity should be. It turns out that the analogue of the points at infinity is the set of embeddings of $K$ into $\mathbb{C}$ modulo complex conjugation. This may seem strange to a reader who is not familiar with this idea, so we make an attempt to explain this briefly. In any case, this will become clearer when we discuss the local theory.

Now each prime $\mathfrak{p}$ of $K$ gives rise to an *absolute value* on $K$, called the $\mathfrak{p}$-adic absolute value. Let us say exactly what this means.

**Definition 3.1.** An absolute value on a field $k$ is a map $|\cdot| : k \to \mathbb{R}_{\geq 0}$ for which:
(1) $|\alpha| \geq 0$ for all $\alpha \in k$, equality holding if and only if $\alpha = 0$;
(2) $|\alpha\beta| = |\alpha||\beta|$ for all $\alpha, \beta \in k$;
(3) [Triangle inequality] $|\alpha + \beta| \leq |\alpha| + |\beta|$ for all $\alpha, \beta \in k$.
An absolute value on $k$ gives rise to a metric via the rule $d(\alpha, \beta) = |\alpha - \beta|$. Two absolute values are *equivalent* if their metrics induce the same topology on $k$.

The $\mathfrak{p}$-adic absolute value on $K$ is defined as follows. For $\alpha \in K$, let $(\alpha)$ be the principal fractional ideal generated by $\alpha$, and let $(\alpha) = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$ be its unique factorization into prime ideals. Define $v_\mathfrak{p}(\alpha) = n_\mathfrak{p}$.

**Definition 3.2.** With notation as above, we define the $\mathfrak{p}$-*adic absolute value* of $\alpha \in K$ by

$$|\alpha|_\mathfrak{p} = (\mathbb{N}\mathfrak{p})^{-v_\mathfrak{p}(\alpha)}.$$

This is an absolute value on $K$, and in fact it satisfies a stronger condition than the triangle inequality:

(3′) [Ultrametric inequality] $|\alpha + \beta| \leq \max\{\alpha, \beta\}$.

An absolute value satisfying the ultrametric inequality is called *non-archimedean.* Otherwise it is *archimedean.* Now we get archimedean absolute values on $K$ by choosing an embedding $K \hookrightarrow \mathbb{C}$ and restricting the absolute value on $\mathbb{C}$ to $K$. The absolute value coming from an embedding $\sigma$ is therefore the same as the absolute value coming from $\bar{\sigma}$, which accounts for the desire to consider the set of embeddings $K \hookrightarrow \mathbb{C}$ modulo complex conjugation.

Finally, there is the *trivial absolute value* on a field $k$, given by $|\alpha| = 1$ if $\alpha \neq 0$. This gives the discrete topology. We will always assume that our absolute values are nontrivial.

**Example.** If $K = \mathbb{Q}$, let $\mathfrak{p}$ be a prime ideal, generated by a positive prime $p$, say. Then the $\mathfrak{p}$-adic absolute value is also called the $p$-adic absolute value, and it does the following. Let $0 \neq \alpha \in \mathbb{Q}$. Write $\alpha = a/b$, $a, b \in \mathbb{Z}$ with $a$ and $b$ coprime. If $p$ divides either $a$ or $b$, we can extract that power of $p$ from the fraction and write $\alpha = p^m(c/d)$ with $m \in \mathbb{Z}$ and $p, c, d$ all coprime. Then $|\alpha|_p = p^{-m}$. In other words, the $p$-adic absolute value extracts the power of $p$ in its argument, then inverts it.

An archimedean absolute value on $\mathbb{Q}$ is the usual one: $|\alpha|$ is $\alpha$ if $\alpha$ is positive, and $-\alpha$ otherwise. In fact, the only absolute values on $\mathbb{Q}$ are this one and the $p$-adic ones for various $p$, as we will see now.

The following theorem in the case $K = \mathbb{Q}$ is called Ostrowski's theorem.

**Theorem 3.3.** *The set of nontrivial absolute values on $K$, up to equivalence, consists of the $\mathfrak{p}$-adic ones, which are all inequivalent for each prime $\mathfrak{p}$, and the ones coming from embeddings $K \hookrightarrow \mathbb{C}$, which are all inequivalent up to complex conjugation.*

Let $V_K$ denote the set of nontrivial absolute values on $K$ up to equivalence. This set is the disjoint union of the set $V_\mathrm{f}$ of non-archimedean absolute values and the set $V_\infty$ of archimedean absolute values. The set $V_\mathrm{f}$ is in bijection with the prime ideals of $K$, and we call its elements *finite primes,* or *finite places.* The set $V_\infty$ is in bijection with the embeddings $K \hookrightarrow \mathbb{C}$ modulo complex conjugation, and we call its elements *infinite primes,* or *infinite places.* For $\mathfrak{p} \in V_\mathrm{f}$, we write $\mathfrak{p} \nmid \infty$, and for $\mathfrak{p} \in V_\infty$, we write $\mathfrak{p}|\infty$. The set $V_K$ is our analogue of the points on a nonsingular projective curve.

Now we are ready to discuss the Riemann-Roch theory. We follow loosely the presentation of Neukirch [9].

First we define the replete ideals.

**Definition 3.4.** A *replete ideal* is an element of the set of formal products

$$J(\bar{\mathcal{O}}_K) = \left\{ \prod_{\mathfrak{p} \in V_\mathrm{f}} \mathfrak{p}^{n_\mathfrak{p}} \times (n_\mathfrak{p})_{\mathfrak{p} \in V_\infty} \;\middle|\; n_\mathfrak{p} \in \mathbb{Z} \text{ if } \mathfrak{p} \nmid \infty,\ n_\mathfrak{p} \in \mathbb{R}_{>0} \text{ if } \mathfrak{p}|\infty,\ n_\mathfrak{p} = 0 \text{ for almost all } \mathfrak{p} \right\},$$

where "almost all" means "all but finitely many".

This is a group under component-wise multiplication. It is isomorphic to $J(\mathcal{O}_K) \times \mathbb{R}_{>0}^{r+s}$, where $J(\mathcal{O}_K)$ is the group of fractional ideals of $\mathcal{O}_K$.

**Definition 3.5.** We define the group (under component-wise addition) of *Arakelov divisors* as

$$\mathrm{Div}(\bar{\mathcal{O}}_K) = \left\{ \sum_{\mathfrak{p} \in V_K} n_{\mathfrak{p}} \mathfrak{p} \;\middle|\; n_{\mathfrak{p}} \in \mathbb{Z} \text{ if } \mathfrak{p} \nmid \infty,\ n_{\mathfrak{p}} \in \mathbb{R} \text{ if } \mathfrak{p} | \infty,\ n_{\mathfrak{p}} = 0 \text{ for almost all } \mathfrak{p} \right\}.$$

This is the analogue of the divisor group. The fact that we choose the infinite components to take on real values stems from the fact that the image of $K^\times$ under the infinite absolute values is dense in $\mathbb{R}_{>0}$, while the image of $K^\times$ under the finite absolute values is a discrete subset of $\mathbb{R}_{>0}$.

Now the groups $J(\bar{\mathcal{O}}_K)$ and $\mathrm{Div}(\bar{\mathcal{O}}_K)$ are obviously isomorphic, but we will define a nontrivial isomorphism between them. Let $L : J(\bar{\mathcal{O}}_K) \to \mathrm{Div}(\bar{\mathcal{O}}_K)$ be defined by

$$\prod_{\mathfrak{p} \in V_K} \mathfrak{p}^{n_{\mathfrak{p}}} \mapsto \sum_{\mathfrak{p} \nmid \infty} -n_{\mathfrak{p}} \mathfrak{p} + \sum_{\mathfrak{p} \text{ real}} -(\log n_{\mathfrak{p}}) \mathfrak{p} + \sum_{\mathfrak{p} \text{ complex}} -(2 \log n_{\mathfrak{p}}) \mathfrak{p}.$$

This should be viewed as extracting valuations, i.e., taking $v_{\mathfrak{p}}$ of each component. In fact, to unify notation, for $\alpha \in K$, set $v_{\mathfrak{p}}(\alpha) = -\log |\alpha|_{\mathfrak{p}}$ for $\mathfrak{p}$ real, and $v_{\mathfrak{p}}(\alpha) = -2 \log |\alpha|_{\mathfrak{p}}$ for $\mathfrak{p}$ complex. Here $|\cdot|_{\mathfrak{p}}$ means the absolute value induced on $K$ by the embedding $K \hookrightarrow \mathbb{C}$ corresponding to $\mathfrak{p}$.

Define $\mathrm{div} : K^\times \to \mathrm{Div}(\bar{\mathcal{O}}_K)$ by

$$\mathrm{div}(\alpha) = \sum_{\mathfrak{p}} v_{\mathfrak{p}}(\alpha) \mathfrak{p}.$$

This is the analogue of the function div from algebraic geometry. Define also the function $\deg : \mathrm{Div}(\bar{\mathcal{O}}_K) \to \mathbb{R}$ via

$$\sum n_{\mathfrak{p}} \mathfrak{p} \mapsto \sum_{\mathfrak{p} \nmid \infty} n_{\mathfrak{p}} \log \mathbb{N}\mathfrak{p} + \sum_{\mathfrak{p} | \infty} n_p.$$

This is the analogue of the degree, and we have

**Theorem 3.6** (Product Formula)**.**

$$\deg \circ \mathrm{div} = 0.$$

This is a rephrasing of what is classically called the product formula. The classical version is formulated as follows. For $\mathfrak{p} \in V_K$, let $|\cdot|_{\mathfrak{p}}$ be the $\mathfrak{P}$-adic absolute value if $\mathfrak{p}$ comes from a prime ideal $\mathfrak{P}$ of $K$, and let it be the restriction of the absolute value on $\mathbb{C}$ if $\mathfrak{p}$ comes from an embedding $K \hookrightarrow \mathbb{C}$. These are canonical choices of representatives of each equivalence class in $V_K$. If $\mathfrak{p}$ is finite or real, we write $\|\cdot\|_{\mathfrak{p}} = |\cdot|_{\mathfrak{p}}$. If $\mathfrak{p}$ is complex, we write $\|\cdot\|_{\mathfrak{p}} = |\cdot|_{\mathfrak{p}}^2$. The square of the absolute value at the complex places turns out to be a good choice for arithmetic purposes, and we will see this more than once in this paper.

**Theorem 3.7** (Product Formula, Classical)**.** *Let $\alpha \in K^\times$. Then*

$$\prod_{\mathfrak{p} \in V_K} \|\alpha\|_{\mathfrak{p}} = 1.$$

*This product makes sense because all but finitely many of the terms are equal to* 1*.*

We now incorporate Minkowski theory into this situation. Let $\mathfrak{a}$ be a replete ideal. Let $\mathfrak{a}_\mathrm{f}$ denote the finite component of $\mathfrak{a}$, i.e., the fractional ideal obtained via the first projection through the isomorphism $J(\bar{\mathcal{O}}_K) \cong J(\mathcal{O}_K) \times \mathbb{R}_{>0}^{r+s}$. The second projection gives a vector $\mathfrak{a}_\infty$ in $\mathbb{R}^r \times \mathbb{R}^s$, which we view as embedded in $\mathbb{R}^r \times \mathbb{C}^s$. Now $i(\mathfrak{a}_\mathrm{f})$ is a lattice in $\mathbb{R}^r \times \mathbb{C}^s$. Define, by abuse of notation, $i(\mathfrak{a}) = \mathfrak{a}_\infty \cdot i(\mathfrak{a}_\mathrm{f})$, with the multiplication of vectors in $\mathbb{R}^r \times \mathbb{C}^s$ being component-wise. In other words, we skew the lattice $i(\mathfrak{a}_\mathrm{f})$ by the infinite components of $\mathfrak{a}$.

**Definition 3.8.** If $\mathfrak{a} = \prod \mathfrak{p}^{n_\mathfrak{p}}$ is a replete ideal, we define

$$\mathbb{N}\mathfrak{a} = \mathbb{N}\mathfrak{a}_\mathrm{f} \cdot \prod_{\mathfrak{p} \text{ real}} n_\mathfrak{p} \cdot \prod_{\mathfrak{p} \text{ complex}} n_\mathfrak{p}^2.$$

We denote the volume of the fundamental parallelepiped of $i(\mathfrak{a})$ by $\mathrm{Vol}(\mathfrak{a})$ so that

$$\mathrm{Vol}(\mathfrak{a}) = \mathbb{N}\mathfrak{a}\sqrt{|\Delta_K|}.$$

There is no $2^{-s}$ because we have given $\mathbb{C}$ twice the Lebesgue measure. Now we define

$$\chi(\mathfrak{a}) = -\log \mathrm{Vol}(\mathfrak{a}).$$

This is the *Euler characteristic.* We can also define it on $\mathrm{Div}(\bar{\mathcal{O}}_K)$ by precomposition with $L^{-1}$. The Euler characteristic of an Arakelov divisor is the analogue of the quantity $\ell(D) - \ell(K - D)$, which is also called the Euler characteristic of $D$ in algebraic geometry.

**Remark.** Let $X$ be a projective scheme over a field $k$, and $\mathcal{L}$ a line bundle on $X$. One can define the Euler characteristic $\chi(\mathcal{L})$ to be the alternating sum of the dimensions of the cohomology vector spaces of $\mathcal{L}$. The terms in this sum are finite by a theorem of Serre, and they vanish beyond the dimension of $X$ by a theorem of Grothendieck. See Hartshorne [3] for details.

In case $X$ is a nonsingular curve and $k$ is algebraically closed, the Euler characteristic $\chi(\mathcal{L}(D))$ is equal to $\ell(D) - \ell(K - D)$ by Serre duality. As well, if $\mathcal{O}_X$ denotes the structure sheaf of $X$, then $\chi(\mathcal{O}_X) = \ell(0) - \ell(K) = 1 - g$. Hence the Riemann-Roch theorem states

$$\chi(\mathcal{L}(D)) = \deg D + \chi(\mathcal{O}_X).$$

Let $\mathcal{O}$ denote the Arakelov divisor which is the identity of the group $\mathrm{Div}(\bar{\mathcal{O}}_K)$. To differentiate the following theorem from the one in the title of this paper, we use the word "formula" instead of "theorem". Its proof is a trivial computation.

**Theorem 3.9** (Riemann-Roch Formula, First Form)**.** *For any $D \in \mathrm{Div}(\bar{\mathcal{O}}_K)$ we have*

$$\chi(D) = \deg D + \chi(\mathcal{O})$$

Even though the analogy with algebraic geometry will be just slightly less clear, it will now be convenient to begin stating results in terms of replete ideals instead of Arakelov divisors. Any function we have on $\mathrm{Div}(\bar{\mathcal{O}}_K)$ we understand to be defined on $J(\bar{\mathcal{O}}_K)$ by precomposition with $L^{-1}$, and vice-versa by composition with $L$. Note also that deg and $\mathbb{N}$ are related by

$$\deg(L(\mathfrak{a})) = -\log \mathbb{N}\mathfrak{a}.$$

**Definition 3.10.** Let $\mathfrak{a} = \prod_{V_\mathrm{f}} \mathfrak{p}^{n_\mathfrak{p}} \times (n_\mathfrak{p})_{V_\infty}$ be a replete ideal. We define

$$H^0(\mathfrak{a}) = \{\alpha \in K^\times \mid v_\mathfrak{p}(\alpha) \geq n_\mathfrak{p} \text{ for } \mathfrak{p} \nmid \infty,\ |\alpha|_\mathfrak{p} \leq n_\mathfrak{p}^{-1} \text{ for } \mathfrak{p}|\infty\} \cup \{0\}.$$

$H^0(\mathfrak{a})$ is (essentially) the analogue of $L(D)$ from algebraic geometry: $L(D)$ is the set of functions on a curve $X$ which have poles of degrees *at most* that which is specified by the divisor, while $H^0(\mathfrak{a})$ is the set of all numbers in $K$ whose valuations are *at least* what is specified by the replete ideal. Notice the discrepancy between "at least" and "at most." This is remedied by defining a set in number theory which consists of 0 and all the reciprocals of elements in $H^0(\mathfrak{a})$. Such a set would be a more ideal analogue of $L(D)$, but it would still be in bijection with $H^0(\mathfrak{a}$. Since $H^0(\mathfrak{a})$ is easier to work with, we take its definition as our working definition of an analogue of $L(D)$.

Now note that $H^0(\mathfrak{a})$ is a finite set: the conditions at the finite places imply that $H^0(\mathfrak{a})$ is a subset of $\mathfrak{a}_\mathrm{f}$. Thus, passing through the Minkowski embedding of $\mathfrak{a}_\mathrm{f}$ into $\mathbb{R}^r \times \mathbb{C}^s$, we realize that $H^0(\mathfrak{a})$ can be viewed as precisely the set of lattice points $(x_1, \ldots, x_{r+s}) \in i(\mathfrak{a}_\mathrm{f})$ subject to the bounds $|x_i| \leq n_{\mathfrak{p}_i}^{-1}$, where $\mathfrak{p}_i$ is the infinite place corresponding to the $i$th embedding of $K$ into $\mathbb{C}$ from the definition of the embedding $i$. We now define

$$\ell(\mathfrak{a}) = \log \frac{|H^0(\mathfrak{a})|}{2^r(2\pi)^s}.$$

This is the analogue of $\ell(D)$.

Some comments are in order. In Neukirch [9], he defines $H^0(\mathfrak{a})$ the same way but without adjoining 0. Then $\ell(\mathfrak{a})$ is defined by our same formula, and hence is not well defined if $H^0(\mathfrak{a})$ has no elements. (Actually Neukrich defines this quantity to be 0 if $H^0(\mathfrak{a})$ is empty). In any case, let us continue and define the *genus* of a number field. We will see some discrepancies appear.

Let $i(\mathfrak{a}) = \ell(\mathfrak{a}) - \chi(\mathfrak{a})$ and call this the *index of specialty* of $\mathfrak{a}$. This is the analogue of $\ell(K - D)$, which is also called the index of specialty in algebraic geometry. The reason for the terminology is that for most divisors (in fact for *all* divisors of sufficiently large degree) we have $\ell(K - D) = 0$. Riemann's contribution to the Riemann-Roch theorem was that most of the time, $\ell(D) = \deg D + 1 - g$. Roch, a student of Riemann, contributed the information about the failure of this formula.

Define the genus of $K$ to be $g = i(\mathcal{O})$. Let $w_K$ be the number of roots of unity in $K$. One computes easily that

$$g = -\log \frac{2^r(2\pi)^s}{(w_K + 1)\sqrt{|\Delta_K|}}$$

We make a (rather philosophical) remark about algebraic number theory.

**Remark.** Let $\zeta_K(s) = \sum_{\text{ideals } \mathfrak{a}} (\mathbb{N}\mathfrak{a})^{-s}$ be the Dedekind zeta function of $K$. This sum converges and defines a holomorphic function for $\Re s > 1$. The class number formula states that $\zeta_K$ can be analytically continued beyond the line $\Re s = 1$ and that

$$\mathrm{Res}_{s=1}\, \zeta_K(s) = \frac{2^r(2\pi)^s}{w_K\sqrt{|\Delta_K|}} \mathrm{Reg}_K\, h_K$$

where $\mathrm{Reg}_K$ is the *regulator* of $K$, which is essentially an analogue of $\Delta_K$ for the units $\mathcal{O}_K^\times$. If we had taken Neukirch's definition of $H^0(\mathfrak{a})$ instead of our own, then the genus would be the constant

$$-\log \frac{2^r(2\pi)^s}{w_K\sqrt{|\Delta_K|}}.$$

Hence our definition of $H^0(\mathfrak{a})$ does not allow the genus to appear in the class number formula. I contend that it should not necessarily appear here, however, for the following reasons.

The constant in the class number formula is the volume of the norm-one idele class group. The functional equation proven by Tate in his famous thesis relates the residues of the poles of zeta functions to this idelic volume. However, in Section 11, we will see that the constants in the Riemann-Roch theorem come from volume computations in the adeles, rather than the ideles. The quantity $2^r(2\pi)^s/\sqrt{|\Delta_K|}$ appears in both the adelic theory and idelic theory, in the former case as the volume of the product of the closed unit balls in $\mathbb{A}_K$, and the latter case as the volume of the product of the unit circles in $\mathbb{I}_K$. This similarity accounts for the appearance of the quantity $2^r(2\pi)^s/\sqrt{|\Delta_K|}$ in both places, and thus shows why the discrepancy lies only at $w_K$.

**Theorem 3.11** (Riemann-Roch Formula, Second Form)**.** *Let $\mathfrak{a}$ be a replete ideal. Then*

$$\ell(\mathfrak{a}) - i(\mathfrak{a}) = \deg \mathfrak{a} + \ell(\mathcal{O}) - g.$$

The proof is again a trivial computation.

We now come to the main theorem of this paper. It is due to Serge Lang.

**Theorem 3.12** (Riemann-Roch Theorem For Number Fields)**.** *As $\mathfrak{a}$ ranges over $J(\bar{\mathcal{O}}_K)$, we have*

$$|H^0(\mathfrak{a}^{-1})| = \frac{2^r(2\pi)^s}{\sqrt{|\Delta_K|}}\mathbb{N}\mathfrak{a} + O((\mathbb{N}\mathfrak{a})^{1-\frac{1}{n}}),$$

*where $H^0$ is as in Definition 3.10, $\Delta_K$ is as in Definition 2.5 and, as usual, the $O$ term denotes a function which grows slower than a constant times its argument.*

We should note that it is an easy exercise to show that the above theorem implies that the index of specialty vanishes very rapidly (exponentially). Thus this theorem may be appropriately viewed as an analogue of Riemann's contribution to the Riemann-Roch theorem.

We outline the proof of the Riemann-Roch theorem for number fields. There are four steps. The first two steps in proving this theorem are reductions, the third is to prove a theorem in Minkowski theory, and the fourth is to apply it.

*Step 1.* We have not yet defined the analogue of the divisor class group, but it is easy to do so. We simply let $P(\bar{\mathcal{O}}_K)$ be the image of div and define $C(\bar{\mathcal{O}}_K) = \mathrm{Div}(\bar{\mathcal{O}}_K)/P(\bar{\mathcal{O}}_K)$. The result is this.

**Proposition 3.13.** *The functions $\ell$ and* deg *factor through $C(\bar{\mathcal{O}}_K)$.*

*Step 2.* We have the following lemma.

**Lemma 3.14.** *Let $h = h_K$ be the class number of $K$ (Definition 2.10) and let $\mathfrak{a}_1, \dots, \mathfrak{a}_h$ be repesentatives for the ideal class group in $J(\mathcal{O}_K)$. Let $c > 0$ and*

$$\mathfrak{A}_i(c) = \left\{ \mathfrak{a} = \prod \mathfrak{p}^{n_\mathfrak{p}} \in J(\bar{\mathcal{O}}_K) \;\middle|\; \mathfrak{a}_\mathrm{f} = \mathfrak{a}_i,\ (n_\mathfrak{p})^{f_\mathfrak{p}} \le c(\mathbb{N}\mathfrak{a})^{f_\mathfrak{p}/n} \text{ for } \mathfrak{p}|\infty \right\}$$

*where $f_\mathfrak{p} = 1$ if $\mathfrak{p}$ is real or $f_\mathfrak{p} = 2$ if $\mathfrak{p}$ is complex. Then $c$ may be chosen so that*

$$J(\bar{\mathcal{O}}_K) = \bigcup_{i=1}^{h} \mathfrak{A}_i(c) P(\bar{\mathcal{O}}_K).$$

By definition of the ideal class group, the finite part of a replete ideal $\mathfrak{a}$ differs from one of the $\mathfrak{a}_i$'s by an element of $P(\bar{\mathcal{O}}_K)$. Once the finite part is fixed, however, one can only vary the infinite part of $\mathfrak{a}$ via multiplication by a unit. But units are ubiquitous; recall that (after applying log) they span a lattice in a hyperplane in $\mathbb{R}^{r+s}$. Hence we can bring (the logarithm of) the infinite part $\mathfrak{a}_\infty \in \mathbb{R}^{r+s}$ close to the origin, depending on how big it was to begin with. This tells us what our constant $c$ should be, and suffices to prove the lemma.

Note that we used the finiteness of the ideal class group and the unit theorem. One feature of the proof in Section 11 is that it does not use either of these theorems. In fact, the finiteness of the ideal class group, the unit theorem, and the Riemann-Roch theorem for number fields can all be shown to be consequences of the compactness of the norm-one idele class group.

*Step 3.* So it suffices to consider to consider $\mathfrak{a} \in \mathfrak{A}_i(c)$ as in the lemma. To estimate the norms (i.e., $\mathbb{N}$'s) of these replete ideals, one first makes the following definition.

We call a set $E \subset \mathbb{R}^n$ *$k$-Lipschitz parametrizable* if there are finitely many Lipschitz maps from the $k$-dimensional unit cube $I^k$ to $\mathbb{R}^n$ whose images cover $E$. The notion of Lipschitz is the usual one; a function $f$ between two metric spaces $(X, d) \to (X', d')$ is Lipschitz with Lipschitz constant $C$ if for all $x, y \in X$, we have

$$d'(f(x), f(y)) \le C d(x, y).$$

The theorem in Minkowski theory, due again to Lang, is this.

**Theorem 3.15.** *Let $D \subset \mathbb{R}^n$ be a bounded region and assume $\partial D$ is $(n-1)$-Lipschitz parametrizable. Let $\Lambda \subset \mathbb{R}^n$ be a lattice with fundamental parallelepiped $F$. For $t \in \mathbb{R}_{>0}$, let $N(t)$ be the number of lattice points of $\Lambda$ in $tD$. Then*

$$N(t) = \frac{\mathrm{Vol}(D)}{\mathrm{Vol}(F)} t^n + O(t^{n-1})$$

*In this case, the constant in the $O$ term depends on $D$, $\Lambda$, and the Lipschitz constants.*

*Step 4.* Finally, one completes the proof by showing that the conditions defining the sets $H^0(\mathfrak{a}^{-1})$ at the infinite places give rise to a region in $\mathbb{R}^n$ whose boundary is $(n-1)$-Lipschitz parametrizable. Here $\mathfrak{a} \in \mathfrak{A}_i(c)$. Our set $D$ will have volume $2^r(2\pi)^s$ because it is a product of $r$ intervals $[-1, 1]$ and $s$ unit discs. The fundamental parallelepiped will be that of the lattice defined by $\mathfrak{a}^{-1}$ and will have volume $\sqrt{|\Delta_K|}\mathbb{N}\mathfrak{a}^{-1}$. We then scale $\mathfrak{a}$ by $t^{1/n}$ at the infinite places.

# 4 Function Fields

We now discuss function fields, by which we will *not* mean the function fields of curves over an algebraically closed field, though these are related. Instead we will be referring to what are essentially the characteristic $p > 0$ analogues of number fields. In analogy with number fields we make the following definition.

**Definition 4.1.** A *function field* is a field which is isomorphic to a finite separable extension of the field of rational functions $\mathbb{F}_q(t)$ over the finite field of $q$ elements.

Here $q$ is a power of a prime $p$. One important difference (though there is a plethora of deep similarities!) between number fields and function fields is that function fields contain infinitely many subfields isomorphic to $\mathbb{F}_q(t)$, while number fields contain only one copy of $\mathbb{Q}$. Function fields also arise in the following way.

Let $X$ be a nonsingular curve over the algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$. We say $X$ is *defined over* $\mathbb{F}_q$ if it is the common zero locus in $\mathbb{P}^n$ of a set of homogeneous polynomials with coefficients in $\mathbb{F}_q$ (not in any bigger field).

Now the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ acts on $\mathbb{P}^n$ by acting on each coordinate. This is a well defined action. Assume $X$ is defined over $\mathbb{F}_q$. It follows that the action of the absolute Galois group on $\mathbb{P}^n$ induces an action on $X$.

If $X$ is defined over $\mathbb{F}_q$, then there is a unique subfield of $K \subset K(X)$ which is a function field, in the above sense, and for which $K \cap \bar{\mathbb{F}}_q = \mathbb{F}_q$. In fact,

**Proposition 4.2.** *Via the above construction, there is an equivalence of categories between:*

*(1) The category of nonsingular curves defined over $\mathbb{F}_q$ with morphisms nonconstant morphisms of curves commuting with the action of* $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$*; and*

*(2) The category of finitely, separably generated extensions $K$ of $\mathbb{F}_q$ of transcendence degree* 1 *such that $K \cap \bar{\mathbb{F}}_q = \mathbb{F}_q$, with morphisms homomorphisms of fields fixing $\mathbb{F}_q$.*

Let $K$ be a function field corresponding to a nonsingular curve $X$ defined over $\mathbb{F}_q$. Then the discrete valuation rings in $K$ with fraction field $K$ no longer correspond to points of $X$, but rather $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$-orbits of points in $X$. We call the discrete valuation rings of $K$ with fraction field $K$ the *primes* of $K$.

Recall that a discrete valuation ring $A$ is called so because it comes equipped with a *valuation,* i.e., a map $v : A\backslash\{0\} \to \mathbb{Z}$ such that $v(\alpha\beta) = v(\alpha) + v(\beta)$ and $v(\alpha + \beta) \geq \min\{\alpha, \beta\}$, for all $\alpha, \beta, \alpha + \beta \in A\backslash\{0\}$. The number $v(\alpha)$ is the power of a generator of the maximal ideal occuring in $\alpha$, which is independent of the choice of generator. The map $v$ extends by multiplicativity to the nonzero elements of the fraction field $K$ of $A$, and hence defines a homomorphism there.

When $K$ is a function field and $\mathfrak{p}$ is a prime of $K$, we let $q^f$ be the order of the residue field of $A$, which is a finite extension of $\mathbb{F}_q$. Let $v_\mathfrak{p}$ be the associated valuation on $K$ coming from $\mathfrak{p}$. Then $|\cdot|_\mathfrak{p} : K \to \mathbb{R}_{\geq 0}$ given by $|\alpha|_\mathfrak{p} = q^{-fv_\mathfrak{p}(\alpha)}$ and $|0|_\mathfrak{p} = 0$ is a non-archimedean absolute value on $K$. In fact, all nontrivial absolute values on $K$, up to equivalence, arise in this way. This is in perfect analogy with the $\mathfrak{p}$-adic absolute values on a number field. We denote the set of all nontrivial absolute values up to equivalence on $K$ by $V_K$. It is actually in bijection with the primes of $K$ via this construction.

Note that there are no archimedean absolute values on a function field. One justification

for this is that an absolute value on a field is non-archimedean if and only if the image of $\mathbb{Z}$ is bounded. But since a function field $K$ has positive characteristic, the image of $\mathbb{Z} \to K$ is finite, and so it is certainly bounded.

Let us describe the absolute values on the function field $K = \mathbb{F}_q(t)$. The corresponding nonsingular curve is $\mathbb{P}^1$. There is a subring $A = \mathbb{F}_q[t] \subset \mathbb{F}_q(t)$, which is the intersection of the ring of regular functions on $\mathbb{A}^1$ with $\mathbb{F}_q(t)$. The ring $A$ in $K$ is the analogue of the integers in $\mathbb{Q}$. It is a principal ideal domain, hence a unique factorization domain, and a prime ideal in $A$ is generated by an irreducible element which is unique up to multiplication by a unit.

Let $\mathfrak{p}$ be a prime ideal in $A$ with generator $\pi$. The localization $A_\mathfrak{p}$ is a discrete valuation ring with fraction field $K$ and maximal ideal generated by the element $\pi$. Let $n$ be the degree of $\pi$ as a polynomial. Then the residue field of $A_\mathfrak{p}$ is $\mathbb{F}_{q^n}$, the field with $q^n$ elements. Therefore we get the $\mathfrak{p}$-adic absolute value $|\cdot|_\mathfrak{p}$ on $K$ given by $|f\pi^r|_\mathfrak{p} = q^{-nr}$ if $f$ is a rational function with no power of $\pi$ in its numerator or denominator.

These give all of the absolute values coming from primes which do not correspond to the point at infinity on $\mathbb{P}^1$. The point at infinity is fixed by $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$, and its local ring, intersected with $K$, is $\mathbb{F}_q(t^{-1})_{(t^{-1})}$, the localization of the polynomial ring in $t^{-1}$ at the ideal generated by $t^{-1}$. We call this prime $\infty$. It gives the following valuation:

$$v_\infty(f/g) = \deg(g) - \deg(f),$$

and so

$$|f/g|_\infty = q^{\deg(f)-\deg(g)}.$$

We get the following analogue of Ostrowski's theorem.

**Theorem 4.3.** *Let $K$ be the function field $\mathbb{F}_q(t)$. Then $V_K$ is in natural bijection with the prime ideals of $\mathbb{F}_q[t]$ along with the absolute value $|\cdot|_\infty$ as above.*

Note that we have made no reference to the infinite absolute values on a general function field. This is because it depends on the choice of subfield isomorphic to $\mathbb{F}_q(t)$, as we will soon see. Even in the case $K = \mathbb{F}_q(t)$, we chose the subring $\mathbb{F}_q[t]$ in order to define the infinte absolute value, but we could have chosen a subring like $\mathbb{F}_q[t^{-1}]$ instead. We would then get a different infinite absolute value. By the way, the map given by $t \mapsto t^{-1}$ corresponds to an automorphism of $\mathbb{P}^1$, which does not fix $\infty$.

We now discuss extensions of function fields. In the number field case, the discussion depended heavily on the ring of integers. We have not defined the analogous construction for function fields, but this will not deter us from discussing ramification. Let us first explain why, however, we do not discuss the analogue of the ring of integers.

Let $K$ be a function field and choose a subfield $F$ isomorphic to $\mathbb{F}_q(t)$. In it, we have the subring $\mathbb{F}_q[t]$. This is a Dedekind domain, and its integral closure $\mathcal{O}$ in $K$ can be considered an analogue of the ring of integers of a number field. The infinite primes would then be those primes which are not localizations of $\mathcal{O}$. This depended on a choice of subring isomorphic to $\mathbb{F}_q[t]$. On the geometric side of the picture, this means we chose an open affine subset of the curve corresponding to the function field (which is fixed by $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$), and $\mathcal{O}$ is its ring of regular functions. Thus a ring of integers depends on an arbitrary choice, and this is why it is not considered here.

Now let $L/K$ be an extension of function fields. This corresponds to a nonconstant morphism of nonsingular curves $X \to Y$, where $X$ corresponds to $L$, and $Y$ to $K$. We say a prime $\mathfrak{P}$ of $L$ *lies over* a prime $\mathfrak{p}$ of $K$ if $\mathfrak{P} \cap K = \mathfrak{p}$. This would mean that the Galois orbit of points corresponding to $\mathfrak{P}$ has the Galois orbit corresponding to $\mathfrak{p}$ as its image under the given morphism. Since nonconstant morphisms of nonsingular curves are surjective, it follows that every prime $\mathfrak{p}$ of $K$ has a prime $\mathfrak{P}$ of $L$ lying above it.

Now restrict the valuation $v_{\mathfrak{P}}$ on $L$ coming from $\mathfrak{P}$, to a valuation on $K$. The image of $K$ under $v_{\mathfrak{P}}$ is a subgroup of $\mathbb{Z}$, hence is equal to $e\mathbb{Z}$ for some $e \geq 1$. This $e$ is the *ramification index* of $\mathfrak{P}$ over $\mathfrak{p}$. We should note that the analogue of this definition for number fields is equivalent to the definition we gave there of the ramification index.

Define the *inertia degree* of $\mathfrak{P}$ over $\mathfrak{p}$ to be the degree of the extension of the residue field of $\mathfrak{P}$ over the residue field of $\mathfrak{p}$. Then we have an analogue of Theorem 2.4.

**Theorem 4.4.** *Let $L/K$ be an extension of function fields, let $\mathfrak{p}$ be a prime of $K$, and let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be the primes of $L$ lying above $\mathfrak{p}$ (there are only finitely many). Let $e_i, f_i$ be, respectively, the ramification index and inertia degree of $\mathfrak{P}_i$ over $\mathfrak{p}$. Then*

$$\sum_{i=1}^{r} e_i f_i = n.$$

*If $L/K$ is moreover Galois, then the Galois group $\mathrm{Gal}(L/K)$ permutes the primes above $\mathfrak{p}$ transitively. Consequently, all of the ramification indices are equal, to $e$, say, and all of the inertia degrees are equal, to $f$, say, and hence*

$$ref = n.$$

Finally, let us discuss the divisor theory. Let $K$ be a function field. A *divisor* on $K$ is a formal sum of primes of $K$ with integer coefficients, and the set of all divisors is denoted $\mathrm{Div}(K)$. Let $X$ be the nonsingular curve corresponding to $K$. Since primes correspond to Galois orbits of points, $\mathrm{Div}(K)$ is isomorphic to the group of divisors in $\mathrm{Div}(X)$ which are fixed under the action of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. The isomorphism is given by mapping $\mathfrak{p}$ to the sum of all points in the corresponding Galois orbit, each with coefficient 1.

In $\mathrm{Div}(X)$ we have a notion of degree, and it is this notion of degree that we want to use on $\mathrm{Div}(K)$. Thus if $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p}$ is a divisor on $K$, we define its *degree* $\deg D$ not to be $\sum n_{\mathfrak{p}}$, but rather its degree when considered as a divisor on $X$. In other words, if $f_{\mathfrak{p}}$ is the number of points in the Galois orbit corresponding to the prime $\mathfrak{p}$, then we define $\deg \mathfrak{p} = f_{\mathfrak{p}}$.

It is equivalent to define $f_{\mathfrak{p}}$ to be the degree of the residue field of $\mathfrak{p}$ over $\mathbb{F}_q$. This should seem reasonable because in the case of $\mathbb{F}_q(t)$, if $\mathfrak{p}$ is a prime which comes from an irreducible polynomial $\pi$ of $\mathbb{F}_q[t]$, then the points of $\mathbb{A}^1 \subset \mathbb{P}^1$ to which $\mathfrak{p}$ corresponds will be exactly those points where $\pi$ vanishes. The number of such points is the number of roots of $\pi$, i.e., the degree of the extension $\mathbb{F}_q[t]/(\pi)$ over $\mathbb{F}_q$. Localizing at $(\pi)$ does not affect the residue field, so we see, at least in this case, that our two notions of $f_{\mathfrak{p}}$ correspond.

Now let $f \in K$. We define $\mathrm{div}(f) = \sum_{\mathfrak{p}} v_{\mathfrak{p}}(f)\mathfrak{p}$. The function div is a homomorphism $K^\times \to \mathrm{Div}(K)$. We get the following result.

**Theorem 4.5** (Product Formula)**.**

$$\deg \circ \mathrm{div} = 0.$$

We define $P(K)$ to be the image of div, and $\mathrm{Cl}(K) = \mathrm{Div}(K)/P(K)$. A warning to the reader: If $X$ is the nonsingular curve corresponding to $K$, it is *not* true that the group $\mathrm{Cl}(K)$ is the same as $\mathrm{Cl}(X)$.

The group $\mathrm{Cl}(K)$ is not quite the appropriate analogue of the ideal class group. Instead we do the following. By the product formula, the degree function deg factors through $\mathrm{Cl}(K)$. We define the group $\mathrm{Pic}(K)$ to be the subgroup of $\mathrm{Cl}(K)$ consisting of elements of degree 0. This is the appropriate analogue because:

**Theorem 4.6.** *The group* $\mathrm{Pic}(K)$ *is finite.*

Let $D \in \mathrm{Div}(K)$, $D = \sum n_{\mathfrak{p}}\mathfrak{p}$. Let

$$L(D) = \{f \in K^\times \mid v_{\mathfrak{p}}(f) \geq -n_{\mathfrak{p}} \text{ for all } \mathfrak{p}\}.$$

This is a finite dimensional $\mathbb{F}_q$-vector space, and we let $\ell(D)$ denote its dimension. The number $\ell(D)$ is independent of the class of $D$ in $\mathrm{Cl}(K)$. We have

**Theorem 4.7** (Riemann-Roch Theorem For Function Fields)**.** *Let $K$ be a function field. Then there is a divisor class $\mathcal{K} \in \mathrm{Cl}(K)$ such that for any $D \in \mathrm{Div}(K)$, we have*

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

*where $g = \ell(\mathcal{K})$ is called the* genus *of $K$.*

Any divisor in the class $\mathcal{K}$ above is called a *canonical divisor.* Actually, this terminology is the same in algebraic geometry; any divisor in the class $K$ from the Riemann-Roch theorem in Section 1 is called a canonical divisor.

In Section 10 we will prove the Riemann-Roch theorem for function fields using the methods of Tate's thesis, and obtain a description of the divisor class $\mathcal{K}$. It will turn out that $\mathcal{K}$ is the analogue of the different from algebraic number theory.

One last thing to mention is that there is not really a deep analogue of the unit theorem here. However, there is a nice way to say what the units are, as follows.

In algebraic number theory, it is not hard to prove that we have an exact sequence

$$0 \to \mathcal{O}_K^\times \to K^\times \to J(\mathcal{O}_K) \to C(\mathcal{O}_K) \to 0,$$

where $K$ is a number field. The analogue of this sequence, when $K$ is a function field, is

$$0 \to \mathbb{F}_q^\times \to K^\times \to \mathrm{Div}^\circ(K) \to \mathrm{Pic}(K) \to 0,$$

where $\mathrm{Div}^\circ(K)$ are the divisors of degree 0. Thus the units in this theory are $\mathbb{F}_q^\times$. Notice they are all roots of unity.

We did not mention this in Section 1, but for a nonsingular curve $X$ over an algebraically closed field $k$, the rational functions with no zeros or poles (i.e., those in $\ker \mathrm{div}$) are exactly the constants (i.e., the elements of $k^\times$). As one can see, it is the same way in the theory of function fields. When $K$ is a number field, the units are exactly those elements of $K^\times$ with all *finite* valuations zero. The roots of unity, on the other hand, are exactly those elements of $K^\times$ whose finite and infinite valuations are zero, the infinite valuations meaning the logarithms of the infinite absolute values. This leads to the philosophy that the roots of unity and zero play the role of constants in algebraic number theory. This is consistent with the philosophy of the "field with one element," which we will not go into here.

# 5 Local Fields

Since function fields and number fields are so similar, we bring them together in the following definition. A *global field* is either a number field or a function field.

To define a local field, we must first define the notion of *topological group*. A topological group is a group $G$ with a topology on it for which the multiplication $G \times G \to G$ is continuous in the product topology and the inversion $G \to G$ is continuous. For any $g \in G$, the map $x \mapsto gx$ is a homeomorphism, and so is the inversion, because these maps have obvious inverses which are also continuous. An isomorphism in this category is an isomorphism of groups which is also a homeomorphism. An example of a topological group is a field with an absolute value on it as in Section 3. The topology here is the metric topology induced by the absolute value.

To specify a base for the topology on a topological group, it is enough to specify a base about a single element because translation then gives a base everywhere. We will often specify a topology this way, and we will usually pick the identity as the element around which we specify the base.

**Definition 5.1.** A *local field* is a field $k$ which is locally compact as a topological field (so the multiplication and its inversion are continuous, as well as addition and its inversion) with a topology which is not discrete.

It turns out that the topology on a local field is always metric, and that a local field is complete with respect to this metric.

Now it happens that local fields are often the best tools at hand to study the local properties of global fields. Every local field comes from a global field through a process which we now describe.

Let $k$ be a field equipped with a nontrivial absolute value $|\cdot|$. We define the *completion* $\hat{k}$ as follows. Let $R$ be the ring of Cauchy sequences in $k$, in the usual sense, i.e., a sequence $\{x_n\}$ in $k$ is Cauchy if for every $\epsilon > 0$, there is an $N$ such that $n, m > N$ implies $|x_n - x_m| < \epsilon$. The addition and multiplication on $R$ are component-wise. Let $M \subset R$ be the ideal of all sequences in $R$ which converge to 0. Then $M$ is maximal and we let $\hat{k}$ be the field $R/M$. The field $k$ injects into $\hat{k}$ by assigning to any element $x \in k$ the constant sequence $\{x\}$. The underlying set of $\hat{k}$ is the completion of $k$ in the sense of metric topology, essentially by definition. Hence we get a metric on $\hat{k}$ which agrees with the metric on $k$. The metric topology makes the additive group of $\hat{k}$ a topological group, and is induced by an absolute value which extends the one on $k$. The image in $\mathbb{R}_{\geq 0}$ of the absolute value on $\hat{k}$ is the closure of the image of the absolute value on $k$.

The first examples of local fields are $\mathbb{R}$ and $\mathbb{C}$. These are the completions of number fields at the infinite absolute values. The next examples are the $p$-adic numbers and their finite extensions: The field $\mathbb{Q}_p$ of *$p$-adic numbers* is the completion of $\mathbb{Q}$ with respect to the $p$-adic absolute value. Elements of $\mathbb{Q}_p$ may be written formally as Laurent series in the variable $p$,

$$\alpha = \sum_{i=-n}^{\infty} a_i p^i, \qquad a_i \in \{0, 1, \ldots, p-1\}.$$

In this representation, addition and multiplication are given by carrying as in base $p$ arithmetic. The absolute value of an element $\alpha = \sum a_i p^i \in \mathbb{Q}_p$ is $p^n$ where $-n$ is the smallest

index $i$ for which $a_i \neq 0$.

More generally, we can complete any global field with respect to an absolute value on it. The completion does not depend on the equivalence class of the absolute value, so we can speak of completing a global field $K$ *at a place* of $K$. Recall that a place is just an equivalence class of an absolute value; these were classified for number fields in Theorem 3.3 and for function fields, they all came from primes.

Completing a number field $K$ at a finite place corresponding to a prime $\mathfrak{p}$ of $K$ gives rise to a finite extension field $K_\mathfrak{p}$ of $\mathbb{Q}_p$, where $p$ is the prime in $\mathbb{Z}$ over which $\mathfrak{p}$ lies. The field $K_\mathfrak{p}$ is called the field of $\mathfrak{p}$-*adic numbers.* The degree $[K_\mathfrak{p} : \mathbb{Q}_p]$ is $ef$, where $e$ is the ramification index of $\mathfrak{p}$ over $p$ and $f$ is the inertia degree. This will be explained later in this section. In particular, $[K_\mathfrak{p} : \mathbb{Q}_p] \leq [K : \mathbb{Q}]$.

The field $K_\mathfrak{p}$ has a canonical subring $\mathcal{O}_\mathfrak{p}$, which is the maximal subring with respect to the property of being compact. It is also the set of elements $\alpha \in K_\mathfrak{p}$ with $|\alpha| \leq 1$. This is a ring because the absolute value on $K_\mathfrak{p}$ is still non-archimedean. It is also the topological closure of $\mathcal{O}_K$ in $K_\mathfrak{p}$, and $\mathcal{O}_\mathfrak{p} \cap K$ is the localization $(\mathcal{O}_K)_\mathfrak{p}$ of $\mathcal{O}_K$ at the prime $\mathfrak{p}$. Thus we see that the field $K_\mathfrak{p}$ focuses in on the structure of $K$ about the prime $\mathfrak{p}$. This is exactly why $K_\mathfrak{p}$ is viewed as a local construction.

Now $\mathcal{O}_\mathfrak{p}$ is a Dedekind domain which is local, and hence it is a discrete valuation ring. We therefore call $\mathcal{O}_\mathfrak{p}$ the *valuation ring of* $K_\mathfrak{p}$. The valuation ring of $\mathbb{Q}_p$ is called the ring of $p$-*adic integers,* and is denoted $\mathbb{Z}_p$. The valuation ring of $K_\mathfrak{p}$ is essentially a local analogue of the ring of integers in $K$. In fact, if $\mathfrak{p}$ lies over $p$, then $\mathcal{O}_\mathfrak{p}$ is the integral closure of $\mathbb{Z}_p$ in $K_\mathfrak{p}$.

Now if $K$ is a function field, there is very little difference in the discussion. If we complete $K$ with respect to an absolute value corresponding to the prime $\mathfrak{p}$, we get a non-archimedean local field $K_\mathfrak{p}$. In the case of $\mathbb{F}_q(t)$, if we complete with respect to the place coming from the ideal $(t) \subset \mathbb{F}_q[t]$, we obtain the field $\mathbb{F}_q((t))$ of Laurent series over $\mathbb{F}_q$ (with the usual addition and multiplication). The absolute value here is the one which assigns to a series $\sum a_i t^i$ the value $q^n$ where $-n$ is the smallest index $i$ for which $a_i \neq 0$.

The properties above for $\mathfrak{p}$-adic fields carry over to the completions of function fields. Let $K$ be a function field and $\mathfrak{p}$ a prime of $K$. Then: $K_\mathfrak{p}$ is an extension of a completion of $\mathbb{F}_q(t)$ at the prime over which $\mathfrak{p}$ lies, of degree the ramification index multiplied by the inertia degree; the subring of elements of absolute value at most 1 form a maximal compact subring $\mathcal{O}_\mathfrak{p}$ of $K_\mathfrak{p}$, called the *valuation ring;* and the ring $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring and is the integral closure of the valuation ring of the completion of $\mathbb{F}_q(t)$ at the prime over which $\mathfrak{p}$ lies.

Now we have the following classification.

**Theorem 5.2.** *Let $k$ be a local field. Then either:*
*(1) [Archimedean case] $k = \mathbb{R}$ or $k = \mathbb{C}$ with the usual topology;*
*(2) [Non-archimedean case,* $\operatorname{char} k = 0$*] $k$ is a finite extension of $\mathbb{Q}_p$; or*
*(3) [Non-archimedean case,* $\operatorname{char} k > 0$*] $k$ is a finite separable extension of $\mathbb{F}_q((t))$.*
*Every local field arises as a completion of a global field.*

Let us briefly discuss the topology of non-archimedean local fields. Let $k$ be a non-archimedean local field, with valuation ring $\mathcal{O}$ and prime $\mathfrak{p}$, i.e., $\mathfrak{p}$ is the maximal ideal in $\mathcal{O}$. The subgroup $\mathcal{O}$ is both open and closed, as is any fractional ideal. A base of

neighborhoods about 0 is given by $\mathfrak{p}^n$, $n \in \mathbb{N}$.

The group $k^\times$ will also be important for us. It is also a locally compact abelian group, but under multiplication. A base of neighborhoods about 1 is given by $1 + \mathfrak{p}^n$, $n \in \mathbb{N}$. This base is contained in the units $\mathcal{O}^\times$, which consists of all elements of absolute value 1.

The next proposition gives a description of $\mathcal{O}$ which shows that its topology is very close to discrete. It says, in fact, that $\mathcal{O}$ is profinite, but we will not go into this.

**Proposition 5.3.** *The valuation ring $\mathcal{O}$ in a non-archimedean local field $k$ is the inverse limit, both algebraically and topologically, of the groups $\mathcal{O}/\mathfrak{p}^n$, $n \geq 1$, where $\mathfrak{p}$ is the prime of $\mathcal{O}$. Here, the groups $\mathcal{O}/\mathfrak{p}^n$ are given the discrete topology, and the maps between them are the projections. Symbolically,*

$$\mathcal{O} \cong \varprojlim_{n \in \mathbb{N}} \mathcal{O}/\mathfrak{p}^n.$$

Let $l/k$ be an extension of non-archimedean local fields, with respective valuation rings $\mathcal{O}_l$ and $\mathcal{O}_k$, with, respectively, primes $\mathfrak{p}_l$ and $\mathfrak{p}_k$. Since $\mathcal{O}_l$ is the integral closure of $\mathcal{O}_k$ in $l$, we can apply our theory of ramification, because the valuation rings are, of course, Dedekind. Since there is only one prime, the degree of the extension is the ramification degree multiplied by the inertia degree of the prime extension $\mathfrak{p}_l/\mathfrak{p}_k$.

If $L/K$ is an extension of global fields and $\mathfrak{q}$ is a prime of $L$ lying over a prime $\mathfrak{p}$ of $K$, then $L_\mathfrak{q}$ is naturally an extension of $K_\mathfrak{p}$, and the extension of primes in the local case has the same ramification index and inertia degree as that in the global case. Thus one can learn information about extensions of global fields by patching together local information.

Important for us will be the *local different*. It is defined just as in the global case:

**Definition 5.4.** If $l/k$ is an extension of non-archimedean local fields, then the *local different* $\mathfrak{D}_{l/k}$ of $l/k$ is defined by

$$\mathfrak{D}_{l/k} = \mathfrak{C}_{l/k}^{-1},$$

where

$$\mathfrak{C}_{l/k} = \{a \in l \mid \mathrm{Tr}_{l/k}(a) \in \mathcal{O}_k\}.$$

The local different is an ideal of $\mathcal{O}_l$.

The local differents patch together to give the global different. More precisely, if $L/K$ is an extension of number fields, and $\mathfrak{q}/\mathfrak{p}$ is an extension of primes in $L/K$, then the power of the prime of $L_\mathfrak{q}$ occuring in the local different is exactly the power of $\mathfrak{q}$ occuring in the global different. In fact, one can prove that the global different measures ramification, as in Theorem 2.7, by first proving it in the local case and then patching together the results.

Now no discussion of local fields will be complete without mentioning *Hensel's lemma.* This result is about the nice behavior of polynomials in non-archimedean local fields, and is often a good reason to reduce to the local case. Although we will not use it directly in any of our discussion, it should be noted that some of the results we have mentioned so far use Hensel's Lemma in their proof.

**Theorem 5.5** (Hensel's Lemma)**.** *Let $k$ be a non-archimedean local field with valuation ring $\mathcal{O}$ and prime $\mathfrak{p}$. Let $f$ be a polynomial in $\mathcal{O}[x]$, and let $\bar{f}$ be the reduction of $f$ modulo $\mathfrak{p}$ (i.e., reduce its coefficients modulo $\mathfrak{p}$). Assume $\alpha$ is a root of $\bar{f}$, and that $\bar{f}'(\alpha) \neq 0$, where the prime denotes the formal derivative. Then $f$ has a root which, moreover, is congruent to $\alpha$ modulo $\mathfrak{p}$.*

# 6 Adeles and Ideles

The adeles will be, very directly, a patching-together of local information about a global field at all of its places. Let us give the definition.

Let $K$ be a global field. As is customary, we will denote a general element of the set $V_K$ of all places of $K$ with the letter $v$, instead of the $\mathfrak{p}$ we used before, and so the completion of $K$ at a place $v$ will be denoted $K_v$. The *adeles* of $K$ are the set

$$\mathbb{A}_K = \left\{ (\alpha_v) \in \prod_{v \in V_K} K_v \;\middle|\; \alpha_v \in \mathcal{O}_v \text{ for all but finitely many } v \right\}.$$

They become a ring under component-wise addition and multiplication, and are thus a subring of the direct product of all of the completions of $K$. In fact, they become a topological group (additively) when we declare a base of neighborhoods about 0 to be

$$\left\{ \prod_{v \in V_K} U_v \;\middle|\; U_v \text{ open in } K_v,\, 0 \in U_v,\, U_v = \mathcal{O}_v \text{ for all but finitely many } v \right\}.$$

It should be noted that the condition "$U_v = \mathcal{O}_v$" is vacuous at the infinite places of a number field.

The *ideles* $\mathbb{I}_K$ are the units of $\mathbb{A}_K$. Alternatively they are defined by

$$\mathbb{I}_K = \left\{ (\alpha_v) \in \prod_{v \in V_K} K_v^\times \;\middle|\; \alpha_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v \right\}.$$

They are turned into a topological group by declaring a base of neighborhoods about 1 to be

$$\left\{ \prod_{v \in V_K} U_v \;\middle|\; U_v \text{ open in } K_v^\times,\, 1 \in U_v,\, U_v = \mathcal{O}_v^\times \text{ for all but finitely many } v \right\}.$$

Please note that this is *not* the subspace topology for the ideles as a subset of $\mathbb{A}_K$.

As with the local case, both the adeles and ideles are locally compact topological groups. This is easy to see using Tychonoff's theorem.

Hopefully we can give some intuition about these definitions as follows. The adeles function are a global analogue of the notion of local field, since we stuck together all the local fields associated to a global field in order to define them. A general element of the adeles is a vector $(a_{v_1}, a_{v_2}, \dots)$ where $v_1, v_2, \dots$ is an ordering of the elements of $V_K$ and $a_{v_i} \in K_{v_i}$. These vectors are subject to a global condition that all but finitely many of the $a_{v_i}$ must be integral, i.e., in $\mathcal{O}_{v_i}$. Tate called adeles "valuation vectors" in his thesis before the term "adele" was modernized. This is a nice and lucid description for the adeles. As a matter of notation, if $K$ is a number field, we think of these vectors as containing first the entries at the finite places, and then the entries at the infinite places come at the end. For instance, $(1/2, 1/3, 0, 0, 0, \dots, \pi^2/6)$ is an adele of $\mathbb{Q}$. The topology on the adeles gives

$$\prod_{v \in V_\mathrm{f}} \mathcal{O}_v \times \prod_{V \in V_\infty} K_v \subset \mathbb{A}_K$$

the product topology.

The ideles are named so because, for a number field $K$, they are a natural "thickening" of the fractional *ideals* (in fact, the replete ideals) of $K$. We will see how this is so at the end of this section.

In practice, it is often wise to be careful when thinking about the adeles $\mathbb{A}_K$ to distinguish between the case of $K$ a number field and of $K$ a function field. This is because there is an archimedean part when $K$ is a number field which will often make computations different. For instance, in reference to an earlier remark, when mimicking Tate's thesis for function fields, the problem of finding the residues of the poles of certain zeta functions comes down to a volume computation in the ideles which is considerably easier in the function field case than in the number field case.

Adelic methods are often the correct ones for working globally. As an illustration of this, we will use the ideles to prove the finiteness of the class number. A proof of the unit theorem can also be given like this without too much effort. First we need some theorems on the topology of the adeles and ideles.

Now there is an embedding $K \hookrightarrow \mathbb{A}_K$ which is the diagonal embedding, i.e., $\alpha \in K$ maps to the adele with $\alpha$ at all components. It is well defined because only finitely many valuations of an element in $K$ are negative. Restricting this to $K^\times$ gives an embedding $K^\times \hookrightarrow \mathbb{I}_K$. In fact, $K^\times$ lands in a certain subgroup of $\mathbb{I}_K$ described as follows.

For $v \in V_K$, let $\|\cdot\|_v$ denote the canonical absolute value corresponding to $v$ if $v$ is not complex, and let it denote the square of the canonical absolute value if $v$ is complex. For an idele $a = (\alpha_v) \in \mathbb{I}_K$, we let

$$\|a\| = \prod_{v \in V_K} \|\alpha_v\|_v.$$

This product is well defined because almost all of the terms $\|a_v\|_v$ are 1, and it defines a homomorphism $\mathbb{I}_K \to \mathbb{R}_{>0}$. We call $\|a\|$ the *norm* of the idele $a$. Define $\mathbb{I}_K^1$ to be the subgroup of $\mathbb{I}_K$ of all ideles of norm 1. We have the following variant of the product formula.

**Theorem 6.1** (Product Formula, Adelic)**.** *The image of $K^\times$ under the embedding $K^\times \hookrightarrow \mathbb{I}_K$ above, is in $\mathbb{I}_K^1$.*

We also have the following compactness theorem.

**Theorem 6.2.** *The group $K$ is discrete in $\mathbb{A}_K$ and the quotient $\mathbb{A}_K/K$, under the quotient topology, is compact.*

*The group $K^\times$ is discrete in $\mathbb{I}_K^1$ and the quotient $\mathbb{I}_K^1/K^\times$, under the quotient topology, is compact.*

Let $K$ be a number field, so that we have archimedean absolute values. We said above that the ideles are a thickening of the fractional ideals. This is how: We can define a surjective homomorphism $p : \mathbb{I}_K^1 \to J(\mathcal{O}_K)$ by

$$(x_v) \mapsto \prod_{v \nmid \infty} \mathfrak{p}_v^{v_{\mathfrak{p}_v}(x_v)},$$

where $\mathfrak{p}_v$ is the prime associated to $v \in V_K$. The kernel is the set of all ideles whose finite components all have absolute value 1. We denote this set $\mathbb{I}_\infty^1$. This subgroup is open since,

at the finite places, it is the product of the open sets $\mathcal{O}_v$. The quotient $\mathbb{I}_K^1/\mathbb{I}_\infty^1$ is therefore discrete since the quotient of a topological group by an open subgroup is discrete.

We can also pass to the quotient $C(\mathcal{O}_K)$, and the kernel of $\mathbb{I}_K^1 \to C(\mathcal{O}_K)$ is thus $\mathbb{I}_\infty^1 \cdot K^\times$. Hence we obtain an isomorphism $\mathbb{I}_K^1/\mathbb{I}_\infty^1 \cdot K^\times \cong C(\mathcal{O}_K)$. The group $\mathbb{I}_K^1/\mathbb{I}_\infty^1 \cdot K^\times$ is discrete since $\mathbb{I}_K^1/\mathbb{I}_\infty^1$ is, and it is compact since $\mathbb{I}_K^1/K^\times$ is. Therefore it is finite, thus proving that the ideal class group is finite!

This concludes the first half of this paper. We will now incorporate abstract Fourier analysis into the picture in a serious way. This is what John Tate did in his famous 1950 thesis, which can be found in Cassels and Fröhlich [1], where it was first published (in 1967). He reproved the analytic continuation of certain zeta functions in a manner which is perhaps best described as extremely local-to-global. However, we will use his methods to reprove the Riemann-Roch theorem for number fields, and we will not touch upon the theory of zeta functions.

# 7 Abstract Harmonic Analysis

The purpose of this section is to describe the basic theory of abstract harmonic analysis on locally compact abelian groups.

We begin by recalling a fundamental result from the theory of Borel measures on locally compact spaces.

**Theorem 7.1** (Riesz Representation Theorem)**.** *Let $X$ be a locally compact Hausdorff topological space and $L$ a positive linear functional on the space $C_c(X, \mathbb{R})$ of continuous complex-valued functions with compact support on $X$. Then there is a unique regular Borel measure $\mu$ such that the functional $L$ is given by*

$$Lf = \int_X f(x)\, d\mu(x).$$

This is basic to abstract measure theory.

We will care only about measures on locally compact abelian groups $G$ ($G$ will always be Hausdorff). On these groups, there is one particular kind of measure which is extremely important.

Let $G$ be a locally compact abelian group. A regular Borel measure $\mu$ on $G$ is called a *Haar measure* if it is translation invariant, i.e. $\mu(x + E) = \mu(E)$ for all measurable $E$ and all $x \in G$. Here $x + E = \{x + y \mid y \in E\}$.

One example is the Lebesgue measure on $\mathbb{R}$ or $\mathbb{C}$. The first result on Haar measures is the following.

**Theorem 7.2.** *Let $G$ be a locally compact abelian group. Then there exists a Haar measure $\mu$ on $G$ which is as unique as possible, in the following sense: If $\nu$ denotes another Haar measure on $G$, then there is a positive constant $c$ such that $\nu = c\mu$.*

One proves the theorem by constructing a positive linear functional on $C_c(G)$ which is invariant under translation by elements of $G$. Often, we will specify a Haar measure on a specific group $G$ explicitly, and by this theorem, it will be unique up to scaling.

**Proposition 7.3.** *Let $G_1, \ldots, G_n$ be locally compact abelian groups with Haar measures $\mu_1, \ldots \mu_n$ respectively. Then the product measure $\mu_1 \times \cdots \times \mu_n$ is a Haar measure on $G_1 \times \cdots \times G_n$ with the product topology (under which $G_1 \times \cdots \times G_n$ is locally compact by Tychonoff's theorem). Note that in this case, the product measure will be characterized by the formula*

$$\mu_1 \times \cdots \times \mu_n(K_1 \times \cdots \times K_n) = \mu_1(K_1) \cdots \mu_n(K_n)$$

*for compacts $K_i \subset G_i$ (because the Haar measure is regular). The analogous statement holds for infinite products, as long as all but finitely many terms are compact with total measure* 1*.*

Now we construct the Pontryagin dual of a locally compact abelian group. Let $T$ denote the unit circle in $\mathbb{C}$, which we will consider with its usual topology. Fix a locally compact abelian group $G$ with Haar measure $\mu(x)$ (often we will write $dx$ instead), and write

$$\widehat{G} = \{\xi : G \to T \mid \xi \text{ is a continuous homomorphism}\}.$$

Then $\widehat{G}$ is a group, called the *Pontryagin dual,* or simply the *dual* of $G$. Its elements are called *(unitary) characters* of $G$. We give $\widehat{G}$ a topology as follows. Let $K \subset G$ be compact and $U \subset T$ open. Let $B(K, U)$ be the set of all elements of $\widehat{G}$ for which $f(K) \subset U$. Then we declare the topology on $G$ is the one which has a subbase consisting of all $B(K, U)$ as $K$ varies over compacts in $K$ and $U$ over opens in $T$. In other words, we give $\widehat{G}$ the compact-open topology.

Another way to describe this topology is as follows. Let $\{f_\alpha\}$ be a net in $\widehat{G}$. Then $\{f_\alpha\}$ converges to $f \in \widehat{G}$ if and only if these functions converge uniformly to $f$ on compact subsets of $G$.

**Proposition 7.4.** *Let $G$ be a locally compact abelian group. Then $\widehat{G}$ is also a locally compact abelian group.*

We give some propositions concerning the behavior of this group.

**Proposition 7.5** (Orthogonality Relation)**.** *Assume $G$ is compact with Haar measure $\mu = dx$. If $\xi \in \widehat{G}$ and $\xi \neq \mathrm{id}$, then*

$$\int_G \xi(x)\, dx = 0.$$

*Otherwise, if $\xi = \mathrm{id}$, then of course, this integral equals $\mu(G)$.*

**Proposition 7.6.** *If $G$ is compact, then $\widehat{G}$ is discrete, and vice-versa; if $G$ is discrete, then $\widehat{G}$ is compact.*

**Proposition 7.7.** *Let $G_1, \ldots, G_n$ be locally compact abelian groups, and let $G$ be the product $G = G_1 \times \cdots \times G_n$ with the product topology. Then*

$$\widehat{G} \cong \widehat{G}_1 \times \ldots \times \widehat{G}_n,$$

*the isomorphism being one of topological groups.*

One may also develop a theory for arbitrary products of compact groups. We will not do this since we do not need that theory. However, we will develop the theory for *restricted direct products* in Section 9.

Next we discuss the Fourier analysis on locally compact abelian groups. Let $G$ be a locally compact abelian group. For $f \in L^1(G)$, we define a function $\hat{f}$ on $\widehat{G}$ by

$$\hat{f}(\xi) = \int_G f(x)\overline{\xi}(x)\,dx.$$

(Note that the complex conjugate $\overline{\xi}$ is the multiplicative inverse of $\xi$). This is called the *Fourier transform* of $f$, and it is the analogue in this theory of the classical Fourier transform. Actually, it specializes to the classical Fourier transform, for in fact, $\mathbb{R} \cong \widehat{\mathbb{R}}$ via the map $x \mapsto (y \mapsto e^{-2\pi ixy})$, which therefore gives

$$\hat{f}(y) = \int_{\mathbb{R}} f(x)e^{2\pi ixy}\,dx.$$

The main result on the Fourier transform is as follows.

**Theorem 7.8** (Fourier Inversion Theorem)**.** *For $f \in L^1(G)$ and $\hat{f} \in L^1(\widehat{G})$, there is a Haar measure $d\xi$ on $\widehat{G}$ such that*

$$f(x) = \int_{\widehat{G}} \xi(x)\hat{f}(\xi)\,d\xi.$$

One uses this to prove the following theorem.

**Theorem 7.9** (Pontryagin Duality)**.** *The dual of $\widehat{G}$ is topologically isomorphic to $G$ via the map*

$$x \mapsto (\xi \mapsto \xi(x)) : G \to \widehat{\widehat{G}}.$$

Finally, let us discuss the analogue of the Poisson summation formula.

First, for $G$ a locally compact abelian group and $H$ a closed subgroup, define

$$H^\perp = \{\xi \in \widehat{G} \mid \xi(x) = 1 \text{ for all } x \in H\}.$$

**Proposition 7.10.** *(a) $H^\perp$ is a closed subgroup of $\widehat{G}$;*

*(b) If $G$ is identified with its double dual under Pontryagin duality, then $(H^\perp)^\perp = H$;*

*(c) Let $\pi : G \to G/H$ be the projection. Define $\Phi : (G/H)\widehat{\ } \to H^\perp$ by $\eta \mapsto \eta \circ \pi$. Then $\Phi$ is well defined and an isomorphism of topological groups;*

*(d) Let $[\xi]$ denote the class of $\xi$ in $\widehat{G}/H^\perp$. Define $\Psi : \widehat{G}/H^\perp \to \widehat{H}$ by $[\xi] \mapsto \xi|_H$. Then $\Psi$ is well defined and an isomorphism of topological groups.*

**Theorem 7.11** (Poisson Summation Formula)**.** *Let $H$ be a closed subgroup of $G$. Assume $f$ is continuous and in $L^1(G)$ and $\hat{f} \in L^1(H^\perp)$. Assume further that the integral $\int_H f(x+y)\,dy$ converges absolutely and uniformly (in the obvious sense) on some compact subset containing $x \in G$. Then, with appropriate Haar measures, we have*

$$\int_H f(x+y)\,dy = \int_{H^\perp} \hat{f}(\xi)\xi(x)d\xi.$$

The proof is a nice exercise using the Fourier inversion theorem. One first proves it for $f \in C_c(G)$ and then reduces to this case.

As an example, consider $G = \mathbb{R}$ and $H = \mathbb{Z}$ (the latter with the discrete topology). We also identify $\mathbb{R}$ with its dual as above. Give $\mathbb{Z}$ the counting measure, which is a Haar measure because $\mathbb{Z}$ is discrete. Then we have that $\mathbb{Z}^\perp = \mathbb{Z}$ under this identification, and the formula says

$$\sum_{n\in\mathbb{Z}} f(x+n) = \sum_{n\in\mathbb{Z}} \hat{f}(n)e^{2\pi inx}.$$

This is what is classically called the Poisson summation formula.

Finally, let us set some notation. Following Lang, we denote by $\mathrm{Inv}(G)$ the set of all complex valued functions $f$ on $G$ which are continuous and in $L^1(G)$, and such that $\hat{f}$ is continuous and in $L^1(\widehat{G})$. In particular, any $f \in \mathrm{Inv}(G)$ satisfies the hypotheses of the Fourier inversion theorem. Finally, we always take the Haar measures on $G$ and $\widehat{G}$ to be *self-dual,* i.e., the Haar measure on $\widehat{G}$ must make the Fourier inversion theorem hold given the choice of Haar measure on $G$.

# 8 Analysis On Local Fields

Throughout this section, $k$ will denote a local field. Then $k$ and $k^\times$ are locally compact abelian groups, the first one under addition and the second one under multiplication. We define a character on $k$, which we will call the *standard character.*

Assume first that $k = \mathbb{Q}_p$. Write $\alpha \in \mathbb{Q}_p$ as $\alpha = \sum_{i=-n}^{\infty} a_i p^i$. Define a map $\lambda : \mathbb{Q}_p \to \mathbb{R}/\mathbb{Z}$ as follows. We map $\alpha$ to $\sum_{i=-n}^{-1} a_i p^i$, this finite sum being taken in the rational numbers, viewing $p \in \mathbb{Q}$. This obviously defines an additive homomorphism $\mathbb{Q}_p \to \mathbb{Q}/\mathbb{Z}$, which we take to be $\lambda$. Note that it is trivial on $\mathbb{Z}_p$. Then we define $\psi = e^{2\pi i\lambda}$.

If $k = \mathbb{F}_p((t))$, we define a very similar map $\lambda$, given by $\sum_{i=-n}^{\infty} a_i t^i \mapsto \sum_{i=-n}^{-1} a_i p^i$, the field $\mathbb{F}_p$ being identified with the set $\{0, 1, \ldots, p-1\}$. Then $\psi$ is again $e^{2\pi i\lambda}$.

If $k = \mathbb{R}$ then we define $\psi(\alpha) = e^{-2\pi i\alpha}$.

Any local field is a finite (separable) extension of these three fields above. With this in mind, for $k$ a general local field, define $\psi(\cdot) = \psi_0(\mathrm{Tr}(\cdot))$, where $k_0$ is a choice of subfield isomorphic to $\mathbb{Q}_p$, $\mathbb{F}_p((t))$, or $\mathbb{R}$, $\psi_0$ is the standard character on $k_0$, and the trace Tr is taken over the extension $k/k_0$. For instance, the standard character on $\mathbb{C}$ becomes $\psi(\alpha) = e^{-4\pi i\Re(\alpha)}$. Also, note that the kernel of the standard character in the non-archimedean case is the set of all $\alpha \in k$ such that $\mathrm{Tr}(\alpha)$ is in the valuation ring of $k_0$. By definition, this set is precisely the local inverse different $\mathfrak{D}^{-1}$.

For any $\alpha \in k$, the map $\beta \mapsto \psi(\alpha\beta)$ is also a character on $k$. In fact, this construction gives the following duality.

**Theorem 8.1.** *Let $k$ be a local field and $\psi$ the standard character on $k$. Then there is a topological isomorphism $k \cong \hat{k}$ via $\alpha \mapsto (\beta \mapsto \psi(\alpha\beta))$.*

This theorem is also true if $\psi$ is replaced by any other nontrivial character on $k$.

A notation which we will use frequently is as follows. Let $k$ be non-archimedean. The function $\mathbb{N}$ on fractional ideals of $k$ is defined on the prime $\mathfrak{p}$ of the valuation ring $\mathcal{O}$ by $\mathbb{N}\mathfrak{p} = |\mathcal{O}/\mathfrak{p}|$, and then extended by linearity to all fractional ideals (which are just the

integer powers of $\mathfrak{p}$). This is analogous to the definition for number fields given in Section 2.8

Now we choose a Haar measure $\mu$ on the local field $k$. If $k = \mathbb{R}$, then we choose $\mu$ to be the Lebesgue measure. If $k = \mathbb{C}$, then we choose $\mu$ to be twice the Lebesgue measure (which gives the unit disc measure $2\pi$; this will be important later). If $k$ is non-archimedean, we choose $\mu$ to be such that the valuation ring $\mathcal{O}$ in $k$ has measure $\mu(\mathcal{O}) = (\mathbb{N}\mathfrak{D})^{-1/2}$. Note that the measure of $\mathcal{O}$ determines the Haar measure $\mu$ as follows. Let $\mathfrak{p} \subset \mathcal{O}$ be the prime. The open sets $\mathfrak{p}^m$ for $m \geq 0$ form a base of neighborhoods about 0. Let $\{\alpha\}$ be a set of representatives for $\mathcal{O}/\mathfrak{p}^m$. Then $\mathcal{O}$ is the disjoint union of $(\mathbb{N}\mathfrak{p})^m$ open balls of radius $(\mathbb{N}\mathfrak{p})^{-m}$, namely the sets $\alpha + \mathfrak{p}^m$. Hence the open balls of radius $(\mathbb{N}\mathfrak{p})^{-m}$ have measure $(\mathbb{N}\mathfrak{p})^{-m}(\mathbb{N}\mathfrak{D})^{-1/2}$.

Our choice of Haar measure $\mu$ is reasonable because it is the one which is self-dual:

**Proposition 8.2.** *The measure $\mu$ above is such that $\mu$ is self-dual, considered as a measure both on $k$ and $\hat{k}$, where $\hat{k}$ is identified with $k$ as in the previous theorem. In particular, if $\psi$ is the standard character, if $f \in \mathrm{Inv}(k)$, and $\hat{f}$ is the Fourier transform of $f$ with respect to $\psi$, then*

$$\hat{\hat{f}}(x) = f(-x).$$

For completeness, we briefly discuss Haar measure on $k^\times$. Let $dx$ be a Haar measure on the additive group $k$. If $k$ is archimedean, define

$$d^\times x = \frac{dx}{\|x\|},$$

and if $k$ is non-archimedean, define

$$d^\times x = \frac{\mathbb{N}\mathfrak{p}}{\mathbb{N}\mathfrak{p} - 1}\frac{dx}{\|x\|}.$$

Recall that $\|\cdot\|$ is the usual absolute value unless $k = \mathbb{C}$, in which case it is the square of the usual absolute value.

The measure $d^\times x$ is a Haar measure on $k^\times$, and we have

**Proposition 8.3.** *If $k$ is a non-archimedean local field, then*

$$\int_{\mathcal{O}^\times} d^\times x = (\mathbb{N}\mathfrak{D})^{-1/2}.$$

Thus $\mathcal{O}^\times$ gets the same measure in $k^\times$ as $\mathcal{O}$ does in $k$.

# 9 Analysis On Adeles and Ideles

Now we patch together the local results of the previous section into something global. It is convenient to introduce the following general concept.

Consider the following set-up: The set $\{v\}$ is a set of indices, $G_v$ are locally compact abelian groups indexed by the $v$'s, and $H_v \subset G_v$ is an open compact (hence also closed) subgroup, one for all but finitely many $v$. The set of such $v$ for which $G_v$ does not have

a specified open compact subgroup like this, is denoted $S_\infty$. Then we define the restricted direct product of the $G_v$'s with respect to the $H_v$'s, as a group, to be

$$G = \prod_v{}' G_v = \left\{ (x_v) \in \prod_v G_v \,\middle|\, x_v \in H_v \text{ for all but finitely many } v \notin S_\infty \right\}.$$

The prime on the product indicates that it is restricted, and it is defined exactly by the right hand side above. We put a topology on $G$ by declaring a base of neighborhoods about 0 to be

$$\left\{ \prod_v U_v \,\middle|\, U_v \subset G_v \text{ open}, U_v = H_v \text{ for all but finitely many } v \notin S_\infty \right\}.$$

Note that since the $G_v$'s have a base of compact neighborhoods about $0 \in G_v$ for each $v$, the restricted direct product $G$ is locally compact by Tychonoff's Theorem.

Finally, note that the adeles and the ideles are restricted direct products of groups indexed by the places of a global field. More precisely, let $K$ be a global field. Then if we take $\{v\} = V_K$, $S_\infty = V_\infty$ (in the number field case), $G_v = K_v$, and $H_v = \mathcal{O}_v$, then $G = \mathbb{A}_K$. On the other hand, if we take instead $G_v = K_v^\times$ and $H_v = \mathcal{O}_v^\times$, then $G = \mathbb{I}_K$.

Now in the general setting above, we have the following theorem.

**Theorem 9.1.** *The characters on $G$ are precisely those maps of the form*

$$\chi(x) = \prod_v \chi_v(x_v)$$

*where $x = (x_v)$, $\chi_v$ is a character on $G_v$ which is equal to the restriction of $\chi$ to $G_v$, and where all but finitely many of the $\chi_v$'s are trivial on $G_v$ (so that the product is finite for all $x$).*

This theorem allows us to describe the structure of the Pontryagin dual of a restricted direct product: Consider the case where our indexed groups are $\widehat{G}_v$ and the subgroups are $H_v^\perp$. Since $H_v$ is open in $G_v$, $G_v/H_v$ is discrete, and so $(G_v/H_v)\widehat{\ }$ is compact. Also, since $H_v$ is compact, $\widehat{H}_v$ is discrete. Hence, since $\widehat{G}/H_v^\perp \cong \widehat{H}_v^\perp$, we see that $H^\perp$ is also open. Thus we may take the restricted direct product of the $\widehat{G}_v$'s with respect to the subgroups $H_v^\perp$.

**Theorem 9.2.** *The group $\widehat{G}$ is topologically isomorphic to the restricted direct product of the groups $\widehat{G}_v$ with respect to the subgroups $H_v^\perp$. The isomorphism is given by the map $\chi \mapsto \prod \chi_v$.*

Now we discuss Haar measure. If $S$ is a finite set of indices $v$, we let $G_S$ denote the set of all $x \in G$ such that $x_v \in H_v$ for all $v \notin S$. Then $G_S$ is open, and is equal to the following product:

$$G_S = \prod_{v \notin S} H_v \times \prod_{v \in S} G_v.$$

Assume $dx_v$ is a Haar measure on $G_v$, and the these measures are chosen so that $H_v$ has measure 1 for all but finitely many $v$. Then each $G_S$ gets a Haar measure which is the

product measure of the $dx_v$'s. By taking unions and using countable additivity, we get a Haar measure $dx$ on $G$.

As for $\widehat{G}$, if $d\chi_v$ is the dual measure of $dx_v$, then the same construction above yields a Haar measure $d\chi$ on $\widehat{G}$, considered as a restricted direct product of the groups $\widehat{G_v}$. The measure $d\chi$ is dual to $dx$.

The Fourier analysis behaves very well with these constructions:

**Theorem 9.3.** *Let $f_v \in \mathrm{Inv}(G_v)$ for all $v$, and assume $f_v$ is the characteristic function of $H_v$ for almost all $v$. Then $f = \prod f_v$ is in $\mathrm{Inv}(G)$ and we have*

$$\hat{f}(\chi) = \prod \hat{f}_v(\chi_v)$$

We now specialize to the adeles and ideles. So we let $K$ be a global field, and we let $\psi_v$ denote the standard character on the additive group of the completion $K_v$ at the place $v$. Then $\psi_v$ is trivial on $\mathcal{O}_v$ for all non-archimedean $v$ because $\mathcal{O}_v$ is contained in the local inverse different $\mathfrak{D}_v^{-1}$. Hence we get a character $\psi = \prod_v \psi_v$ on $\mathbb{A}_K$ which we call the *standard character* on $\mathbb{A}_K$.

All of the general theory above allows us to put the together local self-duality at each place and obtain a global self-duality. The result is this.

**Theorem 9.4.** *The group $\mathbb{A}_K$ is topologically isomorphic to its own dual under the map*

$$x \mapsto (y \mapsto \psi(xy)).$$

*Moreover, under this identification, $K^\perp = K$. Finally, the product of the usual Haar measures on the local fields $K_v$ is a Haar measure on $\mathbb{A}_K$, which becomes self-dual under this identification.*

## 10 The Riemann-Roch Theorem of Tate

We first state two lemmas which will be useful to us in the sequel. The first one is also used in the proof of the Riemann-Roch theorem of Tate, which we omit.

**Lemma 10.1.** *Let $K$ be a global field, and let $\|\cdot\|$ be the usual norm on $\mathbb{I}_K$. If $dx$ is the Haar measure on $\mathbb{A}_K$, then for $y \in \mathbb{I}_K$, we have $d(yx) = \|y\|dx$.*

**Lemma 10.2.** *Let $k$ be a non-archimedean local field. Let $\mathcal{O}$ be the valuation ring of $k$, and let $f$ be the characteristic function of $\mathcal{O}$. Then the Fourier transform $\hat{f}$ of $f$ with respect to the standard character and the usual Haar measure on $k$ is $\mathbb{N}\mathfrak{D}_v^{1/2}$ times the characteristic function of the inverse local different $\mathfrak{D}^{-1}$.*

**Theorem 10.3** (Riemann-Roch Theorem of Tate)**.** *Let $K$ be a global field. Let $f, \hat{f} \in \mathrm{Inv}(\mathbb{A}_K)$ both be continuous. Assume that the series $\sum_{\alpha\in K} f(y(x+\alpha))$ converges for all $x \in \mathbb{A}_K$ and all $y \in \mathbb{I}_K$, uniformly in $x$ on compact subsets of $\mathbb{A}_K$ and uniformly in $y$ on compact subsets of $\mathbb{I}_K$. Assume also that $\sum_{\alpha\in K} \hat{f}(\alpha y)$ converges for all $y \in \mathbb{I}_K$. Then*

$$\frac{1}{\|y\|}\sum_{\alpha\in K} \hat{f}\left(\frac{\alpha}{y}\right) = \sum_{\alpha\in K} f(\alpha y).$$

The proof of this theorem is actually just a very straightforward application of the Poisson summation formula, using the fact that $K^\perp = K$. To illustrate why this theorem bears the name of Riemann-Roch, we use it to prove the Riemann-Roch theorem for function fields as in Theorem 4.7.

Let $K$ be a function field, and let $f$ be the characteristic function of the adelic unit ball $B = \prod_v \mathcal{O}_v$ in $\mathbb{A}_K$. Let $D = \sum n_v v$ be a divisor on $K$, where we identify the set of primes of $K$ with $V_K$. We can associate an idele $x(D)$ to the divisor $D$ as follows. Choose a prime element $\pi_v$ in $\mathcal{O}_v$ for all $v$. Then we define $x(D) = (\pi_v^{n_v})$. Note

$$\|x(D)\| = \prod_v \|\pi_v^{n_v}\| = \prod_v q^{-f_v n_v} = q^{-\deg D}.$$

Now we claim that

$$q^{\ell(D)} = \sum_{\alpha \in K} f(\alpha x(D)).$$

This sum is finite since $x(D)^{-1}B$ is compact and $K$ is discrete, and the sum just counts how many elements of $K$ are in $x(D)^{-1}B$. Now let $\alpha \in K^\times$. Then $v(\alpha) \geq -n_v$ for all $v$ means precisely that $\alpha \in x(D)^{-1}B$. But this condition is the same as the one for $\alpha$ to be in $L(D)$. Since also $0 \in L(D)$ and $f(0) = 1$, the sum above just counts elements of $L(D)$. So it is equal to $|L(D)| = q^{\ell(D)}$, as desired. Note that this implies that $\ell(D)$ is finite.

Now let $\psi$ be the standard character on $\mathbb{A}_K$. It is trivial at each place on the inverse of the local different, and nontrivial at each place on any larger ideal. Let $m_v$ be the valuation of the generator of the local different $\mathfrak{D}_v$, and set $\mathcal{K} = -\sum m_v v$. Now Tate's Riemann-Roch theorem obviously applies to $f$, and we get

$$\frac{1}{\|x(D)\|} \sum_{\alpha \in K} \hat{f}(\alpha x(D)^{-1}) = \sum_{\alpha \in K} f(\alpha x(D)),$$

i.e.,

$$\sum_{\alpha \in K} \hat{f}(\alpha x(D)^{-1}) = q^{\ell(D) - \deg D}.$$

It thus remains to show that $g = \ell(\mathcal{K})$ is such that $\sum \hat{f}(\alpha x(D)) = q^{\ell(\mathcal{K}-D)+1-g}$.

Now putting together the information of Lemma 10.2 as all places, we see that $\hat{f}$ is $\prod_v \mathbb{N}\mathfrak{D}_v^{-1/2}$ times the characteristic function of the product of the local inverse differents. By definition, the product of the inverse local differents is just $x(\mathcal{K})B$. Thus, like above, $\alpha \in K^\times$ is counted by $\hat{f}$ if and only if it is in $x(\mathcal{K})^{-1}x(D)B$, and so $\hat{f}$ counts the elements in $L(\mathcal{K} - D)$ with a factor of $\prod_v \mathbb{N}\mathfrak{D}_v^{-1/2}$. If we prove that $1 - g = \log_q(\prod_v \mathbb{N}\mathfrak{D}_v^{-1/2})$, then we get the theorem by taking $\log_q$'s. Let us prove this now.

One sees easily, using, for instance, the product formula, that only the constants $\mathbb{F}_q$ are in $L(0)$, and so $\ell(0) = 1$. One also computes easily that $q^{\deg \mathcal{K}} = \prod_v \mathbb{N}\mathfrak{D}_v$. Thus the formula reads

$$\ell(\mathcal{K}) - 1 = \deg \mathcal{K} + 1 - \ell(\mathcal{K}),$$

i.e.,

$$2g - 2 = \log_q(\prod_v \mathbb{N}\mathfrak{D}_v).$$

We are done.

# 11 An Analytic Proof of the Riemann-Roch Theorem for Number Fields

In this section we provide an analytic proof of the Riemann-Roch theorem for number fields. Since the material of this section is new, we carry out the details with considerable care.

We recall the Riemann-Roch theorem for number fields here for the convenience of the reader. See Definitions 2.5, 3.4, 3.8, and 3.10. for notation.

**Theorem 11.1** (Riemann-Roch Theorem For Number Fields)**.** *Let $K$ be a number field of degree $n$ with $r$ real embeddings and $s$ complex embeddings. As $\mathfrak{a}$ ranges through $J(\bar{\mathcal{O}}_K)$, we have the estimate*

$$|H^0(\mathfrak{a}^{-1})| = \frac{2^r(2\pi)^s}{\sqrt{|\Delta_K|}}\mathbb{N}\mathfrak{a} + O((\mathbb{N}\mathfrak{a})^{1-\frac{1}{n}}).$$

Actually, we will not prove this directly. Instead, we prove a similar result which is completely adelic, as follows:

Let $B \subset \mathbb{A}_K$ be the product of the closed unit balls in $K_v$, $v \in V_K$, and let $\chi_B$ be its characteristic function. As $a$ ranges through $\mathbb{I}_K$, we have the estimate

$$\sum_{\alpha \in K} \chi_B(\alpha a^{-1}) = \frac{2^r(2\pi)^s}{\sqrt{|\Delta_K|}}\|a\| + O(\|a\|^{1-\frac{1}{n}}).$$

The first instinct may be to apply Tate's Riemann-Roch theorem to $\chi_B$, like one does in the case of function fields. This would not work, however, since the infinite components of $\widehat{\chi}_B$ violate the hypotheses of that theorem for reasons related to continuity. Instead, we will convolve $\chi_B$ with a bump function, use Riemann-Roch to estimate a sum involving the resulting function, and compare this sum to the one above. The estimations we need will rely on the following notion of surface area.

Fix a *region* $D \subset \mathbb{A}_K$, by which we mean $D$ is compact and equal to the closure of its interior, and the finite component of $D$ is compact and open. Given another region $E \subset \mathbb{A}_K$, we define

$$E_D = \{x + (y_1 - y_0) \mid x \in E,\, y_1, y_0 \in D\}.$$

This region is simply the union of all translates of $D$ which intersect $E$.

Actually, we will want to consider this construction when $D$ is skewed. Given an idele $a \in \mathbb{I}_K$ and a subset $X \subset \mathbb{A}_K$, we define $aX = \{ax \mid x \in X\}$. If $t > 0$ is a real number, we may also view $t$ as the idele whose finite components are all 1 and whose infinite components are all $t$, so that the expression $tD$ makes sense and is a region. Then we define the *adelic surface area* of $E$ with respect to $D$ to be the derivative

$$S_D(E) = \lim_{t \to 0^+} \frac{\mathrm{Vol}(E_{tD}) - \mathrm{Vol}(E)}{t},$$

if it exists.

**Lemma 11.2.** *Let $D, E$ be regions for which $S_{aD}(E)$ exists for all norm 1 ideles $a$. Let $C : [0,1] \times \mathbb{I}_K^1 \to \mathbb{R}$ be defined by*

$$C(t,a) = \begin{cases} \frac{\mathrm{Vol}(E_{taD}) - \mathrm{Vol}(E)}{t} & \text{if } t \neq 0 \\ S_{aD}(E) & \text{if } t = 0. \end{cases}$$

*Then $C$ is continuous and defined everywhere.*

*Proof.* Let $a = (a_v)_{v \in V_K}$ be a norm 1 idele. Since volume is translation invariant, we may assume $0 \in D$, and hence in $aD$. Then there is a finite subset $S \subset V_K$, including the infinite places, such that $aD$ is the product $\prod_{v \notin S} \mathcal{O}_v$ away from the places in $S$. Let $\epsilon > 0$ and let $b = (b_v)$ be a norm 1 idele such that: $\|b_v/a_v - 1\| < \epsilon$ for all infinite places $v$; $\|b_v/a_v - 1\|$ is so small for $v \in S \cap V_{\mathrm{f}}$ that skewing $aD$ at the place $v$ does not change the region $aD$; and $b_v \in \mathcal{O}_v^\times$ for $v \notin S$. The set of all $b$ satisfying these conditions is open in $\mathbb{I}_K^1$.

Now these conditions on $b$ imply that $bD = (b/a)aD$ is such that $(1+\epsilon)^{-1}bD \subset aD$ and $(1+\epsilon)^{-1}aD \subset bD$. Thus

$$(1+\epsilon)^{-1}aD \subset bD \subset (1+\epsilon)aD,$$

and hence, for $t > 0$,

$$E_{(1+\epsilon)^{-1}taD} \subset E_{tbD} \subset E_{(1+\epsilon)taD}.$$

Therefore, taking volumes, subtracting the volume of $E$ and dividing by $t$, we get

$$(1+\epsilon)^{-1}C((1+\epsilon)^{-1}t, a) \leq C(t,b) \leq (1+\epsilon)C((1+\epsilon)t, a)$$

This proves that $C$ is continuous on $(0,1] \times \mathbb{I}_K^1$ and taking the limit of the above estimate as $t \to 0$ gives continuity everywhere. □

In what follows, $B \subset \mathbb{A}_K$ is the product of the closed unit balls at each place, $B = \prod_{v \in V_{\mathrm{f}}} \mathcal{O}_v \times \prod_{v \in V_\infty} \overline{B(0,1)}$. This is a region in $\mathbb{A}_K$. Also, $D$ will denote the closure of a fixed fundamental domain of $\mathbb{A}_K$ modulo $K$ for which $S_{aD}(E)$ exists for all norm 1 ideles $a$. Also, we let $\varphi$ be a continuous function with support in $D$ and total integral 1, such that the series $\sum_{\alpha \in K} |\widehat{\varphi}(\alpha b)|$ converges and is continuous for ideles $b$. We will exhibit such a pair $D, \varphi$ in a moment, but for now, we will assume that they exist.

Now for two functions $g, h$ on $\mathbb{A}_K$, define their convolution $g * h$ as usual:

$$g * h(x) = \int_{\mathbb{A}_K} g(y)h(x-y)\,dy.$$

Then $(g*h)\hat{} = \hat{g}\hat{h}$. Let $f = \chi_B * \varphi$.

**Lemma 11.3.** *Let $a \in \mathbb{I}_K^1$ and $t > 1$. There is a constant $c_1$, depending only on $D$ and $\varphi$, such that*

$$\sum_{\alpha \in K} \chi_B(\alpha(ta)^{-1}) \leq \sum_{\alpha \in K} f(\alpha(ta)^{-1}) + c_1.$$

*Proof.* We have

$$f((ta)^{-1}\alpha) = \int \chi_B(x)\varphi((ta)^{-1}\alpha - x)\,dx = \int_{taB} \varphi((ta)^{-1}(\alpha - x))t^{-n}\,dx.$$

Since $\varphi$ has total integral 1, this integral is equal to $\chi_B((ta)^{-1}\alpha)$ whenever the support of $\varphi((ta)^{-1}(\alpha - x))$ is contained completely inside or outside $taB$, i.e., it does not intersect the boundary of $taB$. Now the support of $\varphi((ta)^{-1}(\alpha - x))$ intersects the boundary of $taB$ only when $ta(\alpha - D)$ intersects the boundary of $taB$, which happens if and only if $\alpha - D$ intersects the boundary of $B$, and this happens only finitely many times. Thus $f((ta)^{-1}\alpha) \neq \chi_B((ta)^{-1}\alpha)$ for finitely many $\alpha$, say $c$ of them, and the difference is at most 1. Thus we are done if we take $c_1 = c$. □

**Lemma 11.4.** *There is a continuous function $C_1$ on $\mathbb{I}_K^1$ such that, in the notation of Lemma 11.2,*

$$\sum_{\alpha \in K^\times} f(at\alpha) \leq t^{-1} C_1(a) C(t^{-1}, a^{-1}).$$

*Proof.* We have

$$\begin{aligned} \hat{f}(at\alpha) &= \widehat{\chi}_B(at\alpha)\widehat{\varphi}(at\alpha) \\ &= \widehat{\varphi}(at\alpha) \int_B \psi(at\alpha x)\, dx \\ &= t^{-n}\widehat{\varphi}(at\alpha) \int_{taB} \psi(\alpha x)\, dx. \end{aligned}$$

Now since the integral of $\psi(\alpha x)$ is zero over any translate $D$ for $\alpha \in K^\times$ (because the integral of a character over a compact group is zero), the integral $\int_{taB} \psi(\alpha x)\, dx$ is equal to $-\int_{E \backslash taB} \psi(\alpha x)\, dx$, where $E$ is the union of all $K$-translates of $D$ which intersect $taB$. Since the maximum value of $\psi$ is 1, this is smaller in absolute value than $\mathrm{Vol}(E \backslash taB)$. But by the definition of $E$, we know that $E \subset (taB)_D$. So

$$\mathrm{Vol}(E \backslash taB) \leq \mathrm{Vol}((taB)_D) - \mathrm{Vol}(taB) = t^n(\mathrm{Vol}(B_{t^{-1}a^{-1}D}) - \mathrm{Vol}(B)) = t^{n-1} C(t^{-1}, a^{-1}).$$

Thus

$$|\hat{f}(at\alpha)| \leq t^{-1} C(t^{-1}, a^{-1}) |\varphi(at\alpha)|.$$

Summing over all $\alpha \in K^\times$ gives the result since the series $\sum_{\alpha \in K^\times} |\hat{\varphi}(at\alpha)|$ is continuous by assumption and must eventually decrease as $t$ increases. □

Now we exhibit a partcular $D$ and $\varphi$ for which the above theory works.

**Lemma 11.5.** *Let $D$ have finite component $\prod_{v \in V_\mathrm{f}} \mathcal{O}_v$ and infinite component equal to a fundamental parallelepiped of $\mathcal{O}_K$ in $\mathbb{R}^n$. Let $\varphi$ have finite component the characteristic function of $\prod_{v \in V_\mathrm{f}} \mathcal{O}_v$ and infinite component any smooth function supported in the fundamental parallelepiped of $\mathcal{O}_K$ in $\mathbb{R}^n$, such that the total integral of $\varphi$ is 1. Then:*

*(1) $D$ is a fundamental domain for $\mathbb{A}_K$ modulo $K$ and is a region;*

*(2) $S_{aD}(B)$ exists and is finite for all norm 1 ideles $a$;*

*(3) The series $\sum_{\alpha \in K} |\widehat{\varphi}(\alpha b)|$ converges and is continuous for ideles $b$.*

*Proof.* The assertion (1) is trivial and well known. Assertion (3) follows from the fact that $\widehat{\varphi}(\alpha b)$ is only nonzero for $\alpha$ in a certain fractional ideal, and from the fact that the infinite component of $\widehat{\varphi}$ is a Schwartz function, because the infinite component of $\varphi$ is.

For (2), let $P$ be the infinite component of $aD$, and let $B'$ be the infinite component of $B$, so $B'$ is a product of $r$ intervals and $s$ discs. The finite components of $B_{taD}$ are the same for all $t$, so we only need to show that the derivative of $\mathrm{Vol}(B'_{tP})$ exists, where the regions we are dealing with are now in $\mathbb{R}^n$, and $B'_{tP}$ has the same meaning as above, but is a region in $\mathbb{R}^r \times \mathbb{C}^s$.

For this, let $O$ be in the interior of $B'$ and choose spherical coordinates $(t, \theta) = (t, \theta_1, \ldots, \theta_{n-1})$ around $O$. Let $f(t, \theta)$ be the function which sends $(t, \theta)$ to the distance from the point $O$ to the boundary of $B'_{tP}$. This is single-valued because each $B'_{tP}$ is convex

and it is continuous because its graph, which is the boundary of $B'_{tP}$, is connected. By definition, the volume $\mathrm{Vol}(B'_{tP})$ is equal to the integral

$$\int_{S^{n-1}} f(t,\theta)\,d\theta.$$

for an appropriate normalization of the form $d\theta$, where $S^{n-1}$ is the $(n-1)$-sphere about $O$. Thus we want to show that the limit

$$\lim_{t\to 0^+} \frac{1}{t}\int_{S^{n-1}} (f(t,\theta)-f(0,\theta))\,d\theta$$

exists.

To do this, we show that the difference quotient

$$\frac{f(t,\theta)-f(0,\theta)}{t}$$

is increasing and uniformly bounded above in $\theta$. This will prove that the integral

$$\lim_{t\to 0^+} \int \frac{f(t,\theta)-f(0,\theta)}{t}\,d\theta$$

is increasing and bounded above, and hence has a limit, as desired. So to prove this, we first note that

$$\frac{f(t,\theta)-f(0,\theta)}{t} \le \frac{\mathrm{diam}(tP)}{t} = \mathrm{diam}\,P,$$

because the distance between any point on the boundary of $B'_{0P} = B'$ from the boundary of $B'_{tP}$ is at most the distance between any two points in $P$, by definition.

Now to show that the above difference quotient is increasing, we only need to show that function $f(t,\theta)$ for fixed $\theta$ is concave-down, in the sense of freshman calculus. This means that for any $t$ and any $0 < c < 1$, we must have

$$cf(t,\theta) \le f(ct,\theta).$$

We claim that if $v$ is a vector in the direction of $\theta$, if $x \in B'$ is the point on the ray from $O$ in the direction of $\theta$, and $x+v \in B'_{tP}$, then $x+cv \in B'_{ctP}$. This assertion implies immediately that $f(t,\theta)$ is concave down in $t$, and its verification will complete the proof of the lemma.

Now for such $x$ and $v$, let $y \in B_\infty$ such that $x+v = y+(p_1-p_0)$ for some $p_1, p_0 \in tP$. Then we compute

$$x+cv = x+cx-cx+cv = (1-c)x+c(x+v) = (1-c)x+c(y+p_1-p_0) = ((1-c)x+cy)+(cp_1-cp_0).$$

But $(1-c)x+cy \in B'$ because $B'$ is convex, and $cp_1, cp_0 \in ctP$, so $x+cv \in B'_{ctP}$. We are done. □

Now we can complete the proof of our main theorem.

**Theorem 11.6.** *As $a$ ranges through $\mathbb{I}_K$, we have the estimate*

$$\sum_{\alpha\in K} \chi_B(\alpha a^{-1}) = \frac{2^r(2\pi)^s}{\sqrt{|\Delta_K|}}\|a\| + O(\|a\|^{1-\frac{1}{n}}).$$

*Proof.* We apply Tate's Riemann-Roch theorem to $f$: In the notation of Lemmas 11.2, 11.3, 11.4, we have

$$\begin{aligned}\sum_{\alpha\in K}\chi_B(\alpha(ta)^{-1}) &\le \sum_{\alpha\in K} f(\alpha(ta)^{-1}) + c_1\\ &= \|ta\|\sum_{\alpha\in K} f(\alpha ta) + c_1\\ &\le \|ta\|\hat{f}(0) + c_1 + t^{-1}\|ta\|C_1(a)C(t^{-1},a^{-1}).\end{aligned}$$

Now

$$\hat{f}(0) = \widehat{\varphi}(0)\widehat{\chi}_B(0) = \mathrm{Vol}(B) = \frac{2^r(2\pi)^s}{\sqrt{|\Delta_K|}}$$

and $t^{-1}\|ta\| = \|ta\|^{1-\frac{1}{n}}$ because $a$ has norm 1. Thus we have the desired estimate in $t$ for each $a$ separately. To get a uniform estimate, we note that the quantity

$$\sum_{\alpha\in K}\chi_B(\alpha(ta)^{-1})$$

does not depend on the class of $a$ modulo $K^\times$. Thus we may replace the function $(t,a)\mapsto C_1(a)C(t^{-1},a^{-1})$ by the function $C' : [0,1]\times(\mathbb{I}_K^1/K^\times)\to\mathbb{R}$ defined by

$$C'(t^{-1},x) = \inf\{C_1(a)C(t^{-1},a^{-1}) \mid \pi(a) = x\}$$

where $\pi : \mathbb{I}_K^1 \to \mathbb{I}_K^1/K^\times$ is the quotient map. Since $[0,1]\times(\mathbb{I}_K^1/K^\times)$ is compact, the following lemma suffices to complete the proof of the theorem. □

**Lemma 11.7.** *(a) Let $f$ be a positive continuous real valued function on a topological space $X$, and let $\pi : X\to Y$ be a quotient map. Then $F : Y\to\mathbb{R}$ given by $F(y) = \inf\{f(x) \mid x\in\pi^{-1}(y)\}$ is upper semicontinuous on $Y$, which means that the sets $F^{-1}([a,\infty))$ are closed in $Y$ for all $a\in\mathbb{R}$.*

*(b) An upper semicontinuous function on a compact topological space is bounded above by a constant.*

*Proof.* Though this is an easy exercise, we include its proof for lack of a suitable reference.

(a) With the notation as in the lemma, we need to show that the sets $F^{-1}((-\infty,a))$ are open. Let $b\in\mathbb{R}$. The set $U = f^{-1}((-\infty,b))\subset X$ is open by continuity of $f$. Then $\pi(U)$ is open in $Y$. But $\pi(U)$ contains all points $y\in Y$ for which there is an $x\in X$ with $\pi(x) = y$ and $f(x) < b$. This means exactly that $F(x) < b$, and so $F^{-1}((-\infty,b))$ is the open set $\pi(U)$.

(b) Let $F$ be an upper semicontinuous function on the compact space $Y$. The sets $F^{-1}((-\infty,a))$ for $a\in\mathbb{R}$ form an open cover of $Y$. Thus it has a finite subcover, say $\{F^{-1}((-\infty,a_i))\}$. Let $j$ be such that $a_j$ is maximal amongst the $a_i$'s. Then $F^{-1}((-\infty,a_j)) = Y$ since all of the sets $F^{-1}((-\infty,a_i))$ are subsets of this one. Hence $F(y) < a_j$ for all $y\in Y$. □

Now we apply the theorem above to give a proof of the Riemann-Roch theorem for number fields:

*Proof (of Theorem 11.1).* For $x = (x_v)_{v \in V_K} \in \mathbb{I}_K$, let $\mathfrak{a}_x$ be the replete ideal defined by

$$\mathfrak{a}_x = \prod_{\mathfrak{p} \in V_{\mathrm{f}}} \mathfrak{p}^{-v_{\mathfrak{p}}(x_{\mathfrak{p}})} \times (|x_v|)_{v \in V_\infty}.$$

Then, by definition, $\mathbb{N}\mathfrak{a}_x = \|x\|$ and the sum

$$\sum_{\alpha \in K} \chi_B(\alpha x^{-1})$$

counts the number of elements in $H^0(\mathfrak{a}_x^{-1})$. Then we apply our theorem for ideles $x$ to get the Riemann-Roch theorem for replete ideals $\mathfrak{a}_x$. Since the map $x \mapsto \mathfrak{a}_x$ from $\mathbb{I}_K$ to $J(\overline{\mathcal{O}}_K)$ is clearly surjective, we obtain the Riemann-Roch theorem for number fields. □

**Some comments:**

I do not assert that the proof above is easier than Lang's original proof. Rather, I think that the techniques of the above proof are very general and that they perhaps contain more major ideas. In particular, this proof uses the Riemann-Roch theorem of Tate in a fashion similar to the proof of the Riemann-Roch theorem for function fields given in the previous section. Thus we have a bridge between these three Riemann-Roch theorems which was not previously known.

## References


[1] J. W. S. Cassels and A. Frohlich, *Algebraic Number Theory*. Academic Press, London, 1967

[2] G. Folland, *A Course in Abstract Harmonic Analysis*. Studies in Advanced Mathematics. CRC Press, Boca Raton, 1995.

[3] R. Hartshorne, *Algebraic Geometry*. Graduate Texts in Mathematics 52. Springer-Verlag, Berlin, 1977.

[4] S. Lang, *Algebraic Number Theory*, Second Edition. Graduate Texts in Mathematics 84. Springer-Verlag, Berlin, 1994.

[5] D. Marcus, *Number Fields*. Universitext. Springer-Verlag, Berlin, 1977.

[6] Yu. I. Manin, A. A. Panchishkin, *Introduction to Modern Number Theory*, Second Edition. Encyclopaedia of Mathematical Sciences 49. Springer-Verlag, Berlin, 2005.

[7] D. Mumford, *The Red Book of Varieties and Schemes*, Second Expanded Edition. Lecture Notes in Mathematics 1358. Springer-Verlag, Berlin, 1974.

[8] S. Mundy, *A New Proof of an Arithmetic Riemann-Roch Theorem*, http://arxiv.org/abs/1410.8025.

[9] J. Neukirch, *Algebraic Number Theory*. Grundlehren der Mathematischen Wissenschaften 322. Springer-Verlag, Berlin, 1999.

[10] D. Ramakrishnan and R. Valenza, *Fourier Analysis on Number Fields*. Graduate Texts in Mathematics 186. Springer-Verlag, Berlin, 1999.

[11] M. Rosen, *Number Theory in Function Fields*. Graduate Texts in Mathematics 210. Springer-Verlag, Berlin, 2002.

[12] J.-P. Serre, *Algebraic Groups and Class Fields*. Graduate Texts in Mathematics 117. Springer-Verlag, Berlin, 1988.

[13] I. Shafarevich, *Basic Algebraic Geometry I*, Third Edition. Springer-Verlag, Berlin, 2007.

[14] J. Silverman, *The Arithmetic of Elliptic Curves*, Second Edition. Graduate Texts in Mathematics 106. Springer-Verlag, Berlin, 2009.

[15] A. Weil, *Basic Number Theory*. Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete 144. Springer-Verlag, Berlin, 1967.