Local Compactness and Number Theory

Sam Mundy

May 1, 2015

Introduction

The present document is a slightly expanded version of a series of lectures I gave at the University of New Mexico in the spring of 2015. The series has a title: "Local Compactness and Number Theory," the same as this document. The main idea is to develop number theory from a topological point of view, much like in Weil's *Basic Number Theory* [11]. However, the main goal of these lectures is more broad, in that the point here is to motivate material and to give an overview of relevant topics, rather than to give all proofs in detail. If I were to do the latter, I may as well just lecture from Weil.

The first lecture is on the main apparatus which will be used in most the rest of the lectures, namely the locally compact abelian groups. Such groups come equipped with a natural measure called the Haar measure. This will allow a nice integration theory on such groups, and eventually, a Fourier analysis. But the Fourier theory will come near the end of the lectures. Afterwards, we define the local fields, which will be locally compact by definition. The analysis of these fields will be very topological. We will classify them without proof.

Next we will define the global fields and look at them algebraically. (The more enlightened readers will recognize our analysis also as geometric at its core). We describe a process which constructs any local field out of some global field. Now the global fields will not be a gluing together of local fields in any obvious way; instead, the gluing together of local fields results in another locally compact group (actually a ring), the adeles. The geometric structure of the adeles (or more accurately, their units, also locally compact) gives rise to rich information about the global fields.

Next, we describe class field theory and the theory of curves over finite fields in order to give a taste of what is beyond the basic theory we develop. In fact we go as far as to give a description of the Weil Conjectures for varieties over finite fields. While this subject deviates far from the main focus of the material, it raises an important point: We will not have even touched the theory of zeta functions. This is remedied immediately as we give examples of classical zeta functions in number theory. Here we will touch upon class field theory again. But then we will want to generalize our zeta functions.

To do this, we need the aforementioned Fourier analysis. This will lead to a detailed description of Tate's thesis, where the zeta functions we know, and many more, are constructed from local analogues, like the adeles are constructed from local fields. But the general theory will be very lucrative: Tate's thesis will allow us to obtain important analytic information about the zeta functions which can be translated into valuable arithmetic data.

When I presented these lectures, I skipped Lectures 6 and 7 in this document because the audience had, for the most part, seen this material in other courses. Since I had fifteen lectures planned, and there are thirteen in this document, this left an extra four lectures at the end of the course. I filled them each with brief overviews of the following topics, in order: Modular forms, Eichler-Shimura theory in weight 2, automorphic representations and the adelization of modular forms, and Langlands functoriality.

Prerequisites and Unproved Results

The basic prerequisites for these lectures are: Abstract algebra on the level of Galois theory, basic topology, a first course in complex analysis, and real analysis at the level of basic abstract integration theory. With respect to this last prerequisite, we review the notion of a measure in Lecture 1, but we will make use of integration theory without recalling the definition of an integral. In particular, we will need to make use of Fubini's Theorem in Lecture 11. See Rudin [8] Chapter 1 for the basic theory, Chapter 2 for the Riesz Representation Theorem, and Chapter 8 for Fubini's Theorem.

Now the lectures themselves only give an overview of the material covered, and as such, there are very many results which are not proved in full. A lot of this is made up for in the exercises, but many results are still left unproved. Here is a list: The existence of a Haar measure in Lecture 1; the classification of local fields in Lecture 2; Artin Reciprocity and the Existence Theorem from class field theory in Lecture 5; basic facts about algebraic geometry in Lectures 6 and 7; properties of ℓ-adic cohomology in Lecture 8, which is inessential for the rest of the lectures; the classification of irreducible representations of abelian groups in Lecture 9; and basic abstract harmonic analysis in Lecture 10. In any case, all of the results we need are stated in full. If the goal one has in mind is to understand Lecture 13 completely, for instance, then the only necessary arithmetic result which is missing from this treatment is the classification of local fields.

References for the missing material are as follows: The missing results which are necessary to understand the material in Lectures 1 and 2 are in Ramakrishnan and Valenza [9]. Folland [2] also gives a treatment of the subset of these results which are analytic. For class field theory, one can read Cassels and Fröhlich [1], which also contains Tate's Thesis. The small result in Lecture 9 on the representation theory of abelian group follows easily from basic character theory, which is usually discussed early on in any treatment of the representation theory of finite groups. As for the algebraic geometry, the results stated in Lectures 6 and 7 can be found in Hartshorne [3] when the base field is algebraically closed. Otherwise, one may consult the first two chapters of Silverman's book [10] on elliptic curves for arbitrary base field, where he gives references for complete proofs. The ℓ-adic cohomology is described in Appendix C in Hartshorne [3], but proofs are not given. For the proofs, one must delve deep into the theory. One can read the source directly (SGA) and these references are given in Hartshorne. One can also read Milne's book [6] for some of this material.

The approach taken to algebraic number theory in these lectures is nonstandard, and it complements a treatment like Lang [4], or even Marcus [5].

Conventions

All rings are commutative with identity and all topological groups are Hausdorff. Integration of a function f against a measure μ is denoted by $\int f(x)\,d\mu(x)$, or the same but with a variable different from x. All measurable functions are complex valued. $L^1(X)$ denotes the space of integrable (complex valued) functions on the measure space X. Varieties, as they are defined in the lectures, are irreducible. If N is an integer, the symbol for the integers modulo N is $\mathbb{Z}/N\mathbb{Z}$; the symbol $\mathbb{Z}_p$ is reserved for the p-adic integers (defined in Lecture

1) and is only used when p is prime. The finite field with q elements is denoted $\mathbb{F}_q$.

Contents

Lecture 1

Locally Compact Abelian Groups

We begin by recalling some basic notions which are fundamental for these lectures. First, a group G is a *topological group* if there is a topology on it for which multiplication

$$\cdot : G \times G \to G$$

and inversion

$$(\cdot)^{-1} : G \to G$$

are continuous. The first things one must note about such a group G is that, for any $g \in G$, the map $h \mapsto gh$ which left-multiplies an element in G by g, is continuous. Not only that, but it is a homeomorphism because multiplication by g^{-1} supplies an inverse which is continuous. As well, the inversion map is a homeomorphism because it is its own inverse.

One consequence of these facts is that, in order to describe the topology on G, it is enough to specify a base of open sets about a given element of G, for then one may just translate this base to all element of G and get a base for the full topology.

The key property which we want our groups to satisfy is *local compactness.* Recall that a topological space X is locally compact if every point in X has an open neighborhood which is contained in a compact set. A topological group G will be called a *locally compact group* if, of course, it is locally compact as a topological space. We are interested in such groups because there is a rich analysis on them, especially if they are abelian. In particular, we get a very special measure on them for free, which we now describe.

Recall that a data of a measure μ on a set S consists of both σ-algebra on S and the measure μ itself. A *σ-algebra* on S is a collection $\mathfrak{M}$ of subsets of S for which the empty set and the whole set S are in $\mathfrak{M}$, any countable union of set in $\mathfrak{M}$ is in $\mathfrak{M}$, and the complement in S of any set in $\mathfrak{M}$ is in $\mathfrak{M}$. The fact that μ is a measure means that there is a σ-algebra on S, call it $\mathfrak{M}$ again, such that, for any $E \in \mathfrak{M}$, one can assign an element of $\mathbb{R}_{\geq 0} \cup \{\infty\}$ denoted $\mu(E)$ such that, for any countable collection $\{E_i\}_{i=1}^{\infty}$ of disjoint sets in $\mathfrak{M}$, we have

$$\mu(\bigcup_{i=1}^{\infty} E_i) = \sum_{i=1}^{\infty} \mu(E_i).$$

This condition is referred to as *countable additivity.* We require that $\mu(E) \neq \infty$ for some E in $\mathfrak{M}$. Any set E in $\mathfrak{M}$ is called *measurable* and $\mu(E)$ is its *measure.* One immediate

consequence of this definition is that the empty set always has measure zero.

Now if X is a topological space, we can consider the smallest σ-algebra $\mathfrak{B}$ which contains the open sets (and hence also the closed sets) of X. The elements of this σ-algebra are called the *Borel sets* of X. We call a measure μ a *Borel measure* if it is defined on all Borel sets. Finally, we call a regular Borel measure μ on a topological space X a *Radon measure* if it Borel and we have, for all E in the σ-algebra on which it is defined, that $\mu(E)$ is the supremum over all compacts K in E of the real numbers $\mu(K)$ and, from the other perspective, that $\mu(E)$ is the infimum over all open sets U containing E, of $\mu(U)$. These conditions are referred to as *inner* and *outer regularity,* respectively. Because of inner regularity, Radon measures are determined by their values on compact sets.

Now given any topological group G and any subset $S \subset G$ and any element $g \in G$, we denote by gS the set $\{gh \mid h \in S\}$. We are now ready to state the fundamental result.

Theorem 1.1. *Let G be a locally compact group. Then there is a nonzero Radon measure μ on G which is translation invariant, i.e., for all $g \in G$ and all measurable E, we have*

$$\mu(gE) = \mu(E).$$

Such a measure is called a Haar Measure *on G. Furthermore, this measure is as unique as possible, in the following sense: If ν is another Haar measure on G, then there is a $c > 0$ such $\mu = c\nu$.*

One comment is in order here: We have technically only defined the Haar measure to be *left* translation invariant. But one can show that this implies right translation invariance. Since we will only care about the Haar measure on locally compact *abelian* groups, this is immaterial to us.

So what is the role of local compactness in all of this? Recall the Riesz Representation Theorem, which says that given a locally compact space X and any continuous linear functional L on the compactly supported continuous functions $C_c(X)$ on X, there is a unique Radon measure μ for which

$$Lf = \int f(x)\, d\mu(x)$$

for any $f \in C_c(X)$. Thus, on a locally compact space X, measures are the same as continuous linear functionals on $C_c(X)$. See Rudin [8] for the proof. Here the local compactness is essential, and the way one constructs the Haar measure on a locally compact group G is by constructing a functional H on $C_c(G)$ such that $H \circ L_g = H$ for all $g \in G$, where $L_g : C_c(G) \to C_c(G)$ is the linear operator defined by the formula $(L_g f)(h) = f(gh)$.

Before we give examples, we first establish some general facts about the measures of open and compact sets in a locally compact group.

Proposition 1.2. *Let G be a locally compact group with Haar measure μ. Then every open set has positive (or infinite) measure and every compact set has finite measure.*

Proof. Let E be a set in G with finite positive measure under μ, which exists by the nontriviality of the Haar measure. Then by inner regularity, for any $\epsilon > 0$, there is a compact set K in E with $\mu(E) - \mu(K) < \epsilon$. In particular, we can choose K to have positive

measure.

Now let U be an open set and $x \in U$. Then $\{ax^{-1}U \mid a \in K\}$ is an open cover of K, and hence there is a finite subcover, say $\{a_1x^{-1}U, \dots, a_nx^{-1}U\}$, $a_1, \dots, a_n \in K$. Then $0 < \mu(K) \leq \mu(a_1x^{-1}U) + \cdots + \mu(a_nx^{-1}U) = n\mu(U)$. Thus U has positive measure.

On the other hand, using outer regularity, we can get an open set U' containing E with finite positive measure. Let K' be any compact set in G. Then like above, we can get a finite cover of K' by translates of U'. Since these translates all have finite measure, so does their union, and hence so does K'. This completes the proof. □

Example 1.3. First we consider $G = \mathbb{R}$, under addition, of course. $\mathbb{R}$, with its usual (euclidean) topology is locally compact, so we have a Haar measure. It is easy to see that it must be (a multiple of) the Lebesgue measure, since this is obviously translation invariant.

Example 1.4. We can consider more generally $G = \mathbb{R}^n$. Again this has the Lebesgue measure as a Haar measure. In fact, there is the following theorem.

Theorem 1.5. *Let $G_1, \dots, G_n$ be locally compact groups with respective Haar measures $\mu_1, \dots, \mu_n$. Then $G_1 \times \cdots \times G_n$ is a locally compact group with the product topology and Haar measure $\mu_1 \times \cdots \times \mu_n$. This measure is characterized by*

$$\mu_1 \times \cdots \times \mu_n(E_1 \times \cdots \times E_n) = \mu_1(E_1) \cdots \mu_n(E_n)$$

for measurable $E_i \subset G_i$, $i = 1, \dots, n$.

Example 1.6. Let $p \in \mathbb{Z}$ be a prime. Consider the projective system $\{\mathbb{Z}/p^n\mathbb{Z}\}_{n\in\mathbb{N}}$, with the maps being the natural projections. Then we can take the projective limit,

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

Explicitly,

$$\mathbb{Z}_p = \{(a_1, a_2, a_3, \dots) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \mid a_{i+1} \equiv a_i \pmod{p^i}\}.$$

The ring $\mathbb{Z}_p$, called the *p-adic integers,* is an integral domain of characteristic zero; this is an easy exercise, especially in light of the following considerations. The ring structure itself is made more explicit as follows. First write the element $(a_1, a_2, a_3, \dots) \in \mathbb{Z}_p$ instead like

$$(\alpha_0 + p\mathbb{Z}, \alpha_1 p + \alpha_0 + p^2\mathbb{Z}, \alpha_2 p^2 + \alpha_1 p + \alpha_0 + p^3\mathbb{Z}, \dots),$$

where each $\alpha_i \in \{0, 1, \dots, p-1\}$. We can do this because of the projectivity of the system. Then we write formally

$$\sum_{i=0}^{\infty} \alpha_i p^i$$

for this element. Then this is like a base p expansion which is infinite in length, and the addition and multiplication are given by carrying in base p. The canonical example of this is the amusing computation

$$1 + \sum_{i=0}^{\infty} (p-1)p^i = 0,$$

meaning $\sum(p-1)p^i = -1$.

Now $\mathbb{Z}_p$ has a topology given by the inverse limit when considering each $\mathbb{Z}/p^n\mathbb{Z}$ to have the discrete topology. We can describe this topology explicitly as follows. A base of neighborhoods about zero is $\{p^n\mathbb{Z}_p\}_{n\in\mathbb{N}}$. These sets, actually ideals, are just the sets of p-adic numbers whose first n entries are zero, in either the vector representation or the power series representation above. Remember that we get a description of the topology everywhere by translating. Under this topology, $\mathbb{Z}_p$ is compact. This is left as an exercise, but can be proved for instance by showing that $\mathbb{Z}_p$ is sequentially compact and Hausdorff. The ideals $p^n\mathbb{Z}_p$ are then homeomorphic to $\mathbb{Z}_p$ via the map given by multiplication by p^n. So the sets $p^n\mathbb{Z}_p$ are both compact and open. This is very different than the topology on $\mathbb{R}$. In fact, $\mathbb{Z}_p$ is even metric. The metric is given by $d(a,b) = |a-b|$ with $|\sum_{i=m}\alpha_i p^i| = p^{-m}$ if $\alpha_m \neq 0$. In other words, two p-adic integers are close if their expansions agree at many places before they begin to disagree, i.e., if their difference is divisible by a large power of p.

Some other algebraic structure worth noting is that $\mathbb{Z}_p$ local and principal, with only one prime ideal $p\mathbb{Z}_p$. So it is a discrete valuation ring, and its fraction field is therefore just $\mathbb{Z}_p[p^{-1}]$. Now let us denote the fraction field of $\mathbb{Z}_p$ by $\mathbb{Q}_p$. It is called the field of *p-adic numbers.* It is not too hard to show from this that elements of $\mathbb{Q}_p$ may be written as Laurent series in p, like

$$\sum_{i=-m}^{\infty}\alpha_i p^i.$$

The rules of addition and multiplication are still like in base p arithmetic.

We can give $\mathbb{Q}_p$ the topology which is specified by the same base about 0, $\{p^n\mathbb{Z}_p\}_{n\in\mathbb{N}}$, but now $\mathbb{Q}_p$ is only locally compact. For instance the sequence $\{\sum_{i=-m}^{0} p^i\}_{m\in\mathbb{N}}$ does not have a convergent subsequence. But in any case we can still ask for a description of the Haar measure μ on $\mathbb{Q}_p$.

Give $\mathbb{Z}_p$ measure 1 in $\mathbb{Q}_p$. I claim that this determines the Haar measure. A base of neighborhoods about 0 are the ideals $p^n\mathbb{Z}_p$. But the cosets $\alpha + p^n\mathbb{Z}_p$ for $\alpha = 0,\ldots,p^n-1$ are disjoint and cover $\mathbb{Z}_p$. This implies that their measures add to 1. But they are translates of one another, so they all have the same measure. This determines the measure on all basic open sets in $\mathbb{Z}_p$, hence on any Borel set in $\mathbb{Z}_p$. Then the sets $p^{-n}\mathbb{Z}_p$ are similarly disjoint unions of translates of $\mathbb{Z}_p$, so this determines the measure everywhere.

Finally, we note that we can extend the metric on $\mathbb{Z}_p$ to $\mathbb{Q}_p$ by the same formula $d(a,b) = |a-b|$ with $|\sum_{i=m}\alpha_i p^i| = p^{-m}$ if $\alpha_m \neq 0$. These distances are allowed to be arbitrarily large in $\mathbb{Q}_p$.

Example 1.7. Finally we consider the characteristic p analogue of $\mathbb{Q}_p$. This will simply be the field $\mathbb{F}_q((t))$ of Laurent series over the finite field with $q = p^r$ elements. There are many fundamental similarities between these fields which we now summarize.

Inside of $\mathbb{F}_q((t))$ we have the ring of power series $\mathbb{F}_q[[t]]$. One sees easily that

$$\mathbb{F}_q[[t]] = \varprojlim_n \mathbb{F}_q[t]/t^n\mathbb{F}_q[t],$$

and so, like above, we get the projective limit topology on $\mathbb{F}_q((t))$ viewing each $\mathbb{F}_q[t]/t^n\mathbb{F}_q[t]$ as discrete. This can be described as either the topology specified by the base of neighborhoods about 0 given by the ideals $\{t^n\mathbb{F}_q[[t]]\}_{n\in\mathbb{N}}$, or as the topology given by the metric

$d(a,b) = |a-b|$ where $|\sum_{i=m}^{\infty} \alpha_i t^i| = q^{-m}$ if $\alpha_m \neq 0$. This topology on $\mathbb{F}_q[[t]]$ then extends to its fraction field $\mathbb{F}_q((t))$ via the same base of neighborhoods about 0, or by the same formula for the metric. Similarly to the previous example, $\mathbb{F}_q[[t]]$ is compact and hence $\mathbb{F}_q((t))$ is locally compact, but not compact. We leave these details to the reader. Note also that $\mathbb{F}_q[[t]]$ is a discrete valuation ring with its only prime ideal the one generated by t. Finally, the Haar measure is determined by its value on $\mathbb{F}_q[[t]]$, and the ideals $t^n\mathbb{F}_q[[t]]$ have measure $1/q^n$ times that of $\mathbb{F}_q[[t]]$.

Lecture 2

Local Fields

This lecture and the next will be devoted to the study of local and global fields. Local fields will turn out to come from global fields by a process which may very well be viewed as a localization. However, we go the other way in these lectures for the sake of the progression of the material.

To define a local field, we need

Definition 2.1. Let k be a field. A function $|\cdot| : k \to \mathbb{R}_{\geq 0}$ is called an *absolute value* on k if the following properties hold:

(1) [Positive definiteness]. For any $a \in k$, we have that $|a| = 0$ if and only if $a = 0$;

(2) [Multiplicativity]. For any $a, b \in k$, we have $|ab| = |a||b|$;

(3) [Triangle inequality]. For any $a, b \in k$, we have $|a + b| \leq |a| + |b|$.

An absolute value $|\cdot|$ on a field k gives rise to a metric d on k defined by $d(a, b) = |b - a|$. Thus k also gets a topology, and it is easy to check that addition and multiplication, as well as their respective inversions (excluding 0 in the multiplicative case), are continuous. A field with a topology for which these four operations are continuous is called a *topological field.*

We will always assume that any topological field k we consider does not have the discrete topology. If $|\cdot|$ is an absolute value on k, this is the same as saying that $|\cdot|$ is not trivial, i.e., it is not the case that $|a| = 1$ for all $a \in k$, $a \neq 0$.

Definition 2.2. A field k is called a *local field* if either of the following two equivalent conditions holds:

(1) k is a (nondiscrete) topological field which is locally compact;

(2) k has a (nontrivial) absolute value such that the resulting metric topology is complete and locally compact.

These conditions are not obviously equivalent. In fact, we will not prove their equivalence here, but we will show now how to construct the absolute value assuming condition (1). Let μ be a Haar measure on a field k satisfying condition (1) of the definition. Let $a \in k^\times$. Then we define the measure μ_a to be the measure given by $\mu_a(E) = \mu(aE)$ for measurable sets E. The measure μ_a is again a Haar measure, and so by the uniqueness of the Haar measure, there is a positive constant c such that $\mu_a = c\mu$. Define $\mathrm{mod}(a) = c$.

This is called the *module* of a and it is characterized by $\mu(aE) = \mathrm{mod}(a)\mu(E)$ for all measurable sets E (equivalently, for some E of nonzero measure). This gives the absolute value on k if we set $\mathrm{mod}(0) = 0$.

In fact, there is an advantage to this discussion: The absolute value on a field k satisfying condition (2) is not determined by the topology which it induces. For instance, any positive power of that absolute value will give the same topology. However, the module is completely determined by the topology on k, so it provides a sort of canonical choice of absolute value.

Theorem 2.3. *Let k be a local field. Then k is isomorphic to a finite separable extension of any of the following three types of fields:*

(1) The p-adic numbers $\mathbb{Q}_p$;

(2) The Laurent series field $\mathbb{F}_q((t))$;

(3) The real numbers $\mathbb{R}$.

Furthermore, given an extension l/k of local fields and an absolute value on k, there is a unique absolute value on l which, when restricted to k, gives the one on k.

Let k be any field with an absolute value $|\cdot|$. We call $|\cdot|$ *nonarchimedean* if the image of $\mathbb{Z}$ in k is bounded, which means that there is a constant c such that $|n| \leq c$ for any $n \in \mathbb{Z}$. Otherwise, we call $|\cdot|$ *archimedean.* On the other hand, let us call $|\cdot|$ *ultrametric* if it satisfies the *strong triangle inequality*:

$$|a + b| \leq \max\{|a|, |b|\}$$

for all $a, b \in k$. It is a fact that $|\cdot|$ is nonarchimedean if and only if it is ultrametric. In the above classification, the finite separable extensions of $\mathbb{Q}_p$ and $\mathbb{F}_q((t))$ are nonarchimedean, which means that the only archimedean local fields are $\mathbb{R}$ and $\mathbb{C}$.

Let us explore the arithmetic of the nonarchimedean local fields and their extensions. Let k be a nonarchimedean local field. Let $\|\cdot\|$ be the absolute value given by the module, so $\|\cdot\| = \mathrm{mod}(\cdot)$. Let B_r, C_r be, respectively, the open and closed balls of radius r about 0. So $B_r = \{a \in k \mid \|a\| < r\}$ and $C_r = \{a \in k \mid \|a\| \leq r\}$. The closed unit ball C_1 is clearly closed under multiplication, but it is also closed under addition by the strong triangle inequality. Then the set B_1 becomes an ideal in C_1. Let us denote C_1 by $\mathcal{O}_k$ and B_1 by $\mathfrak{p}$, or $\mathfrak{p}_k$, if there is more than one local field in question.

The set $\mathcal{O}_k \backslash \mathfrak{p}$ consists of invertible elements in the ring $\mathcal{O}_k$. Therefore, $\mathcal{O}_k$ is local with maximal ideal $\mathfrak{p}$. If we take for granted that the sets C_r are compact (proved in Exercise 2.2), then we can prove the following proposition.

Proposition 2.4. *The field $\mathcal{O}_k/\mathfrak{p}$ is finite, say with q elements, and the maximum value of the module on $\mathfrak{p}$ is q^{-1}. Furthermore, $\mathfrak{p}$ is principal and generated by any element with module q^{-1}.*

Proof. The cosets of $\mathfrak{p}$ in $\mathcal{O}_k$ are disjoint if they are distinct, of course, and they form an open cover of $\mathcal{O}_k$. Since $\mathcal{O}_k$ is compact, there are only finitely, say q, many cosets. This proves that $\mathcal{O}_k/\mathfrak{p}$ is finite.

Now let M be the measure of $\mathcal{O}_k$ under some Haar measure. Since the q cosets of $\mathfrak{p}$ are disjoint, are translates of one another, and have union $\mathcal{O}_k$, we find that each of $\mathfrak{p}$ and its

cosets have equal measure $q^{-1}M$. Now $\mathfrak{p}$ is the complement of an open set (the union of its cosets different from itself) in a compact (namely $\mathcal{O}_k$), so it is itself compact. Since the module is continuous (which is shown directly in Exercise 2.1), it attains a maximum value on $\mathfrak{p}$, say r, which must be smaller than 1 because $\mathfrak{p} = B_1$. Therefore $\mathfrak{p}$ and C_r are actually equal as sets.

Let $\pi \in k$ be such that $\|\pi\| = r$. If $a \in \mathcal{O}_k$, then $\|a\pi\| \leq r$. Conversely if $\|a\pi\| \leq r$, then $\|a\| \leq r/\|\pi\| = 1$, and so $a \in \mathcal{O}_k$. Thus $\mathfrak{p} = \pi\mathcal{O}_k$. This proves that $\mathfrak{p}$ is principal with generator any element with maximal module in $\mathfrak{p}$. Furthermore,

$$q^{-1}M = \mu(\mathfrak{p}) = \mu(\pi\mathcal{O}_k) = \|\pi\|\mu(\mathcal{O}_k) = \|\pi\|M,$$

so $q^{-1} = \|\pi\|$. This completes the proof. □

An element which generates $\mathfrak{p}$ is called a *prime element,* and the field $\mathcal{O}_k/\mathfrak{p}$ is called the *residue field* of k.

The proposition shows that $\mathcal{O}_k$ is a discrete valuation ring, which just means it is a local principal ideal domain. But clearly its fraction field is k since if $a \in k$ with $\|a\| \geq 1$, then $\|a^{-1}\| \leq 1$. It follows from standard facts about discrete valuation rings that all ideals in $\mathcal{O}_k$ are of the form $\mathfrak{p}^m$ for some integer $m \geq 0$. Therefore, given any prime element π, we get a decomposition $k^\times \cong \mathcal{O}_k^\times \times \pi^{\mathbb{Z}}$, where $\pi^{\mathbb{Z}}$ is the multiplicative group generated by π.

For any $a \in k$, we define $v(a)$ to be the largest integer n for which $a \in \pi^n\mathcal{O}_k$. This does not depend on the choice of π because the sets $\pi^n\mathcal{O}_k$ do not. Then $\|a\| = q^{-v(a)}$, where $q = |\mathcal{O}_k/\mathfrak{p}|$. The number $v(a)$ is called the *valuation* of a. It is the same as the one coming from the discrete valuation ring $\mathcal{O}_k$.

Now let l/k be an extension of nonarchimedean local fields. Let $\|\cdot\|_k$ and $\|\cdot\|_l$ be the respective modules, and let v_k and v_l be the respective valuations. Let π_k be a prime element of k. Then $v_l(\pi_k)$ is equal to some integer $e = e(l/k)$, and this is called the *ramification index* of l/k. This can also be described via the equality

$$\mathfrak{p}_k\mathcal{O}_l = \mathfrak{p}_l^{e(l/k)}.$$

Since $\mathfrak{p}_k \subset \mathfrak{p}_l$, we get an extension of residue fields $\mathcal{O}_k/\mathfrak{p}_k \subset \mathcal{O}_l/\mathfrak{p}_l$. Since both fields are finite, this extension is finite. We denote the degree of this extension by $f = f(l/k)$. Note that this discussion implies that we can find which of the fields $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$ is contained in a given nonarchimedean local field k: The characteristic of the residue field gives p, and the characteristic of k itself determines whether it is $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$. Furthermore, none of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$ is an extension of another.

We finish this lecture by stating a useful theorem about extensions of nonarchimedean local fields.

Theorem 2.5. *Let l/k be an extension of nonarchimedean local fields. Then*

$$[l : k] = e(l/k)f(l/k).$$

Lecture 3

Global Fields

We begin with the main definition.

Definition 3.1. A *global field* is either a finite extension of $\mathbb{Q}$ or a finite separable extension of $\mathbb{F}_q(t)$. The former of these fields are called *number fields* and the latter are called *function fields.*

Number theory is concerned with the arithmetic of these fields and their extensions.

Our first task will be to describe the absolute values on these fields. This will ultimately lead to important arithmetic data of these fields. Let $|\cdot|_1$ and $|\cdot|_2$ be absolute values on a field k. We say $|\cdot|_1$ and $|\cdot|_2$ are *equivalent* if they induce the same topology on k.

Now if K is a global field, V_K will denote the set of absolute values on K up to equivalence. An element of V_K will be called a *place.* To describe V_K, we need a definition.

Definition 3.2. Let K be a global field. A *prime ring* in K is a subring $\mathfrak{P}$ of K which is a discrete valuation ring and whose fraction field is K.

Let us give some examples. Let p be an integer prime, and let $\mathbb{Z}_{(p)}$ be the localization of $\mathbb{Z}$ at that prime. Then $\mathbb{Z}_{(p)}$ is a prime ring in $\mathbb{Q}$, as is easily checked.

One can do something similar with $\mathbb{F}_q(t)$. We have a subring $\mathbb{F}_q[t] \subset \mathbb{F}_q(t)$ which is a principal ideal domain. The irreducible polynomials in $\mathbb{F}_q[t]$ generate prime ideals, and all prime ideals are generated this way. So if P is an irreducible polynomial in $\mathbb{F}_q[t]$, we can localize at the ideal it generates and obtain a prime ring in $\mathbb{F}_q(t)$.

There is a prime ring in $\mathbb{F}_q(t)$ which does not come from a prime ideal in $\mathbb{F}_q[t]$, but rather from a prime ideal in an isomorphic subring. It is obtained by localizing the ring $\mathbb{F}_q[t^{-1}]$ at the ideal generated by t^{-1}. This is the only prime ring in $\mathbb{F}_q(t)$ which does not come from localizing $\mathbb{F}_q[t]$ at one of its prime ideals.

Now let K be a global field and $\mathfrak{P}$ a prime ring in K. Just as in the previous lecture, there is a valuation associated to $\mathfrak{P}$ on K, which is defined explicitly as follows. The maximal ideal in $\mathfrak{P}$ is generated by one element π, and for every $\alpha \in K$, there is a unique unit u in $\mathfrak{P}$ and a unique $n \in \mathbb{Z}$ such that $\alpha = u\pi^n$. The integer n does not depend on the choice of π, and is called the *valuation of α at $\mathfrak{P}$.* The function which extracts valuations at $\mathfrak{P}$ is denoted $v_{\mathfrak{P}}$. It is a homomorphism $K^\times \to \mathbb{Z}$.

Now the prime ring $\mathfrak{P}$ gives rise to a nonarchimedean absolute value on K as follows. Let r be a real number greater than 1. Define $|\alpha|_{r,\mathfrak{P}} = r^{-v_{\mathfrak{P}}(\alpha)}$ for $\alpha \in K^\times$, and $|0|_{r,\mathfrak{P}} = 0$.

Then $|\cdot|_{r,\mathfrak{P}}$ is positive definite, multiplicative, and one sees that it satisfies the strong triangle inequality upon noticing that $v_{\mathfrak{P}}$ satisfies $v_{\mathfrak{P}}(\alpha+\beta) \geq \min\{v_{\mathfrak{P}}(\alpha), v_{\mathfrak{P}}(\beta)\}$ for all $\alpha, \beta \in K^\times$. The induced topology does not depend on the number r, so each $r > 1$ gives an equivalent absolute value.

A lot of this theory seems to mirror the corresponding theory for local fields. As it turns out, we can use these absolute values to construct local fields, as follows. Given a global field and a prime ring $\mathfrak{P}$, let R be the ring of $\mathfrak{P}$-Cauchy sequences of elements of K, i.e., an element of R is a sequence $\{\alpha_1, \alpha_2, \dots\}$ such that for all $\epsilon > 0$, there is an N such that if $n, m \geq N$, then $|\alpha_n - \alpha_m|_{r,\mathfrak{P}} < \epsilon$ ($\mathfrak{P}$-Cauchyness does not depend on the choice of r). Let M be the set of sequences which converge to 0. Then R/M is a field into which K injects, which inherits the nonarchimedean absolute value $|\cdot|_{r,\mathfrak{P}}$ from K, and which is complete with respect to this absolute value. It is therefore a nonarchimedean complete field, and actually it is a local field (Exercise 3.1). We denote it by $K_{\mathfrak{P}}$. We write $\mathcal{O}_{\mathfrak{P}}$ for the valuation ring $\mathcal{O}_{K_{\mathfrak{P}}}$.

Now the inclusion $K \subset K_{\mathfrak{P}}$ restricts to an inclusion $\mathfrak{P} \subset \mathcal{O}_{\mathfrak{P}}$ and an inclusion of the maximal ideal in $\mathfrak{P}$ to that in $\mathcal{O}_{\mathfrak{P}}$. This then induces an inclusion of their residue fields, which is actually an isomorphism (Exercise 3.17). Thus, if q is the number of elements in the residue field of $\mathcal{O}_{\mathfrak{P}}$, then $|\cdot|_{q,\mathfrak{P}}$ is the absolute value on K which extends to the one given by the module on $K_{\mathfrak{P}}$. We write $\|\cdot\|_{\mathfrak{P}}$ for $|\cdot|_{q,\mathfrak{P}}$.

Returning to the classification of absolute values on a global field, we now state a theorem which says we are actually done describing V_K in the case of K a function field.

Theorem 3.3. *Let K be a function field. Then each absolute value on K is equivalent to one of the form $\|\cdot\|_{\mathfrak{P}}$ for some prime ring $\mathfrak{P}$ in K. Furthermore, if $\mathfrak{P}, \mathfrak{Q}$ are distinct prime rings in K, then $\|\cdot\|_{\mathfrak{P}}$ is not equivalent to $\|\cdot\|_{\mathfrak{Q}}$. In other words, the map $\mathfrak{P} \mapsto \|\cdot\|_{\mathfrak{P}}$ gives a bijection between the set of prime rings in K and V_K.*

This is not the end of the story for number fields, however. There are some nonarchimedean absolute values on any given number field. Let us describe them. Let K be a number field, and let n be its degree over $\mathbb{Q}$. (For short, we often say n is the *degree* of K). Then by basic field theory, there are exactly n embeddings (of fields) of K into the algebraically closed field $\mathbb{C}$. Some of these embeddings may have image contained in $\mathbb{R}$, and we call these embeddings *real.* The rest will be, by definition, *complex.* The complex embeddings will come in pairs, namely if $\sigma : K \to \mathbb{C}$ is a complex embedding, then its complex conjugate $\overline{\sigma}$ is another complex embedding.

Now $\mathbb{C}$ has its usual absolute value, and for each embedding $\sigma : K \to \mathbb{C}$, we can restrict this absolute value to an absolute value $|\cdot|_\sigma$ on K. If σ is complex, it must be the same as the one coming from its conjugate.

Theorem 3.4. *Let K be a number field. Then V_K is the disjoint union of two sets V_{f} and V_∞ such that: V_{f} consists of the equivalence classes of absolute values $\|\cdot\|_{\mathfrak{P}}$ coming from prime rings $\mathfrak{P}$ in K, all of which are different for different $\mathfrak{P}$; and V_∞ consists of equivalence classes of absolute values $|\cdot|_\sigma$ coming from embeddings $\sigma : K \to \mathbb{C}$, all of which are different for different σ's which are not complex conjugate to each other. Furthermore, all archimedean places are in V_{f} and all nonarchimedean places are in V_∞.*

The elements of V_{f} are called *finite* places and those of V_∞ are called *infinite* places. If K is a number field, $\sigma : K \to \mathbb{C}$ an embedding, then we can complete K with respect to

the $|\cdot|_\sigma$ as we did with the absolute values coming from prime rings. We will obtain either $\mathbb{R}$ or $\mathbb{C}$ depending on whether σ is, respectively, real or complex.

Now for number fields, the theory of the finite places has another important incarnation. To describe it, we need some results and definitions which belong to commutative algebra.

Definition 3.5. Let R be a subring of a ring S. An element $b \in S$ is called *integral over* R if there is are elements $a_0, a_1, \ldots, a_{n-1} \in R$ such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0.$$

Proposition 3.6. *Let A be a noetherian integral domain, K its field of fractions, and L a finite extension of K. The set B of all elements of L which are integral over A forms a ring, called the* integral closure *of A in L. In the case $L = K$, if $A = B$ then A is said to be* integrally closed. *In any case, no matter what L is, B is integrally closed.*

Definition 3.7. An integral domain A is called a *Dedekind domain* if it is noetherian, integrally closed, and all nonzero prime ideals in A are maximal.

Proposition 3.8. *If A is a Dedekind domain with fraction field K and L is a finite extension of K, then the integral closure of A in K is Dedekind.*

See Lang [4], or the exercises, for proofs of these facts.

As an example, all unique factorization domains are integrally closed. Here is a quick argument: Let A be a unique factorization domain and K its fraction field, and let a/b be a fraction which is fully reduced. If

$$(a/b)^n + c_{n-1}(a/b)^{n-1} + \cdots + c_1(a/b) + c_0 = 0$$

with $c_0, \ldots, c_{n-1} \in A$, then upon multiplying by b^n, we find that a^n is a multiple of b, contradiction. It follows that $\mathbb{Z}$ is integrally closed. Of course, $\mathbb{Z}$ is noetherian and all nonzero prime ideals in $\mathbb{Z}$ are maximal, so $\mathbb{Z}$ is a Dedekind domain.

Definition 3.9. Let K be a number field. The integral closure of $\mathbb{Z}$ in K is called the *ring of integers* in K and is denoted $\mathcal{O}_K$.

Let K be a number field and $\mathfrak{p}$ a nonzero prime (that is, prime ideal) in K. Then the localization $(\mathcal{O}_K)_{(\mathfrak{p})}$ of $\mathcal{O}_K$ at $\mathfrak{p}$ is a prime ring in K. This process is reversible: Given a prime ring $\mathfrak{P}$ with maximal ideal $\mathfrak{q}$, the ideal $\mathfrak{q} \cap \mathcal{O}_K$ is a nonzero prime, and the localization of $\mathcal{O}_K$ at it is $\mathfrak{P}$. This is Exercise 3.18. Thus we get a bijection between prime rings in K and nonzero primes in K, and hence also between these and finite places of K.

Now the nonzero primes of K give rise to a very important structure associated to K.

Definition 3.10. Let A be a Dedekind domain with fraction field K. A nonzero finitely generated A-submodule of K is called a *fractional ideal.* If $\mathfrak{a}, \mathfrak{b}$ are fractional ideals, we define their *product* $\mathfrak{ab}$ by as the A-submodule of K generated by the products $\{\alpha\beta \mid \alpha \in \mathfrak{a}, \beta \in \mathfrak{b}\}$. It is also finitely generated, and hence is a fractional ideal. We define the *inverse* $\mathfrak{a}^{-1}$ of a fractional ideal $\mathfrak{a}$ by $\mathfrak{a}^{-1} = \{\beta \in K \mid \alpha\mathfrak{a} \subset A\}$. This is also finitely generated because, briefly, for any $\alpha \in \mathfrak{a}$, $\alpha\mathfrak{a}^{-1}$ is in A, and A is noetherian. Hence $\mathfrak{a}^{-1}$ is a fractional ideal. The set of all fractional ideals of A will be denoted $J(A)$. Note that the fractional ideals contained in A are just the (nonzero) ideals.

The fundamental theorem about fractional ideals is this.

Theorem 3.11. *Let A be a Dedekind domain.*

(1) If $\mathfrak{a}, \mathfrak{b}$ are fractional ideals of A, then $\mathfrak{a} \subset \mathfrak{b}$ if and only if there is an ideal $\mathfrak{c} \subset A$ such that $\mathfrak{cb} = \mathfrak{a}$. In either case, we say that $\mathfrak{b}$ divides *$\mathfrak{a}$.*

(2) The set $J(A)$ is a group with product and inverse as above, with identity A. Moreover,

(3) $J(A)$ is free abelian on the nonzero prime ideals of A.

This theorem implies that every ideal in a Dedekind domain A factors uniquely into prime ideals. This is important arithmetically because not all rings of integers of number fields are unique factorization domains. In fact, usually they are not.

Now, using the theorem above, we can define directly a valuation associated to a prime in a number field. Let K be a number field and let $\alpha \in K$ be nonzero. Then we define $v_{\mathfrak{p}}(\alpha)$ to be the power of $\mathfrak{p}$ which occurs in the factorization of the fractional ideal $\alpha\mathcal{O}_K$. This is the same as the one associated to the prime ring $(\mathcal{O}_K)_{(\mathfrak{p})}$.

What about function fields? The ring $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ is indeed Dedekind, and in fact, all of the theory works for it except for the fact that there is a nonarchimedean place of $\mathbb{F}_q(t)$ which does not come from a prime ideal of $\mathbb{F}_q(t)$, namely the one associated to the prime ring $\mathbb{F}_q[t^{-1}]_{((t^{-1}))}$. But actually, it is worse: An arbitrary function field contains many copies of $\mathbb{F}_q(t)$, so the integral closure of some $\mathbb{F}_q[t]$ contained in a function field need not be unique. So it is not always clear what one should say is the analogue here of the ring of integers in a number field. However, in any function field K, it is the case that any choice of integral closure of a copy of $\mathbb{F}_q[t]$ in K gives a Dedekind domain in K whose localizations provide all but finitely many prime rings of K. It is also the case that no copy of $\mathbb{F}_q[t]$ in K will have an integral closure which provides all the prime rings of K. To remedy these complications, we take as an analogue of the group of fractional ideals the free abelian group on the prime rings of K. It is denoted $\mathrm{Div}(K)$ and its elements are called *divisors.* We will study a little the theory of divisors later.

Lecture 4

Adeles and Ideles

We begin with a theorem about Dedekind domains.

Theorem 4.1. *Let A be a Dedekind domain. Then A is a unique factorization domain if and only if it is a principal ideal domain.*

It is also easy to see that a Dedekind domain A is a principal ideal domain if and only if all of its fractional ideals are principal, i.e., generated as A-modules by one element. Furthermore, it is clear that even if A is not principal, the principal fractional ideals form a subgroup of $J(A)$.

Definition 4.2. Let A be a Dedekind domain. Denote the group of principal fractional ideals of A by $P(A)$. The group $C(A) = J(A)/P(A)$ is called the *ideal class group* of A.

Let K be a number field. We denote by h_K the order of the ideal class group, and call this the *class number* of K. A priori, the class number of a given number field may be an infinite cardinality. We will show in this lecture that this is not the case. Philosophically, this will say that the ring of integers in a number field does not deviate too far from having unique factorization (note that a Dedekind domain A is principal, and hence has unique factorization, if and only if the order of $C(A)$ is 1).

To begin, we let K be any global field. For $v \in V_K$, we denote by K_v the local field which is the completion of K at an absolute value which represents v. Then K_v is archimedean if and only if K is a number field and $v \in V_\infty$. If v is nonarchimedean, we denote by $\mathcal{O}_v$ the valuation ring of K_v.

Definition 4.3. The *adeles* of K, denoted $\mathbb{A}_K$, are the following subring of the direct product of all the completions of K:

$$\mathbb{A}_K = \left\{ (a_v)_{v \in V_K} \in \prod_{v \in V_K} K_v \;\middle|\; a_v \in \mathcal{O}_v \text{ for almost all } v \notin V_\infty \right\}.$$

Here, "almost all" means "all but finitely many," and the condition $v \notin V_\infty$ is supposed to be vacuous if K is a function field. The addition and multiplication is given componentwise,

of course. We also topologize $\mathbb{A}_K$ by declaring a base of neighborhoods about 0 to be

$$\left\{ \prod_{v \in V_K} U_v \;\middle|\; U_v \subset K_v \text{ is open for all } v,\ 0 \in U_v \text{ for all } v,\ U_v = \mathcal{O}_v \text{ for almost all } v \notin V_\infty \right\}.$$

The adeles of a global field are locally compact in view of Tychonoff's theorem. It is easily checked that the adeles also form a topological group. Some remarks: In his thesis, Tate called adeles *"valuation vectors,"* which gives a nice description for what they are. Philosophically, the adeles should also be viewed as the global analogue of a local field, since they contain all local information of a global field in each component.

Now we look at the units in the adeles.

Definition 4.4. Let K be a global field. The *ideles* of K are the group $\mathbb{I}_K = \mathbb{A}_K^\times$. So

$$\mathbb{I}_K = \left\{ (a_v)_{v \in V_K} \in \prod_{v \in V_K} K_v^\times \;\middle|\; a_v \in \mathcal{O}_v^\times \text{ for almost all } v \notin V_\infty \right\}.$$

We give it the topology with a base of neighborhoods about 1 given by

$$\left\{ \prod_{v \in V_K} U_v \;\middle|\; U_v \subset K_v^\times \text{ is open for all } v,\ 1 \in U_v \text{ for all } v,\ U_v = \mathcal{O}_v^\times \text{ for almost all } v \notin V_\infty \right\}.$$

The ideles of a global field are a locally compact abelian group again by Tychonoff. However, the topology we gave the ideles is *not* the subspace topology as a subset of the adeles!

Let K be a global field. Since K embeds into all of its completions, we have an embedding $K \subset \mathbb{A}_K$ which is given by the diagonal $\alpha \mapsto (\alpha, \alpha, \dots)$. This embedding makes sense in view of the fact that only finitely many valuations v have $|\alpha|_v \neq 1$ for any $\alpha \in K^\times$, where $|\cdot|_v$ is an absolute value in the class v. We will take this for granted, though see Exercise 4.2. From this it also follows that we get an embedding $K^\times \subset \mathbb{I}_K$, which we will use later.

Theorem 4.5. *With the embedding above, a global field K is discrete in its adeles $\mathbb{A}_K$.*

We give the idea of the proof, which requires a couple results from the next lecture which do not depend on this theorem. For K a number field, we consider first the open set $U \subset \mathbb{A}_K$ defined by

$$U = \prod_{v \in V_\mathrm{f}} \mathcal{O}_v \times \prod_{v \in V_\infty} K_v.$$

The elements of K which are in U must then have nonnegative valuation at all finite places. It follows that $K \cap U = \mathcal{O}_K$ because, for instance, by the ideal theory discussed in the previous lecture, the fractional ideal generated by an $\alpha \in K \cap U$ contains only positive powers of primes. Now Exercise 4.6 says that $\mathcal{O}_K$ embeds discretely into the component $\prod_{v \in V_\infty} K_v$ of U, and hence there is an open subset U_∞ of $\prod_{v \in V_\infty} K_v$ which contains only 0. Thus the open set $U' = \prod_{v \in V_\mathrm{f}} \mathcal{O}_v \times U_\infty$ is such that $K \cap U' = \{0\}$. It follows that K is discrete in $\mathbb{A}_K$.

For function fields, we use the following theorem, valid for any global field.

Theorem 4.6 (Product Formula)**.** *Let K be a global field and $\alpha \in K^\times$. Then*

$$\prod_{v \in V_K} \|\alpha\|_v = 1,$$

where $\|\cdot\|_v$ is the usual absolute value $\|\cdot\|_{\mathfrak{P}}$ on K if v comes from a prime ring $\mathfrak{P}$ in K, $\|\cdot\|_v = |\cdot|_\sigma$ if v comes from an real embedding σ, and $\|\cdot\|_v = |\cdot|_\tau^2$ if v comes from a complex embedding τ.

One proves this theorem by first proving it for $K = \mathbb{F}_q(t)$ or $K = \mathbb{Q}$, and then reducing to this case using the theory of extensions of places which we will develop in the next lecture. Also, it should be noted that the product in the theorem makes sense because, as we have said, only finitely many valuations v have $\|\alpha\|_v \neq 1$ for any $\alpha \in K^\times$.

Returning to the discreteness of a function field K, let $U = \prod_{v \in V_K} \mathcal{O}_v$. Then $K^\times \cap U$ consists of all elements in K with nonnegative valuation at all places. By the Product Formula, if any valuation of an $\alpha \in K^\times$ is positive, another must be negative. Therefore all valuations of an element in $K^\times \cap U$ are equal to 0. But then one shows that this implies that α is *constant,* i.e., α is contained in the largest extension of $\mathbb{F}_q$ contained in K (this is shown in Exercise 4.3). But such an extension is finite, so U contains only finitely many elements of K. Since the adeles are Hausdorff, $K \cap U$ is discrete, and so K is discrete.

To state our next theorem, we need a definition. We keep the notation $\|\cdot\|_v$ of the previous theorem.

Definition 4.7. Let K be a global field and let $a = (a_v)_{v \in V_K} \in \mathbb{I}_K$. Then we define the *norm* of a, denoted $\|a\|$, via

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

We define the group $\mathbb{I}_K^1$ to consist of those ideles which have norm 1.

By the Product Formula, $K^\times \subset \mathbb{I}_K^1$. We have

Theorem 4.8. *Let K be a global field. Then $K^\times$ is discrete in $\mathbb{I}_K^1$.*

The main theorem, whose proof is left to the exercises, is the following.

Theorem 4.9. *Let K be a global field.*
(1) $\mathbb{A}_K/K$ is compact under the quotient topology.
(2) $\mathbb{I}_K^1/K^\times$ is compact under the quotient topology.

Let us conclude by proving the finiteness of the class number. Let K be a number field. For $v \in V_{\mathrm{f}}$, denote also by v the associated valuation on $K_v^\times$, and denote by $\mathfrak{p}_v$ the prime ideal associated to v. Define a map $\mathbb{I}_K^1 \to J(\mathcal{O}_K)$ by $(a_v)_{v \in V_K} \mapsto \prod_{v \in V_{\mathrm{f}}} \mathfrak{p}_v^{v(a_v)}$. This map is surjective because it is as a map $\mathbb{I}_K \to J(\mathcal{O}_K)$ and, if $b = (b_v)$ is any idele and $c = \prod_{v \in V_{\mathrm{f}}} \|b_v\|_v$, then we can always change the infinite part of b so that $\prod_{v \in V_\infty} \|b_v\| = c^{-1}$, making it norm 1. Now the kernel U of this map is the set of norm 1 ideles with finite component in $\prod_{v \in V_{\mathrm{f}}} \mathcal{O}_v^\times$, and so the kernel is open. Hence the quotient $\mathbb{I}_K^1/U$ is discrete and isomorphic to $J(\mathcal{O}_K)$. But then $C(\mathcal{O}_K) \cong \mathbb{I}_K^1/K^\times \cdot U$, and the latter group is discrete and compact, hence finite. So we are done.

Lecture 5

Class Field Theory

We now apply the adelic theory of the last lecture to a highly arithmetic situation, namely that of class field theory. Class field theory is very deep and the proofs are extremely difficult, and for our purposes we shall be content with just knowing the statements of the main theorems.

To begin, we discuss extensions of global fields. Let K be a global field and L a finite separable extension. Let $\mathfrak{Q}$ be a prime ring of L. One can show that $\mathfrak{P} = \mathfrak{Q} \cap K$ is a prime ring of K. We say that $\mathfrak{Q}$ *lies over* $\mathfrak{P}$. Conversely, if $\mathfrak{P}$ is a prime ring of K, then there is a prime ring $\mathfrak{Q}$ lying over $\mathfrak{P}$. In fact there are a few, and we can try to say how many. For this, note that, as at the end of Lecture 2, the valuation $v_{\mathfrak{Q}}$ on L restricts to a multiple of the valuation $v_{\mathfrak{P}}$ on K. In fact, if π is a prime element of K and $e = e(\mathfrak{Q}/\mathfrak{P})$ is equal to the integer $v_{\mathfrak{Q}}(\pi)$, then $v_{\mathfrak{Q}} = e v_{\mathfrak{P}}$. We call e the *ramification index* of $\mathfrak{Q}/\mathfrak{P}$. Also, again as in Lecture 2, if $\mathfrak{p}$ is the maximal ideal in $\mathfrak{P}$ and $\mathfrak{q}$ that in $\mathfrak{Q}$, then there is a finite extension of residue fields $(\mathfrak{Q}/\mathfrak{q})/(\mathfrak{P}/\mathfrak{p})$. Its degree is denoted $f = f(\mathfrak{Q}/\mathfrak{P})$ and it is called the *inertia degree* of $\mathfrak{Q}/\mathfrak{P}$. All of this discussion goes through if we replace $\mathfrak{P}$ and $\mathfrak{Q}$ with the rings $\mathcal{O}_{\mathfrak{P}}$ and $\mathcal{O}_{\mathfrak{Q}}$ of the completions. Indeed, one easily sees that the extension L/K gives rise to an extension $L_{\mathfrak{Q}}/K_{\mathfrak{P}}$ and that the ramification indices and inertia degrees agree.

Theorem 5.1. *Let L/K be an extension of global fields of degree n. Let $\mathfrak{P}$ be a prime ring in K. Then there are only finitely many prime rings in L lying over $\mathfrak{P}$, call them $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r$, and we have*

$$n = \sum_{i=1}^{r} e(\mathfrak{Q}_i/\mathfrak{P}) f(\mathfrak{Q}_i/\mathfrak{P}).$$

The situation is even better when L/K is Galois. Then the Galois group $\mathrm{Gal}(L/K)$ acts on the prime rings in the obvious way: if $\sigma \in \mathrm{Gal}(L/K)$ then $\sigma\mathfrak{Q}$ is simply the image of $\mathfrak{Q}$ under σ. One shows in this case that the prime rings in L above a given prime ring in K are permuted transitively by the Galois group. Consequently, all ramification indices and inertia degrees are equal for each prime in L lying above the given one in K.

Now assume $\mathfrak{P}$ is a prime ring in a global field K and L is a finite Galois extension of K. Let $\mathfrak{Q}$ in L lie over $\mathfrak{P}$. Then the set of automorphisms σ of L/K for which $\sigma\mathfrak{Q} = \mathfrak{Q}$ is a subgroup D of $\mathrm{Gal}(L/K)$. Let λ and κ be the residue fields $\mathfrak{Q}$ and $\mathfrak{P}$, respectively. One can show (Exercise 5.1) that every $\sigma \in D$ induces an automorphism of λ/κ, and that

this gives an isomorphism $D \cong \mathrm{Gal}(\lambda/\kappa)$ as long as $e(\mathfrak{Q}/\mathfrak{P}) = 1$ (in which case we say $\mathfrak{Q}/\mathfrak{P}$ is *unramified*). In this case, there is an element $\sigma \in D \subset \mathrm{Gal}(L/K)$ whose image is the automorphism $x \mapsto x^q$ with $q = |\lambda|$. This $\sigma \in \mathrm{Gal}(L/K)$ is called the *Frobenius automorphism* associated to $\mathfrak{Q}/\mathfrak{P}$ and is denoted $\mathrm{Frob}(\mathfrak{Q}/\mathfrak{P})$. Furthermore, if $\mathfrak{Q}'$ also lies over $\mathfrak{P}$, then $\mathrm{Frob}(\mathfrak{Q}/\mathfrak{P})$ and $\mathrm{Frob}(\mathfrak{Q}'/\mathfrak{P})$ are conjugate in $\mathrm{Gal}(L/K)$. Thus if L/K is *abelian,* i.e., Galois with abelian Galois group, and $\mathfrak{Q}/\mathfrak{P}$ is unramified, then we can associate to $\mathfrak{P}$ an element $\mathrm{Frob}(\mathfrak{P}) \in \mathrm{Gal}(L/K)$. It is characterized by $\mathrm{Frob}(\mathfrak{P})\alpha \equiv \alpha^q \pmod{\mathfrak{p}}$ for all $\alpha \in \mathfrak{P}$, where $\mathfrak{p}$ is the maximal ideal in $\mathfrak{Q}$ and q is the order of the residue field.

Before we continue, we state one useful theorem. If L/K is any extension of global fields and $\mathfrak{P}$ a prime ring in K, then we say $\mathfrak{P}$ is *ramified* if any of its ramification indices is larger than 1.

Theorem 5.2. *Let L/K be an extension of global fields. Then only finitely many prime rings in K are ramified in L.*

Henceforth for the rest of the lecture we deal only with abelian extensions of global fields, and we will try avoid ramified prime rings. We are now in the setting of class field theory, which is the study of abelian extensions of a given global field.

To state the main theorems, we need a broader notion, in the number field case, of the ideal group, and in the function field case, of the divisor group defined at the end of Lecture 3. In either case, these were (isomorphic to) the free abelian groups on the prime rings of the global field in question. So let K be a global field. If S is a finite set of prime rings in K, we denote by J_K^S the free abelian group on the prime rings which are not in S. Then we denote by K^S the set of $\alpha \in K^\times$ such that $v_{\mathfrak{P}}(\alpha) = 0$ for all $\mathfrak{P} \in S$. Then there is a map $K^S \to J_K^S$ given by

$$\alpha \mapsto \sum_{\mathfrak{P} \notin S} v_{\mathfrak{P}}(\alpha) \cdot \mathfrak{P}.$$

There is also a map $\mathbb{I}_K \to J_K^S$ described as follows. If $v \in V_K$ is nonarchimedean, denote by $\mathfrak{P}_v$ the corresponding prime ring, and denote also by v the associated valuation. Then the map is

$$(a_v)_{v \in V_K} \mapsto \sum_{\mathfrak{P}_v \notin S} v(a_v) \cdot \mathfrak{P}_v.$$

The map $K^\times \to J_K^S$ factors through this one.

Now let L/K be an abelian extension of global fields. If S is the set of prime rings in K which ramify in L, then define a map $\mathrm{Art}_{L/K} : J_K^S \to \mathrm{Gal}(L/K)$ by

$$\mathrm{Art}_{L/K}(\sum n_{\mathfrak{P}}\mathfrak{P}) = \prod \mathrm{Frob}(\mathfrak{P})^{n_{\mathfrak{P}}}.$$

This map is called the *Artin map.*

Finally we define a map $\mathbb{I}_L \to \mathbb{I}_K$. If $w \in V_L$ resticts to v on K, then we say w *lies over* v, and write $w \mid v$. This notion of lying over becomes the same as the one above when w, v are valuations of prime rings. If w lies over v, then we get an extension of local fields L_w/K_v. Let $\mathrm{Nm}_v : \prod_{w|v} L_w \to K_v$ be given by $(a_w)_{w|v} \mapsto \prod_{w|v} \mathrm{Nm}_{L_w/K_v}(a_w)$. Putting all of maps Nm_v together for $v \in V_K$ gives the desired map $\mathrm{Nm} : \mathbb{I}_L \to \mathbb{I}_K$. So

$\mathrm{Nm}((a_w)_{w\in V_L}) = (\prod_{w|v} \mathrm{Nm}_{L_w/K_v}(a_w))_{v\in V_K}$ One proves that this is well defined and restricts to the usual field norm on $L^\times$, or even on L^S.

Now we can state the main theorems. For K a global field, let K^{ab} denote the largest abelian extension of K in some separable algebraic closure of K (exists because the composite of two abelian extensions is abelian).

Theorem 5.3 (Artin Reciprocity)**.** *Let K be a global field. Then there is a continuous homomorphism $\mathbb{A}\mathrm{rt} : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ (the latter group given the Krull topology) such that, for any abelian extension L/K, if S is the set of primes in K ramifying in L, the following diagram commutes:*

$$\begin{array}{ccc} \mathbb{I}_K & \xrightarrow{\mathbb{A}\mathrm{rt}} & \mathrm{Gal}(K^{\mathrm{ab}}) \\ \downarrow & & \downarrow \\ J_K^S & \xrightarrow{\mathrm{Art}_{L/K}} & \mathrm{Gal}(L/K). \end{array}$$

Furthermore, the image of $K^\times$ under $\mathbb{A}\mathrm{rt}$ is trivial and $\mathbb{A}\mathrm{rt}$ induces an isomorphism

$$\mathbb{I}_K/(K^\times \cdot \mathrm{Nm}(\mathbb{I}_L)) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

The map Nm induces a map, which we will also call Nm, from $\mathbb{I}_L/L^\times$ to $\mathbb{I}_K/K^\times$.

Theorem 5.4 (Existence Theorem)**.** *For every open subgroup N of $\mathbb{I}_K/K^\times$ of finite index, there is a finite abelian extension L of K such that $\mathrm{Nm}(\mathbb{I}_L/L^\times) = N$. Hence $\mathbb{A}\mathrm{rt}$ defines an isomorphism $(\mathbb{I}_K/K^\times)/N \cong \mathrm{Gal}(L/K)$.*

Example 5.5. Let K be a number field. Let $M = \ker(\mathbb{I}_K \to J(\mathcal{O}_K))$ and N the image of M in $\mathbb{I}_K/K^\times$. Then the quotient $(\mathbb{I}_K/K^\times)/N$ is isomorphic to $J(\mathcal{O}_K)/P(\mathcal{O}_K) = C(\mathcal{O}_K)$, as is immediately seen. The Existence Theorem and Artin Reciprocity imply the existence of an abelian extension H of K whose Galois group $\mathrm{Gal}(H/K)$ is the ideal class group of K. This is called the *Hilbert class field* of K. In fact, it is the largest extension of K which is both unramified and abelian. One can also make a similar construction with J^S with S a finite set, in place of $J(\mathcal{O}_K)$ to obtain examples of *ray class fields.* These will be unramified outside S.

Lecture 6

Algebraic Varieties

We now begin an interlude into the world of algebraic geometry. We will look at solution sets of polynomial equations over fields as geometric objects and try to study their properties geometrically. It will turn out that the function fields we have studied fit naturally into this picture.

Through most of this lecture, k will be a field which is assumed to be algebraically closed. At the end, we will let it be arbitrary. Let $\mathbb{A}^n$ denote the n-fold cartesian product of k with itself, $\mathbb{A}^n = k^n$. Then we may treat the polynomial ring $k[x_1, \ldots, x_n]$ as a ring of functions on k^n with values in k. For any finite set of functions $\{f_1, \ldots, f_m\}$ in $k[x_1, \ldots, x_n]$, we define $V(f_1, \ldots, f_m)$ to be the set of all points in $\mathbb{A}^n$ at which all of the functions $f_1, \ldots, f_n$ vanish simultaneously. This set may be empty, for instance if one of the functions f_i is a nonzero element of k (i.e., a constant). The set $V(f_1, \ldots, f_m)$ is the same as the set of all points in $\mathbb{A}^n$ at which all of the polynomials in the ideal generated by $f_1, \ldots, f_m$ vanish. But $k[x_1, \ldots, x_n]$ is noetherian, so every ideal is generated by such a finite set of functions. Therefore, it is enough to talk about sets $V(I)$ of points at which all of the functions in an ideal I vanish. Any subset of $\mathbb{A}^n$ of the form $V(I)$ for some ideal $I \subset k[x_1, \ldots, x_n]$ is called an *affine algebraic set.*

Now given any affine algebraic set $V(I)$, we can ask "what are all of the functions in $k[x_1, \ldots, x_n]$ which vanish on $V(I)$?". Sometimes the answer is I itself, but not usually. In fact, the following theorem tells us when:

Theorem 6.1 (Hilbert's Nullstellensatz)**.** *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. Denote by $\sqrt{I}$ the* radical *of I, that is, $\sqrt{I}$ is the set of all elements $f \in k[x_1, \ldots, x_n]$ such that $f^r \in I$ for some r. Then the set of all functions in $k[x_1, \ldots, x_n]$ vanishing on $V(I)$ is precisely $\sqrt{I}$.*

Every prime ideal is radical, i.e., is its own radical ideal. Thus a prime ideal in $k[x_1, \ldots, x_n]$ already contains all of the functions which vanish on its associated affine algebraic set. An affine algebraic set defined by a prime ideal will be called an *affine variety.* These are special geometrically for the following reason. An affine algebraic set is called *irreducible* if it cannot be decomposed into a union of two proper affine algebraic subsets, and it is a fact that an affine algebraic set is irreducible if and only if it is defined by a prime ideal. In fact, we have

Proposition 6.2. *The map $I \mapsto V(I)$ gives a one-to-one correspondence between:*
(1) Radical ideals and affine algebraic sets;

(2) Prime ideals and irreducible affine algebraic sets;
(3) Maximal ideals and points.

Let $V(I)$ be an affine algebraic set. A function $V(I) \to k$ is called *regular* if it is the restriction of a polynomial function in $k[x_1, \ldots, x_n]$ to $V(I)$. Such functions are determined up to a polynomial which vanishes on $V(I)$, i.e., an element of $\sqrt{I}$. Thus the ring of regular functions is just the ring $k[x_1, \ldots, x_n]/\sqrt{I}$. We will denote this ring also by $\mathcal{O}(V(I))$. The affine varieties are thus precisely the affine algebraic sets whose rings of regular functions are integral domains.

Now let X be an algebraic variety. The *dimension* of X is the length d of the longest chain

$$Y_0 \subset Y_1 \subset \cdots \subset Y_d = X$$

of irreducible affine algebraic subsets of X, each inclusion being proper. If $X \subset \mathbb{A}^n$, then the dimension of X is at most n. One proves this by translating the chain condition above into a chain

$$\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_d$$

where each $\mathfrak{p}_i$ is the prime ideal in $k[x_1, \ldots, x_n]$ associated with Y_i. Since it is a fact of commutative algebra that the largest chain of prime ideals in $k[x_1, \ldots, x_n]$ has length n, it follows that $\mathbb{A}^n$ has dimension n and X has smaller dimension. This is nice because it is not unreasonable to want the n-fold cartesian product of k to have dimension n, and any subset to have smaller dimension.

Now we define the projective space $\mathbb{P}^n$. Let $k^\times$ act on the $(n+1)$-fold cartesian product k^{n+1} by scaling each component. Then we can take the quotient by this action, but first we remove the origin $0 = (0, 0, \ldots, 0)$. This is the projective space, $\mathbb{P}^n = (k^{n+1} \backslash 0)/k^\times$. This can be thought of as the set of *lines* through the origin in $\mathbb{A}^{n+1}$; the orbit of each point in $\mathbb{A}^{n+1} \backslash 0$ under the action of $k^\times$ should be a line in $\mathbb{A}^{n+1}$ if we adjoin the origin.

We write the image of a point $(a_0, \ldots, a_n) \in \mathbb{A}^{n+1} \backslash 0$ in $\mathbb{P}^n$ as $[a_0, \ldots, a_n]$. If $c \in k^\times$, then $[a_0, \ldots, a_n] = [ca_0, \ldots, ca_n]$. For $0 \leq i \leq n$, let U_i be the set of all points $[a_0, \ldots, a_n]$ with $a_i \neq 0$. Then the map $[a_0, \ldots, a_n] \mapsto (\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i})$ is a bijection $U_i \to \mathbb{A}^n$.

Let $F_1, \ldots, F_m \in k[x_0, \ldots, x_n]$ be *homogeneous,* i.e. each monomial in F_i is the same degree, for each i separately. Then the set of points in $\mathbb{P}^n$ where each $F_1, \ldots, F_m$ vanish simultaneously is well defined because of the homogeneity. We will denote this set by $V(F_1, \ldots, F_m)$. For each $i = 1, \ldots, m$ and $j = 0, \ldots, n$, let $F_{i,j}$ be the polynomial in $k[x_0, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n]$ obtained by substituting 1 for the variable x_j in F_j. Then $X_j = V(F_1, \ldots, F_m) \cap U_j$ is the affine algebraic set $V(F_{1,j}, \ldots, F_{m,j})$ in $U_j \cong \mathbb{A}^n$. If each X_j is an affine variety, then we say $V(F_1, \ldots, F_m)$ is a *projective variety.* One can also define a projective variety through irreducibility, similar to the affine case.

Now we let k be arbitrary. An affine variety (over $\overline{k}$) is *defined over k* if it is equal to $V(f_1, \ldots, f_n)$ for some polynomials with coefficients in k instead of just in $\overline{k}$. Similarly a projective variety is defined over k if it can be defined by homogeneous polynomials with coefficients in k. In either case, we can let the absolute Galois group $\mathrm{Gal}(\overline{k}/k)$ act on an affine of projective variety X by applying an automorphism to each coordinate of a given point. The *k-points* of X are defined to be the fixed points under this action. For X affine, these are precisely the points with coordinates in k.

Next we define and study maps between varieties. Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be

affine varieties. Then a map $\varphi : X \to Y$ is called *regular* if it is locally given by quotients of polynomials, i.e., if for each $(a_1, \ldots, a_n) \in X$, there are polynomials $P_1, \ldots, P_m, Q_1, \ldots, Q_m$ in n variables with the Q_i's not vanishing on $(a_1, \ldots, a_n)$ such that φ is given by $\varphi(x) = (P_1(x)/Q_1(x), \ldots, P_m(x)/Q_m(x))$. If X, Y are defined over k, then φ is said to be *defined over* k if the P_i's and Q_i's can be taken to have coefficients in k. X and Y are said to be *isomorphic* if there is a regular map between them with a regular two-sided inverse. If X and Y are defined over k, then they are *k-isomorphic* if there is a regular map defined over k with a regular two-sided inverse defined over k. The definitions of regular map for projective varieties are similar, except that the P_i's and Q_i's are homogeneous. Moreover, we may have regular maps between affine and projective varieties, but it is a theorem that every regular map from a projective variety to an affine variety is constant. This also implies that an affine variety and projective variety are isomorphic if and only if they are points.

For an affine variety, one proves that, when $\overline{k}$ is identified with $\mathbb{A}^1$, the regular functions are exactly the regular maps to $\mathbb{A}^1$. Let $\varphi : X \to Y$ be a morphism of affine varieties. Since regular maps can be composed, for every regular function $f \in \mathcal{O}(Y)$, we can define a regular function g on X by $g = f \circ \varphi$. This construction thus gives a homomorphism of rings $\varphi^* : \mathcal{O}(Y) \to \mathcal{O}(X)$.

Theorem 6.3. *A regular map $\varphi : X \to Y$ between affine varieties is entirely determined by the map $\varphi^* : \mathcal{O}(Y) \to \mathcal{O}(X)$, and for every homomorphism $F : \mathcal{O}(Y) \to \mathcal{O}(X)$ there is a regular map ψ such that $F = \psi^*$. This correspondence is functorial (i.e., respects composition). Consequently, X and Y are isomorphic if and only if $\mathcal{O}(X)$ and $\mathcal{O}(Y)$ are.*

Lecture 7

Function Fields and Curves

Let us start with a proposition.

Proposition 7.1. *The dimension of a variety (affine or projective) is an isomorphism invariant. In particular it does not depend on the dimension of the ambient space $\mathbb{A}^n$ or $\mathbb{P}^n$.*

One proves this by defining a certain topology on a variety (the *Zariski topology*) and proving that the dimension is an invariant of this topology, and that regular maps are continuous in this topology (so in particular isomorphisms are homeomorphisms).

Definition 7.2. A *curve* is a variety of dimension 1.

In order to proceed from here, we need a technical definition. Let k be any algebraically closed field (later we will make k arbitrary). Let X be an affine curve over k. The points of the curve are in bijection with the maximal ideals of $\mathcal{O}(X)$ by Theorem 6.2. Let $P \in X$ be a point and let $\mathfrak{m}_P \subset \mathcal{O}(X)$ be the maximal ideal corresponding to P. One proves that the field $\mathcal{O}(X)/\mathfrak{m}_P$ is k. X is called *nonsingular at* P if $\mathfrak{m}_P/\mathfrak{m}_P^2$ is 1-dimensional as a k-vector space, and X is *nonsingular* if it is nonsingular at every point.

If $X \subset \mathbb{P}^n$ is instead a projective curve, then it is called nonsingular if $X \cap U_i$ is nonsingular for all i, where $U_i \cong \mathbb{A}^n$ are the sets from the previous lecture. (One can prove that each $X \cap U_i$ is either empty or an affine curve). We only make these definitions for sake of completeness and we will actually never use them directly. Of course, one needs to use them to prove about them the facts that we do not prove here.

Now if X is a projective curve, it is a fact that the rings $\mathcal{O}(X \cap U_i)$ all have the same fraction field. We denote this field by $K(X)$ and call it the *function field of* X. It coincides with the field of regular maps $X \to \mathbb{P}^1$, so it does not depend on the projective embedding. It has transcendence degree 1 over k.

Now if we restrict our attention to nonsingular projective curves, it turns out that we get a theorem much like Theorem 6.3.

Theorem 7.3. *A nonsingular projective curve is completely determined by its function field, and every field of transcendence degree* 1 *over k is the function field of a nonsingular projective curve over k. Moreover, this correspondence is functorial, so every regular map $X \to Y$ of nonsingular projective curves gives rise to, and comes from, an inclusion of function fields $K(Y) \to K(X)$ in the other direction.*

Let us describe this correspondence a little more explicitly. Let K be a function field of a nonsingular projective curve X over k. Let $P \in X \cap U_i$ for some i. Then the localization $\mathcal{O}_P$ of $\mathcal{O}(X \cap U_i)$ at the maximal ideal corresponding to P is a discrete valuation ring. Its fraction field is K, so we call it a *prime ring* of K or of X. It turns out that all of these prime rings $\mathcal{O}_P$ are distinct and each prime ring is of this form.

Now given an inclusion of function fields $K(Y) \to K(X)$ and given $P \in X$, we can consider the ring $\mathcal{O}_P \cap K(Y)$. One shows that this is a prime ring in $K(Y)$ and that, if we let Q_P denote the point in Y to which it corresponds, then $P \mapsto Q_P$ is the regular map to which the inclusion of function fields corresponds.

Now let k be arbitrary.

Theorem 7.4. *Assume that X is a nonsingular projective curve defined over k. Then there is a unique extension K of k of transcendence degree 1 over k such that $K \cap \bar{k} = k$ and $K \otimes_k \bar{k} = K(X)$. We call it the* k-function field *of X. It coincides with the field of regular maps $X \to \mathbb{P}^1$ which are defined over k.*

For example, if k is a finite field, then the field K whose existence is asserted in the theorem is global field of positive characteristic. This is the example that the reader should bear in mind.

So what are the prime rings of a k-function field K of a nonsingular projective curve X defined over k? They do not correspond to k-points, but rather to $\mathrm{Gal}(\bar{k}/k)$-orbits of points in X. More precisely, if $\mathfrak{P}$ is a prime ring in K, then $\mathfrak{P}$ is the intersection of a prime ring of $K(X)$ with K, and each such prime ring in $K(X)$ corresponds to one of the points in the Galois orbit.

Let $\mathrm{Div}(K)$ be the free abelian group on the prime rings of K. We will call its elements k-divisors. Divisors are an important tool because they actually provide a useful way to describe maps into projective space, but we will not go into this here. For $\mathfrak{P}$ a prime ring of K, let $\deg(\mathfrak{P})$ be the degree over k of the residue field of $\mathfrak{P}$. This is an integer, and for $D = \sum n_{\mathfrak{P}}\mathfrak{P} \in \mathrm{Div}(K)$, let $\deg(D) = \sum n_{\mathfrak{P}} \deg(\mathfrak{P})$. For $f \in K$, let $\mathrm{div}(f) = \sum v_{\mathfrak{P}}(f)\mathfrak{P}$, where $v_{\mathfrak{P}}$ is the valuation associated with the prime ring $\mathfrak{P}$. Then we have the following theorem, which immediately implies the Product Formula 4.6 for function fields in case k is a finite field.

Theorem 7.5.

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

For two k-divisors $D = \sum n_{\mathfrak{P}}\mathfrak{P}$ and $E = \sum n'_{\mathfrak{P}}\mathfrak{P}$, we write $D \geq E$ if $n_{\mathfrak{P}} \geq n'_{\mathfrak{P}}$ for all prime rings $\mathfrak{P}$ in K. If D is a k-divisor, the k-vector space of all elements $f \in K$ with $\mathrm{div}(f) \geq -D$ is finite dimensional and is denoted $L(D)$. Its dimension is denoted $\ell(D)$. $L(D)$ is an important space in the study of projective embeddings of X. We finish with the following extremely important theorem, again important in the study of projective embeddings.

Theorem 7.6 (Riemann-Roch)**.** *Let X be a nonsingular projective curve defined over k and K is k-function field. Then there is a k-divisor $\mathcal{K}$ with the property that*

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

The number $\ell(\mathcal{K})$ does not depend on $\mathcal{K}$ and is called the genus *of X.*

We will prove this theorem later in case k is a finite field using abstract harmonic analysis on the adeles of a global field of positive characteristic.

Lecture 8

The Weil Conjectures

This lecture is not important for the sequel except for motivation. It describes one of the most important problems in number theory and algebraic geometry solved in the twentieth century.

One of the main questions asked in number theory is this: Given a system of polynomial equations with coefficients in a number field or its ring of integers, how many solutions does it have? This question is the one which *Diophantine geometry* tries to answer. In this lecture, we will study the reduction of this question modulo a prime.

So we want to ask how many points does a given variety X defined over $\mathbb{F}_q$ have? As stated, this question is vague. Clearly the answer is always "infinitely many" if we mean to count the $\overline{\mathbb{F}}_q$-points, so we wish to ask how many $\mathbb{F}_{q^n}$-points it has for each n.

To this end, assume X is a projective variety of dimension d defined over $\mathbb{F}_q$. Let a_n be the number of $\mathbb{F}_{q^n}$-points of X. We define the *zeta function of* X to be a power series determined by the a_n's as follows:

$$Z(X,t) = \exp\left(\sum_{n=1}^{\infty} a_n \frac{t^n}{n}\right).$$

This is a sort of *generating function* of the a_n's. In particular, it is determined as a power series in t by the a_n, and vice-versa. So we can hope that arithmetic properties of the variety X can be deduced by function-theoretic properties of $Z(X,t)$.

The Weil Conjectures are then as follows.

(1) [Rationality] The function $Z(X,t)$ is a rational function in t with coefficients in $\mathbb{Q}$.

(2) [Functional Equation] There is an integer E such that

$$Z\left(\frac{1}{q^d t}\right) = \pm q^{dE/2} t^E Z(X,t).$$

(3) [Riemann Hypothesis] We have that the function $Z(X,t)$ has the form

$$Z(X,t) = \prod_{i=0}^{2d} P_i(t)^{(-1)^{i+1}}$$

with $P_0(t) = 1 - t$ and $P_{2d}(t) = 1 - q^d t$, and each P_i decomposes as

$$P_i(t) = \prod_j (1 - \alpha_{ij} t)$$

where α_{ij} are algebraic integers in $\mathbb{C}$ (i.e., in some ring of integers of a number field considered as a subfield of $\mathbb{C}$) with $|\alpha_{ij}| = q^{i/2}$.

There is one more conjecture which is considered as part of the Weil Conjectures and it relates the degrees of the P_i's to topological invariants of an associated complex manifold. We will not describe this in detail here, but we can say what it means in the case of nonsingular curves. If X is a nonsingular curve of genus g, then it says that P_1 has degree $2g$, and also that $E = 2g - 2$.

Let us prove a proposition which illustrates the application of information about the zeta function to arithmetic properties of varieties.

Proposition 8.1. *Let X be a nonsingular projective curve of genus g over $\mathbb{F}_q$. Then the numbers a_n are determined by $a_1, \ldots, a_g$.*

Proof. By the description of the zeta function in the Riemann hypothesis, $(1 - t)(1 - qt)Z(X, t)$ is a polynomial P_1 of degree $2g$. The polynomial

$$P_1(t) = (1 - t)(1 - qt) \exp\left(\sum_{n=1}^{\infty} a_n \frac{t^n}{n} \right)$$

has constant term 1, and the coefficients of $t, t^2, \ldots, t^g$ are just rational combinations of $a_1, \ldots, a_g$, and are therefore determined. The functional equation then implies that

$$\begin{aligned} P_1\left(\frac{1}{qt}\right) &= \left(1 - \frac{1}{qt}\right)\left(1 - \frac{1}{t}\right)(\pm q^{1-g} t^{2-2g}) \frac{1}{(1 - qt)(1 - t)} P_1(t) \\ &= \pm q^{1-g} t^{2-2g} \frac{-1}{qt} \frac{-1}{t} P_1(t) = \pm q^{1-g} t^{-2g} P_1(t). \end{aligned}$$

So the ith coefficient is a multiple of the $(2g - i)$th coefficient. Since we know the first g coefficients, we know all of them. Thus the zeta function is determined, and hence so are the a_n's. □

The rationality of the zeta function was first proved by Dwork in 1960 using methods of p-adic analysis. Then Grothendieck, while developing the theory of schemes, created methods which were able to settle both the functional equation and rationality. This was his ℓ-adic cohomology theory. Grothendieck conjectured the existence of a cohomology theory with extremely deep properties which would provide a proof of the Riemann hypothesis. These conjectures, called the Standard Conjectures, are still far from resolved. However, about a decade after Grothendieck's proof of the functional equation, Deligne developed the ℓ-adic cohomology enough to prove the Riemann hypothesis and settle the Weil Conjectures in their entirety.

Let us discuss the methods of Grothendieck a little. Let ℓ be a prime different from the characteristic of the base field $\mathbb{F}_q$. To each variety over $\mathbb{F}_q$, one can associate a sequence of

vector spaces over the field $\mathbb{Q}_\ell$ of ℓ-adic numbers. These are denoted $H^i(X, \mathbb{Q}_\ell)$, $i \geq 0$. For readers with enough background in algebraic geometry, they are obtained from the étale cohomology groups of the constant sheaf $\mathbb{Z}/\ell^n\mathbb{Z}$ via the limit

$$H^i(X, \mathbb{Q}_\ell) = \varprojlim (H^i_{\text{ét}}(X, \mathbb{Z}/\ell^n\mathbb{Z})) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

These vector spaces are (contravariantly) functorial in X, which means if $\psi : X \to Y$ is a regular map, we get a morphism of vector spaces $\psi^* : H^i(Y, \mathbb{Q}_\ell) \to H^i(X, \mathbb{Q}_\ell)$, and this association respects composition of maps.

Now there is a regular map Frob : $X \to X$, called the *Frobenius map,* which raises each coordinate of a point in X to the power q. The points in X which are fixed by it are exactly the $\mathbb{F}_q$-points, as is easily seen. Similarly, the fixed points of the nth iterate Frob^n are the $\mathbb{F}_{q^n}$-points of X. So to recover a_n, we only need to count the fixed points of Frob^n. But the ℓ-adic cohomology allows us to do this: The ℓ-adic cohomology is supposed to behave like, say, singular cohomology in topology, and there are many important theorems about singular cohomology which have analogues in the ℓ-adic cohomology. For instance, the Lefschetz Fixed Point Formula has an analogue which, when applied to Frob^n states:

Theorem 8.2 (Lefschetz Theorem for Frob^n)**.** *We have*

$$a_n = \sum_{i=0}^{2d} (-1)^i \operatorname{Tr}((\text{Frob}^*)^n; H^i(X, \mathbb{Q}_\ell))$$

Here the trace is taken on the vector space $H^i(X, \mathbb{Q}_\ell)$. This makes sense because the ℓ-adic cohomology groups of X are known to be finite dimensional.

The limit on the sum is $2d$ because the ℓ-adic cohomology groups vanish for $i > 2d$. This is reasonable in light of the analogy with singular cohomology where the ith group will vanish for $i > 2d$ on a complex manifold of complex dimension d.

To prove the rationality of the zeta function, one simply applies the following lemma from linear algebra, whose proof is left as an exercise.

Lemma 8.3. *Let V be a finite dimensional vector space over a field k, and $\varphi : V \to V$ a linear map. Then the identity*

$$\exp\left(\sum_{n=1}^{\infty} \operatorname{Tr}(\varphi^n) \frac{t^n}{n}\right) = \det(1 - \varphi t)^{-1}$$

holds in the ring $k[[t]]$

Therefore

$$Z(X, t) = \prod_{i=0}^{2d} \det(1 - \text{Frob}^* t)^{(-1)^{i+1}}$$

The polynomials $\det(1 - \text{Frob}^* t)$ have $\mathbb{Q}_\ell$-coefficients, and $Z(X, t)$ has rational coefficients. One shows that this implies that $\det(1 - \text{Frob}^* t)$ has rational coefficients, so we get the rationality of the zeta function.

The functional equation is proved similarly, using an analogue of Poincaré duality. We have relegated this to the exercises.

Lecture 9

Zeta Functions and L-Functions

In this lecture, we will continue to define more zeta functions and study their properties. The first type will be one associated to a global field, and in the case of a function field, such a zeta function will be the same after a certain change of variable as the one associated to the curve from which the function field comes (Exercise 9.1).

If K is a global field and $\mathfrak{P}$ a prime ring, we denote by $\mathbb{N}\mathfrak{P}$ the order of its residue field.

Definition 9.1. Let K be a global field. We define the *zeta function* of K of a complex variable s as

$$\zeta_K(s) = \prod_{\mathfrak{P}} (1 - (\mathbb{N}\mathfrak{P})^{-s})^{-1}.$$

Here the product is taken over all prime rings in K. In case K is a number field, ζ_K is called the *Dedekind zeta function* of K, and in case $K = \mathbb{Q}$, it is called the *Riemann zeta function* and denoted simply by ζ.

Proposition 9.2. *The product defining the zeta function of a global field K converges for $\Re s > 1$. Furthermore, in case K is a number field, then*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{(\mathbb{N}\mathfrak{a})^s}$$

where the sum is over all ideals of $\mathcal{O}_K$ and $\mathbb{N}\mathfrak{a}$ is the order of $\mathcal{O}_K/\mathfrak{a}$.

We sketch the proof for number fields. First, it is a standard fact, whose proof we leave to the interested reader, that the Riemann zeta function

$$\zeta(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}$$

converges for $\Re s > 1$ and can be written as

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

This follows from unique prime factorization,

$$\zeta(s) = \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \cdots\right)\left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \cdots\right)\left(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \cdots\right)\cdots.$$

This proves the claim for $K = \mathbb{Q}$, and the formula for general number fields K follows the same way, using unique factorization of ideals and the fact that $\mathbb{N}$ is multiplicative (Exercise 9.2). In general, we know that a prime ring in $\mathbb{Z}$ has at most $n = [K : \mathbb{Q}]$ prime rings in $\mathcal{O}_K$ lying over it by Theorem 5.1. If $\mathfrak{P}$ lies over a prime p, the factor $(1 - (\mathbb{N}\mathfrak{P})^{-s})^{-1}$ is smaller than $(1 - p^{-s})^{-1}$ for $\Re s > 1$, and since there are at most n such factors, the zeta function of K is at worst as big as the nth power of the Riemann zeta function. In any case, it still converges for $\Re s > 1$, so we are done.

Theorem 9.3. *The zeta function of a global field K continues meromorphically to the entire complex plane.*

We will describe how to prove this and much more later. We will get a functional equation and describe the location of the poles, in particular.

Let us now formulate Artin Reciprocity in terms of similar functions to the ones defined above. Let L/K be a finite Galois extension of global fields, and let S be the set of ramified prime rings in K. Let ρ be a representation of $\mathrm{Gal}(L/K)$ on a finite dimensional vector space V over $\mathbb{C}$, i.e., ρ is a homomorphism $\mathrm{Gal}(L/K) \to \mathrm{GL}(V)$. For a prime ring $\mathfrak{P} \notin S$, let $P_{\mathfrak{P}}$ be the polynomial defined by

$$P_{\mathfrak{P}}(t) = \det(1 - \rho(\mathrm{Frob}(\mathfrak{P}))t)$$

Note that $\mathrm{Frob}(\mathfrak{P})$ is only determined up to conjugation, but the polynomial $\det(1 - \varphi t)$ is defined on the conjugacy class of φ for any $\varphi \in \mathrm{GL}(V)$. Thus $P_{\mathfrak{P}}$ is well defined. We define the *Artin L-function* of the representation ρ via

$$L(s, \rho) = \prod_{\mathfrak{P} \notin S} (P_{\mathfrak{P}}((\mathbb{N}\mathfrak{P})^{-s}))^{-1}.$$

There is a way to deal with the ramified primes, and it is not too hard, but it will not be important to us here, so we omit it.

Artin's Conjecture is that $L(s, \rho)$ is analytic in the whole complex plane. This was proved by Weil for function fields, and meromorphicity was proved by Brauer, but the conjecture is still unresolved. We will prove meromorphicity in the case L/K abelian later on. The first step in this direction is a reformulation of Artin Reciprocity, which we now describe.

Let L/K be abelian now. Then one knows from basic representation theory that the representation $\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}(V)$ decomposes into a direct sum of 1-dimensional representations, i.e., there is a decomposition $V = V_1 \oplus \cdots \oplus V_d$ where $d = \dim V$ and $\dim V_i = 1$ for all i, such that for all $\sigma \in \mathrm{Gal}(L/K)$, $\rho(\sigma)$ maps each V_i into itself. Let $\rho_i = \rho|_{V_i}$ and identify $\mathrm{GL}(V_i)$ with $\mathbb{C}^\times$. Then $\rho_i(\sigma)$ is a scalar of absolute value 1, and

$$P_{\mathfrak{P}}(t) = \prod_{i=1}^{d} (1 - \rho_i(\mathrm{Frob}(\mathfrak{P}))t).$$

Therefore

$$L(s, \rho) = \prod_{i=1}^{d} L(s, \rho_i).$$

So $L(s, \rho)$ has a meromorphic continuation for all ρ if and only if the same is true for 1-dimensional ρ. So we consider this case.

Now let $\chi : \mathbb{I}_K/K^\times \to S^1$ be a continuous homomorphism, where S^1 is the unit circle in $\mathbb{C}^\times$, and assume χ is trivial on the image in $\mathbb{I}_K/K^\times$ of the product $\prod_{\mathfrak{P}} \mathcal{O}_{\mathfrak{P}}^\times$ of all the local units. We will call such a homomorphism a *Hecke character*. We define the *Hecke L-function* of χ via

$$L(s, \chi) = \prod_{\mathfrak{P} \notin S} (1 - \chi(\pi_{\mathfrak{P}})(\mathbb{N}\mathfrak{P})^{-s})^{-1}$$

where $\pi_{\mathfrak{p}}$ is a prime element of $K_{\mathfrak{P}}$ on the $\mathfrak{P}$ component of $\mathbb{I}_K$ and 1 everywhere else, and we recall that S is the set of ramified prime rings in K. This does not depend on the choice of $\pi_{\mathfrak{P}}$ because of the condition on the local units. We can now restate Artin Reciprocity.

Theorem 9.4 (Artin Reciprocity, Second Form)**.** *Let L/K be an abelian extension of global fields. Let ρ be a representation of* $\mathrm{Gal}(L/K)$ *on a 1-dimensional complex vector space. Then there is a Hecke character χ such that*

$$L(s, \rho) = L(s, \chi).$$

A Hecke character χ defines a homomorphism $\psi : \mathbb{I}_K/K^\times \to S^1$. For any representation $\rho : \mathrm{Gal}(L/K) \to S^1$, this theorem says that there is such a ψ such that these two homomorphisms agree after passing though Frobenius. An easy exercise in representation theory says that if $f : G \to H$ is a homomorphism of abelian groups such that any 1-dimensional representation of H is determined by a 1-dimensional representation of G via f, then f is surjective. Applied to our situation, this says exactly that, if we accept that the Artin map is injective after taking the quotient by $\mathrm{Nm}(\mathbb{I}_L/L^\times)$, then it is an isomorphism $\mathbb{I}_K/(K^\times \mathrm{Nm}(\mathbb{I}_L)) \to \mathrm{Gal}(L/K)$.

In any case, we will show later (in the exercises for Lecture 13) that the Hecke L-functions have a meromorphic continuation, and hence so do the Artin L-functions.

Lecture 10

Abstract Fourier Analysis

In his thesis, John Tate used Fourier analysis on the adeles in order to reprove the analytic continuation and functional equation of Hecke L-functions, first proven by Hecke himself. In doing so, he gave in a very elegant and unified theory which turned out to be instrumental for many later advances in number theory, including the Langlands program. In this lecture we describe the basic tools necessary to develop the material in Tate's Thesis, i.e., the Fourier analysis.

Let G be a locally compact abelian group. A *character* on G is a continuous homomorphism $\chi : G \to S^1$ where S^1 is the unit circle in $\mathbb{C}^\times$. As functions, characters can be multiplied, and as such, they form a group $\widehat{G} = \{\text{characters on } G\}$. The group $\widehat{G}$ is called the *Pontryagin dual* of G. We give it a topology as follows. Let B be the collection of sets of the form $\{\psi \in \widehat{G} \mid \psi(K) \subset U\}$ for compacts $K \subset G$ and open sets $U \subset S^1$. We declare B to be a subbase for the topology on $\widehat{G}$, i.e., a base is generated by finite intersections in B.

Theorem 10.1. *The Pontryagin dual $\widehat{G}$ of G is a locally compact abelian group.*

The proof is not easy; one way, carried out in Folland [2], is to study representations of locally compact groups on infinite dimensional Hilbert spaces.

Let G be a locally compact abelian group. We can define a map $G \to \widehat{\widehat{G}}$ as follows. If $x \in G$, we map x to the character $\psi \mapsto \psi(x)$. This is a continuous homomorphism, and in fact:

Theorem 10.2 (Pontryagin Duality)**.** *The map $G \to \widehat{\widehat{G}}$ given by $x \mapsto (\psi \mapsto \psi(x))$ is an isomorphism of topological groups.*

Example 10.3. Let k be a local field. The duality theory for k is very easy. Let ψ be any nontrivial character. It is easy enough to see that one must exist, otherwise if not, then by duality, k itself would have to be trivial. Then for any $x \in k$, we can define the character ψ_x by $\psi_x(y) = \psi(xy)$. It turns out that the map $x \mapsto \psi_x$ is an isomorphism of topological groups, so $k \cong \hat{k}$!

Now we can also construct explicitly a nontrivial character ψ. For $k = \mathbb{R}$ we let $\psi(x) =$

$e^{2\pi ix}$. For $k = \mathbb{Q}_p$ we let

$$\psi\left(\sum_{i=-m}^{\infty} a_i p^i\right) = \exp\left(2\pi i \sum_{i=-m}^{-1} a_i p^i\right),$$

where $a_i \in \{0, \ldots, p-1\}$ and the p on the right hand side is treated as an element of $\mathbb{Q} \subset \mathbb{R}$. Similarly, for $\mathbb{F}_p((t))$, we let

$$\psi\left(\sum_{i=-m}^{\infty} a_i t^i\right) = \exp\left(2\pi i \sum_{i=-m}^{-1} a_i p^i\right).$$

Any other local field is an extension of one of these, and so we let $\psi(x) = \psi_0(\mathrm{Tr}_{k/k_0}(x))$ where k_0 is one of the three local fields listed above and ψ_0 is its character. The character ψ is called the *standard character* of k. Note that the standard character is not canonically defined for k of characteristic $p > 0$ because the subfield isomorphic to $\mathbb{F}_p((t))$ is not unique.

We state two useful propositions before we proceed to the Fourier analysis.

Proposition 10.4. *Let G be a compact abelian group and ψ a nontrivial character on it. Then*

$$\int_G \psi(x)\, d\mu(x) = 0$$

where μ is a Haar measure on G.

Proposition 10.5. *If G is compact then $\widehat{G}$ is discrete, and vice-versa; if G is discrete then $\widehat{G}$ is compact.*

Now let G be any locally compact abelian group with Haar measure μ. Let $f \in L^1(G)$. We define the *Fourier transform* $\hat{f}$ of f by

$$\hat{f}(\psi) = \int_G f(x)\psi(x)\, d\mu(x).$$

It is a function on $\widehat{G}$. There is also an inversion formula:

Theorem 10.6 (Fourier Inversion)**.** *Let G be a locally compact abelian group with Haar measure μ. Then there is a Haar measure $\hat{\mu}$ such that if $f \in L^1(G)$ and $\hat{f} \in L^1(\widehat{G})$, then*

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

(Note that the complex conjugate of a character is its multiplicative inverse). In other words

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

A pair $(\mu, \hat{\mu})$ of Haar measures on G and $\widehat{G}$ is called *self-dual.* We have $(c\mu)\hat{} = c^{-1}\hat{\mu}$.

Example 10.7. Let k be a local field and ψ its standard character. Since $\hat{k} \cong k$ via $x \mapsto (y \mapsto \psi(xy))$, we can ask what is the Haar measure on k so that the pair (μ, μ) is self-dual. We state the result and leave it for the exercises. For $\mathbb{R}$ it is the Lebesgue measure, and for $\mathbb{C}$, it is twice the Lebesgue measure. If k is $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$, it is the measure which gives the valuation ring measure 1; cf. Lecture 1.

Now assume k is an extension of $k_0 = \mathbb{Q}_p$ or $k_0 = \mathbb{F}_p((t))$. Let $\mathfrak{C} = \{a \in k \mid \mathrm{Tr}_{k/k_0} \in \mathcal{O}_{k_0}\}$. The set $\mathfrak{C}$ is a fractional ideal of the valuation ring $\mathcal{O}_k$ in k, and its inverse $\mathfrak{D} = \mathfrak{C}^{-1}$ is called the *different* of k/k_0. Its *norm* $\mathbb{N}\mathfrak{D} = |\mathcal{O}_k/\mathfrak{D}|$ is such that the self dual measure μ is the one which gives $\mathcal{O}_k$ measure $(\mathbb{N}\mathfrak{D})^{-1/2}$.

Of course, all of this depends on the choice of character ψ, so this measure is not quite canonical, but its choice is reasonable. Canonicity is especially absent in characteristic $p > 0$ once again because of the choice of the subfield k_0.

We conclude with an abstract version of the Poisson Summation Formula. We need some preparation first. If G is a locally compact abelian group and H a closed subgroup of G, we denote by $H^\perp$ the subgroup

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

Proposition 10.8. *Let H be a closed subgroup of G.*

(1) $H^\perp$ is closed in $\widehat{G}$.

(2) $(H^\perp)^\perp = H$ under the identification $\widehat{\widehat{G}} \cong G$.

(3) If $p : G \to G/H$ is the projection, then the map $(G/H)\widehat{\ } \to H^\perp$ given by $\chi \mapsto \chi \circ p$ is well defined and an isomorphism of topological groups.

(4) If $q : \widehat{G} \to \widehat{G}/H^\perp$ is the projection, then the map $\widehat{G}/H^\perp \to \widehat{H}$ given by $q(\xi) \mapsto \xi|_H$ is well defined and an isomorphism of topological groups.

Theorem 10.9 (Poisson Summation)**.** *Let G be a locally compact abelian group and H a closed subgroup of G. Give H a Haar measure ν. Let $f \in L^1(G)$ and assume the following two conditions: first, $\hat{f}|_{H^\perp} \in L^1(H^\perp)$, and second, that for all $x \in G$, the integral $\int_H f(x+y)\, d\nu(y)$ converges absolutely and uniformly on compact sets containing x. Then there is a Haar measure $\nu^\perp$ on $H^\perp$ such that*

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

Lecture 11

Tate's Thesis: Local Zeta Functions

We have described the character theory for the additive groups of a local field k. Now we look at $k^\times$. The units of any local field decompose group theoretically and topologically into their elements of absolute value 1, and the subgroup of $\mathbb{R}^\times$ which is the image of the absolute value. In the nonarchimedean case, this means $k^\times \cong \mathcal{O}_k^\times \times \mathbb{Z}$, and in the real case, this says $k \cong \{\pm 1\} \times \mathbb{R}$, and in the complex case, $k \cong S^1 \times \mathbb{R}$.

A *quasi-character* on a locally compact abelian group G is a continuous homomorphism $G \to \mathbb{C}^\times$. On a compact group, all quasi-characters are characters. Thus a quasi-character c on $k^\times$ is the product of a character on the elements of absolute value 1 and either a continuous homomorphism $\mathbb{Z} \to \mathbb{C}^\times$ or $\mathbb{R} \to \mathbb{C}^\times$. Any homomorphism $\mathbb{Z} \to \mathbb{C}^\times$ or $\mathbb{R} \to \mathbb{C}^\times$ is of the form $x \mapsto |x|^s$ for some $s \in \mathbb{C}$ (exercise). Thus we get

Proposition 11.1. *Let k be a local field and let U be the elements of k with absolute value 1. Then for any quasi-character c on $k^\times$, there is a character χ on U and an $s \in \mathbb{C}$ such that*

$$c = \chi \| \cdot \|^s$$

If k is archimedean, then s is unique, and if k is nonarchimedean, then s is determined up to a multiple of $2\pi i/\log(\mathbb{N}\mathfrak{p})$ where $\mathfrak{p}$ is the prime ideal of k.

The absolute value $\| \cdot \|$ on k in the proposition is the one defined before: For k nonarchimedean with prime ideal $\mathfrak{p}$ and prime element π, $\|\pi\| = (\mathbb{N}\mathfrak{p})^{-1}$; for $k = \mathbb{R}$, it is the usual absolute value, and for $k = \mathbb{C}$, it is the square of the usual absolute value. Let μ be the Haar measure which is self dual under the duality given by the standard character, as per the examples in the previous lecture. Using this absolute value and this measure, we define a Haar measure $\mu^\times$ on $k^\times$ for any local field k. For archimedean local fields, it is given by the functional

$$f \mapsto \int_{k^\times} f(x) \frac{1}{\|x\|} \, d\mu(x),$$

and if k is nonarchimedean with prime $\mathfrak{p}$, it is given by

$$f \mapsto \int_{k^\times} \frac{\mathbb{N}\mathfrak{p}}{\mathbb{N}\mathfrak{p} - 1} f(x) \frac{1}{\|x\|} \, d\mu(x).$$

The reason for this scaling is

Proposition 11.2. *Let k be a nonarchimedan local field, let U the set of elements of absolute value 1 in k, and let B be the set of elements of absolute value at most 1. Then*

$$\mu^\times(U) = \mu(B).$$

This is straightforward.

Now we can begin to define zeta functions. Following Lang, we denote by $\mathrm{Inv}(G)$ the set of complex functions which are continuous and in $L^1(G)$, and such that $\hat{f}$ is continuous and in $L^1(\widehat{G})$. Until the end of the lecture, we will assume that our functions on a local field k are in $\mathrm{Inv}(k)$, and that $f(x)\|x\|^\sigma$ and $\hat{f}(x)\|x\|^\sigma$ are both in $L^1(k^\times)$ for $\sigma > 0$.

Definition 11.3. Let $f \in \mathrm{Inv}(k)$ and c a quasi-character on $k^\times$. We define the *local zeta function* of f to be

$$\zeta(f, c) = \int_{k^\times} f(x)c(x)\, d\mu^\times(x).$$

If we write $c = \chi\|\cdot\|^s$ as in Proposition 11.1 and if we fix χ, then it becomes a function of the complex variable s, and we write

$$\zeta(f, c) = \zeta(f, \chi, s).$$

One sees easily that local zeta functions are defined and holomorphic for $\Re s > 0$.

Example 11.4. Let us consider $k = \mathbb{Q}_p$. Take f to be the charactistic function of $\mathbb{Z}_p$, and let $\chi = 1$ be the trivial character on $\mathbb{Z}_p^\times$. Then

$$\zeta(f, 1, s) = \int_{\mathbb{Q}_p^\times \cap \mathbb{Z}_p} \|x\|^s\, d\mu^\times(x).$$

The set $\mathbb{Q}_p^\times \cap \mathbb{Z}_p$ is equal to the union $\bigcup_{j=0}^\infty p^j\mathbb{Z}_p^\times$, and so we can write the zeta function as

$$\zeta(f, 1, s) = \sum_{j=0}^\infty \int_{p^j\mathbb{Z}_p^\times} \|x\|^s\, d\mu^\times(x).$$

The function $\|x\|^s$ is constant on $p^j\mathbb{Z}_p^\times$ for all j and equal to p^{-js} on each. Thus

$$\zeta(f, 1, s) = \sum_{j=0}^\infty \int_{p^j\mathbb{Z}_p^\times} p^{-js}\, d\mu^\times(x) = \sum_{j=0}^\infty p^{-js}\mu^\times(p^i\mathbb{Z}_p^\times).$$

But since $\mu^\times$ is a Haar measure, the measure of $p^i\mathbb{Z}_p^\times$ is the same as that of $\mathbb{Z}_p^\times$, which is 1. Thus

$$\zeta(f, 1, s) = \sum_{j=0}^\infty p^{-js} = (1 - p^{-s})^{-1}.$$

This is the pth factor of the Riemann zeta function. We will see these local zeta functions "glue together" later when we globalize this discussion.

We will now prove the functional equation for local zeta functions, save for one technical detail. Let k be any local field. For $c = \chi\|\cdot\|^s$ a quasi-character on $k^\times$, let $\hat{c}$ be the quasi-character defined by $\hat{c} = \overline{\chi}\|\cdot\|^{1-s}$, so $\hat{c} = c^{-1}\|\cdot\|$.

Lemma 11.5. *Let $f, g \in \mathrm{Inv}(k)$ satisfy the assumptions given above, and let c be a quasi-character. Then*

$$\zeta(f,c)\zeta(\hat{g},\hat{c}) = \zeta(\hat{f},\hat{c})\zeta(g,c).$$

Proof. This is just a computation in measure theory. Write $c = \chi\|\cdot\|^s$. Let us first write out the definitions of the zeta functions and use Fubini's Theorem:

$$\begin{aligned}\zeta(f,c)\zeta(\hat{g},\hat{c}) &= \int_{k^\times}\int_{k^\times} f(x)\hat{g}(y)\chi(x)\overline{\chi}(y)\|x\|^s\|y\|^{1-s}\,d\mu^\times(x)\,d\mu^\times(y)\\ &= \int_{k^\times}\int_{k^\times} f(x)\hat{g}(y)\chi(xy^{-1})\|xy^{-1}\|^s\|y\|\,d\mu^\times(x)\,d\mu^\times(y)\end{aligned}$$

Next we write out the definition of $\hat{g}$ and use Fubini:

$$\begin{aligned}\zeta(f,c)\zeta(\hat{g},\hat{c}) &= \int_k\int_{k^\times}\int_{k^\times} f(x)g(z)\psi(yz)\chi(xy^{-1})\|xy^{-1}\|^s\|y\|\,d\mu^\times(x)\,d\mu^\times(y)\,d\mu(z)\\ &= \int_k\int_k\int_{k^\times} f(x)g(z)\psi(yz)\chi(xy^{-1})\|xy^{-1}\|^s\|y\|\|x\|^{-1}\,d\mu^\times(y)\,d\mu(x)\,d\mu(z).\end{aligned}$$

Then we make a change of variable $y \mapsto yz^{-1}$:

$$\zeta(f,c)\zeta(\hat{g},\hat{c}) = \int_k\int_k\int_{k^\times} f(x)g(z)\psi(y)\chi(xzy^{-1})\|xzy^{-1}\|^s\|y\|\|zx\|^{-1}\,d\mu^\times(y)\,d\mu(x)\,d\mu(z).$$

This expression is symmetric in f and g, so we obtain the lemma. □

Upon dividing each side by $\zeta(\hat{f},\hat{c})\zeta(\hat{g},\hat{c})$, we obtain that the function $\rho(c) = \zeta(f,c)/\zeta(\hat{f},\hat{c})$ is meromorphic in s and independent of f, so long as there is always a function f for each character χ on the elements of absolute value 1 in k such that $\zeta(f,\chi\|\cdot\|^s) \neq 0$. This is a case-by-case computation which is not very difficult, and we leave it for the exercises. Let us state the functional equation.

Theorem 11.6. *There is a function ρ on the quasi-characters of $k^\times$ which, writing $c = \chi\|\cdot\|$, is a nonzero meromorphic function of s for every χ, and such that any local zeta function $\zeta(f,c)$ has the property that*

$$\zeta(f,c) = \rho(c)\zeta(\hat{f},\hat{c}).$$

Lecture 12

Tate's Thesis: Analysis on Adeles and Ideles

Now we begin to globalize our discussion using adeles and ideles. We can treat the measure theory and character theory on them simultaneously as follows.

Let $\{G_v\}_{v\in V}$ be locally compact abelian groups indexed by some set V. Let $S_\infty \subset V$ be a finite subset, and for each $v \notin S_\infty$, let $H_v \subset G_v$ be compact open subgroups. Equip each G_v with a Haar measure μ_v such that $\mu_v(H_v) = 1$ for all but finitely many $v \notin S_\infty$. The restricted direct product of the G_v's with respect to the H_v's is the group

$$G = \left\{ (x_v)_{v\in V} \in \prod_{v\in V} G_v \;\middle|\; x_v \in H_v \text{ for almost all } v \notin S_\infty \right\}$$

with the topology given by the base of neighborhoods of the identity 1

$$\left\{ \prod_{v\in V} U_v \;\middle|\; U_v \subset G_v \text{ is open for all } v,\ 1 \in U_v \text{ for all } v,\ U_v = H_v \text{ for almost all } v \notin S_\infty \right\}.$$

The group G is locally compact by Tychonoff's Theorem, and we give it a measure μ defined as follows. If $U = \prod U_v$ is an open neighborhood of 1 as in the base described above, then for any $x \in G$, we define

$$\mu(x + U) = \mu(U) = \prod_{v\in V} \mu_v(U_v).$$

The right hand side makes sense because $\mu_v(U_v) = \mu_v(H_v)$ for almost all v, and $\mu_v(H_v) = 1$ for almost all v. It is not too hard to check that this is a well defined Haar measure on G.

As for characters, it is not hard to prove that

$$\widehat{G} = \left\{ \prod_{v\in V} \psi_v \in \prod_{v\in V} \widehat{G}_v \;\middle|\; \psi_v|_{H_v} = 1 \text{ for almost all } v \notin S_\infty \right\}.$$

In other words, $\widehat{G}$ is the restricted direct product of the $\widehat{G}_v$'s with respect to the $H_v^\perp$'s. Let us explain why this makes sense, i.e., why $H_v^\perp$ is compact and open. We know $H_v^\perp \cong (G_v/H_v)\widehat{\ }$ which is compact: Since H_v is open, G_v/H_v is discrete and a standard theorem from the

duality theory says that the dual of a discrete group is compact, and vice-versa. Similarly it is open because H_v is compact, which means that $\widehat{G}_v/H_v^\perp \cong \widehat{H}_v$ is discrete.

A character $\psi = \prod_v \psi_v \in \widehat{G}$ is evaluated on an element $x = (x_v)_{v\in V} \in G$ by

$$\psi(x) = \prod_{v\in V} \psi_v(x_v).$$

Example 12.1. Let K be a global field. Let $V = V_K$, $S_\infty = V_\infty$ (which we treat as empty if K is a function field), $G_v = K_v$, and $H_v = \mathcal{O}_v$. Then $G = \mathbb{A}_K$. If instead $G_v = K_v^\times$ and $H_v = \mathcal{O}_v^\times$, then $G = \mathbb{I}_K$.

If μ_v is the standard measure we put on K_v in the previous lecture, then it is a fact that $\mu_v(\mathcal{O}_v) = 1$ for almost all $v \notin V_\infty$. This follows from the fact that a prime ring is ramified if and only if the different of its local field is a proper ideal in the valuation ring of the local field, and this happens only finitely many times. Thus these measures "glue together" as above to give a Haar measure on $\mathbb{A}_K$.

Similarly, if $\mu_v^\times$ is the measure we gave $K_v^\times$ in the previous lecture, then since $\mu_v^\times(\mathcal{O}_v^\times) = \mu_v(\mathcal{O}_v)$ for all $v \notin V_\infty$, we have that the measures $\mu_v^\times$ glue to a Haar measure on $\mathbb{I}_K$.

The standard character ψ on $\mathbb{A}_K$ is the product of all the local standard characters ψ_v. One checks that $\psi_v|_{\mathcal{O}_v} = 1$ for almost all $v \notin V_\infty$, so this makes sense. By the description of the dual of a restricted direct product, it follows that $x \mapsto (y \mapsto \psi(xy))$ is a topological isomorphism between $\mathbb{A}_K$ and its dual; the adeles are self-dual! The measure μ on $\mathbb{A}_K$ is self-dual with respect to this identification. This identification makes it possible to state the next proposition.

Proposition 12.2. *Let K be a global field embedded in its ring of adeles. Then in $\mathbb{A}_K$, we have $K^\perp = K$.*

We can now state an important theorem.

Theorem 12.3 (Tate's Riemann-Roch)**.** *Let $f \in \mathrm{Inv}(\mathbb{A}_K)$ satisfy the following technical assumptions: $\sum_{\alpha\in K} f(a(x+\alpha))$ converges for all $x \in \mathbb{A}_K$ and all $y \in \mathbb{I}_K$, the convergence being uniform in x on compact subsets of $\mathbb{A}_K$ and uniform also in y on compact subsets of $\mathbb{I}_K$, and $\sum_{\alpha\in K} \hat{f}(\alpha y)$ converges for all $y \in \mathbb{I}_K$. Then we have the following formula, valid for all ideles y:*

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

We sketch the proof. Let f_y be the function given by $f_y(x) = f(xy)$. We apply the Poisson summation formula to it with respect to the discrete closed subgroup K. We get

$$\sum_{\alpha\in K} f(\alpha y) = \sum_{\alpha\in K} \hat{f}_y(\alpha).$$

The integral becomes a sum because the Haar measure on a discrete group is the counting measure. But

$$\hat{f}_y(\alpha) = \int_{\mathbb{A}_K} f(xy)\psi(\alpha x)\, d\mu(x).$$

Now one can prove that for any measurable $E \subset \mathbb{A}_K$, we have that $\mu(aE) = \|a\|\mu(E)$, i.e., the norm of an idele is its module. So we make the change of variable $x \mapsto xy^{-1}$ and get

$$\hat{f}_y(\alpha) = \frac{1}{\|y\|} \int_{\mathbb{A}_K} f(x)\psi\left(\frac{\alpha}{y}x\right)\, d\mu(x) = \frac{1}{\|y\|}\hat{f}\left(\frac{\alpha}{y}\right).$$

Substituting this into the formula above gives the theorem.

Now we will prove the Riemann-Roch Theorem 7.6 for curves over finite fields. Let K be the $\mathbb{F}_q$-function field of a curve X over $\mathbb{F}_q$. Then K is a global field of positive characteristic. Let us fix a copy K_0 of $\mathbb{F}_q(t)$ of which it is an extension. For any idele $y = (y_v)_{v\in V_K}$, we let D_y be the element of $\mathrm{Div}(K)$ given by

$$D_y = \sum_{v\in V_K} v(y_v)\mathfrak{P}_v$$

where $\mathfrak{P}_v$ is the prime ring associated to v, and where we denote also by v the valuation associated to $v \in V_K$. The degree of D_y is, by definition, $\deg(D_y) = \sum_{v\in V_K} v(y_v)f_v$ where f_v is the degree of the residue field of $\mathfrak{P}$ over $\mathbb{F}_q$. Thus

$$q^{-\deg D_y} = \prod_{v\in V_k} q^{-v(y_v)f_v} = \prod_{v\in V_K} \|y_v\|_v = \|y\|.$$

Now $\ell(D_y)$ is the dimension of the $\mathbb{F}_q$-vector space of $\alpha \in K$ such that $v(\alpha) \geq -v(y_v)$ for all $v \in V_K$. This is the same as $0 \geq -v(\alpha)f_v - v(y_v)f_v$, which is the same as $1 \geq q^{-v(\alpha)f_v - v(y_v)f_v} = \|\alpha y_v\|_v$. Hence $q^{\ell(D_y)}$ counts the $\alpha \in K$ such that $\|\alpha y_v\|_v \leq 1$ for all $v \in V_K$. If $B = \prod_{v\in V_K} \mathcal{O}_v \subset \mathbb{A}_K$, we obtain

$$q^{\ell(D_y)} = \sum_{\alpha\in K} \chi_B(\alpha y).$$

Here χ_E denotes the characteristic function of the set E.

Now we have in K_v,

$$\widehat{\chi}_{\mathcal{O}_v}(a) = \int_{\mathcal{O}_v} \psi_v(ax)\, d\mu_v(x).$$

By Proposition 10.4, this is zero unless $\psi_v(ax)$ is trivial on $\mathcal{O}_v$, in which case it is the measure of $\mathcal{O}_v$. Let v_0 be the valuation of K_0 over which v lies, and let ψ_0 be the standard character of $(K_0)_{v_0}$. Then the character $\psi_v = \psi_0(\mathrm{Tr}_{K_v/(K_0)_{v_0}})$ is therefore trivial when the trace of its argument is in $\mathcal{O}_{v_0}$. It follows that ψ is trivial on the inverse of the different $\mathfrak{D}_v$ of $K_v/(K_0)_{v_0}$, and so

$$\widehat{\chi}_{\mathcal{O}_v} = \mu_v(\mathcal{O}_v^{-1})\chi_{\mathfrak{D}_v^{-1}} = (\mathbb{N}\mathfrak{D}_v)^{-1/2}\chi_{\mathfrak{D}_v^{-1}}.$$

Let z_v be any generator of $\mathfrak{D}_v$, and let $\mathcal{K} = D_z$ where $z = (z_v)_{v\in V_K}$. We apply Tate's Riemann-Roch Theorem to χ_B to get

$$\sum_{\alpha\in K} \chi_B(\alpha y) = \frac{1}{\|y\|}\left(\prod_{v\in V_K} \sqrt{\mathbb{N}\mathfrak{D}_v}\right)^{-1} \sum_{\alpha\in K} \chi_{z^{-1}B}(\alpha y^{-1}),$$

or

$$q^{\ell(D_y)} = q^{\deg D_y}\|z\|^{1/2}\sum_{\alpha\in K}\chi_B(\alpha z y^{-1}) = q^{\deg D_y}q^{(\deg \mathcal{K})/2}q^{\ell(\mathcal{K}-D_y)}.$$

So

$$\ell(D_y) - \ell(\mathcal{K} - D_y) = \deg D_y - \frac{1}{2}\deg \mathcal{K}.$$

If we substitute $\mathcal{K}$ for D_y, we get

$$\ell(\mathcal{K}) - 1 = \frac{1}{2}\deg \mathcal{K}.$$

Substituting this back in gives

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

Since the map $y \mapsto D_y$ is clearly surjective onto $\mathrm{Div}(K)$, we are done.

Lecture 13

Tate's Thesis: Global Zeta Functions

In this final lecture, we prove the functional equation for global zeta functions. In the exercises, we apply the result to Hecke L-functions and also the zeta functions of global fields.

Let μ be the measure determined on $\mathbb{A}_K$ last lecture, and $\mu^\times$ that on $\mathbb{I}_K$. Let c be a quasi-character on $\mathbb{I}_K$ which is trivial on $K^\times$. Let T be the image in $\mathbb{R}_{>0}$ of the norm map, so $T = \mathbb{R}_{>0}$ if K is a number field, and T is discrete if K is a function field, say generated by q. Since $\mathbb{I}_K/K^\times \cong (\mathbb{I}_K^1/K^\times) \times T$, we find, just as in the local case, that $c = \chi\|\cdot\|^s$ for some $s \in \mathbb{C}$. Here s is uniquely determined in the number field case, and determined up to $2\pi i/\log q$ in the function field case.

Definition 13.1. Let $f \in \mathrm{Inv}(\mathbb{A}_K)$ satisfy the hypotheses of Tate's Riemann-Roch Theorem, and assume $f(y)\|y\|^\sigma$ and $\hat{f}(y)\|\sigma\|^\sigma$ are in $L^1(\mathbb{I}_K)$ for all $\sigma > 1$. Then we define the *global zeta function* of f to be

$$\zeta(f,c) = \int_{\mathbb{I}_K} f(x)c(x)d\mu^\times(x),$$

where c is a quasi-character on $\mathbb{I}_K$ which is trivial on $K^\times$.

If we write $c = \chi\|\cdot\|^s$, then $\zeta(f,c)$ becomes a function of χ and s, like in the local case, and it is holomorphic in s for $\Re s > 1$. Sometimes we write $\zeta(f,c) = \zeta(f,\chi,s)$.

Let E be a fundamental domain for $\mathbb{I}_K^1/K^\times$, i.e., $E \subset \mathbb{I}_K^1$ is a set of representatives for $\mathbb{I}_K^1/K^\times$, its closure is compact, and its measure is the same as that of its closure (the existence of E it not obvious, and we omit its proof). Denote its measure by κ.

If $c = \chi\|\cdot\|^s$ is a quasi-character on $\mathbb{I}_K$ which is trivial on $K^\times$, we write $\hat{c}$ for the quasi-character $\overline{\chi}\|\cdot\|^{1-s}$.

Theorem 13.2 (Global Functional Equation)**.** *The functions $\zeta(f,c)$ continue analytically to the whole complex plane, except when $c = \chi\|\cdot\|^s$ and $\chi = 1$. In this case, if K is a number field, there are simple poles at $s = 0$ and $s = 1$ with, respectively, residues $\kappa f(0)$ and $\kappa\hat{f}(0)$. If k is a function field, and if q generates T, then there are simple poles at*

$2\pi in/\log q$ and $1 + 2\pi in/\log q$ for all $n \in \mathbb{Z}$ with, respectively, residues $\kappa f(0)/\log q$ and $\kappa\hat{f}(0)/\log q$. Furthermore, we have the functional equation

$$\zeta(f, c) = \zeta(\hat{f}, \hat{c}).$$

Proof. Write t for a variable in T and denote by $\nu^\times$ the measure on $\mathbb{I}_K^1$ induced by the decomposition $\mathbb{I}_K^1 \times T$. We have

$$\begin{aligned}
&\int_{\mathbb{I}_K^1} f(ty)c(ty)\,d\nu^\times(y) + f(0)\int_E c(ty)\,d\nu^\times(y) \\
&\qquad = \sum_{\alpha\in K^\times}\int_{\alpha E} f(ty)c(ty)\,d\nu^\times(y) + f(0)\int_E c(ty)\,d\nu^\times(y) \\
&\qquad = \sum_{\alpha\in K^\times}\int_E f(\alpha ty)c(ty)c(\alpha)\,d\nu^\times(y) + f(0)\int_E c(ty)\,d\nu^\times(y). \\
&\qquad = \int_E \sum_{\alpha\in K^\times} f(\alpha ty)c(ty)\,d\nu^\times(y) \\
&\qquad = \int_E \sum_{\alpha\in K} \hat{f}\left(\frac{\alpha}{ty}\right)\frac{1}{\|ty\|}c(ty)\,d\nu^\times(y).
\end{aligned}$$

In the last step we applied Riemann-Roch. Replacing f with $\hat{f}$ and c with $\hat{c}$ gives

$$\int_{\mathbb{I}_K^1}\hat{f}(t^{-1}y)\hat{c}(t^{-1}y)\,d\nu^\times(y)+\hat{f}(0)\int_E \hat{c}(t^{-1}y)\,d\nu^\times(y) = \int_E\sum_{\alpha\in K}\hat{\hat{f}}\left(\frac{\alpha t}{y}\right)\frac{1}{\|t^{-1}y\|}\hat{c}(t^{-1}y)\,d\nu^\times(y).$$

We replace α with $-\alpha$, change the variable $y \mapsto y^{-1}$, and use $\hat{\hat{f}}(x) = f(-x)$ and $\hat{c} = c^{-1}\|\cdot\|$ to get that this equals

$$\int_E \sum_{\alpha\in K} f(\alpha ty)\|y\|c(ty)\,d\nu^\times(y).$$

But we already saw that this is equal to

$$\int_{\mathbb{I}_K^1} f(ty)c(ty)\,d\nu^\times(y) + f(0)\int_E c(ty)\,d\nu^\times(y).$$

Therefore

$$\begin{aligned}
&\int_{\mathbb{I}_K^1} f(ty)c(ty)\,d\nu^\times(y) + f(0)\int_E c(ty)\,d\nu^\times(y) = \\
&\qquad\qquad \int_{\mathbb{I}_K^1}\hat{f}(t^{-1}y)\hat{c}(t^{-1}y)\,d\nu^\times(y) + \hat{f}(0)\int_E \hat{c}(t^{-1}y)\,d\nu^\times(y).
\end{aligned}$$

Now we evaluate the integrals over E. They are the same as integrals over $\mathbb{I}_K^1/K^\times$, so we can apply Proposition 10.4:

$$\int_E c(ty)\,d\nu^\times(y) = t^s\int_E \chi(y)\,d\nu^\times(y) = t^s\delta_{\chi,1}\nu^\times(E) = \delta_{\chi,1}t^s\kappa.$$

Here we used $c = \chi\|\cdot\|^s$, and $\delta_{\chi,1}$ is 1 if χ is trivial and zero otherwise. A similar computation for $\int_E \hat{c}(t^{-1}y)\, d\nu^\times(y)$ gives

$$\int_{\mathbb{I}_K^1} f(ty)c(ty)\, d\nu^\times(y) = \int_{\mathbb{I}_K^1} \hat{f}(t^{-1}y)\hat{c}(t^{-1}y)\, d\nu^\times(y) + \delta_{\chi,1}(t^{s-1}\kappa\hat{f}(0) - t^s\kappa f(0)).$$

Now in the number field case, we integrate from $t = 0$ to $t = 1$ to get

$$\int_{\|x\|\le 1} f(x)c(x)\, d\mu^\times(x) = \int_{\|x\|\ge 1} \hat{f}(x)\hat{c}(x)\, d\mu^\times(x) + \delta_{\chi,1}\left(\frac{\kappa\hat{f}(0)}{s-1} - \frac{\kappa f(0)}{s}\right).$$

One checks easily that the right hand side has all of the desired analytic properties (meromorphic everywhere with poles as stated). If we replace f with $\hat{f}$ and c with $\hat{c}$ and add the results together, we get

$$\int_{\mathbb{I}_K} f(x)c(x)\, d\mu^\times(x) = \int_{\mathbb{I}_K} \hat{f}(x)\hat{c}(x)\, d\mu^\times(x),$$

i.e.,

$$\zeta(f, c) = \zeta(\hat{f}, \hat{c}).$$

We are done in the number field case. In the function field case, we must instead sum $t = q^{-m}$ for nonnegative integers m. This gives

$$\int_{\|x\|\le 1} f(x)c(x)\, d\mu^\times(x) = \int_{\|x\|\ge 1} \hat{f}(x)\hat{c}(x)\, d\mu^\times(x) + \delta_{\chi,1}\left(\frac{\kappa\hat{f}(0)}{1-q^{1-s}} - \frac{\kappa f(0)}{1-q^{-s}}\right).$$

This gives the desired analytic properties, and also the functional equation as in the number field case. We are done. □

Exercises

Lecture 1

Exercise 1.1. A group G is called *profinite* if it is the projective limit $G = \varprojlim_{i \in I} G_i$ of finite groups G_i, where I is a directed set. If each G_i is considered with the discrete topology, then G inherits the projective limit topology, making it a topological group. The topology is part of the data of a profinite group.

Let G be a profinite group.

(a) Prove that G is compact and Hausdorff.

(b) Prove that a base of neighborhoods about the identity $1 \in G$ is given by the normal subgroups of finite index.

(c) Prove that a topological group is profinite if and only if it is compact Hausdorff and it admits a base of neighborhoods about 1 consisting of normal subgroups.

(d) Prove that a topological group is profinite if and only if it is compact and totally disconnected, which means that the connected component of every point consists only of the point itself.

(e) Describe the Haar measure on a profinite group G.

Exercise 1.2. (a) Prove that $\mathbb{Z}_p$ and $\mathbb{F}_q[[t]]$ are Hausdorff.

(b) Prove that $\mathbb{Z}_p$ and $\mathbb{F}_q[[t]]$ are sequentially compact, hence compact.

Exercise 1.3. Let A be a discrete valuation ring and K its field of fractions. Let $\mathfrak{p} \subset A$ be the maximal ideal, and let π be an element which generates it.

(a) Prove that all elements $a \in K^\times$ can be written uniquely in the form $u\pi^m$ for some $u \in A^\times$ and $m \in \mathbb{Z}$. This m is denoted $v(a)$ and is called the *valuation* of a.

(b) Prove that the valuation v does not depend on the choice of prime element.

(c) Prove that for all $a, b \in K^\times$ with $(a+b) \in K^\times$, we have $v(a+b) \geq \min\{v(a), v(b)\}$.

Lecture 2

Exercise 2.1. Let k be a local field.

(a) Show directly that the module on k is upper semicontinuous, i.e., the preimage of any open interval $(-\infty, t)$ under mod is open in k. [*Hint:* Let E be a compact neighborhood of 0 and $a \in k$. Show that for any open set U with $aE \subset U$, there is an open neighborhood V of a with $VE \subset U$.]

(b) Show from this that the module is lower semicontinuous, in the obvious sense, and hence continuous. Deduce that the balls B_r are open.

Exercise 2.2. Let k be a local field.

(a) Show that in any neighborhood U of 0, there is an $a \in U$ with $0 < \mathrm{mod}(a) < 1$.

(b) Let E be a compact neighborhood of 0. Show that there is a neighborhood U of 0 such that $UE \subset E$.

(c) With E and U as in (b), show that for any $a \in U \cap E$ with $0 < \mathrm{mod}(a) < 1$ and for any $b \in k$, the infimum $m_b = \inf\{m \geq 0 \mid a^m b \in V\}$ exists.

(d) Show that for all $r > 0$, there is an M such that $m_b \leq M$ for all $b \in C_r$.

(e) Show that C_r is compact for all r.

Exercise 2.3. Show that an absolute value $|\cdot|$ on a field k is nonarchimedean if and only if it is ultrametric. [*Hint:* Expand $(x+y)^n$ using the Binomial Theorem and take absolute values.]

Exercise 2.4. Let l/k be an extension of nonarchimedean local fields. Prove that $\mathcal{O}_l \cap k = \mathcal{O}_k$.

Exercise 2.5 (Hensel's Lemma)**.** Let k be a nonarchimedean local field. Let $f \in \mathcal{O}_k[x]$ be a monic polynomial, and let $\bar{f}$ denote the reduction of f modulo $\mathfrak{p}_k$. Assume $\bar{f}$ has a root α in $\mathcal{O}_k/\mathfrak{p}_k$. Prove that if $\bar{f}$ has nonvanishing derivative, then f has a root a such that $a \equiv \alpha \pmod{\mathfrak{p}_k}$. [*Hint:* Construct a modulo $\mathfrak{p}^2$, and then $\mathfrak{p}^3$, and so on.]

Exercise 2.6. Let k be a field. We say two absolute values on k are *equivalent* if they define the same topology on k via their respective metrics. Prove that two absolute values $|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if there is an $r > 0$ such that $|\cdot|_1 = |\cdot|_2^r$. For the forward direction, work as follows. First prove that if $a \in k$ and $|a|_1 < 1$, then $|a|_2 < 1$. Then take $x, y \in k$ and let α be such that $|x|_1 = |y|_1^\alpha$. Prove that $|x|_2 = |y|_2^\alpha$, and conclude.

Exercise 2.7 (Approximation Theorem)**.** Let k be a field with inequivalent absolute values $|\cdot|_1, \ldots, |\cdot|_m$. Let $a_1, \ldots, a_m \in k$ and let $\epsilon > 0$. Prove that there is a $b \in k$ with $|b - a_i|_i < \epsilon$ for all $i = 1, \ldots, m$.

Exercise 2.8. Let l/k be an extension of nonarchimedean local fields of degree n.

(a) Show that $\mathcal{O}_l = \{a \in l \mid \mathrm{Nm}_{l/k}(a) \in \mathcal{O}_k\}$. [*Hint:* You will need to apply Hensel's lemma to the minimal polynomial of an element a in the latter set.]

(b) Show that $|a| = \sqrt[n]{\mathrm{Nm}_{l/k}(a)}$ is an absolute value on l extending the one on k.

(c) Show that the absolute value defined in (b) is the only one extending the absolute value on k.

Exercise 2.9. Verify that any local field k as given by the classification of local fields in Theorem 2.3 is such that the module on k is an absolute value.

Lecture 3

Exercise 3.1. In this exercise we will show that the completion of a global field is indeed a local field.

(a) Prove that the completion of $\mathbb{Q}$ at the prime ring $\mathbb{Z}_{(p)}$ is $\mathbb{Q}_p$.

(b) Prove that the completion of $\mathbb{F}_q(t)$ at the prime ring $\mathbb{F}_q(t)_{(t)}$ is $\mathbb{F}_q((t))$

(c) Let $\mathfrak{P}$ be a prime ring in $\mathbb{F}_q(t)$ with prime element π. Prove that the completion of $\mathbb{F}_q(t)$ at $\mathfrak{P}$ is $\mathbb{F}_q((\pi))(t)$.

(d) Let K be a global field and $\mathfrak{P}$ be a prime ring in K. Let K_0 be a copy of $\mathbb{Q}$ or $\mathbb{F}_q(t)$ of which K is a finite separable extension. Since K is separable over K_0, there is an $\alpha \in K$ such that $K = K_0(\alpha)$. Let $\mathfrak{P}_0 = K_0 \cap \mathfrak{P}$. Prove that $K_{\mathfrak{P}} = (K_0)_{\mathfrak{P}_0}(\alpha)$. Conclude that $K_{\mathfrak{P}}$ is a local field.

The following exercises 3.2-3.15 essentially constitue much of the first chapter of Lang [4], but the language of prime rings is not used there. Still, the reader may wish to refer to this text for much of this material.

Exercise 3.2. Let A be a integral domain with fraction field K and L a finite extension of K.

(a) Prove that $\beta \in L$ is integral over A if and only if there is a finitely generated A-submodule M of L such that $\beta M \subset M$. [*Hint:* Write down generators for M and write the linear transformation $M \to M$ given by $x \mapsto \beta x$ as a matrix in terms of these generators. Then take the characteristic polynomial of this matrix.]

(b) Prove that the integral closure of A in L is a ring.

(c) Prove that if $A \subset R \subset S$ where R, S are integral domains, and if S is integral over R and R is integral over A, then S is integral over A.

(d) Let B be the integral closure of A in L and assume L/K is separable. Prove that the norm and trace of any element in B is in A. [*Hint:* Use (c) to reduce to the case when L/K is Galois.]

(e) Let F/K be a finite extension. Let $x \in F$. Show that there is an $\alpha \in A$ such that αx is integral over A.

(f) Assume A is noetherian and that L/K is separable. If B is the integral closure of A in L, show that B is finitely generated as an A-module. [*Hint:* It is enough to show that B is contained in a finitely generated A module M. Construct M as follows. Let $x_1, \ldots, x_n$ be a basis for L as a K-vector space, and let $x_1', \ldots, x_n'$ be the basis which is dual to $x_1, \ldots, x_n$ via the perfect pairing $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$. Use (e) to construct an $\alpha \in A$ such that $\alpha x_i, \alpha x_i' \in B$ for all $i = 1, \ldots, n$. Then let $M = \alpha^{-1}(Ax_1 + \ldots + Ax_n)$.]

(g) Assume in addition to the hypotheses of (f) that A is principal. Let $n = [L : K]$. Show that B is of rank n as a free A-module.

Exercise 3.3 (Nakayama's Lemma)**.** Let A be a local ring with maximal ideal $\mathfrak{p}$ and M a finitely generated A-module. Prove that if $\mathfrak{p}M = M$, then $M = 0$.

Exercise 3.4. Prove that discrete valuation rings are integrally closed.

The following exercises 3.5-3.9 prove some basic facts about prime rings in field extensions.

Exercise 3.5. Let K be a field and $\mathfrak{P}$ and let L be a finite extension of K. Let $\mathfrak{Q}$ be a *prime ring* in L, i.e., a discrete valuation ring with fraction field L. Show that $\mathfrak{Q} \cap K$ is a prime ring of K.

Exercise 3.6. Let K be a field and $\mathfrak{P}$ a prime ring in K. Let $\mathfrak{p}$ be the prime ideal of $\mathfrak{P}$, and let L/K be a finite extension of K

(a) Let B be the integral closure of $\mathfrak{P}$ in L. Prove that $\mathfrak{p}B \neq B$.

(b) Prove that there is a prime ring $\mathfrak{Q}$ in L *lying over* $\mathfrak{P}$, which means that $\mathfrak{Q} \cap K = \mathfrak{P}$. [*Hint:* $\mathfrak{Q}$ will be a localization of B.]

Exercise 3.7 (Chinese Remainder Theorem)**.** Let A be a ring and $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ ideals in A with $\mathfrak{a}_1 + \cdots + \mathfrak{a}_m = A$. Let $x_1, \ldots, x_m \in A$. Prove that there is an element $x \in A$ with $x \equiv x_i \pmod{\mathfrak{a}_i}$ for all $i = 1, \ldots, m$.

Exercise 3.8 (Chinese Remainder Theorem for Prime Rings)**.** Let K be a field and $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ be prime rings in K with respective valuations $v_1, \ldots, v_m$. Let $x_1, \ldots, x_m \in K$. Show that there is an element $x \in K$ such that $v_i(x - x_i) > 0$ for all $i = 1, \ldots, m$.

Exercise 3.9. Let K be a field and $\mathfrak{P}$ a prime ring in K.

(a) Let L be a finite Galois extension of K. Prove that $\mathrm{Gal}(L/K)$ permutes the prime rings lying over $\mathfrak{P}$ transitively.

(b) Let F be any finite extension of K, Galois or not. Prove there are only finitely many prime rings in F lying over $\mathfrak{P}$.

In the following exercises 3.10-3.15 we prove some basic facts about Dedekind domains.

Exercise 3.10. In this exercise we will prove Theorem 3.11. Let A be a Dedekind domain with fraction field K.

(a) Prove that any ideal contains a product of nonzero prime ideals. [*Hint:* Assume not, and use noetherianity to produce an ideal which is maximal with respect the property that it does not contain a product of primes. Contradict the existence of this ideal.]

(b) Prove that $\mathfrak{p}\mathfrak{p}^{-1} = A$ for all nonzero primes $\mathfrak{p}$.

(c) If $\mathfrak{a}$ is a nonzero ideal, show that there exists a fractional ideal $\mathfrak{b}$ with $\mathfrak{a}\mathfrak{b} = A$.

(d) Show that the fractional ideal $\mathfrak{b}$ from above equals $\mathfrak{a}^{-1}$.

(e) Prove that $J(A)$ is a group.

(f) Prove that $J(A)$ is free abelian on the nonzero prime ideals of A.

Exercise 3.11. (a) Let A be an integrally closed domain with a multiplicative subset S. Prove that $S^{-1}A$ is integrally closed. Conclude that any localization of a Dedekind domain at a multiplicative subset is again Dedekind.

(b) Let now B be the integral closure of A in a finite extension L of K. Prove that $S^{-1}B$ is the integral closure of $S^{-1}A$ in L.

Exercise 3.12. Prove that a Dedekind domain with only finitely many prime ideals is principal.

Exercise 3.13. If A is a local ring with maximal ideal $\mathfrak{p}$ and M is a free A-module of rank n, show that $M/\mathfrak{p}M$ is a free $A/\mathfrak{p}$-module of rank n.

Exercise 3.14. Let A be a Dedekind domain with a principal prime ideal $\mathfrak{p}$. Prove that $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ is a free $A/\mathfrak{p}$-module of rank 1.

Exercise 3.15. Let A be a Dedekind domain with fraction field K and L a finite separable extension of K of degree n. Let B be the integral closure of A in L, which is Dedekind by Exercise 3.11. Let $\mathfrak{p}$ be a prime in A. Then the ideal $\mathfrak{p}B$ splits into a product of primes in

B, $\mathfrak{p}B = \mathfrak{q}_1^{e_1}, \ldots, \mathfrak{q}_r^{e_r}$. The numbers e_i are called *ramification indices.*

(a) Prove that the primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ are precisely all the primes in B with the property that their intersection with A is $\mathfrak{p}$. We say $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ *lie over* $\mathfrak{p}$.

(b) If $\mathfrak{q}_i$ is any of the primes of B lying over $\mathfrak{p}$, show that $B/\mathfrak{q}_i$ is a finite extension of $A/\mathfrak{p}$. Its degree f_i is called the *inertia degree.*

(c) Prove that

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

by exhibiting an isomorphism of $A/\mathfrak{p}$-modules

$$B/\mathfrak{p}B \cong (B/\mathfrak{q}_1) \oplus \cdots \oplus (B/\mathfrak{q}_r).$$

Exercise 3.16. Let $\mathfrak{P}$ be a prime ring in a field K. Let L/K be a finite separable extension of K.

(a) Prove that every prime ring lying over $\mathfrak{P}$ is a localization of the integral closure of $\mathfrak{P}$ in L at some maximal ideal.

(b) Let $\mathfrak{p}$ be the prime in $\mathfrak{P}$ and let $\pi \in \mathfrak{p}$ be a prime element. Let $\mathfrak{Q}$ be a prime ring of L lying over $\mathfrak{P}$. Let $e = v_{\mathfrak{Q}}(\pi)$. This is called the *ramification index* of $\mathfrak{Q}$ over $\mathfrak{P}$. Show that if $\mathfrak{Q}$ is the localization of the integral closure B of $\mathfrak{P}$ at a prime $\mathfrak{q}$, then this agrees with the definition of the ramification index of $\mathfrak{q}$ over $\mathfrak{p}$ as in Exercise 3.15. Show also that if $\mathfrak{q}'$ is the prime in $\mathfrak{Q}$, then the inertia degree is equal to the degree of $\mathfrak{Q}/\mathfrak{q}'$ over $\mathfrak{P}/\mathfrak{p}$.

All of the theory developed in these exercises so far suffices to prove Theorems 2.5 and 5.1.

Exercise 3.17. Prove that the residue field of a prime ring $\mathfrak{P}$ in a global field K is finite, and that it is isomorphic to the residue field of $K_{\mathfrak{P}}$.

Exercise 3.18. Let K be a number field and $\mathfrak{P}$ a prime ring in K. Let $\mathfrak{p}$ be the prime in $\mathfrak{P}$. Prove that the localization of $\mathcal{O}_K$ at the prime ideal $\mathfrak{p} \cap \mathcal{O}_K$ is equal to $\mathfrak{P}$.

The following exercises classify the places of a global field.

Exercise 3.19 (Ostrowski's Theorem)**.** Prove that the only absolutes on $\mathbb{Q}$ up to equivalence are the p-adic absolute values $|\cdot|_p$ and the real absolute value $|\cdot|_\infty$. Conclude that every prime ring comes from a localization of $\mathbb{Z}$ at a prime ideal. [*Hint:* In the nonarchimedean case, prove that the ideal $\{\alpha \in \mathbb{Z} \mid |\alpha| < 1\}$ is prime. In the archimedean case, take two integers m and n and write m to base n and estimate the expansion to obtain $|m|^{1/\log m} = |n|^{1/\log n}$.]

Exercise 3.20. Let K be a global field and let $|\cdot|$ be a nonarchimedean absolute value. Prove that $\{\alpha \in K \mid |\alpha| \leq 1\}$ is a prime ring in K with prime ideal $\{\alpha \in K \mid |\alpha| \leq 1\}$. Prove that the nonarchimedean absolute values are in one-to-one correspondence with prime rings in K. This proves Theorem 3.3

Exercise 3.21. Let K be a number field. Prove that the prime rings, and hence the nonarchimedean absolute values, are in one-to-one correspondence with the prime ideals in the obvious way.

Exercise 3.22. Let K be a number field. Classify the nonarchimedean absolute values on K. [*Hint:* Use Ostrowski's theorem to prove that the completion of K must be a finite extension of $\mathbb{R}$.]

Exercise 3.23. Prove that every prime ring in $\mathbb{F}_q(t)$ is either a localization of $\mathbb{F}_q[t]$ at a prime, or is $\mathbb{F}_q[t^{-1}]_{(t^{-1})}$.

Lecture 4

Exercise 4.1. Prove that a Dedekind domain is principal if and only if it is a unique factorization domain.

Exercise 4.2. Let K be a global field and $\alpha \in K$. Prove that only finitely many valuations v on K have $v(\alpha) \neq 0$. [*Hint:* Use Exercises 3.19 and 3.23 to prove the result for $\mathbb{Q}$ and $\mathbb{F}_q[t]$, respectively. Use that there are only finitely many prime rings in K lying above a given prime ring in $\mathbb{Q}$ or $\mathbb{F}_q[t]$ to prove the result in general.]

Exercise 4.3. (a) Prove that the only elements $\alpha \in \mathbb{F}_q(t)$ which have $v(\alpha) = 0$ for all valuations v on $\mathbb{F}_q(t)$ are those in $\mathbb{F}_q$.

(b) Let K be a function field. Prove that the set

$$R = \{\alpha \in K \mid v(\alpha) = 0 \text{ for all } v \in V_K\} \cup \{0\}$$

is closed under addition.

(c) Prove that if α is in the set R above, then the minimal polynomial of α over $\mathbb{F}_q(t)$ has coefficients in $\mathbb{F}_q$. Conclude that the elements of R are in $\mathbb{F}_q$ for some q a power of p.

Exercise 4.4. Let K by a number field of degree n. By Exercise 3.2, $\mathcal{O}_K$ is free abelian of rank n. Let $\alpha_1, \ldots, \alpha_n$ be a basis of $\mathcal{O}_K$ over $\mathbb{Z}$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K into $\mathbb{C}$. Form the matrix M whose (i,j)-entry is $\sigma_i(\alpha_j)$. Let $\Delta_K = \det M^2$. The number Δ_K is called the *discriminant* of K.

(a) Prove that Δ_K is nonzero and is independent of the choice of basis $\alpha_1, \ldots, \alpha_n$.

(b) Prove that Δ_K is the determinant of the matrix M' whose (i,j)-entry is $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)$. Conclude that $\Delta_K \in \mathbb{Z}$.

Exercise 4.5. Let $\Lambda \subset \mathbb{R}^n$ be a *lattice,* i.e., a discrete subgroup of maximal rank in $\mathbb{R}^n$. Prove that the rank of Λ is n. Let $\lambda_1, \ldots, \lambda_n$ be a basis. Prove that the set $P = \{\sum_{i=1}^n a_i\lambda_i \mid 0 \leq a_i \leq 1 \text{ for all } i\}$ is compact. P is called a *fundamental parallelepiped* of Λ.

Exercise 4.6. Let K be a number field with r real embeddings and s complex embeddings. Identify $\prod_{v \in V_\infty} K_v$ with $\mathbb{R}^r \times \mathbb{C}^s$. Let $i : K \to \mathbb{R}^r \times \mathbb{C}^s$ be the diagonal embedding, $\alpha \mapsto, (\alpha, \alpha, \ldots, \alpha)$.

(a) Prove that $i(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^r \times \mathbb{C}^s$.

(b) Accept (or prove, if you want) the standard fact that a fundamental parallelepiped of a lattice Λ spanned over $\mathbb{Z}$ by vectors $\lambda_1, \ldots, \lambda_n$ in $\mathbb{R}^n$ has volume the absolute value of the determinant of the matrix whose ith column is λ_i. Use this to prove that, if $\mathbb{C}$ is identified with $\mathbb{R}^2$ in the usual way $x + iy \mapsto (x, y)$, then a fundamental parallelepiped of $i(\mathcal{O}_K)$ has volume $2^{-s}\Delta_K$.

Exercise 4.7. Let K be a global field. Prove that $K^\times$ is discrete in $\mathbb{I}_K^1$.

Exercise 4.8 (Adelic Approximation Theorem)**.** Let K be a global field. Let $U = \prod_{v \notin V_\infty} \mathcal{O}_v \times \prod_{v \in V_\infty} K_v$, where V_∞ is supposed to be empty if K is a function field. Prove that $U + K = \mathbb{A}_K$.

Exercise 4.9. Let K be a global field. Let $U_0 = \prod_{v \notin V_\infty} \mathcal{O}_v$, where V_∞ is supposed to be empty if K is a function field. If K is a number field, let P be a fundamental parallelpiped of $\mathcal{O}_K$ in $\prod_{v \in V_\infty} K_v$, and let $U = U_0 \times P$. Otherwise, if K is a function field, let $U = U_0$. Prove that under the map $\mathbb{A}_K \to \mathbb{A}_K/K$, U surjects onto $\mathbb{A}_K/K$. Conclude that $\mathbb{A}_K/K$ is compact.

Exercise 4.10. Let K be a global field. Prove that $\mathbb{I}_K^1/K^\times$ is compact. [*Hint:* Try something similar to Exercise 4.9. Be careful at archimedean places.]

Lecture 5

Exercise 5.1. Let L/K be a Galois extension of global fields and let $\mathfrak{P}$ be a prime ring of K. Let $\mathfrak{Q}$ be a prime ring of L lying over $\mathfrak{P}$ and unramified over $\mathfrak{P}$, and let $D(\mathfrak{Q})$ be the group of automorphisms σ in $\mathrm{Gal}(L/K)$ with $\sigma\mathfrak{Q} = \mathfrak{Q}$. Let λ be the residue field of $\mathfrak{Q}$ and κ the residue field of $\mathfrak{P}$.

(a) Prove that $D(\mathfrak{Q}) \cong \mathrm{Gal}(\lambda/\kappa)$.

(b) Prove that if $\sigma \in \mathrm{Gal}(L/K)$, then $\mathrm{Frob}(\sigma\mathfrak{Q}/\mathfrak{P}) = \sigma^{-1}\,\mathrm{Frob}(\mathfrak{Q}/\mathfrak{P})\sigma$. Conclude that the Frobenius automorphism $\mathrm{Frob}(\mathfrak{Q}/\mathfrak{P})$ only depends on $\mathfrak{P}$ if L/K is abelian.

The following exercises 5.2-5.4 classify the ramified primes in an extension of global fields.

Exercise 5.2. Let l/k be an extension of nonarchimedean local fields. Define the *different* $\mathfrak{D}_{l/k}$ of l/k by $\mathfrak{D}_{l/k}^{-1} = \{a \in l \mid \mathrm{Tr}_{l/k}(a) \in \mathcal{O}_k\}$. The *discriminant* $\Delta_{l/k}$ of l/k is the ideal generated by the norm of any element with maximal absolute value in $\mathfrak{D}_{l/k}$. Prove that the discriminant does not depend on the choice of element with maximal absolute value. Furthermore, by Exercise 3.2, $\mathcal{O}_l$ is freely generated by $n = [l : k]$ elements $a_1, \ldots, a_n$. Prove that $\Delta_{l/k}$ is generated by the determinant of the matrix whose (i, j)-entry is $\mathrm{Tr}_{l/k}(a_i a_j)$.

Exercise 5.3. Let l/k be an extension of local fields. Prove that $\Delta_{l/k} = \mathcal{O}_k$ if and only if l/k is unramified. To do this, let π_k be a prime element of k. Use Exercise 5.2 to show that $\Delta_{l/k} = \mathcal{O}_k$ if and only if each of the element of the basis $a_1, \ldots, a_n$ of that exercise is invertible modulo $\pi_k\mathcal{O}_l$, and hence that $\mathcal{O}_l/\pi_k\mathcal{O}_l$ is a field.

Exercise 5.4. Let K be a global field. Let K_0 be the field $\mathbb{F}_q(t)$ or $\mathbb{Q}$ of which K is an extension. Let $A \subset K_0$ denote either $\mathbb{Z}$ or $\mathbb{F}_q[t]$, whichever is in K_0, and let B be the integral closure of A in K. Then B is Dedekind. We define the *different* of K/K_0 by $\mathfrak{D}^{-1} = \{\alpha \in K \mid \mathrm{Tr}(aB) \subset A\}$. Define the *discriminant* of K/K_0 to be the ideal Δ generated by the norms of elements in $\mathfrak{D}$ (this agrees in the number field case with the definition in Exercise 4.4, but you do not need to prove this).

(a) Let $\mathfrak{P}$ be a prime ring in K_0. Prove that

$$\Delta\mathcal{O}_\mathfrak{P} = \prod_{\mathfrak{Q}} \Delta_{K_\mathfrak{Q}/(K_0)_\mathfrak{P}}$$

where the product is over all prime rings $\mathfrak{Q}$ in K lying above $\mathfrak{P}$. Conclude that the prime ideal in A ramifying in B are precisely the ones which divide the discriminant.

(b) Prove that ramification indices are multiplicative in towers of field extensions.

(c) Conclude that there are only finitely many prime rings which ramify in a given extension of global fields.

Lecture 8

For the next two exercises, accept the following property of the ℓ-adic cohomology.

Theorem (Poincaré Duality)**.** *Let X be a variety over $\mathbb{F}_q$ of dimension d. Then for each i with $0 \leq i \leq 2d$, there is a perfect pairing of vector spaces*

$$H^i(X, \mathbb{Q}_\ell) \times H^{2d-i}(X, \mathbb{Q}_\ell) \to H^{2d}(X, \mathbb{Q}_\ell)$$

which commutes with the map f^* for any regular map $f : X \to X$.

Exercise 8.1. Let $V \times W \to k$ be a perfect pairing of k-vector spaces for some field k. Let $m = \dim V = \dim W$. Let $\varphi : V \to V$ and $\psi : W \to W$ be linear maps such that $(\varphi v, \psi w) = \lambda(v, w)$ for some $\lambda \in k$, where $(\cdot, \cdot)$ denotes the pairing. Then

$$\det(1 - \psi t) = (-1)^m \frac{\lambda^m t^m}{\det \varphi} \det\left(1 - \frac{\psi}{\lambda t}\right)$$

and

$$\det \psi = \frac{\lambda^m}{\det \varphi}.$$

Exercise 8.2. Let X be a variety over $\mathbb{F}_q$ of dimension d.

(a) Show using the deduction of the rationality of $Z(X, t)$ in the lectures, that $H^0(X, \mathbb{Q}_\ell)$ and $H^{2d}(X, \mathbb{Q}_\ell)$ are one dimensional and the Frob* is multiplication by q^d on $H^{2d}(X, \mathbb{Q}_\ell)$.

(b) Prove the functional equation for $Z(X, t)$ using Exercise 8.1 and Poincaré Duality.

Lecture 9

Exercise 9.1. Let K be a function field over $\mathbb{F}_q$ and X the curve to which it corresponds. Using the fact that a prime ring $\mathfrak{P}$ corresponds to a $\mathbb{F}_{q^n}$-point in X if and only if the residue field of $\mathfrak{P}$ is $\mathbb{F}_{q^n}$, prove that

$$\zeta_K(s) = Z(X, q^{-s}).$$

Exercise 9.2. Let K be a number field. Prove that the function $\mathbb{N}$ on the ideals of $\mathcal{O}_K$ is multiplicative. [*Hint:* Use the Chinese Remainder Theorem to reduce to the case of a prime ideal.]

Lecture 10

Exercise 10.1. Let k be a local field and identify k with its dual via the standard character. Prove that the self-dual measure on k is:

The Lebesgue measure if $k = \mathbb{R}$;

Twice the Lebesgue measure if $k = \mathbb{C}$;

The measure which gives $\mathcal{O}_k$ measure $(\mathbb{N}\mathfrak{D})^{-1/2}$ if k is nonarchimedean.

Exercise 10.2. Let k be a local field. Prove that the standard character ψ identifies k with its dual using the following outline: $x \mapsto (y \mapsto \psi(xy))$ is a homomorphism; it is injective; it is continuous; its image is dense; it is bicontinuous; its image is closed.

Lecture 11

In the exercises for this lecture, we prove that the local zeta functions are not zero for each choice of character. By the functional equation, it is enough to check this for one example of function f for each character χ. The computations that follow are carried out in Lang [4]. They will be useful to us in the exercises for Lecture 13.

Notation 11.1. Let $k = \mathbb{R}$. Then $\mathbb{R}^\times = \{\pm 1\} \times \mathbb{R}_{>0}$, and a character on $\{\pm 1\}$ is either trivial, or the sign function $\mathrm{sign}(x) = x/|x|$. Given a quasi-character c on $\mathbb{R}^\times$, write $c = \chi\|\cdot\|^s$ as in the lectures. Write $f_c(x) = x^{m(\chi)}e^{-\pi x^2}$, where $m(\chi) = 0$ if χ is trivial, or $m(\chi) = 1$ if $\chi = \mathrm{sign}$.

Exercise 11.1. With the notation just described, prove the following formulas:

$$\hat{f_c} = i^{m(\chi)} f_c;$$
$$\zeta(f_c, c) = \pi^{-(s+m(\chi))/2}\Gamma((s + m(\chi))/2);$$
$$\zeta(\hat{f_c}, \hat{c}) = i^{m(\chi)}\pi^{-(1-s+m(\chi))/2}\Gamma((1 - s + m(\chi))/2).$$

Here, $\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}\,dt$ is the usual gamma function.

Notation 11.2. Let $k = \mathbb{C}$. Then $\mathbb{C}^\times = S^1 \times \mathbb{R}_{>0}$, and a character on S^1 is thus of the form $z \mapsto z^m$ for $m \in \mathbb{Z}$ (this is standard from the duality of locally compact abelian groups). Write $c = \chi\|\cdot\|^s$ for a quasi-character c on $\mathbb{C}^\times$ as usual, and let $m(\chi)$ be so that $\chi(z) = z^{m(\chi)}$. Let f_c be defined by

$$f_c(z) = \frac{1}{2\pi}\overline{z}^{|m(\chi)|}e^{-2\pi|z|^2}, \qquad \text{if } m(\chi) \geq 0$$

and

$$f_c(z) = \frac{1}{2\pi}z^{|m(\chi)|}e^{-2\pi|z|^2}, \qquad \text{if } m(\chi) \leq 0.$$

Finally, write $c^- = \overline{\chi}\|\cdot\|^s$.

Exercise 11.2. With the notation just described, prove the following formulas:

$$\hat{f_c} = i^{|m(\chi)|} f_{c^-};$$
$$\zeta(f_c, c) = (2\pi)^{-s-(|m(\chi)|/2)}\Gamma(s + (|m(\chi)|/2));$$
$$\zeta(\hat{f_c}, \hat{c}) = i^{|m(\chi)|}(2\pi)^{-(1-s)-(|m(\chi)|/2)}\Gamma(1 - s + (|m(\chi)|/2)).$$

[*Hint:* For the first formula, prove it for $m \geq 0$ by induction. For the induction step, apply the differential operator $(4\pi i)^{-1}[(\partial/\partial x) + i(\partial/\partial y)]$ where $z = x + iy$ is the complex variable of f_c.]

Notation 11.3. Let k be nonarchimedean, with prime $\mathfrak{p}$. Write $c = \chi\|\cdot\|^s$ for a quasi-character on $k^\times$. Since the subgroups $1 + \mathfrak{p}^n$ form a base of neighborhoods about 1 in U, it follows easily that for n large enough, c is trivial on $1 + \mathfrak{p}^n$. We let $m(\chi)$ be the smallest such n, and we call the ideal $\mathfrak{f}_\chi = \mathfrak{p}^{m(\chi)}$ the *conductor* of c, or of χ. We also call $m(\chi)$ the *ramification index* of c or of χ. We say that c or χ is *unramified* if $m = 1$.

Let k be an extension of some $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$, and let $\mathfrak{D}$ be the different of that extension. Let g be the characteristic function of the set $(\mathfrak{D}\mathfrak{f}_\chi)^{-1}$, and define $f_c = \psi g$ where ψ is the standard character. Let l denote the power of $\mathfrak{p}$ in the different $\mathfrak{D}$. Let $\mu^\times$ be the usual Haar measure on $k^\times$. Let $\{\epsilon\}$ denote a set of representatives for $\mathcal{O}_k^\times$ modulo $\mathfrak{f}_\chi$. Let $\pi \in \mathfrak{p}$ be a prime element. Finally, let

$$\tau(\chi) = \sum_\epsilon (\chi\psi)(\epsilon\pi^{-l-m(\chi)}).$$

Exercise 11.3. With the notation just described, prove that τ is independent of the choice of ϵ's and that we have the following formulas:

$$\hat{f_c}(x) = \begin{cases} (\mathbb{N}\mathfrak{D})^{1/2}(\mathbb{N}\mathfrak{f}_\chi) & \text{if } x \equiv 1 \pmod{\mathfrak{f}_\chi} \\ 0 & \text{if } x \not\equiv 1 \pmod{\mathfrak{f}_\chi}; \end{cases}$$
$$\zeta(f_c, c) = (\mathbb{N}(\mathfrak{D}\mathfrak{f}_\chi))^s \mu(1 + \mathfrak{f}_\chi)\tau(\chi);$$
$$\zeta(\hat{f_c}, \hat{c}) = (\mathbb{N}\mathfrak{D})^{1/2}(\mathbb{N}\mathfrak{f}_\chi)\mu(1 + \mathfrak{f}_\chi).$$

Conclude that the function ρ from the functional equation is nonzero and meromorphic for all functions f.

Lecture 12

Exercise 12.1. Let $\{G_v\}_{v\in V}$ be locally compact abelian groups indexed by the set V with a finite subset $S_\infty \subset V$ and for each $v \notin S_\infty$, let $H_v \subset G_v$ be compact open subgroups. Let μ_v be a Haar measure on G_v such that $\mu_v(H_v) = 1$ for almost all $v \notin S_\infty$. Let G be the restricted direct product of the G_v's with respect to the H_v's.

(a) Prove that $\widehat{G}$ is just the restricted direct product of the $\widehat{G}_v$'s with respect to the $H_v^\perp$'s.

(b) Prove that the measure defined by

$$\mu(x + U) = \mu(U) = \prod_{v\in V} \mu_v(U_v)$$

on basic open sets U in G, is indeed a well defined Haar measure on G.

Exercise 12.2. Let L/K be an extension of global fields. Let v be a place of K. Prove that

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_w \mathrm{Tr}_{L_w/K_v}(\alpha),$$

where the sum is over all places w of L extending v. Prove the same for the norm (the sum being replaced by a product).

Exercise 12.3. Let K be a global field. Identify $\mathbb{A}_K$ with its dual via the standard character. Prove that $K^\perp = K$. [*Hint:* To show $K \subset K^\perp$, reduce to the case $K = \mathbb{Q}$ or $K = \mathbb{F}_q(t)$ using Exercise 12.2. Then prove $K^\perp/K$ is compact and discrete, hence finite, and conclude.]

Lecture 13

Notation 13.1. We keep the notation from the local computations of the exercises of Lecture 11. The next exercise will also depend on these local computations.

Let K be a number field of degree n with r_1 real embeddings and $2r_2$ complex embeddings. Let $\mathfrak{D}$ be the different of K over $\mathbb{Q}$. For a quasi-character $c = \chi\|\cdot\|^s$ of $\mathbb{I}_K$ which is trivial on $K^\times$, we let $\mathfrak{f}_\chi$ be the *conductor* of χ, which is the product of all the local conductors $\mathfrak{f}_{\chi,v}$ of the restrictions of χ to K_v for $v \in V_\mathrm{f}$. Let $\mathfrak{D}_\chi = \mathfrak{f}_\chi\mathfrak{D}$ and $\Delta_\chi = \mathbb{N}\mathfrak{D}_\chi$.

For $v \in V_K$, let $f_{c,v}$ be the f_c as specified in the exercises for Lecture 11 for the corresponding local field K_v, and similarly let $m_v(\chi)$ be the local $m(\chi)$. Also, for $v \in V_K$, let n_v denote the *local degree*, i.e., if v_0 is the place of $\mathbb{Q}$ which v extends, then $n_v = [K_v : \mathbb{Q}_{v_0}]$. If $v \in V_\infty$, we let

$$g_{c,v}(x) = f_c(\Delta_\chi^{1/2n}x)(n_v\pi)^{|m_v(\chi)|/2}.$$

If $v \in V_\mathrm{f}$, let

$$g_{c,v}(x) = \frac{1}{\mu_v^\times(1+\mathfrak{f}_{\chi,v})} f_{c,v}(x),$$

where $\mu_v^\times$ is the usual local measure. Let

$$g_c((x_v)_{v\in V_K}) = \prod_{v\in V_K} g_{c,v}(x_v).$$

Now for $v \in V_\mathrm{f}$, let π_v be the idele having component some prime element of K_v at v, and component 1 everywhere else. Let S_χ be the set of all infinite places and all finite places at which χ is ramified (i.e., where the restriction of χ to K_v is ramified). Let

$$L(s,\chi) = \prod_{v\notin S_\chi} (1 - \chi(\pi_v)(\mathbb{N}\mathfrak{p}_v)^{-s})^{-1}$$

where $\mathfrak{p}_v$ is the prime in K_v. Let

$$\Lambda(s,\chi) = (2^{-r_2}\pi^{-n/2}\Delta_\chi^{1/2})^s \prod_{v\in S_\infty} \Gamma\left(\frac{n_v s + |m_v(\chi)|}{2}\right) L(s,\chi)$$

Finally, let $M = \sum_{v\in V_\infty} |m_v(\chi)|$ and let $\tau_v(\chi)$ be the local $\tau(\chi)$ from the exercises of Lecture 11, for $v \in V_\mathrm{f}$.

Exercise 13.1 (Functional Equation for L-functions)**.** By applying the functional equation to $\zeta(g_c, c)$, prove that

$$W(\chi)\Lambda(s,\chi) = \Lambda(1-s,\overline{\chi})$$

where

$$W(\chi) = i^{-M}(\mathbb{N}\mathfrak{f}_\chi)^{-1/2} \prod_{v\in S_\chi\setminus V_\infty} \tau_v(\chi) \prod_{v\notin S_\chi} \chi(\mathfrak{D}_v^{-1})$$

where $\chi(\mathfrak{D}_v)$ means χ evaluated on a power of π_v which generates the local different at v. Can you prove an analogue for function fields?

Since Hecke L-functions are examples of the $L(s,\chi)$ above, this suffices to prove the analytic continuation and functional equation for them, and hence also for the Artin L-functions of abelian extensions.

Bibliography

[1] J. W. S. Cassels and A. Fröhlich, *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] J. S. Milne, *Étale Cohomology*. Princeton University Press, Princeton, New Jersey, 1980.

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

[8] W. Rudin, *Real and Complex Analysis*, Third Edition. McGraw-Hill, 1987.

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

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

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