Lectures On Algebraic Number Theory

Dipendra Prasad

Notes by Anupam

1 Number Fields

We begin by recalling that a complex number is called an algebraic number if it satisfies a polynomial with rational coefficients or equivalently with integer coefficients. A complex number is called an algebraic integer if it satisfies a polynomial with integral coefficients having leading coefficient as 1. Let $\overline{\mathbb{Q}}$ be the set of all algebraic numbers inside $\mathbb{C}$. It is well known that $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$. Any finite extension of $\mathbb{Q}$ is called an Algebraic Number Field.

Some of the most studied examples of number fields are:

1. $\mathbb{Q}$, the field of rational numbers.
2. Quadratic extensions $\mathbb{Q}(\sqrt{d})$; where $d \in \mathbb{Z}$ is a non-square integer.
3. Cyclotomic fields $\mathbb{Q}(\zeta_n)$, $\zeta_n = e^{\frac{2\pi i}{n}}$.
4. Kummer extensions $K(a^{\frac{1}{n}})$ where $a \in K^*$ and K is a number field.

Definition. *A Dedekind domain is an integral domain R such that*

1. *Every ideal is finitely generated;*
2. *Every nonzero prime ideal is a maximal ideal;*

3. The ring R is integrally closed (in its field of fractions).

Let K be a number field. Let us denote the set of algebraic integers inside K by O_K.

Theorem 1.1. *1. If K is a number field then O_K, the set of algebraic integers inside K, forms a subring of K. This subring O_K is a finitely generated $\mathbb{Z}$ module of the same rank as $deg_{\mathbb{Q}}K$.*

2. The ring O_K is a Dedekind domain. In particular, every ideal in O_K can be written uniquely as a product of prime ideals.

Unlike $\mathbb{Z}, O_K$ need not be a PID and typically it is not. Gauss conjectured that there are exactly nine imaginary quadratic fields which are PID, and this was proved in 60's by Baker and Stark. These are $\mathbb{Q}(\sqrt{-d})$ for $d = 3, 4, 7, 8, 11, 19, 43, 67, 163$. Using Minkowski bound on class number (see later section) it is easy to prove that these are PID. Gauss also conjectured that there are infinitely many real quadratic fields which are PID. This is NOT YET SOLVED. The following theorem will be proved in one of the later lectures. Let us denote O_K^* for the units in O_K i.e. elements in O_K which has inverse in O_K. Then O_K^* is a group.

Theorem 1.2 (Dirichlet Unit Theorem)**.** *The group O_K^* is finitely generated abelian group. The rank of O_K^* is $= r_1 + r_2 - 1$, where r_1 is number of real embeddings of K in $\mathbb{R}$ and r_2 is number of complex embeddings of K in $\mathbb{C}$ up to complex conjugation.*

As some simple consequences of the theorem we note the following.

1. The group O_K^* is finite if and only if $K = \mathbb{Q}$ or is a quadratic imaginary field.

2. If K is real quadratic, then O_K^* is $\mathbb{Z}/2 \times \mathbb{Z}$. If $K = \mathbb{Q}(\sqrt{d})$ then $O_K = \mathbb{Z}(\sqrt{d})$ if $d \not\equiv 1(\text{mod}4)$ and $O_K = \mathbb{Z}(\frac{1+\sqrt{d}}{2})$ if $d \equiv 1(\text{mod}4)$. Thus existence of units inside O_K is equivalent to solving the Pell's equation $a^2 - db^2 = 1$. (Observe that $x \in O_K$ is unit if and only if $x\overline{x} = \pm 1$).

Here are few Questions about quadratic fields which are still unsolved !

1. For which real quadratic fields does there exist a unit with norm $= -1$.
2. Are there estimates on the fundamental unit of $Q(\sqrt{d}), d > 1$ in terms of d?

Exercise: If $K = \mathbb{Q}[m^{\frac{1}{n}}]$, then O_K contains $\mathbb{Z}[m^{\frac{1}{n}}]$ as a subgroup of finite index. Calculate the index of $\mathbb{Z}[m^{\frac{1}{n}}]$ in O_K.

2 Class Group of A Number Field

Definition. *A nonzero additive subgroup $\mathcal{A} \subset K$ is called a fractional ideal if there exists $\lambda \in K$ such that $\lambda\mathcal{A} \subset O_K$ and $\mathcal{A}O_K \subset \mathcal{A}$.*

It is easy to see that nonzero fractional ideals form a group under multiplication with O_K as the identity and

$$\mathcal{A}_1\mathcal{A}_2 = \left\{ \sum \lambda_i \mu_i \ / \ \lambda_i \in \mathcal{A}_1, \mu_i \in \mathcal{A}_2 \right\}.$$

Definition.

$$\text{Class Group} := \frac{\text{The group of all nonzero fractional ideals}}{\text{group of all nonzero principal ideals}}.$$

Theorem 2.1. *The Class Group of a number field is finite.*

Remark: The finiteness of class group is not true for arbitrary Dedekind domains. It is a special feature of number fields.

There exists an analytic expression for the class number as the residue of the zeta function associated to the number fields, which is given by the following theorem. The theorem will be proved later.

Theorem 2.2 (Class Number Formula)**.** *Let K be a number field. Then,*

$$\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{d}_K} . \frac{1}{s-1} + \text{holomorphic function}$$

where r_1 is number of real embeddings of K in $\mathbb{C}$, r_2 is number of complex embeddings of K in $\mathbb{C}$ upto complex conjugate, h is class number of K, R is the regulator of number field K, w is number of roots of unity in K and d_K is the modulus of discriminant.

3 More Algebraic Background

Let K be a number field. It is sometimes convenient to write it pictorially as follows

$$\begin{array}{ccc} O_K & \longrightarrow & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \longrightarrow & \mathbb{Q} \end{array}$$

Let $p \in \mathbb{Z}$ be a prime. Denote the decomposition of the ideal $(p) = pO_K$ in O_K as $pO_K = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$ with $\mathfrak{p}_i$ prime ideal in O_K. This e_i is called ramification index of $\mathfrak{p}_i$ over p.

One of the basic questions in algebraic number theory is the following. Given a polynomial $f(x) \in \mathbb{Z}[x]$, look at the reduced polynomial modulo p as polynomial in $\mathbb{Z}/p[x]$, say $\bar{f}(x)$, and write it as product of powers of irreducible polynomials $\bar{f}(x) = \prod \bar{f}_i(x)^{e_i}$ in $\mathbb{Z}/p[x]$. The question is whether one can describe a LAW which tells us how many of $\bar{f}_i$'s occur and what are the possible degrees in terms of p.

Example : Let $f(x) = x^2 - 5$, then quadratic reciprocity law gives the answer. Let p be an odd prime. Then $x^2 - 5 = 0$ has solution in $\mathbb{Z}/p$ if and only if there exist $x_0 \in \mathbb{Z}/p$ such that $x_0^2 = 5$. And $x_0^2 = 5$ has solution in $\mathbb{Z}/p$ if and only if $5^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$ (which is by defenition denoted as $(\frac{5}{p})$ $= 1$). This can be seen by noting that $(\mathbb{Z}/p)^*$ is a cyclic group. So if $p/5$ then $\bar{f}(x) = x^2$. If $(\frac{5}{p}) = 1$ then $\bar{f}(x) = (x - x_0)(x + x_0)$, where $x_0^2 = 5$ in $\mathbb{Z}/p$. And if $(\frac{5}{p}) = -1$ then $\bar{f}(x)$ is irreducible in $\mathbb{Z}/p$.

We will later prove the following theorem. There exists a "law" of decomposing polynomials mod p as primes in arithmetic progression if and only if

the polynomial defines an abelian extension of $\mathbb{Q}$.

Let us look at following field extension.

$$\begin{array}{ccc} O_K & \longrightarrow & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \longrightarrow & \mathbb{Q} \end{array}$$

Let $p \in \mathbb{Z}$ be a prime and let $\mathfrak{p}$ be a prime ideal lying over p in O_K. Let $pO_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$. Then we get field extensions of finite fields $\mathbb{Z}/p \longrightarrow O_K/\mathfrak{p}$ of degree, say f_i. This f_i is called residual degree of $\mathfrak{p}_i$ over p.

Lemma 3.1. *Let K be a number field. Then $\sum_{i=1}^{g} e_i f_i = [K : \mathbb{Q}]$, where the notations are defined as above. If K is Galois extension of $\mathbb{Q}$, then Galois group acts naturally on the set of primes $\mathfrak{p}_i$ lying above p. In this case f_i's are the same, e_i's are the same and $efg = [K : \mathbb{Q}]$, where e is the ramification index, f is the residual degree and g is the number of primes lying over p.*

4 Artin Reciprocity Theorem

Let K be a number field which is Galois over a number field k. We keep notations of previous section. Let $\mathfrak{p}$ be a prime ideal in O_K lying over a prime ideal p in O_k. Let $D_\mathfrak{p} \subseteq G$ denote the subgroup of Galois group $Gal(K/k)$ preserving the prime $\mathfrak{p}$; the subgroup $D_\mathfrak{p}$ is called the Decomposition group of the prime $\mathfrak{p}$. We have following exact sequence associated to the prime ideal $\mathfrak{p}$.

$$0 \longrightarrow I_\mathfrak{p} \longrightarrow D_\mathfrak{p} \longrightarrow Gal\left(\frac{O_K/\mathfrak{p}}{O_k/p}\right) \longrightarrow 0$$

The kernel $I_\mathfrak{p}$ is called the inertia group of $\mathfrak{p}$.

We call K/k is unramified if $e = 1 \Leftrightarrow I_\mathfrak{p} = 1$. In case of the finite field extension $\mathbb{F}_q \subset \mathbb{F}_{q^e}$, the map $\sigma : \mathbb{F}_{q^e} \longrightarrow \mathbb{F}_{q^e}, x \mapsto x^q$ is called the Frobenius element. It generates the Galois group of $\mathbb{F}_{q^e}$ over $\mathbb{F}_q$. In the case

of unramified extension the decomposition group gets a prefered element, called the Artin symbol $\sigma_{\mathfrak{p}} =< \mathfrak{p}, K/k >\in Gal(K/k)$.

The following is the most fundamental theorem in algebraic number theory, called the "Artin Reciprocity Theorem".

Theorem 4.1 (Artin Reciprocity Theorem)**.** *Let K be an abelian extension over $\mathbb{Q}$. Then Artin symbol defines a map from $I(C) \longrightarrow Gal(K/\mathbb{Q})$, where C is some ideal in K and contains in its kernel P_C (group of principal ideals containing a generator which is congruent to 1 mod C). Thus $Gal(K/\mathbb{Q})$ is a quotient of $I(C)/P_C$, generalised class group.*

5 Quadratic form associated to a number field

Let K be a number field. Let $x \in K$. Considering K as a $\mathbb{Q}$ vector space, we get a $\mathbb{Q}$-linear map $l_x : K \longrightarrow K$ defined by $l_x(\lambda) = \lambda x$. Define $tr^K_{\mathbb{Q}}(x)$ as trace of l_x and $Nm^K_{\mathbb{Q}}(x)$ as determinant of l_x. If there is no possibility of confusion, we will denote $tr^K_{\mathbb{Q}}(x)$, $Nm^K_{\mathbb{Q}}(x)$ simply as tr and Nm.

Example : If $p \in \mathbb{Q}$ then $tr(p) = p.[K : \mathbb{Q}]$ *and* $N(p) = p^{[K:\mathbb{Q}]}$.

Define a bilinear form $B : K \times K \longrightarrow \mathbb{Q}$ by $B(x, y) = tr(xy)$. One can restrict this bilinear form to the ring of integers O_K to get a bilinear form $B : O_K \times O_K \longrightarrow \mathbb{Z}$. Recall that O_K is a free $\mathbb{Z}$ module of rank same as deg of $K/\mathbb{Q}$.

Definition. *Let B be a bilinear form $B : \mathbb{Z}^d \times \mathbb{Z}^d \longrightarrow \mathbb{Z}$. One can associate an integer, called the discriminant of the quadratic form, and denoted be d_B to be* $\det(B(e_i, e_j))$*, where $\{e_1, ...e_d\}$ is an integral basis of $\mathbb{Z}^d$.*

Note that d_B does not depend on the basis chosen as can be seen as follows. Let B' be another integral basis of $\mathbb{Z}^d$. Then there exists an integeral matrix A such that $B = AB'A^t$. Hence,

$d_B = \det B = \det(AB'A^t) = (\det A)^2 \det B' = \det B'$

Here we have used that for $A \in GL(n, \mathbb{Z}), \det A = 1$ *or* -1. This discriminant of the trace form on the ring of integers of a number field is called the

discriminant of number field.

The following theorem will be proved later.

Theorem 5.1 (Minkowski)**.** *Let K be a number field, with d_K as its discriminant. Then $|d_K| > 1$ if $K \neq \mathbb{Q}$.*

Problem of determining the fields of given discriminant is yet to be ANSWERED.

Exercise: Quadratic form associated above to a number field does not determine number field uniquely. As specific examples, construct cubic number fields with same quadratic form. This question will be answered later. Note, however, a quadratic number field is determined by the quadratic form uniquely.

6 Dirichlet Unit Theorem[1]

Dirichlet Unit Thoerem is a statement about the structure of the unit group of the ring of integers of a number field. What it says is that such a group is necessarily finitely generated and it gives the rank as well as a description of the torsion part. The proof however, in its natural set up, belongs to the realms of Geometric theory of numbers, also reffered as Minkowski Theory. So let us take a birds eye view of Minkowski Theory.

The central notion in Minkowski Theory is that of a Lattice. A Lattice for us means the following,

Definition. *Let $\mathbb{V}$ be an n-dimensional $\mathbb{R}$-vector space. A Lattice in $\mathbb{V}$ is a subgroup of the form*

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$$

with linearly independent vectors $v_1, \cdots, v_m$ of V. The set

$$\Phi = \{x_1v_1 + \cdots + x_mv_m |\ x_i \in \mathbb{R},\ 0 \ \leq x_i \ \leq \ 1\}$$

is called a fundamental mesh of the lattice.

[1]This section is written by Purusottam Rath.

The lattice is said to have rank m and is called a complete lattice if its rank is equal to n. Let us enumerate some properties of a lattice.

Lemma 6.1. *A subgroup* Γ *of* $\mathbb{V}$ *is a lattice if and only if it is discrete.*

Note that $\mathbb{Z} + \mathbb{Z}\sqrt{3}$ is not a lattice in $\mathbb{R}$.

Lemma 6.2. *A lattice* Γ *in* $\mathbb{V}$ *is complete if and only if there exists a bounded subset* $\mathbb{M} \subseteq \mathbb{V}$ *such that the collection of all translates* $\mathbb{M} + \gamma, \gamma \in \Gamma$ *covers the whole space* $\mathbb{V}$.

Now suppose $\mathbb{V}$ is a euclidean vector space, hence endowed with an inner product

$$(\ , \ ) : \mathbb{V} \times \mathbb{V} \to \mathbb{R}$$

Then we have on $\mathbb{V}$ a notion of volume (more precisely a Haar measure). Then if Φ is a fundamental mesh of a lattice Γ with basis vectors $v_1, \cdots, v_m$ then we define volume of Γ as

$$\text{vol } \Gamma := \text{vol } (\Phi)$$

Note this is independent of choice of basis vectors of the lattice as any such two have a change of basis matrix in $SL_m(\mathbb{Z})$.

We now come to the most important theorem about lattices. A subset $\mathbb{X}$ of $\mathbb{V}$ is called centrally symmetric, if for any $x \in \mathbb{X}$, the point $-x$ also belongs to $\mathbb{X}$. It is called convex if for any two points $x, y \in \mathbb{X}$ the line segment $\{ty + (1-t)x |\ 0 \ \leq t \ \leq \ 1\}$ joining x and y is contained in $\mathbb{X}$. With these definitions we have,

Theorem 6.1 (Minkowski Theorem)**.** *Let* Γ *be a complete lattice in a euclidean vector space* $\mathbb{V}$ *and let* $\mathbb{X}$ *be a centrally symmetric, convex subset of* $\mathbb{V}$. *Suppose that*

$$vol(\mathbb{X}) \ > \ 2^n \ vol(\Gamma)$$

Then $\mathbb{X}$ *contains at least one nonzero lattice point* $\gamma \ \in \Gamma$.

The Minkowski Theorem stated above would be crucial to our proof of the unit theorem. In fact it plays a pivotal role in number theory and has some really non-trivial applications. For instance we can prove the famous four-square theorem using this as is done below.

Theorem 6.2 (Four Square Theorem)**.** *Every positive integer is a sum of four squares.*

Proof : Suffices to show that any odd prime is a sum of four squares. Let p be any odd prime. Now there exists positive integers a, b such that $a^2 + b^2 + 1 \equiv 0 \pmod{p}$. Conside the lattice Γ in $\mathbb{R}^4$ with basis vectors

$$\begin{aligned} v_1 &= (p,0,0,0), v_2 = (0,p,0,0), \\ v_3 &= (a,b,1,0), v_3 = (b,-a,0,1). \end{aligned}$$

Any vector v in Γ has the form $(r_1p + r_3a + r_4b, r_2p + r_3b - r_4a, r_3, r_4)$. Thus we see that the integer $|v|^2$ is a multiple of p.

Consider the open ball $\mathcal{B}$ in $\mathbb{R}^4$ of radius $\sqrt{2p}$ centered at origin. It is a convex centrally symmetric set with volume $2\pi^2p^2$ which is strictly greater than 2^4p^2. Since Γ has volume p^2, by Minkowski Theorem, $\mathcal{B}$ contains a non-zero point $u = (A, B, C, D)$, say.

Now, $0 < |u|^2 < 2p$ and $|u|^2$ is a multiple of p. Hence $|u|^2 = p$, that is, $A^2 + B^2 + C^2 + D^2 = p$. $\square$

The basic idea in the proof of Minkowski Unit Theorem is to interpret the elements of a number field $\mathbb{K}$ over $\mathbb{Q}$ of degree n as points lying in an n-dimensional space. We consider the canonical mapping

$$\begin{aligned} j &: \mathbb{K} \longrightarrow \mathbb{K}_{\mathbb{C}} = \prod_{\tau} \mathbb{C} \\ a &\longmapsto ja = (\tau a) \end{aligned}$$

which results from the n embeddings of $\mathbb{K}$ in $\mathbb{C}$. Let these embeddings be given by the ordered set

$$X = \{\rho_1, \cdots, \rho_r, \sigma_1, \bar{\sigma_1}, \cdots, \sigma_s, \bar{\sigma_s}\}$$

where the ρ's give the r real embeddings and σ's and $\bar{\sigma}$'s give the $2s$ pairwise conjugate complex embeddings. We see that the image of $\mathbb{K}$ under this canonical mapping into $\mathbb{C}^n = \prod_{\tau \in X} \mathbb{C}$ actually lies inside the following set known as the Minkowski Space.

$$\mathbb{K}_{\mathbb{R}} = \left\{ (z_\tau) \in \prod_{\tau \in X} \mathbb{C} \mid z_\rho \in \mathbb{R}, z_{\bar{\sigma}} = \bar{z_\sigma} \right\}$$

We note that this space is isomorphic to $\prod_{\tau \in X} \mathbb{R} = \mathbb{R}^{r+2s}$ given by the map $F : (z_\tau) \mapsto (x_\tau)$ where $x_\rho = z_\rho,\ x_\sigma = Re(z_\sigma),\ x_{\bar{\sigma}} = Im(z_\sigma)$. However this map is not volume preserving and

$$Vol_{\text{canonical}}(Y) = 2^s\ Vol_{\text{Lebesgue}}(F(Y))$$

where the canonical volume is the volume on $\mathbb{K}_{\mathbb{R}}$ induced from the standard inner product on $\mathbb{C}^n$. A little reflection will show that the mapping $j : \mathbb{K} \longrightarrow \mathbb{K}_{\mathbb{R}}$ identifies the vector space $\mathbb{K}_{\mathbb{R}}$ with the tensor product $\mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R}$,

$$\begin{array}{ccc} \mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R} & \longleftrightarrow & \mathbb{K}_{\mathbb{R}} \\ a \otimes x & \mapsto & (ja)x \end{array}$$

Lemma 6.3. *If $I \neq 0$ is an ideal in $O_{\mathbb{K}}$, the ring of integers of $\mathbb{K}$, then $\Gamma := j(I)$ is a complete lattice in $\mathbb{K}_{\mathbb{R}}$ with volume $\sqrt{|d_{\mathbb{K}}|}.[O_{\mathbb{K}} : I]$, where $d_{\mathbb{K}}$ is the discriminant of $\mathbb{K}$.*

Proof : Just note that I has an integral basis i.e. a $\mathbb{Z}$ basis $\alpha_1, \cdots, \alpha_n$, so that $\Gamma = \mathbb{Z}j\alpha_1 + \cdots + \mathbb{Z}j\alpha_n$. Consider the matrix A $=(\tau_l(\alpha_i))$ with τ's running over the embeddings of $\mathbb{K}$ in $\mathbb{C}$. Then we have

$$\langle j\alpha_i, j\alpha_k \rangle = \sum_{1 \leq l \leq n} \tau_l(\alpha_i)\bar{\tau}_l(\alpha_k) = A\bar{A}^t$$

Then we get

$$Vol(\Gamma) = |det(\langle j\alpha_i, j\alpha_k\rangle)|^{\frac{1}{2}} = |det(A)| = \sqrt{|d_{\mathbb{K}}|}.[O_{\mathbb{K}} : I] \qquad \square$$

So via the canonical embedding $j : \mathbb{K} \longrightarrow \mathbb{K}_{\mathbb{C}}$, we can identify the ideals of $O_{\mathbb{K}}$ with lattices in $\mathbb{R}^n$. But since we are interested in the units of the ring of integers, $O_{\mathbb{K}}^*$, we pass on to the multiplcative group $\mathbb{K}^*$ by using the standard logarithm map

$$l : \mathbb{C}^* \longrightarrow \mathbb{R},\ z \longrightarrow \log|z|$$

It induces the surjective homomorphism

$$l : \mathbb{K}_{\mathbb{C}}^* = \prod_{\tau} \mathbb{C}^* \longrightarrow \prod_{\tau} \mathbb{R}\ ,\ (z_\tau) \longrightarrow (\log|z_\tau|$$

Note that image of $\mathbb{K}_{\mathbb{R}}^*$ under the above map lies in the following set

$$\left[\prod_{\tau} \mathbb{R}\right]^+ := \left\{(x_\tau) \in \prod_{\tau} \mathbb{R} \mid x_\rho \in \mathbb{R}, x_{\bar{\sigma}} = x_\sigma\right\}$$

Further the multiplicative group $\mathbb{K}_{\mathbb{C}}^*$ admits the homomorphism $\mathbb{N} : \mathbb{K}_{\mathbb{C}}^* \longrightarrow \mathbb{C}^*$ given by the product of the coordinates and we have the homomorphism

$$Tr : \left[\prod_{\tau} \mathbb{R}\right]^+ \longrightarrow \mathbb{R}$$

given by the sum of the coordinates. Also note that the $\mathbb{R}$-vectorspace $[\prod_\tau \mathbb{R}]^+$ is isomorphic to $\mathbb{R}^{r+s}$. Now conside the following subgroups

$$\begin{aligned} O_{\mathbb{K}}^* &= \{\epsilon \in O_{\mathbb{K}} \mid N_{\mathbb{K}|\mathbb{Q}} = \pm 1\} \\ S &= \{y \in \mathbb{K}_{\mathbb{R}}^* \mid \mathbb{N}(y) = \pm 1\} \\ H &= \{x \in [\prod_{\tau} \mathbb{R}]^+ \mid Tr(x) = 0\} \end{aligned}$$

It is clear that $j(O_{\mathbb{K}}^*) \subseteq S$ and $l(S) \subseteq H$. Thus we obtain the homomorphisms

$$O_{\mathbb{K}}^* \xrightarrow{j} S \xrightarrow{l} H$$

and the composite $\lambda := l \; o \; j : O_{\mathbb{K}}^* \to H$. The image will be denoted by

$$\Gamma = \lambda(O_{\mathbb{K}}^*) \; \subseteq H$$

and we obtain the

Theorem 6.3. *Let $\mathbb{K}$ be a number field. Then the sequence*

$$1 \longrightarrow \mu(\mathbb{K}) \longrightarrow O_{\mathbb{K}}^* \xrightarrow{\lambda} \Gamma \longrightarrow 0$$

is exact, where $\mu(\mathbb{K})$ is the group of roots of unity that lie in $\mathbb{K}$.

Proof : The only non obvious part is to show that $\ker(\lambda)$ lies in $O_{\mathbb{K}}^*$. Now $\lambda(\epsilon) = l(j\epsilon) = 0$ implies $|\tau\epsilon| = 1$ for each embedding τ of $\mathbb{K}$. Thus $(j\epsilon) = (\tau\epsilon)$ lies in a bounded domain of the $\mathbb{R}$-vector space $\mathbb{K}_{\mathbb{R}}$. But $(j\epsilon)$ is a point in the lattice $jO_{\mathbb{K}}$ of $\mathbb{K}_{\mathbb{R}}$. Therefore the kernel of λ can contain only finitely many elements, and thus, being a finite group, contains only the roots of unity in $\mathbb{K}$. $\square$

Given this theorem, it remains to determine the group Γ. For this we need the following lemma which depends on Minkowski Lattice Point Theorem.

Lemma 6.4. *Let $I \neq 0$ be an integral ideal of $\mathbb{K}$, and let $c_\tau > 0$, for $\tau \in Hom(\mathbb{K}, \mathbb{C})$, be real numbers such that $c_\tau = c_{\bar{\tau}}$ and*

$$\prod_\tau c_\tau \; > \; A[O_{\mathbb{K}} : I]$$

where $A = (\frac{2}{\pi})^s \sqrt{|d_{\mathbb{K}}|}$. Then there exists $a \in I, a \neq 0$, such that

$$|\tau a| \; < \; c_\tau \text{ for all } \tau \in Hom(\mathbb{K}, \mathbb{C})$$

Proof : We just note that the the set

$$Y = \{(z_\tau) \in \mathbb{K}_{\mathbb{R}} \mid |z_\tau| < c_\tau\}$$

is centrally symmetric, convex and has volume $2^{r+s}\pi^s \prod_\tau c_\tau$. Now, $\Gamma = j(I)$ is a lattice with volume $\sqrt{|d_{\mathbb{K}}|}.[O_{\mathbb{K}} : I]$. So we have

$$\text{Vol}(Y) \; > \; 2^{r+s}\pi^s(\frac{2}{\pi})^s \sqrt{|d_{\mathbb{K}}|}.[O_{\mathbb{K}} : I] = 2^n \text{Vol}(\Gamma)$$

So the assertion now follows from Minkowski Lattice Point Theorem. $\square$

Finally we determine the structure of Γ.

Theorem 6.4. *The group* Γ *is a complete lattice in the* $(r+s-1)$*- dimensional* $\mathbb{R}$*-vector space* H *.*

Proof : Since $[\prod_\tau \mathbb{R}]^+$ has dimension $(r+s)$, H is of dimension $(r+s-1)$, being the kernel of the linear functional Tr. The mapping $\lambda := l\ o\ j : O_{\mathbb{K}}^* \to H$ arises by restricting the mapping

$$\mathbb{K}^* \xrightarrow{j} \prod_\tau \mathbb{C}^* \xrightarrow{l} \prod_\tau \mathbb{R}$$

Thus it suffices to show, that for any $c > 0$, the bounded domain $\{(x_\tau) \in \prod_\tau \mathbb{R} \mid |x_\tau| \leq c\}$ contains only finitely many points of Γ. Since $l((z_\tau)) = (\log|z_\tau|)$, the preimage of this domain with respect to l is the bounded domain

$$\left\{(z_\tau) \in \prod_\tau \mathbb{C}^* \mid e^{-c} \leq |z_\tau| \leq e^c\right\}$$

But it contains only finitely many points of the set $j(O_{\mathbb{K}}^*)$ as this is a subset of the lattice $j(O_{\mathbb{K}})$. Therefore Γ is a lattice in H. Finally we show that Γ is a complete lattice in H. We chose real numbers $c_\tau > 0$, for $\tau \in \mathrm{Hom}(\mathbb{K}\ , \mathbb{C})$, satisfying $c_\tau = c_{\bar{\tau}}$ and

$$C = \prod_\tau c_\tau > A[O_{\mathbb{K}} : I]$$

where $A = (\frac{2}{\pi})^s \sqrt{|d_{\mathbb{K}}|}$, and we consider the set

$$W = \{(z_\tau) \in \mathbb{K}_{\mathbb{R}} \mid |z_\tau| < c_\tau\}$$

For an arbitrary point $y = (y\tau) \in S$, it follows that

$$Wy = \{(z_\tau) \in \mathbb{K}_{\mathbb{R}} \mid |z_\tau| < \tilde{c_\tau}\}$$

where $\tilde{c_\tau} = c_\tau |y_\tau|$ and one has $\tilde{c_\tau} = \tilde{c}_{\bar{\tau}}$, $\prod_\tau c_\tau = \prod_\tau \tilde{c_\tau} = C$ because $\prod_\tau |y_\tau| = |\mathbb{N}(y)| = 1$. Then, there exists a point

$$ja = (\tau a) \in Wy,\ a \in O_{\mathbb{K}},\ a \neq 0$$

Now, upto multiplication by units, there are only finitely many elements $\alpha \in O_{\mathbb{K}}$ of a given norm $N_{\mathbb{K}|\mathbb{Q}} = a$. Thus we may pick up a system of $\alpha_1, \cdots, \alpha_M \in O_{\mathbb{K}}, \alpha_i \neq 0$ such that every $a \in O_{\mathbb{K}}$ with $0 < |N_{\mathbb{K}|\mathbb{Q}}(a)| \leq C$ is associated to one of these numbers. The set

$$T = S \cap \bigcup_{i=1}^{M} W(j\alpha_i)^{-1}$$

is a bounded set as W is bounded and we have

$$S = \bigcup_{\epsilon \in \Theta_{\mathbb{K}}^*} Tj\epsilon$$

Because for any $y \in S$, we find, by the above, an $a \in O_{\mathbb{K}}, a \neq 0$, such that $ja \in Wy^{-1}$, so $ja = xy^{-1}$ for some $x \in W$. Since

$$|N_{\mathbb{K}|\mathbb{Q}}(a)| = |\mathbb{N}(xy^{-1})| = |\mathbb{N}(x)| < \prod_{\tau} c_\tau = C,$$

a is associated to some α_i , $\alpha_i = \epsilon a, \epsilon \in O_{\mathbb{K}}^*$. Consequently, we have

$$y = xja^{-1} = xj(\alpha_i^{-1}\epsilon)$$

Since $y, j\epsilon \in S$, one finds $xj\alpha_i^{-1} \in S \cap Wj\alpha_i^{-1} \subseteq T$, and thus $y \in Tj\epsilon$. Now $M = l(T)$ is also a bounded set as for any $x = (x_\tau) \in T$, the absolute values $|x_\tau|$ are bounded above and are also away from zero (because $\prod_\tau x_\tau = 1$). Now we have

$$H = \bigcup_{\gamma \in \Gamma} (M + \gamma)$$

Hence the translates $(M + \gamma), \gamma \in \Gamma$, M bounded , covers the whole space H. Thus Γ is a complete lattice in H(using lemma 6.2). $\square$

From previous theorems we immediately deduce,

Theorem 6.5 (Dirichlet's Unit Theorem)**.** *The group of units $O_{\mathbb{K}}^*$ of $O_{\mathbb{K}}$ is isomorphic to the finitely generated abelian group given by*

$$\mu(\mathbb{K}) \ \times \ \mathbb{Z}^{r+s-1}$$

where $\mu(\mathbb{K})$ is the finite torsion group consisting of the roots of unity contained in $\mathbb{K}$.

7 Discrete Valuations on a field

Definition. *Let K be a field. Then Discerete valuation on the field K is a map $v : K^* \longrightarrow \mathbb{Z}$ such that*

- $v(xy) = v(x) + v(y)$
- $v(x + y) \geq \min\{\mathrm{v(x), v(y)}\}$

Given a discrete valuation on a field K, let $\mathrm{A} = \{0\} \bigcup \{x \in K^* | v(x) \geq 0\}$. Then A is a ring, called the valuation ring of v.

Examples :

1. Let us consider discrete valuations on $\mathbb{Q}$. Let p be a prime in $\mathbb{Z}$. For any $a \in \mathbb{Q}$ write $a = p^r.b$ such that neither the numerator nor the denominator of b has p power. Define $v_p : \mathbb{Q}^* \longrightarrow \mathbb{Z}$ by $v_p(a) = r$. This is the discrete valuation on $\mathbb{Q}$ associated to the prime p, called p-adic valuation. The valuation ring is

$$A = \mathbb{Z}_{(p)} = \mathbb{Z}\left[\frac{1}{q}\right]_{q \neq p}$$

   It can be seen that these are the only discrete valuations on $\mathbb{Q}$.

2. Let K be a number field. Let $\mathfrak{p}$ be a prime ideal in O_K. Then the localization $(O_K)_{\mathfrak{p}}$ is a discrete valuation ring with $\mathfrak{p}$ (actually image) as prime ideal. And for any $x \in K$ we get $xO_K = \mathfrak{p}^n$ where $n \in \mathbb{Z}$. We define $v_{\mathfrak{p}} : K^* \longrightarrow \mathbb{Z}$ by $v_{\mathfrak{p}}(x) = n$. Then this is a valuation on K. It can be seen that these are all the valuations on K.

3. (**Function fields**) Let $f(x)$ be an irreducible polynomial in $K[x]$. Write a general rational function $g(x) = f(x)^r.b(x)$ such that neither the numerator nor the denominator of $b(x)$ is divisible by $f(x)$. We define $v_f : K(x)^* \longrightarrow \mathbb{Z}$ by $v_f(g(x)) = r$. This gives a discrete valuation on $K(x)$. It can be seen that all the discrete valuations on $K[x]$ is v_f for some irreducible polynomial in $K[x]$, or is v_∞ given by

$v_\infty\left(\frac{f}{g}\right) = \deg(\mathrm{f}) - \deg(\mathrm{g})$ for $f, g \in K[x]$. And a function field is finite extension of the field $K(x)$, or equivalently finitely generated extension of K of transcendence degree 1. If K is algebraically closed then any irreducible polynomial is just a liner polynomial, and hence discrete valuations are in one-one correspondance with points of $\mathbb{A}^1$ together with valuation v_∞.

4. (**Global Field**) A global field is either an algebraic number field or a function field over finite field $\mathbb{F}_q$.

Proposition 7.1. *An integral domain A is a discrete valuation ring (dvr) if and only if A is a principal ideal domain having a unique nonzero prime ideal.*

One notes that for any Dedekind domain localization at any prime ideal is a discrete valuation ring.

Given $v : K^* \longrightarrow \mathbb{Z}$, a discrete valuation with valuation ring A, one can define $\mathfrak{m} \subseteq A$ to be $\mathfrak{m} = \{x \in A | v(x) > 0\} \bigcup \{0\}$. This is an ideal in A. Any element in $A - \mathfrak{m}$ is invertible and hence A is a local ring with $\mathfrak{m}$ as its maximal ideal, in fact, A is PID. Without loss of generality one can assume that image of v is $\mathbb{Z}$. It can be seen that $\mathfrak{m}$ is generated by any element $\pi \in A$ such that $v(\pi) = 1$. Elements $\pi \in A$ such that $v(\pi) = 1$ are called uniformizing elements. A is thus a local integral domain of dim 1, which can be checked to be integrally closed in K.

Definition. *An absolute value on K is a map to positive reals $|.| : K \longrightarrow \mathbb{R}$ such that*

1. *$|xy| = |x||y|$ and $|x| = 0$ if and only if $x = 0$.*
2. *$|x + y| \leq |x| + |y|$.*

   If we have the stronger property,
3. *$|x + y| \leq \max\{|\mathrm{x}|, |\mathrm{y}|\}$*

   then the absolute value is called a non-archmedian absolute value.

Examples :

1. The usual absolute value on $\mathbb{Q}$.

2. For p-adic valuations on $\mathbb{Q}$ we can define absolute values as $|x|_p = p^{-v_p(x)}$. This is a non-archmedian absolute value on $\mathbb{Q}$.

The absolute values on fields define metric and hence we can talk of completion of the field with respect to the metric. Two absolute values $|.|$ and $|.|'$ on field K are equivalent if there is a positive constant t such that $|a|' = |a|^t \ \forall a \in K$. Equivalent absolute values give rise to equivalent topology on the field. A place on the field K is an equivalence class of non-trivial absolute values. Completion of $\mathbb{Q}$ with respect to absolute value v_p is defined to be $\mathbb{Q}_p$, called p-adic field. These correspond to places which are called finite places. Note that with respect to usual absolute value on $\mathbb{Q}$ the completion is $\mathbb{R}$, which corresponds to the infinite place.

An element in $\mathbb{Q}_p$ is a sequence $\{a_n\}$ of rational numbers such that for every $i > 0$; $p^i | a_m - a_n$ for all $m, n >> 0$ or equivalentily $v_p(a_m - a_n) \geq 0$.

Another way to look at $\mathbb{Q}_p$ is to define $\mathbb{Z}_p$ by inverse limit:

$$\mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z}/p^n$$

Then $\mathbb{Q}_p = \mathbb{Z}_p \bigotimes_{\mathbb{Z}} \mathbb{Q}$ is a field containing $\mathbb{Z}_p$ such that $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$.

Theorem 7.1 (Ostrowski's Theorem)**.** *Let K be a prime global field i.e. $K = \mathbb{Q}$ or $K = \mathbb{F}_q(t)$. Then*

1. *Suppose that $K = \mathbb{Q}$. Then every non-trivial place of K is represented by either the usual absolute value, denoted as $|.|_\infty$, or a p-adic one $|.|_p$, for some prime p.*

2. *Suppose that $K = \mathbb{F}_q(t)$ and let $R = \mathbb{F}_q[t]$. Then every non-trivial place of K is given by either the infinite place $|.|_\infty$ defined by $|f/g|_\infty = q^{deg(f)-deg(g)}$ or by the finite place $|.|_p$ corresponding to an irreducible polynomial $p(t) \in R$.*

Let K be a number field with O_K as its ring of integers. Let $\mathfrak{p}$ be a prime ideal is O_K. Let $x \in K^*$ be a nonzero element. Look at the fractional ideal xO_K and write it as product of prime ideals $xO_K = \prod \mathfrak{p}^{n_\mathfrak{p}(x)}$. Define a discrete valuation on K as $v_\mathfrak{p} : K^* \longrightarrow \mathbb{Z}$ as $v_\mathfrak{p}(x) = n_\mathfrak{p}(x)$. Using this discrete valuation we can define absolute value on K as $|.|_\mathfrak{p} : K \longrightarrow \mathbb{R}^{\geq 0}$ by $|x|_\mathfrak{p} = (\#O_K/\mathfrak{p})^{-n_\mathfrak{p}(x)}$. The completion of K with respect to this absolute value is written as $K_\mathfrak{p}$.

Any element of a discrete valuation ring A looks like

$$a_0\pi^r + a_1\pi^{r+1} + ...$$

where a_i's are representations of $A/\mathfrak{m}$, $a_0 \neq 0$ in $A/\mathfrak{m}$ and $r \in \mathbb{Z}$.

Example : Let us take $K = \mathbb{C}[|t|][t^{-1}]$, which is a field. Any element of this field looks like

$$f(t) = \sum_{n \geq m \in \mathbb{Z}} a_n t^n$$

where $a_n \in \mathbb{C}$.

We have thus defined completion of a number field at various prime ideals. These prime ideals are also called finite places of the number field. There are infinite places (or archmedian absolute values) which correspond to embeddings of the number field K in $\mathbb{C}$. Two embeddings of K into $\mathbb{C}$ are said to define the same infinite place if and only if they are complex conjugate of each other. The set of finite places together with infinite places constitute the set of places of the number field K.

There is another way of looking at completion of a number field. If K is a finite field extension of $\mathbb{Q}$ then $K \bigotimes_\mathbb{Q} \mathbb{Q}_p$ is a separable algebra which is a product of fields.

$$K \bigotimes_\mathbb{Q} \mathbb{Q}_p = \bigoplus_{v|p} K_v$$

Similarly,

$$K \bigotimes_\mathbb{Q} \mathbb{R} = \mathbb{R}^{r_1} \bigoplus \mathbb{C}^{r_2}$$

8 A sample calculation of the ring of integers of a number field

We will calculate the ring of integers of the field $K = \mathbb{Q}(\zeta_p),\ \zeta_p = e^{\frac{2\pi i}{p}}$. The Galois group in this case is $Gal(K/\mathbb{Q}) = (\mathbb{Z}/p)^*$. In general $\mathbb{Q}(\zeta_n)$ are called cyclotomic fields. These have Galois group which are abelian and isomorphic to $(\mathbb{Z}/n)^*$.

The following theorem will be proved later as a consequence of the class field theory.

Theorem 8.1 (Kronecker)**.** *Let K be a number field which is an abelian extension of $\mathbb{Q}$, i.e. K is Galois over $\mathbb{Q}$ with abelian Galois group. Then K is contained in $\mathbb{Q}(\zeta_n)$, for some n.*

Proposition 8.1. *Let $K = \mathbb{Q}(\zeta_p),\ \zeta_p = e^{\frac{2\pi i}{p}}$. Then the ring of integers of K is $O_K = \mathbb{Z}[\zeta_p]$.*

Remark: The theorem is true for p any positive integer. But we will prove here for p a prime. Also ring of integers need not be generated by a single element but it is always generated by at most two elements.

Proof : Clearly $\mathbb{Z}[\zeta_p] = \mathbb{Z}[1-\zeta_p] \subset O_K$. Let $x \in O_K$ we write $x = a_0 + a_1(1-\zeta_p) + ... + a_{p-2}(1-\zeta_p)^{p-2}$ with $a_i \in \mathbb{Q}$. We need to show $a_i \in \mathbb{Z}$. By using valuation theory we claim that there exists a valuation with property that $v(1-\zeta_p) = 1\ ,\ v(p) = p-1$. To see this we note,

$$\begin{aligned} f(x) &= 1 + x + x^2 + ... + x^{p-1} \\ &= \prod_{i=1}^{p-1}(x - \zeta_p^i). \end{aligned}$$

Putting $x = 1$ in this equation,

$$\begin{aligned} p &= \prod_{i=1}^{p-1}(1-\zeta_p^i) \\ &= (1-\zeta_p)^{p-1}.\prod \frac{1-\zeta_p^i}{1-\zeta_p} \end{aligned}$$

Note that $\frac{1-\zeta_p}{1-\zeta_p^i} \in \mathbb{Z}[\zeta_p]$ is unit. For this observe that $(i,p)=1$, there exists$j$ such that $ij = 1 \mod p$.Therefore

$$\frac{1-\zeta_p}{1-\zeta_p^i} = \frac{1-(\zeta_p^i)^j}{1-\zeta_p^i} = 1+\zeta_p^i+..... \in \mathbb{Z}[\zeta_p]$$

proving that $\frac{1-\zeta_p}{1-\zeta_p^i} \in \mathbb{Z}[\zeta_p]$. Clearly $\frac{1-\zeta_p^i}{1-\zeta_p} \in \mathbb{Z}[\zeta_p]$. Thus $\frac{1-\zeta_p}{1-\zeta_p^i} \in \mathbb{Z}[\zeta_p]$ is a unit in $\mathbb{Z}[\zeta_p]$. Thus the equation $p = (1-\zeta_p)^i\pi$ implies that $v(p) = p-1$. As the degree of field is $p-1$ which is equal to ramification index of $1-\zeta_p$ which shows that $< 1-\zeta_p >$ is a prime ideal. There exists a valuation on $\mathbb{Q}(\zeta_p)$ s.t. $v(x) \geq 0 \ \ \forall x \in O_K$ with $v(1-\zeta_p) = 1$, $v(p) = p-1$. Also

$$\begin{aligned} v(x) &= \min\left(\mathrm{v(a_0)}, ...\mathrm{v(a_{p-2}(1-\zeta_p)^{p-2})}\right) \\ &= \min\left(\mathrm{v(a_0)}, ...\mathrm{v(a_{p-2})}\right) \geq 0 \end{aligned}$$

This proves that a_i's do not have p in the denominator. The rest of the argument is simpler.

Let $x = b_0 + b_1\zeta_p + ... + b_{p-2}(\zeta_p)^{p-2}$ with $b_i \in \mathbb{Q}$ and b_i have no p in denominator. Note that if $x \in O_K$ then $tr(x\zeta_p^{-i}) \in \mathbb{Z} \ \ \forall i$. Using $tr\zeta_p^j = -1 \ \ \forall j \neq 0$ and $tr1 = p-1$ we get

$$\begin{aligned} (p-1)b_i - (b_0 + ...b_{i-1} + b_{i+1} + ... + b_{p-2}) &\in \mathbb{Z} \\ pb_i - \sum_{i=0}^{p-2} b_i &\in \mathbb{Z}. \end{aligned}$$

This implies that $p(b_0 - b_i) \in \mathbb{Z}$. Since b_i's do not have p in denominator we get $b_0 - b_i \in \mathbb{Z}$. If we can prove that $b_0 \in \mathbb{Z}$ then we will be done.

$$\begin{aligned} x &= b_0 + b_1\zeta_p + ... + b_{p-2}\zeta_p^{p-2} \\ &= b_0 + (b_1 - b_0)\zeta_p + ... + (b_{p-2} - b_0)\zeta_p^{p-2} + b_0(\zeta_p + ... + \zeta_p^{p-2}) \\ &= (b_1 - b_0)\zeta_p + ... + (b_{p-2} - b_0)\zeta_p^{p-2} + b_0(1 + \zeta_p + ... + \zeta_p^{p-2}) \\ &= -b_0\zeta_p^{p-1} + \sum (b_i - b_0)\zeta_p^i \end{aligned}$$

On taking trace we get $b_0 \in \mathbb{Z}$. This completes the proof. $\square$

Remark : Not always the ring of integers O_K of a number field is generated by one element but it is always generated by atmost two elements.

9 The different and the discriminant of a number field

Let $\mathfrak{a}$ be a fractionl ideal in a number field K. We look at the map $tr : K \times K \longrightarrow \mathbb{Q}$ defined by $tr(x, y) = tr_{\mathbb{Q}}^K(xy)$.

Definition. *The set* $\mathfrak{a}' = \{x \in K | tr(xy) \in \mathbb{Z},\ \forall y \in \mathfrak{a}\}$ *is called complementry set.*

It is not difficult to see that $\mathfrak{a}'$ is also a fractional ideal.

Definition. $O'_K = \{x \in K | tr(xy) \in \mathbb{Z},\ \forall y \in O_K\}$. *Then* $K \supseteq O'_K \supset O_K$ *and* O'_K *is a fractional ideal. The inverse of* O'_K*, denoted as* δ*, is called the "different", which is an ideal in* O_K*.*

Definition (Norm of an ideal)**.** *Let* $I \subset O_K$ *is an ideal then we define* $Nm(I)$ *to be the cardinality of* O_K/I*.*

Theorem 9.1. *Let* K *be a number field. Then* $Nm(\delta) = disc(K)$*.*

Exercise: $disc(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = p^{p-2}$

Theorem 9.2. *Let $\mathfrak{p}$ be a prime ideal in O_K lying over p. Let e be the ramification index of $\mathfrak{p}$ over p. Then $\mathfrak{p}^{e-1}$ divides δ. Hence, in a number field the primes which are ramified (ramification index ≥ 2) are exactly primes dividing the discriminant of the number field.*

Exercises : $Nm(IJ) = Nm(I)Nm(J)$

$Nm(\alpha) = |Nm_{K/\mathbb{Q}}(\alpha)|$.

An example calculation of different :

Let $p \in \mathbb{Z}$ be a prime. Take $K = \mathbb{Q}_p(\sqrt{p})$ then $O_K = \mathbb{Z}_p[\sqrt{p}]$, for any prime p. Let us take case $p \neq 2$. We claim $\delta_K =< \sqrt{p} >$. Recall that $\delta_K^{-1} = \{x \in K | tr(xy) \in \mathbb{Z}_p, \forall y \in O_K\}$. Let $a + b\sqrt{p}, a, b \in \mathbb{Z}_p$ is an element of $\mathbb{Z}_p[\sqrt{p}]$. Then $\frac{1}{\sqrt{p}}(a+b\sqrt{p}) = \frac{a}{\sqrt{p}} + b \implies tr(\frac{a}{\sqrt{p}} + b) = 2b \in \mathbb{Z}_p \forall a, b$. That means $\frac{1}{\sqrt{p}} \in \delta_K^{-1}$.

Let us take case when $p = 2$ the we claim that $2 \in \delta_K$. $\frac{1}{2}(a + b\sqrt{2}) = \frac{1}{2}a + \frac{b}{\sqrt{2}} \implies tr(\frac{1}{2}a + \frac{b}{\sqrt{2}}) = a \in \mathbb{Z}_2 \implies 2 \in \delta_K$.

Lemma 9.1. *If L is a finite extension of a local field K, with π_K and π_L uniformizing parameter such that $\pi_L^e = \pi_K.u$, u a unit in O_L. Then $\pi_L^{e-1}/\delta_{L/K}$. In fact $\delta_{L/K} = \pi_L^{e-1} \iff p/e$.*

Proof: Let us prove that $\pi_L^{e-1}/\delta_{L/K}$. For this we show $tr(\pi_L^{e-1}O_L) \subset O_K$. But then $tr(\pi_L^{e-1}O_L) = tr\left(\frac{\pi_L}{\pi_K}O_L\right) = \frac{1}{\pi_K}tr(\pi_L O_L) \subset \frac{1}{\pi_K}\pi_K O_K \subset O_K$. □

10 The Riemann Zeta Function

The Riemann zeta function is defined as follows:

$$\zeta_{\mathbb{Q}}(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \geq 2} \frac{1}{1 - \frac{1}{p^s}}$$

where the product is taken over all primes. The expression of $\zeta_{\mathbb{Q}}(s)$ in the product form is called Euler product of $\zeta_{\mathbb{Q}}$. The Euler product for $\zeta_{\mathbb{Q}}(s)$ is equivalent to the fundamental theorem of arithmetic: every positive integer

is uniquely a product of primes. Both the expressions are valid for $Re(s) > 1$. The function $\zeta_{\mathbb{Q}}(s)$ has an analytic continuation to a meromorphic function in s-plane with a simple pole at $s = 1$ with residue 1. That is

$$\zeta_{\mathbb{Q}}(s) = \frac{1}{s-1} + \text{holomorphic function around s} = 1$$

The Riemann zeta function satisfies a functional equation relating its value at s to $1 - s$. It is best expressed by introducing another function $\xi(s)$.

$$\xi(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta_{\mathbb{Q}}(s)$$

The function $\xi(s)$ satisfies $\xi(s) = \xi(1 - s)$.

Riemann conjectured in 1850's that all the zeros of $\zeta_{\mathbb{Q}}(s)$ are on the line $Re(s) = \frac{1}{2}$. This is one of the most famous unsolved problems in mathematics, called the *Riemann Hypothesis*.

11 Zeta Function of a Number Field (Dedekind Zeta Function)

Let K be a number field. We define Dedekind zeta function as follows.

$$\zeta_K(s) = \sum_{I \neq 0, I \subset O_K} \frac{1}{(NI)^s} = \prod_{\mathcal{P}} \frac{1}{1 - \frac{1}{(N\mathcal{P})^s}}$$

where I ranges over all nonzero ideals of O_K, NI is the norm of the ideal I and $\mathcal{P}$ is a prime ideal in O_K. Both the expressions are valid for $re(s) > 1$. The function $\zeta_K(s)$ is called the Dedekind zeta function of the number field K. It has an analytic continuation to a meromorphic function in s-plane with a simple pole at $s = 1$.

Theorem 11.1 (Class Number Formula)**.** *Let K be a number field. Then,*

$$\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{d_K}} \cdot \frac{1}{s-1} + \text{holomorphic function around s} = 1$$

where r_1 is the number of real embeddings of K in $\mathbb{C}$, r_2 is the number of complex embeddings of K in $\mathbb{C}$ upto complex conjugate, h is class number of K, R is the regulator of the number field K, w is number of roots of unity in K and d_K is the modulus of discriminant.

This theorem will be proved later. Let us check convergence of

$$\begin{aligned}\zeta_K(s) &= \sum_{I\neq 0, I\subset O_K} \frac{1}{(NI)^s} \\ &= \prod_{\mathcal{P}} \frac{1}{1-\frac{1}{(N\mathcal{P})^s}} \\ &\quad \text{for Re(s)} > 1. \text{ Since the equality} \\ \sum_{I\neq 0, I\subset O_K} \frac{1}{(NI)^s} &= \prod_{\mathcal{P}} \frac{1}{1-\frac{1}{(N\mathcal{P})^s}}\end{aligned}$$

is formal, so it suffices to check the convergence of the product.

$$\begin{aligned}\log(\zeta_K(s)) &= -\sum_{\mathcal{P}} \log(1-\frac{1}{(N\mathcal{P})^s}) \\ &= \sum_{\mathcal{P}, m\geq 1} \frac{1}{m(N\mathcal{P})^{ms}}\end{aligned}$$

We have $N\mathcal{P} = p^f$ where $\mathcal{P}$ is prime lying over p and number of primes lying over p of resudial degree f is $\leq N = [K:\mathbb{Q}]$. Then,

$$\log(\zeta_K(s)) \leq \sum_{p,\ m\geq 1,\ N\geq f\geq 1} \frac{N}{mp^{fms}}$$

where p is prime.

Therefore upto a function which is bounded in a neighborhood of 1,

$$\log(\zeta_K(s)) = \sum \frac{a_p}{p^s}$$

a_p denotes number of primes above p of degree 1.

Thus $\log(\zeta_K(s))$ for $s > 1$ is bounded by $\sum \frac{N}{p^s}$, thus it is convergent for $re(s) > 1$. Actually we will be proving later that

$$\log(\zeta_K(s)) = \log \frac{1}{s-1} = \sum \frac{1}{p^s} \quad \text{(up to a bounded function)}.$$

12 Exercises

1. (Problem of Erdos) If m and n are integers, such that the order of m is same as order of n in $(\mathbb{Z}/p)^*$ for almost all primes, then $m = n$.

2. Define the zeta function $\zeta_{\mathbb{A}^1}(s)$ of the affine line $\mathbb{A}^1$ over the finite field $\mathbb{F}_p$ as follows.
$$\zeta_{\mathbb{A}^1}(s) = \prod_{p(x)} \frac{1}{(1 - \frac{1}{Np(x)})^s}$$
where $p(x)$ runs over irreducible polynomials in $\mathbb{F}_p[x]$ with leading term 1 and f(x) is monic polynomial over $\mathbb{F}_p$. And $Nf(x) = p^n$ where $n = deg\ f(x)$. But then
$$\begin{aligned} \zeta_{\mathbb{A}^1}(s) &= \prod_{p(x)} \frac{1}{(1 - \frac{1}{Np(x)})^s} \\ &= \sum_{f(x)} \frac{1}{(Nf(x))^s} \\ &= \sum_{d} \frac{p^d}{p^{ds}} \\ &= \frac{1}{1 - \frac{p}{p^s}} \end{aligned}$$

3. Let $K = \mathbb{Q}(i)$, then $\zeta_K(s) = \sum \frac{1}{(m^2+n^2)^s}$

13 Class Number Formula [2]

13.1 Introduction

Let G be a finite cyclic group of even order. Then the number of squares in G is equal to the number of non-squares in G. In particular, for a prime p, taking $G = (\mathbb{Z}/p\mathbb{Z})^*$, number of quadratic residue modulo p is equal to the number of quadratic non-residue mod p. One can ask how the quadratic residues are distributed in $I_p = \{1, 2, \cdots, (p-1)/2\}$. Let R_p = Number of quadratic residues in I_p and N_p = Number of quadratic non-residues in I_p. Then the question is

$$\text{Is } R_p = N_p \text{ ?}$$

If $p \equiv 1 \mod 4$, then $\left(\frac{-1}{p}\right) = 1$. Hence the map

$$\phi : \left\{1, \cdots, \frac{p-1}{2}\right\} \longrightarrow \left\{\frac{p+1}{2}, \cdots, p-1\right\}$$

defined by $k \longrightarrow -k$ is an one-one correspondence, preserving squares. So, we conclude that exactly half of the quadratic residues are in I_p implying $R_p = N_p$. If $p \equiv 3 \mod 4$ then the following result answers our question.

Theorem 13.1. *Let $p > 3$ be a prime such that $p \equiv 3 \mod 4$. Also let h_p denote the class number of the quadratic field $\mathbb{Q}(\sqrt{-p})$. Then*

$$h_p = \begin{cases} R_p - N_p & \text{if } p \equiv 7 \mod 8, \\ \frac{1}{3}(R_p - N_p) & \text{if } p \equiv 3 \mod 8. \end{cases}$$

Remark 13.1. *As $h_p \geq 1$, we have $R_p > N_p$ for prime $p > 3$ and $p \equiv 3 \mod 4$. Moreover 3 divides $R_p - N_p$ if $p \equiv 3 \mod 8$.*

Proof of Theorem 13.1 depends on the Class number formula for quadratic extensions of $\mathbb{Q}$. Let $K = \mathbb{Q}(\sqrt{d})$ where d is the discreminant of K. Let w be the number of roots of unity in K. For an ideal class $\mathcal{C}$ of K and a real

[2] This section is written by Anirban Mukhopadhyay.

number $X > 0$, we define $N(X, \mathcal{C})$ = number of integral ideals I in $\mathcal{C}$ such that $N(I) < X$ where $N(I)$ denotes the norm of I. We have

Theorem 13.2.

$$\lim_{X \to \infty} \frac{N(X, \mathcal{C})}{X} = \kappa$$

where

$$\kappa = \begin{cases} \frac{2 \log \eta}{\sqrt{d}} & \text{if } d > 0, \ \eta \text{ is the unique fundamental unit } > 1, \\ \frac{2\pi}{w\sqrt{|d|}} & \text{if } d < 0. \end{cases}$$

Now we state the class number formula for the quadratic field $K = \mathbb{Q}(\sqrt{d})$.

Theorem 13.3. *For a quadratic number field K,*

$$\lim_{s \to 1+} (s-1)\zeta_K(s) = h\kappa$$

where h =Class number of K and ζ_K is the Dedekind zeta function.

In the rest of the article we give proofs of these results.

13.2 Proof of Theorem 13.1

Here we write a sequence of lemmas leading to the proof of Theorem 1. Throughout this section we assume $K = \mathbb{Q}(\sqrt{d})$. Following lemma gives a simple expression for ζ_K.

Lemma 13.1. *For $s > 1$, we have*

$$\zeta_K(s) = \zeta(s) L_d(s)$$

where $\zeta(s)$ is the Riemann zeta function and

$$L_d(s) = \sum_{m=1}^{\infty} \left(\frac{d}{m}\right) m^{-s}$$

with $\left(\frac{d}{m}\right)$ denoting the quadratic residue symbol.

The series $L_d(s)$ converges for $s > 0$. Hence using the fact that $\lim_{s\to 1+}(s-1)\zeta(s) = 1$ we derive from the above Lemma

$$\lim_{s\to 1+}(s-1)\zeta_K(s) = \lim_{s\to 1+}(s-1)\zeta(s) = L_d(1).$$

Thus we have the following simplier expression for class number formula.

$$h = \begin{cases} \frac{2\log\eta}{\sqrt{d}} L_d(1) & \text{if } d > 0,\ \eta \text{ is the unique fundamental unit } > 1, \\ \frac{2\pi}{w\sqrt{|d|}} L_d(1) & \text{if } d < 0. \end{cases}$$

Now to prove Theorem 13.1 we consider the particular case $d = -p$ where $p > 3$ is a prime such that $p \equiv 3 \mod 4$. It is easy to see that the number of roots of unity in K, $w = 2$. For a Dirichlet character χ, the Dirichlet series is defined to be $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$. In this case we define χ to be the quadratic character $(\frac{\cdot}{p})$. Using above expression for class number one can easily derive that $h_p = \frac{\sqrt{p}}{\pi} L(1,\chi)$. Next Lemma expresses $L(1,\chi)$ as a finite sum.

Lemma 13.2. *We have*

$$L(1,\chi) = \frac{i\pi\tau_1(\chi)}{p^2} \sum_{k=1}^{p-1} \chi(k)k.$$

where

$$\tau_k(\chi) = \sum_{1\le a<p} \chi(a)\rho^{ak}.$$

with ρ denoting the p-th primitive root of unity.

proof : For $s > 1$ we have

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{1\le a<p} \chi(a) \sum_{n\equiv a \mod p} \frac{1}{n^s}.$$

We write

$$\sum_{n\equiv a \mod p} \frac{1}{n^s} = \sum_{n=1}^{\infty} \frac{c_n}{n^s}$$

where $c_n = 1$ if $n \equiv a \mod p$ and $c_n = 0$ otherwise. If ρ denote the p-th primitive root of unity, we can write

$$c_n = \frac{1}{p} \sum_{k=0}^{p-1} \rho^{(a-n)k}.$$

Thus

$$L(s,\chi) = \frac{1}{p} \sum_{1 \le a < p} \chi(a) \sum_{n=1}^{\infty} \sum_{k=0}^{p-1} \rho^{(a-n)k} = \frac{1}{p} \sum_{k=0}^{p-1} \left\{ \sum_{1 \le a < p} \chi(a) \rho^{ak} \right\} \sum_{n=1}^{\infty} \frac{\rho^{-nk}}{n^s}.$$

We observe that $\tau_0(\chi) = 0$ and $\chi(k)\tau_k(\chi) = \tau_1(\chi)$. Using these observations along with the fact that $L(s,\chi)$ is continuous in $(0,\infty)$, we get

$$L(1,\chi) = \frac{\tau_1(\chi)}{p} \sum_{k=1}^{p-1} \frac{1}{\chi(k)} \log \frac{1}{1-\rho^{-k}}.$$

Let S be the sum in the last formula. Since χ is an even character we have

$$2S = \sum_{k=1}^{p-1} \frac{1}{\chi(k)} \left[\log \frac{1}{1-\rho^{-k}} - \log \frac{1}{1-\rho^{k}} \right].$$

Using the expressions $\log(1-\rho^{-k}) = i\left(\frac{\pi}{2} - \frac{k\pi}{p}\right) + \log|1-\rho^{-k}|$ we get

$$S = \frac{i\pi}{p} \sum_{k=1}^{p-1} \chi(k) k.$$

This completes the lemma. $\square$

We recall that $\tau_1(\chi) = i\sqrt{p}$. Thus

$$h_p p = -\sum_{k=1}^{p-1} \chi(k) k.$$

We split this sum as

$$\begin{aligned} -h_p p &= \sum_{k=1}^{(p-1)/2} \left(\frac{k}{p}\right) k + \sum_{k=(p+1)/2}^{p-1} \left(\frac{k}{p}\right) k \\ &= \sum_{k=1}^{(p-1)/2} \left(\frac{k}{p}\right) (k-(p-k)) \\ &= 2\sum_{k=1}^{(p-1)/2} \left(\frac{k}{p}\right) k - p(R_p - N_p). \end{aligned}$$

On the other hand we can write,

$$\begin{aligned} -h_p p &= \sum_{k=1}^{(p-1)/2} \left(\frac{2k}{p}\right) 2k + \sum_{k=1}^{(p-1)/2} \left(\frac{p-2k}{p}\right) (p-2k) \\ &= 4\left(\frac{2}{p}\right) \sum_{k=1}^{(p-1)/2} \left(\frac{k}{p}\right) k - p\left(\frac{2}{p}\right)(R_p - N_p). \end{aligned}$$

from above two we get

$$\left(2\left(\frac{2}{p}\right) - 1\right) h_p p = -p\left(\frac{2}{p}\right)(R_p - N_p).$$

Now Theorem 13.1 follows from the fact that $(\frac{2}{p}) = 1$ or -1 according as $p \equiv 7 \mod 8$ or $p \equiv 3 \mod 8$.
The next section is dedicated to proofs of Theorems 13.2 and 13.3.

13.3 Proofs of Theorems 13.2 and 13.3

We start with a lemma

Lemma 13.3. *Let Δ be a bounded open set in $\mathbb{R}^2$. For any real number $r > 0$, let*

$$\Delta_r = \left\{(\xi_1, \xi_2) \in \mathbb{R}^2 | \left(\frac{\xi_1}{r}, \frac{\xi_2}{r}\right) \in \Delta\right\}$$

and $N_\Delta(r) =$ *Number of lattice points in* Δ_r. *Then*

$$\lim_{x\to\infty} \frac{1}{r^2} N_\Delta(r) = \textit{Area of } \Delta.$$

First we present a proof of Theorem 13.2. Let $\mathcal{C}$ be any ideal class of K and J be an integral ideal in $\mathcal{C}^{-1}$. Then for any integral ideal $I \in \mathcal{C}$, $IJ = \alpha\mathcal{O}_K$ with $\alpha \in J$. Conversely if $\alpha \in J$ then $J|\alpha\mathcal{O}_K$, hence $I = J^{-1}\alpha\mathcal{O}_K$ is an integral ideal in $\mathcal{C}$. Further $|N_{K/\mathbb{Q}}(\alpha)| = N(I)N(J)$. Thus $N(I) < X$ if and only if $|N_{K/\mathbb{Q}}(\alpha)| < XN(J) = Y$(say). We can conclude that $N(X, \mathcal{C}) =$ Number of pairwise non-associative elements $\alpha \in J$ such that $|N_{K/\mathbb{Q}}(\alpha)| < Y$. We divide the proof in two cases.

Case 1: d > 0 Here η is the fundamental unit > 1. We observe that for any $\alpha \in J, \alpha \neq 0$, there exist an integer m such that

$$0 \leq \log \left| \frac{\omega}{|N(\omega)|^{1/2}} \right| < \log \eta \tag{13.3.1}$$

where $\omega = \eta^m \alpha$ and we use N to denote norm without mentioning the fields involved. It is easy to see that if two associates ω_1 and ω_2 satisfies (13.3.1) then $\omega_1 = \epsilon\omega_2$ with $\epsilon = \pm 1$. Hence

$$2N(X, C) = \left| \left\{ \omega \in J \mid 0 < |N(\omega)| < y, 0 \leq \log \left| \frac{\omega}{|N(\omega)|^{1/2}} \right| < \log \eta \right\} \right|.$$

Let β_1, β_2 be an integral basis for J and let

$$\Omega = \left\{ (\xi_1, \xi_2) \in \mathbb{R}^2 | 0 < |\xi_1||\xi_1'| < 1, 0 < \log \left| \frac{|\xi_1|^{1/2}}{|\xi_1'|^{1/2}} \right| < \log \eta \right\}$$

where $\xi = \xi_1\beta_1 + \xi_2\beta_2$ and $\xi' = \xi_1\beta_1' + \xi_2\beta_2'$, β_1', β_2' denote the conjugates of β_1, β_2. We observe that Ω is bounded.

$$\begin{aligned} 2N(X, \mathcal{C}) &= \text{Number of lattice points in } \Omega_{\sqrt{y}} \\ &\quad + \text{Number of lattice points in} A_y \end{aligned}$$

where

$$A_y = \left\{ (\xi_1, \xi_2) \in \mathbb{Z} \mid |\xi|^2 \leq y, |\xi| = |\xi'| \neq 0 \right\}$$

and ξ is as above. One can easily see that $|A_y| = O(\sqrt{y}) = O(X)$. Now using Lemma 13.3 we derive

$$\lim_{X\to\infty} \frac{2N(X,C)}{X} = \lim_{y\to\infty} \frac{N_\Omega(\sqrt{y})}{y} N(J) = N(J)\text{Area of } \Omega.$$

Area of Ω can be computed to be $\frac{4\log\eta}{N(J)\sqrt{d}}$. This completes the proof in this case.

Case 2: d < 0

In this case we have

$$wN(X,\mathcal{C}) = |\{\omega \in J \mid 0 < N(\omega) < y\}|.$$

Let

$$\Omega = \left\{(\xi_1,\xi_2) \in \mathbb{R}^2 | 0 < |\xi_1\beta_1 + \xi_2\beta_2|^2 < 1\right\}.$$

Then $wN(X,\mathcal{C}) = N_\Omega(\sqrt{y})$, hence

$$\lim_{X\to\infty} \frac{wN(X,C)}{X} = \lim_{y\to\infty} \frac{N_\Omega(\sqrt{y})}{y} N(J) = N(J)\text{Area of } \Omega.$$

Here area of Ω is calculated to be $\frac{2\pi}{N(J)\sqrt{d}}$, completing the proof of Theorem 13.2.

To derive class number formula we need the following lemma

Lemma 13.4. *Let $\{a_m\}$ be a sequence of real numbers. For a positive real number X, we set*

$$A(X) = \sum_{m<X} a_m.$$

Suppose that

$$\lim_{X\to\infty} \frac{A(X)}{X} = c.$$

Then the series

$$f(s) = \sum_{m=1}^{\infty} \frac{a_m}{m^s}$$

converges for $s > 1$ and we have

$$\lim_{s\to 1+} (s-1)f(s) = c.$$

Let a_m = Number of integral ideals I such that $N(I) = m$. Then for a real number $X > 0$, $A(X)$ = number of integral ideals I such that $N(I) < X$. From Theorem 13.2 we get

$$\lim_{X\to\infty} \frac{A(X)}{X} = h\kappa.$$

So, by the above Lemma, $\zeta_K(s)$ is convergent for $s > 1$ and

$$\lim_{s\to 1+} (s-1)\zeta_k(s) = h\kappa.$$

Which gives the required result.

14 Density of Primes (Dirichlet density)

Let K be a number field and M is set of primes, then the density of primes in M is defined to be,

$$\lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in M} \frac{1}{(N\mathfrak{p})^s}}{\log \frac{1}{s-1}}$$

In one of the earlier lecture we had observed that

$$\begin{aligned} \log \frac{1}{s-1} &\sim \log \zeta_K(s) \\ &\sim \sum_{\mathfrak{p}} \frac{1}{(N\mathfrak{p})^s} \\ &\sim \sum_{deg\mathfrak{p}=1} \frac{1}{(N\mathfrak{p})^s} \end{aligned}$$

where $f_1 \sim f_2$ if $(f_1 - f_2)(s-1) \to 0$ *as* $s \to 1$ and $N\mathfrak{p} = p^{deg\mathfrak{p}}$ (in fact *degp* = residual degree).

Theorem 14.1. *Let K be a number field which is a galois extension of $\mathbb{Q}$. If K has degree d over $\mathbb{Q}$ then the set of primes in $\mathbb{Q}$ which split completely in K has density $= \frac{1}{d}$.*

Proof: We have $M = \{p \in \mathbb{Z} \mid pO_K = \mathfrak{p}_1...\mathfrak{p}_d, \mathfrak{p}'s \text{ are completely split}\}$. So using remark preceding theorem we get

$$d\sum_{\mathfrak{p}\in M}\frac{1}{(N\mathfrak{p})^s} = \sum_{deg\mathfrak{p}=1}\frac{1}{(N\mathfrak{p})^s} = \log\frac{1}{s-1}$$

Hence substituting in density formula we get density of completely split primes (primes in M) is $\frac{1}{d}$. $\square$

Theorem 14.2. *Two number fields K_1 and K_2 which are Galois over $\mathbb{Q}$ are the same if and only if they have the same set of split primes, up to density zero primes.*

Proof: We claim that primes which split in K_1K_2 are precisely those which split in both K_1 and K_2. This follows by noting that a prime p is split in a number field K if and only if all embeddings of K in $\bar{\mathbb{Q}}_p$ land inside $\mathbb{Q}_p$. Thus if p splits completely in K_1 and K_2, it does so in K_1K_2 also.

Let K_1 be degree d_1 extension of $\mathbb{Q}$, K_2 be degree d_2 extension of $\mathbb{Q}$ and K_1K_2 degree d extension of $\mathbb{Q}$. Then, split primes in K_1 are of density $\frac{1}{d_1}$, split primes in K_2 are of density $\frac{1}{d_2}$ and split primes in K_1K_2 are of density $\frac{1}{d}$. Since the split primes in K_1, K_2 and K_1K_2 are the same, $\frac{1}{d_1} = \frac{1}{d_2} = \frac{1}{d}$. This implies $d_1 = d_2 = d$, hence $K_1 = K_2 = K_1K_2$. $\square$

Lemma 14.1. *Let K be a number field. Let L denotes the Galois closure of K. Then the primes in $\mathbb{Q}$ which split completely in K are exactly the primes which split completely in L.*

Proof: We have proved earlier that for field extensions K_1, K_2 the primes in $\mathbb{Q}$ which split completely in K_1K_2 are exactly those which split completely in K_1 and K_2. Now noting that L is compositium of conjugates of K, the lemma follows. $\square$

Example: Calculation of density of primes.

Let $K = \mathbb{Q}(2^{\frac{1}{3}})$, and $L = \mathbb{Q}(2^{\frac{1}{3}}, \omega)$ be Galois clousre of K, where ω is cube root of unity. We have $\mathbb{Q} \hookrightarrow K \hookrightarrow L$. Let us denote primes in $\mathbb{Q}$ by p, prime ideals in K by $\mathfrak{p}$ and prime ideals in L by $\mathfrak{q}$.

1. Let us calculate the density of split primes in K, $M = \{p \in \mathbb{Z} \mid pO_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ in\ K\}$. But from previous lemma density of completely split primes in K is same as density of completely split primes in its closure L. Then by the theorem, density of M = $\frac{1}{6}$.

2. Let us calculate the density of primes which can be written as product of two primes. Then $M = \{p \in \mathbb{Z} | pO_K = \mathfrak{p}_1\mathfrak{p}_2\ in\ K\} = \{p \in \mathbb{Z} | pO_L = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\ in\ L\} \equiv \{\mathfrak{p} \subset O_K |\ \mathfrak{p}O_L = \mathfrak{q}_1\mathfrak{q}_2\}$. Hence density of M is $\frac{1}{2}$.

3. Let us calculate the density of primes which remains prime in K. In this case $M = \{p \in \mathbb{Z} |\ pO_K = \mathfrak{p}\ in\ K\}$. But we can see that deg 1 primes in $\mathbb{Z}$ falls in one of the above three categories. Hence the density in this case will be $1 - \frac{1}{6} - \frac{1}{2} = \frac{1}{3}$.

15 Decomposition of primes in the cyclotomic fields

Let $K = \mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{\frac{2\pi i}{n}}$ and $O_K = \mathbb{Z}[\zeta_n]$.

Proposition 15.1. *Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic number field. Then the primes in $\mathbb{Z}$ which ramify in K are exactly the divisors of n.*

Proof: It suffices to prove the proposition for n which is prime power. So let us assume $n = p^m$ i.e. $K = \mathbb{Q}(\zeta_{p^m})$. We need to show that p is the only prime which ramifies in K. In fact, in this case, p is a totally ramified prime i.e. $pO_K = \mathfrak{p}^d$ where $d = \phi(p^m)$.

Observe that the minimal polynomial satisfied by ζ_{p^m} is

$$1 + x^{p^{m-1}} + (x^2)^{p^{m-1}} + ... + (x^{p-1})^{p^{m-1}} = \prod_{\zeta}(x - \zeta)$$

where product is over ζ , all p^mth roots of unity. Putting $x = 1$ we get

$$p = \prod_{(i,p)=1} (1 - \zeta_{p^m}^i). \quad i \in \mathbb{Z}/p^m$$

Let us take $\pi = (1 - \zeta_{p^m})$ then $\sigma(\pi) = 1 - \sigma(\zeta_{p^m})$ for any σ embedding of K in $\mathbb{C}$. Since embeddings of K in $\mathbb{C}$ correspond to $(i,p) = 1 \;\; i \in \mathbb{Z}/p^m$ which sends ζ_{p^m} to $\zeta_{p^m}^i$ we get

$$p = \prod_{\sigma \in Gal(K/\mathbb{Q})} \sigma(\pi).$$

Observe that $\frac{1-\zeta_{p^m}^i}{1-\zeta_{p^m}} \in \mathbb{Z}[\zeta_{p^m}]$ is a unit for $(i,p) = 1$. Hence we get $p = (1-\zeta_{p^m})^{\phi(p^m)}.u$ where u is a unit in $\mathbb{Z}[\zeta_{p^m}]$. By taking $\mathfrak{p} =< 1-\zeta_{p^m} >$ we get $pO_K = \mathfrak{p}^{\phi(p^m)}$. The discriminant of field is power of p hence no other prime ramifies. $\square$

Lemma 15.1. *Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic field. Then the Galois group $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is naturally isomorphic to $(\mathbb{Z}/n)^*$ given by $a \in (\mathbb{Z}/n)^*$ acting on $\mathbb{Q}(\zeta_n)$ by $\zeta_n \longrightarrow \zeta_n^a$. Further, for p prime in $\mathbb{Z}$ with $(p,n) = 1$, the Frobenius element $\sigma_p \in Gal(K/\mathbb{Q})$ is the element $p \in (\mathbb{Z}/n)^*$.*

Proof: For this note that if $(m,n) = 1$ then $\mathbb{Q}(\zeta_n) \bigcap \mathbb{Q}(\zeta_m) = \mathbb{Q}$. This reduces the problem to the case when n is prime power. $\square$

Corollary 15.1. *Let p be a prime in $\mathbb{Z}$. Then p splits completely in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1 (\mathrm{mod}\, n)$. In general, for $\mathfrak{p}$ prime lying over p the residual degree is exactly the order of the element $p \in (\mathbb{Z}/n)^*$.*

Proof: Let p be a prime such that p does not divide n and let $\mathfrak{p}$ be a prime lying over p in $\mathbb{Z}[\zeta_n]$. The frobenius automorphism $\sigma_p : \mathbb{Z}[\zeta_n] \longrightarrow \mathbb{Z}[\zeta_n]$ is defined by $\sigma_p x \equiv x^p \mod \mathfrak{p}$ for all $x \in \mathbb{Z}[\zeta_n]$. But $\sigma_p(\zeta_n) = \zeta_n^p$ whereas order of σ_p is the degree of residue field extension of $\mathfrak{p}$ which is $\mathbb{Z}[\zeta_n]/\mathfrak{p}$. Now

$$\sigma_p^f = 1 \Leftrightarrow \sigma_p^f(\zeta_n) = \zeta_n \Leftrightarrow (\zeta_n)^{p^f} = \zeta_n \Leftrightarrow p^f \equiv 1 \pmod{n}$$

Since p is unramified we get p splits into $\phi(n)/f$ distinct prime ideals. Also p splits completely (e=1 and f=1) if and only if $p \equiv 1(\mathrm{mod} n)$. $\square$

Another Proof of Quadratic Reciprocity Law:

Let $p \equiv 1(\mathrm{mod} 4)$ be a prime. Then $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$. For this consider

$$G = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) e^{\frac{2\pi i a}{p}}$$

It is easy to see that $G^2 = (\frac{-1}{p})p = p$ hence $G = \pm\sqrt{p}$ belongs to $\mathbb{Q}(\zeta_p)$.

Let q be a prime. Then $\sigma_q \in gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\mathbb{Z}/p)^*$ and from previous lemma we get, q is a quadratic residue in $\mathbb{Z}/p$ if and only if the prime q splits in $\mathbb{Q}(\sqrt{p})$.

Now look at the field extension $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{p})$ and corresponding polynomial $x^2 - p = 0$. From this point of view, q splits in $\mathbb{Q}(\sqrt{p})$ if and only if p is a quadratic residue mod q. Combining with earlier statement we get p is a quadratic residue mod q if and only if q is quadratic residue mod p.

Remark: One can prove that $G = \sqrt{p}$ if $p \equiv 1(\text{mod}4)$ and $G = i\sqrt{p}$ if $p \equiv 3(\text{mod}4)$.

16 Subfields of Cyclotomic Fields

Let K be a number field which is contained in $\mathbb{Q}(\zeta_n)$. Let $n = \prod_i p_i^{n_i}$. Then $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n)^* = \prod_i (\mathbb{Z}/p_i^{n_i})^*$. Using Galois theory there is a one-one correspondence between the subfields of $\mathbb{Q}(\zeta_n)$ and subgroups of $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n)^*$.

Definition. *Let G be an abelian group. A group homomorphism $\chi : G \longrightarrow \mathbb{C}^*$ is called a character of a group G.*

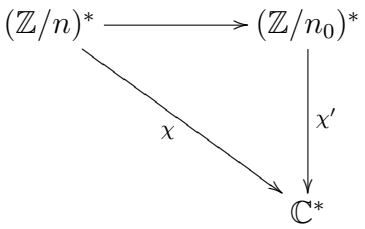
Then $\widehat{G}$, the set of all characters of G, forms a group. This group is called the character group of G.

Lemma 16.1. *If G is a finite abelian group then there exists a bijective correspondance between subgroups of G and subgroups of the character group $\widehat{G}$. This correspondence is given by associating to a subgroup A of G, the set of all characters of G which are trivial on A.*

Combining this lemma with Galois theory we get that subfields K of $\mathbb{Q}(\zeta_n)$ correspond to the subgroups of group of characters of $(\mathbb{Z}/n)^*$ i.e. $\widehat{(\mathbb{Z}/n)^*}$.

A character of $(\mathbb{Z}/n)^*$ which is a homomorphism $\chi : (\mathbb{Z}/n)^* \longrightarrow \mathbb{C}^*$ is called a Dirichlet Character. Let $n|m$ are positive integers. Then we get a homomorphism $(\mathbb{Z}/m)^* \rightarrow (\mathbb{Z}/n)^*$.

Definition. *Let $\chi : (\mathbb{Z}/n)^* \longrightarrow \mathbb{C}^*$ be a Dirichlet character. Let n_0 be the smallest divisor of n such that χ factors through $(\mathbb{Z}/n_0)^*$, i.e. there exist $\chi' : (\mathbb{Z}/n_0)^* \longrightarrow \mathbb{C}^*$ such that following diagram commutes.*



Then n_0 is called the conductor of the Dirichlet character.

Theorem 16.1 (Conductor-Discriminant Formula)**.** *Let K be a number field such that $K \subset \mathbb{Q}(\zeta_n)$, for some n. Let this abelian extension K be defined by a group of characters $X = \{\chi : (\mathbb{Z}/n)^* \longrightarrow \mathbb{C}^*\}$. Then*

$$|d_K| = \prod_{\chi \in X} \text{cond}(\chi)$$

Examples :

1. Let p be a prime and consider $K = \mathbb{Q}(\zeta_p)$. Then the Galois group $G = (\mathbb{Z}/p)^*$ and let $X = \{\chi : (\mathbb{Z}/p)^* \longrightarrow \mathbb{C}^*\}$ be character group. Then conductor of $\chi = p$, $\chi \in X$ if and only if χ is not trivial character. Hence using conductor-discriminant formula we get $|d_K| = p^{p-2}$.

2. Let p be a prime and consider $K = \mathbb{Q}(\zeta_{p^2})$. Then the Galois group $G = (\mathbb{Z}/p^2)^* \cong \mathbb{Z}/(p^2 - p)$ and let $X = \{\chi : (\mathbb{Z}/p^2)^* \longrightarrow \mathbb{C}^*\}$ be character group. Then one can see that trivial character has conductor 1, $p-2$ of them have conductor p and p^2-2p+1 of them have character p^2 . To see this observe that $\mathbb{Z}/(p^2 - p) \cong \mathbb{Z}/p \times \mathbb{Z}/(p-1)$. Hence we get $|d_K| = p^{2p^2-3p}$.

17 L-functions associated to a Dirichlet character

Let $\chi : (\mathbb{Z}/n)^* \longrightarrow \mathbb{C}^*$ be a Dirichlet character. We can extend χ to define a function $\widehat{\chi}$ on $\mathbb{Z}$ by

$$\widehat{\chi}(a) = \begin{cases} \chi(a) & \text{if}(a,n) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Definition. *Let χ be a Dirichlet character. Then*

$$L(s,\chi) = \sum_{n \geq 1} \frac{\widehat{\chi}(n)}{n^s}$$

is called the Dirichlet L-series associated to the Dirichlet character χ.

The Dirichlet L-functions have properties very similar to the Riemann zeta function. For instance, these also have meromorphic continuation to the complex plane and are holomorphic except if $\chi = 1$. These series also have functional equations like Riemann zeta functions.

We recall that if $\xi(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta_{\mathbb{Q}}(s)$, then the functional equation for the Riemann zeta function is expressed as $\xi(s) = \xi(1-s)$. Let K be number field and $\zeta_K(s)$ be the Dedekind zeta function of the number field K. Define

$$\xi_K(s) = (\sqrt{|d_K|})^s(\pi^{\frac{-s}{2}}\Gamma(\frac{s}{2}))^{r_1}(\pi^{-s}\Gamma(s))^{r_2}\zeta_K(s)$$

Then the functional equation for the Dedekind zeta function is expressed by the equality $\xi_K(s) = \xi_K(1-s)$.

There are two basic points here.

1. The L-function $L(s,\chi)$ has a functional equations in which the conductor of χ appears.

2. For an abelian extension K of $\mathbb{Q}$, the zeta function can be written as a product of L-functions as

$$\zeta_K(s) = \prod L(s,\chi)$$

where product runs over all characters of the Galois group of K over $\mathbb{Q}$.

Using these two remarks one can get conductor discriminant formula.

18 Introduction to Tate's thesis

In the following sections we will be discussing the Tate's thesis which is essentially about analytic contituation and functional equation of Dedekind zeta functions, and also of L-functions associated to Grössencharacters. This is the theory of abelian L-functions on the multiplicative group of number fields as well as of local fields. We begin by recalling that local fields are either archmedian ($\mathbb{R}$ *or* $\mathbb{C}$) local fields or non-archmedian (finite extensions of $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$) local fields. Further the global fields are either number fields (finite extensions of $\mathbb{Q}$) or function fields (finite extensions of $\mathbb{F}_p(t)$).

19 Harmonic analysis on p-adic fields

Let G be a locally compact abelian topological group. Let us denote unitary dual of G by $\widehat{G} = \{\xi : G \longrightarrow \mathbb{S}^1\}$. Then $\widehat{G}$ is a locally compact topological group on which the topology is the compact open topology defined by taking basic open sets of $\widehat{G}$ as $W(C,U) = \{\xi \in \widehat{G} | \xi(C) \subset U\}$,where C is a compact set in G and U an open set in $\mathbb{S}^1$.

Theorem 19.1 (Pontryagin duality)**.** *The map $G \longrightarrow \widehat{G}$ is an anti equivalence of categories.*

Let us recall Fourier analysis on $\mathbb{R}$. Let us take the continuous group homomorphism $\psi : \mathbb{R} \longrightarrow \mathbb{C}^*$ defined by $\psi(x) = \exp(2\pi i x)$. Then any unitary character (continuous group homomorphisms from $\mathbb{R}$ to $\mathbb{S}^1$) on $\mathbb{R}$ is of the form $\psi_y : x \longmapsto \psi(xy)$ for some $y \in \mathbb{R}$. Let us define unitary dual of $\mathbb{R}$ by $\widehat{\mathbb{R}} = \{\xi : \mathbb{R} \longrightarrow \mathbb{S}^1 |\ \xi \text{ unitary character of } \mathbb{R}\}$. Then the map

$y \longrightarrow \psi_y$ defines isomorphism of $\mathbb{R}$ with its unitary dual $\widehat{\mathbb{R}}$. One defines for an integrable function f its Fourier transform by

$$\widehat{f}(y) = \int_{\mathbb{R}} f(x)\psi(xy)dx$$

where dx is a Haar measure on $\mathbb{R}$ which, in this case, is the usual Lebesgue measure on $\mathbb{R}$. For an appropriate choice of a Haar measure dx we have, $\widehat{\widehat{f}}(y) = f(-y)$.

There are similar theorems for any local field. Consider the character $\psi : \mathbb{Q}_p \longrightarrow \mathbb{C}^*$ given as follows. For $x \in \mathbb{Q}_p$ write x as

$$x = \sum_{-\infty<j<\infty} a_j(x)p^j$$

where $a_j(x)$ are integers $0 \leq a_j(x) \leq p-1$ and $a_j(x) = 0$ for all but finitely many $j < 0$. Define

$$\psi(x) = \exp\left(2\pi i \sum_{-\infty<j<0} a_j(x)p^j\right)$$

This means that $\psi(x) = 1$ for $x \in \mathbb{Z}_p$.

Lemma 19.1 (Pontryagin Duality)**.** *The map $y \longmapsto \psi_y$ where $\psi_y(x) = \psi(xy)$ from $\mathbb{Q}_p$ to $\widehat{\mathbb{Q}}_p$ is an isomorphism of topological groups.*

Proof: (1) If $\psi \in \widehat{\mathbb{Q}}_p$, then there is an integer k such that $\psi = 1$ on $p^{-k}\mathbb{Z}_p$.

Since ψ is continuous, there is an integer k such that ψ maps $p^{-k}\mathbb{Z}_p$ into $\{z \in \mathbb{S}^1 || z-1| < 1\}$. But $p^{-k}\mathbb{Z}_p$ is a subgroup of $\mathbb{Q}_p$, so its image under ψ is a subgroup of $\mathbb{S}^1$; hence equals $\{1\}$.

Any $\psi \in \widehat{\mathbb{Q}}_p$ is completely determined by its values on the numbers $p^j, j \in \mathbb{Z}$. So if $\psi \neq 1$ there is an integer j_0 such that $\psi(p^j) = 1$ for $j \geq j_0$, but $\psi(p^{j_0-1}) \neq 1$.

(2) Suppose $\psi \in \widehat{\mathbb{Q}}_p, \psi(1) = 1$, and $\psi(p^{-1}) \neq 1$. There is a sequence $\{c_j\}_0^\infty$ with $c_0 \in \{1, ..., p-1\}$ and $c_j \in \{0, 1, ..., p-1\}$ for $j \geq 1$ such that $\psi(p^{-k}) = \exp\left(2\pi i \sum_{j=1}^k c_{k-j}p^{-j}\right)$ for $k = 1, 2, 3....$

Let $\omega_k = \psi(p^{-k})$; then

$$\omega_{k+1}^p = \left(\psi(p^{-k-1})\right)^p = \psi(p.p^{-k-1}) = \psi(p^{-k}) = \omega_k$$

Now $\omega_1 \neq 1$ and $\omega_0 = 1$ so $\omega_1 = \exp(2\pi i c_0 p^{-1})$ for some $c_0 \in \{1, ..., p-1\}$. Proceeding by induction, suppose $\omega_k = \exp\left(2\pi i \sum_{j=1}^{k} c_{k-j} p^{-j}\right)$. Since $\omega_{k=1}$ is pth root of ω_k, there exists $c_k \in \{0, 1, ..., p-1\}$ such that

$$\omega_{k+1} = \exp\left(2\pi i \sum_{j=1}^{k} c_{k-j} p^{-j-1}\right) \exp(2\pi i c_k p^{-1}) = \exp\left(2\pi i \sum_{j=1}^{k+1} c_{k+1-j} p^{-j}\right).$$

(3) If $\psi \in \widehat{\mathbb{Q}}_p, \psi(1) = 1$, and $\psi(p^{-1}) \neq 1$, there exists $y \in \mathbb{Q}_p$ with $|y| = 1$ such that $\psi = \psi_y$.

Let us take $\{c_j\}_0^\infty$ as above and set $y = \sum_0^\infty c_j p^j$. Then $|y| = 1$ since $c_0 \neq 0$, and for $k \geq 1$,

$$\psi(p^{-k}) = \exp\left(2\pi i \sum_{j=1}^{k} c_{k-j} p^{-j}\right) = \exp\left(2\pi i \sum_{j=-k}^{-1} c_{j+k} p^j\right) = \psi_1(\sum_{-k}^{\infty} c_{j+k} p^j)$$

$$= \psi_1(p^{-k} y) = \psi_y(p^{-k})$$

From 1,2 and 3 surjectivity of lemma follows easily. Rest of the proof is easy exrcise. $\square$

Now if we have any finite extension K of $\mathbb{Q}_p$ then we define character using trace map combining with character ψ as follows

$$K \xrightarrow{tr} \mathbb{Q}_p \xrightarrow{\psi} \mathbb{C}^*$$

This is a continuous unitary character on K.

Lemma 19.2 (Pontryagin Duality)**.** *Let K be a field which is finite extension of $\mathbb{Q}_p$. Let ψ be a non trivial character of K (for example above defined ψ). Then ψ defines a topological isomorphism of K to its dual $\widehat{K}$. Which is $K \longrightarrow \widehat{K}$ defined as $y \longmapsto \psi_y$ where $\psi_y(x) = \psi(xy)$.*

Proof: If we use the previous lemma and the fact that dual of direct sum is direct product of duals, the lemma follows. But we give different proof.

It is easy to see that the map is continuous additive homomorphism from K to $\widehat{K}$. Also $\psi_y = 1$ if and only if $y = 0$. Since ψ is a non trivial character there exists y_0 such that $\psi(y_0) \neq 1$ and if $y \neq 0 \implies \psi(y_0) = \psi(y_0 y^{-1} y) = \psi_y(y_0 y^{-1}) \neq 1 \implies \psi_y \neq 1$. And if $y = 0 \implies \psi_y = 1$. This insures injectivity of the map. Moreover it gives that character distinguishes points of K. It remains to prove that the map is surjective.

We claim to show that image of K in $\widehat{K}$ is dense as well as closed. We have Image $= \{\psi_y | y \in K\} \subset \widehat{K}$. Let ϕ be a character in the closure of the image of K. Thus assume that there exists a sequence $x_n \in K$ such that $\psi_{x_n} \longrightarrow \phi$. We can assume that x_n's do not have a convergent subsequence (else if $x_n \longrightarrow x$ then $\psi_{x_n} \longrightarrow \psi_x = \phi$) . Thus we assume that $x_n \longrightarrow \infty$. And $\psi_{x_n} \longrightarrow \phi$ means that for any compact set $X \subset K, \psi_{x_n}(x) \longrightarrow \phi(x) \forall x \in K$ uniformly on K. That is $|\psi_{x_n} - 1| < \epsilon \forall x \in K$ for n sufficiently large. Any neighbourhood of 0 in K contains a subgroup (as it is locally compact, look at its valuation ring or power of its unique maximal ideal) but in $\mathbb{C}^*$ the neighbourhood of 1 does not contain any subgroup. (This is called non-existence of non-trivial subgroups in a neighbourhood of 1.) This gives $\psi_{x_n}(K) = 1$, a contradiction to $x_n \longrightarrow \infty$. $\square$

From previous proposition $K \cong \widehat{K}$ so fourier analysis of standard kind becomes available on K. For any function $f \in L^1$ we define,

$$\widehat{f}(x) = \int_K f(x)\psi(xy)dy$$

where dy is a Haar measure on K and $\psi : K \longrightarrow \mathbb{C}^*$ is a fixed non-trivial character.

Proposition 19.1. *There exists a unique choice of Haar measure dx (depending on ψ) on K such that $\widehat{\widehat{f}}(x) = f(-x)$, for all $f \in s(K)$, schwartz space (space of locally constant compactly supported functions on K).*

Now let us fix a Haar measure on K, a locally compact field, so that

fourier inversion formula holds. Recall that the different ideal $\delta_{K/\mathbb{Q}_p}$ of K is defined by $\delta^{-1}_{K|\mathbb{Q}_p} = \{x \in K | tr(xO_K) \subset \mathbb{Z}_p\}$.

Lemma 19.3. *If A is a compact abelian group and $\chi : A \longrightarrow \mathbb{C}^*$ is a character, then $\int_A \chi(a)da = 0$ if $\chi \neq 1$ and $\int_A \chi(a)da = vol(A)$ if $\chi = 1$.*

Proof: If $\chi = 1$ then $\int_A \chi(a)da = \int_A 1.da = vol(A)$. If $\chi \neq 1$ there exists $x_0 \in A$ such that $\chi(x_0) \neq 1$. Put $I = \int_A \chi(a)da$ then $I = \int_A \chi(a)da = \int_A \chi(a + x_0)da = I.\chi(x_0) \implies I = 0$. $\square$

Let us denote the characteristic function of O_K, the valuation ring of K, by the χ_{O_K}. The fourier transform will be

$$\widehat{\chi}_{O_K}(y) = \int_K \chi_{O_K}(x)\psi(xy)dx = \int_{O_K} \psi(xy)dx$$

Then $\widehat{\chi}_{O_K}(y) = 0$ if $y \notin \delta_K^{-1}$ and $\widehat{\chi}_{O_K}(y) = vol(O_K)$ if $y \in \delta_K^{-1}$. Where $\psi(x) = \exp 2\pi i\ tr(x)$ is a character of K. Then,

$$\widehat{\widehat{\chi}}_{O_K}(y) = \int_K \widehat{\chi}_{O_K}(x)\psi(xy)dx = vol(O_K) \int_{\delta_K^{-1}} \psi(xy)dx$$

$$\widehat{\widehat{\chi}}_{O_K}(0) = vol(O_K) \int_{\delta_K^{-1}} 1.dx = vol(O_K)N(\delta_K)vol(O_K)$$

But $\widehat{\widehat{\chi}}_{O_K}(0) = \chi(0) = 1$. This implies that $vol(O_K) = \frac{1}{\sqrt{N(\delta_K)}}$, where $N(\delta_K) = [\delta_K^{-1} : O_K] = [O_K : \delta_K]$.

20 Local Theory

Let K be a local field and let $\mathcal{S}(K)$ denote the Schwartz space of locally constant compactly supported functions on K. Let χ be a character on K^*. Then we define local zeta function by

$$\mathcal{Z}(f, \chi, s) = \int_{K^*} f(x)\chi(x)|x|^s d^*x$$

for $s \in \mathbb{C}$, where d^*x is normalised Haar measure on K^*. Initially $\mathcal{Z}(f, \chi, s)$ is defined only for $Re(s) > 0$ but actually it has meromorphic continuation to whole of the s-plane. In fact, $\mathcal{Z}(f, \chi, s) \in \mathbb{C}(q^{-s})$ where $q = |\pi|$, π is uniformizing parameter. Let us prove this in case ξ is a ramified character of K^* (i.e. $\chi(O_K^*) \not\equiv 1$), where O_K^* is the group of invertible elements of the ring O_K.

$$\begin{aligned} \mathcal{Z}(f, \chi, s) &= \int_{K^*} f(x)\chi(x)|x|^s d^*x \\ &= \int_{O_K^*} \chi(x)|x|^s d^*x + \text{a term belonging to } \mathbb{C}[\mathrm{q^s}, \mathrm{q^{-s}}] \end{aligned}$$

Now let us look at the term

$$\begin{aligned} \int_{O_K^*} \chi(x)|x|^s d^*x &= \int_{\cup_{n=0}^{\infty}[\pi^n O_K - \pi^{n+1} O_K]} \chi(x)|x|^s d^*x \\ &= \sum_{n=0}^{\infty} \int_{\pi^n O_K^*} \chi(x)|x|^s d^*x \\ &= \sum_{n=0}^{\infty} \int_{O_K^*} \chi(\pi^n x) q^{-ns} |x|^s d^*x \\ &= \sum_{n=0}^{\infty} \chi(\pi^n) \int_{O_K^*} \chi(x) q^{-ns} |x|^s d^*x \\ &= 0 \end{aligned}$$

Therfore for ramified character $\mathcal{Z}(f, \chi, s) \in \mathbb{C}[q^s, q^{-s}]$.

If $\chi|_{O_K^*} \equiv 1$ i.e. χ is unramified then by a similar calculation

$$\mathcal{Z}(\chi_{O_K}, \chi, s) = \sum_{n=0}^{\infty} \chi(\pi^n) q^{-ns} vol(O_K^*) = \frac{1}{1 - \frac{\chi(\pi)}{q^s}} vol(O_K^*)$$

The local zeta functions satisfy a certain functional equation which is basic to the whole theory.

Theorem 20.1. *Let K be a local field, χ a non-trivial character and $f \in \mathcal{S}(K)$ then for all $g \in \mathcal{S}(K)$,*

$$\mathcal{Z}(f,\chi,s)\mathcal{Z}(\widehat{g},\chi^{-1},1-s) = \mathcal{Z}(g,\chi,s)\mathcal{Z}(\widehat{f},\chi^{-1},1-s).$$

Proof: This follows by definitions as we will see.

$$\begin{aligned}
\mathcal{Z}(f,\chi,s)\mathcal{Z}(\widehat{g},\chi^{-1},1-s) &= \int_{K^*\times K^*} f(x)\chi(x)|x|^s\widehat{g}(y)\chi^{-1}(y)|y|^{1-s}d^*xd^*y \\
&\quad \text{We apply change of variable } (\mathrm{x},\mathrm{y}) \longrightarrow (\mathrm{x},\mathrm{xy}). \\
&= \int_{K^*\times K^*} f(x)\chi(x)|x|^s\widehat{g}(xy)\chi^{-1}(xy)|xy|^{1-s}d^*xd^*y \\
&= \int_{K^*}\left(\int_{K^*} f(x)\widehat{g}(xy)|x|d^*x\right)\chi(y^{-1})|y|^{1-s}d^*y \\
&= \int_{K\times K\times K} f(x)g(z)\psi(xyz)|y|^{-s}\chi(y^{-1})dxdydz
\end{aligned}$$

This expression is symmetric in f and g; proving the theorem. $\square$

Corollary 20.1.

$$\mathcal{Z}(f,\chi,s) = \rho(\chi,s)\mathcal{Z}(\widehat{f},\chi^{-1},1-s)$$

where $\rho(\chi,s)$ is independent of f.

Definition. *We define $L(\chi,s) = 1$ if χ is ramified, and $L(\chi,s) = \frac{1}{1-\frac{\chi(\pi)}{q^s}}$ if χ is unramified.*

Note that the value of an unramified character χ on a uniformizing element π does not depend on the choice of uniformizing element π. Rearranging the functional equation, we get

$$\frac{Z(\widehat{f},\chi^{-1},1-s)}{L(\chi^{-1},1-s)} = \epsilon(\chi,s)\frac{\mathcal{Z}(f,\chi,s)}{L(\chi,s)}$$

These epsilons are called local constants. These are monomial function in q^s.

Proposition 20.1. *The local constant $\epsilon(\chi, s)$ is a monomial in q^s.*

Proof : Let assume that χ is ramified. In this case functional equation is

$$\mathcal{Z}(\widehat{f}, \chi^{-1}, 1-s) = \epsilon(\chi, s)\mathcal{Z}(f, \chi, s)$$

We calculated in the beginning of the section that when χ is ramified $\mathcal{Z}(f, \chi, s) \in \mathbb{C}[q^s, q^{-s}]$. This implies that $\epsilon(\chi, s) \in \mathbb{C}[q^s, q^{-s}]$. Similarly $\epsilon(\chi^{-1}, 1-s) \in \mathbb{C}[q^s, q^{-s}]$. Using previous proposition we see that $\epsilon(\chi, s)\epsilon(\chi^{-1}, 1-s) = \chi(-1)$, a constant. Hence $\epsilon(\chi, s)$ is a unit in $\mathbb{C}[q^s, q^{-s}]$ but the only units in $\mathbb{C}[q^s, q^{-s}]$ are monomials. Hence the proposition. $\square$

Proposition 20.2.

$$\epsilon(\chi, s)\epsilon(\chi^{-1}, 1-s) = \chi(-1)$$

Proof follows from the functional equation for local zeta functions and the definition of $\epsilon(\chi, s)$.

21 Language of Adeles and Ideles

Harmonic analysis on the topological groups is most conveniently done when the group is locally compact. By Tychonoff's theorem, an arbitrary product of compact spaces is compact. However such a theorem is not true for locally compact spaces. There is a way out, and there is a general notion in topology of restricted direct product of locally compact topological groups which constructs a locally compact topological group. Suppose we are given system of pairs (G_p, H_p) for $p \in \mathfrak{p}$ (some index set), wher G_p are locally compact groups and H_p are compact open subgroups of G_p. The restricted direct product of the system (G_p, H_p) will be denoted as $\underline{\prod}(G_p, H_p)$ or $\underline{\prod} G_p$. This product is defined as follows.

$$\underline{\prod}(G_p, H_p) = \{(x_p) | x_p \in G_p, \forall p \text{ and } \mathrm{x_p} \in \mathrm{H_p} \text{ for all but finitely many p's}\}$$

A topology on this group is given by declaring the system of neighborhoods of 1 to be:

$$u_1 \times u_2 \times ..... \times u_r \times \prod_{p \neq \{1,2,..r\}} H_p$$

where u_i's are compact open subgroups of G_{p_i} at finitely many places p_i. With this topology $G = \underline{\prod}(G_p, H_p)$ is a locally compact topological group.

The corresponding Schwartz space (space of locally constant and compactly supported functions) will be given by

$$\mathcal{S}(G) = \bigotimes_p \left(\mathcal{S}(G_p), \chi_{H_p}\right) = \lim_{\rightarrow\ \{1,..,r\} \subset \mathfrak{p}} \left\{ \bigotimes_{i=1}^{r} \mathcal{S}(G_{p_i}) \hookrightarrow \bigotimes_{i=1}^{r+1} \mathcal{S}(G_{p_i}) \right\}$$

where the maps are defined as

$$\begin{array}{ccc} \bigotimes_{i=1}^{r} \mathcal{S}(G_{p_i}) & \longrightarrow & \bigotimes_{i=1}^{r+1} \mathcal{S}(G_{p_i}) \\ f_1 \bigotimes .... \bigotimes f_r & \longmapsto & f_1 \bigotimes ... \bigotimes f_r \bigotimes \chi_{H_{r+1}} \end{array}$$

Proposition 21.1. *Let $G = \underline{\prod}_p (G_p, H_p)$ be the restricted direct product of G_p, H_p defined as above. Let dg_p denote the corresponding Haar measure on G_p normalized so that the volume of H_p is 1 for almost all $p \in \mathfrak{p}$. Then there is a unique Haar measure dg on G such that for each finite subset of indices $S \subset \mathfrak{p}$ the restriction of dg on $G_S = \prod_{p \in S} G_p \times \prod_{p \notin S} H_p$ is precisely the product measure.*

Let us take the field $\mathbb{Q}$ of rational numbers and all its completions at finite places $\mathbb{Q}_p$ and infinite place $\mathbb{R} = \mathbb{Q}_\infty$. The corresponding restricted direct product of $\{(\mathbb{Q}_p, \mathbb{Z}_p)\} \bigcup \{\mathbb{R}, \phi\}$ is called the adeles of $\mathbb{Q}$, denoted as $\mathbb{A}_\mathbb{Q} = \mathbb{R} \times \widehat{\mathbb{Q}}$ where $\widehat{\mathbb{Q}} = \mathbb{Q} \bigotimes_\mathbb{Z} \widehat{\mathbb{Z}}$. This is a locally compact topological ring.

Similar notion is associated to the multiplicative group in which we take $\{(\mathbb{Q}_p^*, \mathbb{Z}_p^*)\} \bigcup \{\mathbb{R}^*, \phi\}$. Corresponding restricted direct product is called the idele group of $\mathbb{Q}$ denoted by $\mathbb{J}_\mathbb{Q}$, or $\mathbb{A}_\mathbb{Q}^*$, or $\mathbb{G}_\mathrm{m}$.

For a general number field K one can define adeles and ideles as follows:

$$\mathbb{A}_K = \mathbb{A}_{\mathbb{Q}} \bigotimes_{\mathbb{Q}} K = \underline{\prod}(K_v, O_v)$$

$$\mathbb{J}_K = \left(\mathbb{A}_{\mathbb{Q}} \bigotimes_{\mathbb{Q}} K \right)^* = \underline{\prod}(K_v^*, O_v^*)$$

where K_v denotes completion of K at place v and O_v is corresponding valuation ring. On $\mathbb{J}_K$ the topology is defined by the system of neighbourhoods coming from $O_p^* = (\mathbb{Z}_p \bigotimes_{\mathbb{Z}} O_K)^*$ in usual way. Note that $\mathbb{J}_{\mathbb{Q}} \hookrightarrow \mathbb{A}_{\mathbb{Q}}$ is a continuous map, but $\mathbb{J}_{\mathbb{Q}}$ is not closed in $\mathbb{A}_{\mathbb{Q}}$. Thus the topology on $\mathbb{J}_{\mathbb{Q}}$ is not the one it inherits as a subset of $\mathbb{A}_{\mathbb{Q}}$.

Lemma 21.1. *A number field K embeds inside its adeles $\mathbb{A}_K$ as a discrete, cocompact subgroup, i.e. $\mathbb{A}_K/K$ is a compact group.*

Proof : The map $K \longrightarrow \mathbb{A}_K$ given by $x \longmapsto (x, x, x....)$ (given any $x \in K$ it belongs to O_v for almost all v) will have discrete image if there exists a neighbourhood of $\{0\} \in \mathbb{A}_K$ which does not contain any nonzero element of K. In fact let $U = U_\infty \times \prod_v O_v$ where U_∞ is a small neighborhood of 0 in $K \bigotimes \mathbb{R}$. We have $O_K \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is discrete, where r_1 number of real embedding of K and r_2 is number of complex embeddings of K up to conjugation. Using which we can pull out small neighbourhood for our purpose.

The map $K \longrightarrow K \bigotimes \mathbb{A}_{\mathbb{Q}}$ can be compared to the map $\mathbb{Q}^r \longrightarrow \mathbb{A}_{\mathbb{Q}}^r$ to show the cocompactness. As we can see $\frac{\mathbb{A}_{\mathbb{Q}}}{\mathbb{Q}} = \frac{\prod \mathbb{Z}_p \times \mathbb{R}}{\mathbb{Z}}$ that is $\mathbb{A}_{\mathbb{Q}} = \mathbb{Q} + \prod \mathbb{Z}_p \times \mathbb{R}$. □

Lemma 21.2. *The multiplicative group K^* embedds inside $\mathbb{J}_K$ as a discrete subgroup. Inside $\mathbb{J}_K$ there exists a closed subgroup $\mathbb{J}_K^1 = ker\{|.| : \mathbb{J}_K \longrightarrow \mathbb{C}^*; |x| = \prod_v |x|_v\}$ which contains K^*.*

Theorem 21.1. *The group $\mathbb{J}_K^1/K^*$ is a compact topological group.*

Proof : The discreteness of K^* inside $\mathbb{J}_K$ is analogous. We prove that $K^* \longrightarrow \mathbb{J}_K^1$ is cocompact. For this observe that $K^*\backslash\mathbb{J}_K/\prod_v O_v \prod_\infty K_\infty^*$ is nothing but the class group of K. Look at the map

$$\begin{aligned} \mathbb{J}_K &\longrightarrow \bigoplus_v \mathbb{Z}v = \text{divisors} \\ x_v &\longmapsto \sum_v ord_v(x_v)v \end{aligned}$$

Then $\mathbb{J}_K/\prod_v O_v.\prod_\infty K_\infty^* \equiv$ divisors, going modulo K^* we get $K^*\backslash\mathbb{J}_K/\prod_v O_v.\prod_\infty K_\infty^* \equiv K^*\backslash$divisors, which is the class group of K. Since $\mathbb{J}_K$ is $K^*.(\prod_v O_v \prod_\infty K_\infty^*)$ up to finite index, for the purpose of the proof of compactness of $\mathbb{J}_K^1/K^*$ we can as well look $K^* \longrightarrow K^*.\prod_v O_v\,(\prod_\infty K_\infty^*)^1$. Thus $\mathbb{J}_K^1/K^*$ is compact if and only if $(\prod_\infty K_\infty^*)^1/units$ in K is compact. Which is nothing but Dirichlet unit theorem. $\square$

22 Classical Language

Definition. *Cycles: $\mathcal{C} = \mathcal{C}_f.\infty_\mathcal{C}$ where $\mathcal{C}_f$ is an ideal in O_K and $\infty_\mathcal{C}$ is a set of embeddings of $K \longrightarrow \mathbb{R}$.*

Corresponding to a cycle $\mathcal{C}$ one can define $I(\mathcal{C})$ as ideals coprime to $\mathcal{C}$ and define $P_\mathcal{C}$ to be the principal ideals which have generators x such that $x > 0$ in all embeddings of K corresponding to ∞ primes in $\infty_\mathcal{C}$ and $x - 1 \in \mathcal{C}_f$ i.e. $\mathcal{C}_f = \prod \mathfrak{p}_i^{n_i}$ then $x - 1 \in \mathcal{C}_f \Leftrightarrow v_{\mathfrak{p}_i}(x-1) \geq n_i$.

Notation: We write above one as $x \equiv 1 \mod {}^*\mathcal{C}_f$.

Clearly $I(\mathcal{C})$ is a group and $P_\mathcal{C}$ is a subgroup and thus $I(\mathcal{C})/P_\mathcal{C}$ is a group. This is a finite group.

Example : Let us take $K = \mathbb{Q}$ and $\mathcal{C} = n.\infty$ then $I(\mathcal{C})/P_\mathcal{C} \cong (\mathbb{Z}/n)^*$.

Proof : Let $x = \frac{d_1}{d_2}$ be an element of $I(\mathcal{C})$ with d_1, d_2 coprime to n. Then we define a map $I(\mathcal{C}) \longrightarrow (\mathbb{Z}/n)^*$ as $x \longmapsto d_1(\mod n).(d_2(\mod n))^{-1}$. This is a surjective map with kernel $P_\mathcal{C}$.

Lemma 22.1. *Let $\mathcal{C} = \mathcal{C}_f.\infty_{\mathcal{C}}$ be a cycle. Then*

$$I(\mathcal{C})/P_{\mathcal{C}} \equiv \mathbb{J}_K/K^* \prod_{(v,\mathcal{C})=1} U_v \prod K_\infty^* \prod_{v/\mathcal{C}} U_v(\mathcal{C})$$

where $(v, \mathcal{C}) = 1$ means v coprime to $\mathcal{C}$.

The main theorem of class field theory i.e. Artin Reciprocity will imply that these are precisely the Galois group of abelian extensions of K. Proof of the lemma is an exercise for readers.

23 Character of $\mathbb{A}_K$

Definition. *If a group G operates on a space X then X is called a principal homogeneous space for G if G operates simply transitively on X.*

Lemma 23.1. *The characters of $\mathbb{A}_K$ can be considered to be a principal homogeneous space of $\mathbb{A}_K$.*

Let χ be any non-trivial character on $\mathbb{A}_K$ then $\mathbb{A}_K$ operates on $\widehat{\mathbb{A}_K}$ and give rise to a principal homogeneous structure.

$$\begin{aligned} \mathbb{A}_K \times \widehat{\mathbb{A}_K} &\longrightarrow \widehat{\mathbb{A}_K} \\ (a, \chi) &\longmapsto \chi_a \\ \chi_a(x) &= \chi(ax) \end{aligned}$$

Lemma 23.2. *If $G = \underline{\prod}(G_p, H_p)$ then $\widehat{G} = \underline{\prod}(\widehat{G}_p, H_p^*)$ where $H_p^* \subset \widehat{G}_p$ consists of all characters on G_p which are trivial on H_p which is isomporphic to $\widehat{G_p/H_p}$, a compact group.*

Proof : Since $G = \underline{\prod}(G_p, H_p)$, then $\chi : G \longrightarrow \mathbb{C}^*$ gives rise to a character $\chi_p : G_p \longrightarrow \mathbb{C}^*$. We claim that χ_p is trivial on H_p for almost all p. This follows because $\mathbb{C}^*$ has no small subgroups i.e. there exists a neighbourhood

of 1 which contains no subgroup of $\mathbb{C}^*$ exept 1 itself. This implies by continuity of χ and the definition of almost direct product that $\chi_p = 1$ for almost all p.Then we get $H_p^* = \widehat{G_p/H_p} \subset G_p$ is an open subgroup. To prove this we look at the continuous map $G_p \times \widehat{G_p} \longrightarrow \mathbb{C}^*$ defined by $(a, \chi) \longmapsto \chi(a)$. Define $U = \{\chi \in \widehat{G_p} | \chi(H_p) \subset$ *a ball of radius* $\frac{1}{3}$ *around* $1\}$ This set of characers are open set in $\widehat{G_p}$. But since there are no small subgroups we get $U = H_p^*$. $\square$

Next objective is to construct a non-trivial character on $\mathbb{A}_K/K$. We will do this for $K = \mathbb{Q}$ and then take the trace from $\mathbb{A}_K$ to $\mathbb{A}_\mathbb{Q}$ to construct one for all number fields K.

Construction of character on $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$

The local characters we constructed has the required property. We had

$$\mathbb{Q}_p \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \cong (\mathbb{Q}/\mathbb{Z})_p \longrightarrow \exp(2\pi i x)$$

These mappings can be combined to give a mapping

$$\mathbb{A}_\mathbb{Q}/(\mathbb{R} \times \widehat{\mathbb{Z}}) \cong \bigoplus_p \mathbb{Q}_p/\mathbb{Z}_p \cong \mathbb{Q}/\mathbb{Z} \longrightarrow \mathbb{S}^1$$

But $\mathbb{A}_\mathbb{Q} = (\mathbb{R} + \widehat{\mathbb{Z}}).\mathbb{Q} \implies \frac{\mathbb{A}_\mathbb{Q}}{\mathbb{Q}} \cong \frac{\mathbb{R} \times \hat{\mathbb{Z}}}{\mathbb{Z}}$

This gives a character $\chi(a) = e^{2\pi i a}$ on $\frac{\mathbb{R} \times \hat{\mathbb{Z}}}{\mathbb{Z}}$ and hence on $\frac{\mathbb{A}_\mathbb{Q}}{\mathbb{Q}}$.

Lemma 23.3. *For K, an algebraic number field we have $\widehat{\mathbb{A}_K/K} \cong K$ as a principal homogeneous space.*

Proof Let ψ be a character of $\mathbb{A}_K/K$. For any element $a \in K$, one can define another character $\psi_a : \mathbb{A}_K/K \longrightarrow \mathbb{S}^1$ using $\psi_a(x) = \psi(ax)$. We claim to show that if ψ is non-trivial character of $\mathbb{A}_K/K$ then all characters of $\mathbb{A}_K/K$ are of this form. Note that since $\mathbb{A}_K/K$ is compact its character group is a discrete subgroup of $\mathbb{A}_K$ containing K. Since $\mathbb{A}_K/K$ is compact it follows that its discrete subgroup must contain K as a subgroup of finite index. However a discrete subgroup is a vector space over K. hence the index if not 1 must be infinite. $\square$

Corollary 23.1 (Strong Approximation Theorem)**.** *Let K be a number field. Let v_0 be some place (finite or infinite). Then the image of*

$$K \longrightarrow \prod_{v \neq v_0} K_v$$

is dense.

Proof : If the image is not dense then there exists a non-trivial character of $\mathbb{A}_K$ trivial on $K_{v_0} \times K$. However all characters of $\mathbb{A}_K$, trivial on K are of the form $\psi(ax), a \in K$ and these are non-trivial on K_{v_0}.

Corollary 23.2 (Weak Approximation Theorem)**.** *Let S be any finite set of places of a global field K. Then K is dense in $\prod_{v \in S} K_v$.*

24 Grössencharacter

Characters of idele group $\mathbb{J}_K \longrightarrow \mathbb{C}^*$ which are non-trivial on K^* play a very specific role.

Definition (Grössencharacters)**.** *A Grössencharacter is a character of $\mathbb{J}_K/K^*$ which is a continuous group homomorphism $\mathbb{J}_K/K^* \longrightarrow \mathbb{C}^*$. A continuous group homomorphism $\mathbb{J}_K/K^* \longrightarrow \mathbb{S}^1$ is called unitary Grössencharacter.*

Grössencharacters are trivial on U_v, for almost all v.

Definition (L-function)**.** *Let $\chi : \mathbb{J}_K/K^* \longrightarrow \mathbb{C}^*$ be a character. We define the L-function associated to χ as*

$$L(\chi, s) = \prod_{(p,c)=1} \frac{1}{\left[1 - \frac{\chi(\pi_p)}{(N\pi_p)^s}\right]}$$

where c denotes conductor of χ consists of those primes in K for which χ is non-trivial on U_v and $(p, c) = 1$ denotes the prime ideals p of K which are coprime to the conductor c of χ and the product is taken over all such p.

We can also write $L(\chi, s) = \prod_p L(\chi_p, s)$ where $L(\chi_p, s) = \frac{1}{1-\frac{\chi_p(\pi_p)}{(N\pi_p)^s}}$ if χ_p is an unramified character of K_p^* i.e. it is trivial on O_p^* and define $L(\chi_p, s) = 1$ if χ_p is ramified. By comparing to $\zeta_K(s)$ one finds that $L(\chi, s)$ is holomorphic in the domain $Re(s) > 1$ if χ is unitary.

The infinity-type of a Grössencharacter : If $\chi : \mathbb{J}_K \longrightarrow \mathbb{C}^*$ is a Grössencharacter, the restriction of χ to $K_\infty^* = (K \bigotimes \mathbb{R})^*$ is called the infinity type of character.

Definition (Algebricity of Grössencharacter)**.** *The character χ is called algebraic if and only if χ_∞ is algebraic i.e. $\chi_\infty(x) = x^n$ if $x \in \mathbb{R}^+$ and $\chi_\infty(z) = z^n z^{-m},\ m, n \in \mathbb{Z}$ if $z \in \mathbb{C}^*$.*

Example : For $K = \mathbb{Q}$ we have $\mathbb{J}_\mathbb{Q} = \mathbb{Q}^* \times \mathbb{R}^+ \times \prod \mathbb{Z}_p^*$. This means that $\mathbb{J}_\mathbb{Q}/\mathbb{Q}^* \cong \mathbb{R}^+ \times \prod \mathbb{Z}_p^*$. Thus characters are easy to describe in this case. The characters of $\mathbb{J}_\mathbb{Q}/\mathbb{Q}^*$ of finite order are identified to characters of $(\mathbb{Z}/m)^*$ for some integer m. The trivial character on $\mathbb{J}_K/K^*$ is a Grössencharacter and the corresponding L-function is the Dedekind Zeta function of K.

Exercise :

1. Prove that any Grössencharacter can be written as $\chi = \chi_0||^s$ where χ_0 is a unitary Grössencharacter.

2. Prove that by using formula $L(\chi, s) = L(\chi.||^{s_0}, s) = L(\chi_0, s + s_0)$

25 Fourier Analysis on Adeles and Ideles and Global Zeta Function

We define Global zeta function for $f \in \mathcal{S}(\mathbb{A}_K)$, Schwartz space, and $\chi : \mathbb{J}_K/K^* \longrightarrow \mathbb{C}^*$ a character,

$$\zeta(f, \chi, s) = \int_{\mathbb{J}_K} f(x)\chi(x)|x|^s d^*x$$

where d^*x is a Haar measure on $\mathbb{J}_K$. Note that to define Haar measure on an almost direct product one must have measure$(H_p) = 1$ for almost all p.

In our case $H_p = O_P^*$, we have volume $\frac{Np-1}{Np}$. thus to define Haar measure on $\mathbb{J}_K$ one multiplies local Haar measure by $\frac{Np}{Np-1}\frac{dx}{|x|}$.

If χ is unitary character then $\zeta(f,\chi,s)$ is an analytic function of s in the region $Re(s) > 1$. It suffices to check this for factorizable function $f \in \mathcal{S}(\mathbb{A}_K) = \bigotimes_v \mathcal{S}(K_v)$. So it suffices to assume $f = \prod f_p, \chi = \prod \chi_p$, in which case if we can prove that $\prod_p \mathcal{Z}(f_p,\chi_p,s)$ converges and defines an analytic function in the region $Re(s) > 1$, then the integral defining $\zeta(f,\chi,s)$ will also converge to $\prod_p \mathcal{Z}(f_p,\chi_p,s)$ and will be analytic function in the region $Re(s) > 1$. But we have calculated earlier that $\mathcal{Z}(f_p,\chi_p,s) = \frac{1}{1-\frac{\chi_p(\pi_p)}{(Np)^s}}$ is convergent for $Re(s) > 1$, hence the zeta integral make sense and is analytic in $Re(s) > 1$.

Theorem 25.1. *If χ is a non-trivial Grössencharacter then $\zeta(f,\chi,s)$ has analytic continuation to the entire complex-plane and has functional equation*

$$\zeta(f,\chi,s) = \zeta(\widehat{f},\chi^{-1},1-s)$$

Proof : It has two basic ingradients.

1. **Poisson Summation formula :** We recall that Poisson summation formula of $\mathbb{R}$ states that

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \widehat{f}(n)$$

in case of $\mathbb{R}$. where $f \in \mathcal{S}(\mathbb{R})$. We will be using the analogue of this for $\mathbb{A}_K$.

$$\sum_{\xi\in K} f(\xi) = \sum_{\xi\in K} \widehat{f}(\xi)$$

Hence for $f \in \mathcal{S}(\mathbb{A}_K)$ and $a \in \mathbb{J}_K$ we get $|a|\sum_{\xi\in K} f(a\xi) = \sum_{\xi\in K} \widehat{f}(a\xi)$.

2. **Fubini Theorem :** If $\Gamma \hookrightarrow G$ is a discrete subgroup and dx is a Haar measure on G then it descends to give a Haar measure on G/Γ such that if $f \in L^1(G)$ then $F(x) = \sum_{\gamma\in\Gamma} f(x+\gamma)$ is a L^1-function on G/Γ and $\int_{G/\Gamma} F(x)dx = \int_G f(x)dx$.

We continue with the proof of the theorem. Write $\mathbb{J}_K = \mathbb{J}_K^1 \times \mathbb{R}^+$ (we use (xt) variable).

$$0 \longrightarrow \mathbb{J}_K^1 \longrightarrow \mathbb{J}_K \xrightarrow{Nm} \mathbb{R}^+$$

$$\begin{aligned}
\zeta(f,\chi,s) &= \int_{\mathbb{J}_K} f(x)\chi(x)|x|^s d^*x \\
&= \int_{\mathbb{J}_K} f(xt)\chi(xt)|xt|^s d^*x\frac{dt}{t} \\
&= \int_{\mathbb{R}^+}\int_{\mathbb{J}_K^1} f(xt)\chi(xt)|t|^s dx\frac{dt}{t} \\
&= \int_0^1\int_{\mathbb{J}_K^1} f(xt)\chi(xt)|t|^s dx\frac{dt}{t} + \int_1^\infty\int_{\mathbb{J}_K^1} f(xt)\chi(xt)|t|^s dx\frac{dt}{t}
\end{aligned}$$

The second integral on the right hand side is automatically analytic in the entire plane. We will use Poisson summation formula to transform the first integral on the right hand side to a similar integral but one from 1 to ∞ giving analytic continuation. Define,

$$\zeta_t(f,\chi,s) = \int_{\mathbb{J}_K^1} f(xt)\chi(xt)t^s dx.$$

Then

$$\begin{aligned}
\zeta_t(f,\chi,s) &= \int_{\mathbb{J}_K^1/K^*}\left[\sum_{\xi\in K^*} f(x\xi t)\chi(x\xi t)\right]t^s dx \\
&= \int_{\mathbb{J}_K^1/K^*}\left[\sum_{\xi\in K^*} f(x\xi t)\right]\chi(xt)t^s dx
\end{aligned}$$

since χ is non-trivial,

$$\begin{aligned}
\zeta_t(f,\chi,s) &= \int_{\mathbb{J}_K^1/K^*}\left[\sum_{\xi\in K^*}\widehat{f}\left(\frac{\xi}{xt}\right)\right]\chi(xt)t^{s-1}dx \\
&= \int_{\mathbb{J}_K^1}\widehat{f}\left(\frac{1}{xt}\right)\chi(xt)t^{s-1}dx \\
&= \int_{\mathbb{J}_K^1}\widehat{f}\left(\frac{x}{t}\right)\chi(x^{-1}t)t^{s-1}dx \\
&= \zeta_{\frac{1}{t}}(\widehat{f},\chi^{-1},1-s)
\end{aligned}$$

Thus,

$$\int_0^1\zeta_t(f,\chi,s)=\int_0^1\zeta_{\frac{1}{t}}(\widehat{f},\chi^{-1},1-s)=\int_1^\infty\zeta_t(\widehat{f},\chi^{-1},1-s)$$

Hence,

$$\begin{aligned}
\zeta(f,\chi,s) &= \int_0^1\zeta_t(f,\chi,s)\frac{dt}{t}+\int_1^\infty\zeta_t(f,\chi,s)\frac{dt}{t} \\
&= \int_1^\infty\zeta_{\frac{1}{t}}(\widehat{f},\chi^{-1},1-s)\frac{dt}{t}+\int_1^\infty\zeta_t(f,\chi,s)\frac{dt}{t}
\end{aligned}$$

This is valid initially for $Re(s)>1$ but both integrals are entire giving analytic continuation to $\zeta(f,\chi,s)$ and also functional equation.□

Corollary 25.1. *From this theorem we get analytic continuation and functional equation for L-functions associated to Grössencharacter.*

Proof of Corollary : Let $\chi:\mathbb{J}_K/K^*\longrightarrow\mathbb{C}^*$ be a Grössencharacter and $f:\mathbb{A}_K\longrightarrow\mathbb{C}^*$ be factorizable $f=\prod f_p$ function. We can assume that $\zeta(f_p,\chi_p,s)=L(\chi_p,s)$ for almost all place, say outside a finite set S of places of K. Then from the theorem we have $\zeta(f,\chi,s)=\zeta(\widehat{f},\chi^{-1},1-s)$.

$$\begin{aligned}
\prod_{p\in S}\prod_{p\notin S}\zeta(f_p,\chi_p,s) &= \prod_{p\in S}\prod_{p\notin S}\zeta(\widehat{f_p},\chi_p^{-1},1-s)\\
\prod_{p\in S}\zeta(f_p,\chi_p,s)\prod_{p\notin S}L(\chi_p,s) &= \prod_{p\in S}\zeta(\widehat{f_p},\chi_p^{-1},1-s)\prod_{p\notin S}L(\chi_p^{-1},1-s)\\
&= \prod_{p\in S}\frac{\zeta(\widehat{f_p},\chi_p^{-1},1-s)}{L(\chi_p^{-1},1-s)}\prod_{p\in S}L(\chi_p^{-1},1-s)\\
&= \prod_{p\in S}\frac{\zeta(\widehat{f_p},\chi_p^{-1},1-s)}{L(\chi_p^{-1},1-s)}L(\chi^{-1},1-s)
\end{aligned}$$

But using local functional equation

$$\epsilon(\chi_p,s)=\frac{\zeta(f_p,\chi_p,s)}{L(\chi_p,s)}=\frac{\zeta(\widehat{f_p},\chi_p^{-1},1-s)}{L(\chi_p^{-1},1-s)}$$

We get

$$L(\chi,s)\epsilon(\chi,s)=L(\chi^{-1},1-s)$$

with $\epsilon(\chi,s)=\prod_p\epsilon(\chi_p,s)$ where $\epsilon(\chi_p,s)=1$ at almost all places and is of the form ab^s. $\square$

26 Riemann-Roch Theorem

Let K be a function field over a finite field (i.e. finite extension of $F_q(t)$, q is power of some prime). The field K has valuations, denoted as v, which are considered as points of the corresponding Riemann surface X or X_K. By a divisor D on X we mean an element of the free abelian group on X, i.e. $D=\sum_v n_v v$ where $n_v\in\mathbb{Z}$ and v belongs to the set of places of K such that n_v is nonzero only for finitely many v. We define the degree of a divisor $D=\sum_v n_v v$ to be $\deg(D)=\sum n_v$. We call the finite set of places v with $n_v\neq 0$ the support of the divisor D.

For an element $f \in K$ we associate a divisor, called the divisor of f and denoted as (f), to be described as follows. For $v \in X$, let us denote $n_v = v(f)$ for the valuation of f at the place v. It is easy to see that this is nonzero for only finitely many v. Then we define $(f) = \sum_v v(f)v$. One can check some simple properties of it.

1. If D_1 and D_2 are divisors, then $\deg(\mathrm{D}_1 + \mathrm{D}_2) = \deg(\mathrm{D}_1) + \deg(\mathrm{D}_2)$.

2. If $f_1, f_2 \in K$, then $(f_1 f_2) = (f_1) + (f_2)$.

3. Let $f \in K$. Then the degree $\deg((\mathrm{f})) = 0$.

For a divisor D one defines certain vector space of functions, $L(D) = \{f \in K^* | (f) + D \geq 0\} \bigcup \{0\}$.

Lemma 26.1. *For a divisor D, $L(D)$ is a finite dimensional vector space over $\mathbb{F}_q$.*

There is a divisor on X, called the canonical divisor and denoted by ϖ. Let ξ be a non-trivial character on $\mathbb{A}_K/K$. This defines character $\xi_v : K_v \longrightarrow \mathbb{C}^*$. Define the order of ξ at v tobe the minimal integer n_v such that $\xi|_{O_v.\pi_v^{n_v}} \equiv 1$. Then the canonical divisor $\varpi = \sum n_v.v$ is a divisor on X, and is divisor class group.

Theorem 26.1 (Riemann-Roch Theorem)**.** *Let K be a function field and $L(D)$ defined as above. Then there exists g an integer ≥ 0 such that* $\dim L(D) - \dim L(k - D) = \deg(D) + (1 - g)$.

Proof : The proof follows from Poisson summation formula applied to the characteristic function of $O_D \subset \mathbb{A}_K$ where O_D is defined to be the product of $\pi_v^{n_v} O_v$ for all the places v of K. $\square$

27 Artin Reciprocity

Now we move towards algebraic number fields and Artin reciprocity law.

Let K/k be an abelian extension of number fields. We note few facts from Galois theory. Let $G = Gal(K/k)$ be the Galois group of K over k, and let $\mathfrak{q}$ be a prime in K lying over a prime ideal $\mathfrak{p}$ of k. We define decomposition group of $\mathfrak{q}$ in G to be $D_{\mathfrak{q}} = \{\sigma \in G | \sigma(\mathfrak{q}) = \mathfrak{q}\}$. As residue field $O_K/\mathfrak{q}$ is a finite field and is a finite extension of $O_k/\mathfrak{p}$ of degree f. We have canonical homomorphism,

$$\begin{aligned} \rho_{\mathfrak{q}} \quad : \quad & D_{\mathfrak{q}} \longrightarrow Gal\left(\frac{O_K/\mathfrak{q}}{O_k/\mathfrak{p}}\right) \\ & \sigma \longmapsto (x \mod \mathfrak{q} \to \sigma(x) \mod \mathfrak{q}) \end{aligned}$$

This map is clearly well defined homomorphism of groups.

Proposition 27.1. *The canonical map $\rho_{\mathfrak{q}} : D_{\mathfrak{q}} \longrightarrow Gal\left(\frac{O_K/\mathfrak{q}}{O_k/\mathfrak{p}}\right)$ has the following properties.*

1. *The map $\rho_{\mathfrak{q}}$ is surjective.*
2. *The map $\rho_{\mathfrak{q}}$ is injective if and only if the prime $\mathfrak{p}$ in k is unramified in K; i.e. if and only if the local extension $K_{\mathfrak{q}}/k_{\mathfrak{p}}$ is unramified.*
3. *Each $\sigma \in D_{\mathfrak{q}}$ extends to an automorphism of the completion $K_{\mathfrak{q}}$ that is trivial on the subfield $k_{\mathfrak{p}}$. The induced map $j_{\mathfrak{q}} : D_{\mathfrak{q}} \longrightarrow Gal(K_{\mathfrak{q}}/k_{\mathfrak{p}})$ is in fact an isomorphism.*

One knows from elementry field theory that $Gal\left(\frac{O_K/\mathfrak{q}}{O_k/\mathfrak{p}}\right)$ is cyclic, generated by the Frobenius map $x \to x^q$ where $\#(k/\mathfrak{p}) = q$. In case of $\mathfrak{p}$ being unramified the Frobenius element $Fr_{\mathfrak{p}} \in D_{\mathfrak{q}} \subset G$ is called the Artin symbol attached to $\mathfrak{p}$.

In other language let u be an unramified place of the number field k and v be a place of the number field K lying over u. Let π_u be uniformizing element of O_u and π_v be that of O_v. Then $\pi_u.O_v = \pi_v.O_v$ and the decomposition group $D_u \cong Gal\left(\frac{O_v/\pi_v}{O_u/\pi_u}\right) \cong Gal(K/k)$.

This defines the map

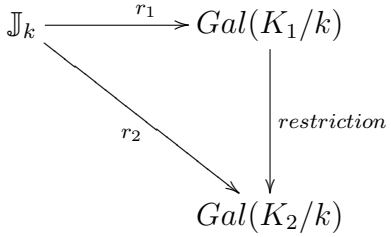
$$\begin{aligned} r \quad : \quad & \prod_{v \notin S} \frac{k_v^*}{O_v^*} \longrightarrow Gal(K/k) \\ & \pi_v \longmapsto Fr_v \end{aligned}$$

where S denotes set of infinite places as well as set of finite places of k.

Theorem 27.1 (Artin Reciprocity)**.** *The map $r : \prod_{v \notin S} k_v^* \longrightarrow Gal(K/k)$ extends uniquely to a group homomorphism $r : \mathbb{J}_k \longrightarrow Gal(K/k)$ which is trivial on k^*.*

Proof : The uniqueness follows from weak approximation theorem i.e. $k^* \hookrightarrow \prod_{v \in S} k_v^*$ is dense. This implies that $k^*.\prod_{v \notin S} k_v^*$ is dense in $\mathbb{J}_k$, hence a character which is trivial on $k^*.\prod_{v \notin S} k_v^*$ is identically 1. In rest of the section we try to prove Artin Reciprocity.□

We have defined a map $\mathbb{J}_k \longrightarrow Gal(K/k)$ for abelian extensions of number fields. These maps as K varies over all abelian extensions of k form a compatible system of maps i.e. if $K_1 \supset K_2 \supset k$ then the following diagram commutes.



Thus we have a map

$$\mathbb{J}_k \longrightarrow \varprojlim Gal(K/k) = Gal(k^{ab}/k)$$

Theorem 27.2. *Let k be a number field. Then,*

$$\mathbb{J}_k/(k^*.k_\infty^+) \cong Gal(k^{ab}/k)$$

i.e. finite abelian extensions of k are in bijective correspondence with open subgroups of finite index of $\mathbb{J}_k/k^*$. Where k_∞^+ denotes identity component of k_∞^*.

Hilbert Class Field : These are maximal abelian everywhere unramified extension of a number field k. These are finite extensions of k with the property that Galois group is isomorphic to the class group of k. In terms of previous theorem these fields correspond to the subgroup

$$k^* k_\infty^* . \prod_{v \in k_f} O_v^* \subset \mathbb{J}_k$$

More generally if $U \subset \mathbb{J}_k$ is an open subgroup containing k^*, then the corresponding abelian extension k_U of k is called the class field associated to U. Also k_U is unramified at a place v if and only if $O_v^* \subset U$.

Ray Class Field : Let $\mathcal{C}$ be a cycle in number field k. We define $U(\mathcal{C}) = \prod_{v \in \mathcal{C}} U_v(n_v)$ where $\mathcal{C} = \{v_1, v_2 .... v_l, v_\infty\}$ and $U_v(n_v) = \{x \in O_v^* | x \equiv 1 \mod (\pi_v^{n_v})\}$. Then we take $U = k^*.U(\mathcal{C})$ and the corresponding field extension is called Ray class field. Just as k_v^* has filtration by congruence subgroups the field k has a distinguished family of abelian extensions generating $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, which corresponds to Ray class field associated to the ideal (n).

Theorem 27.3 (Cebotaraev Density Theorem)**.** *If K/k is a finite Galois extension of global fields with Galois group G and C is a conjugacy class in G then the density (Dirichlet density) of primes $\mathfrak{p}$ in k such that $Fr_\mathfrak{p} \in \mathcal{C}$ is of density $\frac{|\mathcal{C}|}{|G|}$. In particular, the set $X = \{\mathfrak{p} | Fr_\mathfrak{p} \in \mathcal{C}\}$ is nonempty and infinite.*

Corollary 27.1 (Dirichlet Theorem)**.** *There are infinitely many primes in any arithmetic progression $a + nd, n \in \mathbb{Z}$ if $(a, d) = 1$.*

Proof : Let us look at field extension $\mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$. It's Galois group is $\mathbb{Z}/n^*$ and $Fr_p = p$. The Cebotaraev density theorem implies that there are infinitely many primes in arithmetic progression. □

For the purpose of the proof of Artin's reciprocity law it's useful to go back and forth between ideal theoretic and adelic language.

Proposition 27.2. *Let K be a Galois extension of a number field k. Then*

$$\mathbb{J}_k/(k^*.N_k^K\mathbb{J}_K) \cong \frac{I_k(\mathcal{C})}{P_{\mathcal{C}}.N_k^K(I_K(\mathcal{C}))}$$

where $\mathcal{C}$ is a cycle in k divisible by ramified primes such that $O_v(\mathcal{C}_v) \subset N_{k_v}^{K_w}(K_w^*)$ (called admissible cycles) and $I_k(\mathcal{C})$ is ideals in k which are coprime to $\mathcal{C}$.

Proof : We have

$$\mathbb{J}_{\mathcal{C}} = \prod_{v/\mathcal{C}} O_v^*(\mathcal{C}) \prod_{(v,\mathcal{C})=1} k_v^*$$

Let $k_{\mathcal{C}} = \mathbb{J}_{\mathcal{C}} \bigcap k^*$, then $\mathbb{J}_{\mathcal{C}}/k_{\mathcal{C}} \xrightarrow{\approx} \mathbb{J}_k/k^*$. This is injective (by definition) and surjective by weak approximation theorem ($\prod_{v/\mathcal{C}} O_v^*(\mathcal{C}).k^* = \prod_{v/\mathcal{C}} k_v^*$). This gives rise to following diagram.

$$\begin{array}{ccc} I_{\mathcal{C}}/k_{\mathcal{C}} & \xrightarrow{\approx} & \mathbb{J}_k/k^* \\ \downarrow & & \downarrow \\ \frac{I_k(\mathcal{C})}{P_{\mathcal{C}}.N_k^K(I_K(\mathcal{C}))} & \xrightarrow{\approx} & \mathbb{J}_k/(k^*.N_k^K\mathbb{J}_K) \end{array}$$

Check that the isomorphism in the top horizontol arrow descends to give an isomorphism of the bottom horizontol arrow. □

In the light of this proposition we need to define map (called Artin map) from $I_K(\mathcal{C})$ to $Gal(K/k)$. Which we define by $v \longrightarrow Fr_v$. Observe that $N_k^K(I_K(\mathcal{C}))$ lies in the kernel of the Artin map for K/k (Galois extension of degree m). Let $\mathfrak{p}$ be a prime in k and $\mathfrak{q}$ be a prime in K over $\mathfrak{p}$, and suppose this is an unramified prime.

$$\mathfrak{p}O_K = \prod_{i=1}^{d} \mathfrak{q}_i$$

Then $Nm(\mathfrak{q}_i) = \mathfrak{p}^{\frac{m}{d}}$ where $m = d.[O_K/\mathfrak{q}_i : O_k/\mathfrak{p}]$. Which gives $Fr_{\mathfrak{p}}^{m/d} = 1$, thus all the norms are in the kernel of the Artin map. Proving $P_{\mathcal{C}}$ is in kernel of Artin map is non-trivial part.

Steps in the proof of Artin Reciprocity Theorem

1. Prove the reciprocity for cyclic extensions.
   (a) Order of the group $\frac{I_k(\mathcal{C})}{P_{\mathcal{C}}.N_k^K(I_K(\mathcal{C}))}$ and $Gal(K/k)$ is the same.
   (b) The map $I_k(\mathcal{C}) \longrightarrow Gal(K/k)$ is surjective map.
   (c) $P_{\mathcal{C}}$ belongs to the kernel and this is done via recourse to cyclotomic theory.
2. Deduce reciprocity for general abelian extensions.

Below we try to prove some of the steps.

Lemma 27.1. *The Artin map $I_k(\mathcal{C}) \longrightarrow Gal(K/k)$ is non-trivial.*

Proof : If Artin map were trivial then all of the unramified primes are completely split; i.e. $\zeta_K(s) = \zeta_k^m(s), m = [K : k]$. This contradicts simplicity of the poles at $s = 1$ of ζ_K and ζ_k. $\square$

Corollary 27.2. *Artin map $I_k(\mathcal{C}) \longrightarrow Gal(K/k)$ is surjective.*

Proof : Let $G = Gal(K/k)$, an abelian group. Let H be the image of Artin map. Let $L = K^H$, the subfield of K fixed by H. Then $L = K \Leftrightarrow H = G$. But the Artin map for L/k is trivial. Hence by the previous lemma, $L = K \implies G = H$. $\square$

We will in fact prove that the Artin map is surjective restricted to the primes in k.

Theorem 27.4 (Universal Norm Inequality)**.** *With notations all above and Artin map,*

$$\left| \frac{I_k(\mathcal{C})}{P_{\mathcal{C}}.N_k^K(I_K(\mathcal{C}))} \right| \leq [K : k]$$

Proof : Let $H = P_{\mathcal{C}}.N_k^K(I_K(\mathcal{C}))$ and $G = I(\mathcal{C})/H$. Given group G and $G \xrightarrow{\chi} \mathbb{C}^*$, there is the associated L-function $L(s, \chi)$. We will look at the behaviour of this L-function around $s = 1$. We already know that if $\chi = 1$ then $L(s, \chi)$ has simple pole at $s = 1$ and is holomorphic for $\chi \neq 1$. We write

$$L(s, \chi) = (s - 1)^{m(\chi)}.f_\chi(s)$$

where $f_\chi(s)$ at 1 is holomorphic and nonzero and

$$\begin{aligned} m(\chi) &\geq 0 \text{ if } \chi \neq 1 \\ &= -1 \text{ if } \chi = 1 \end{aligned}$$

$$L(s,\chi) = \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s}\right)^{-1}$$

This makes sense for $Re(s) > 1$

$$\begin{aligned} \log(L(s,\chi)) &= -\sum_{\mathfrak{p}} \log\left(1 - \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s}\right) \\ &= \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s} + \text{ higher order terms} \end{aligned}$$

The higher order terms are bounded around $s = 1$. Hence, $\log(L(s,\chi)) = \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s}$ around $s = 1$ (up to bounded function which we will denote by $f \sim g$).

$$\begin{aligned} \log(L(s,\chi)) &\sim \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s} \\ &\sim \sum_{g \in G} \chi(g) \left[\sum_{\mathfrak{p}} \frac{1}{(N\mathfrak{p})^s}\right] \end{aligned}$$

where $\mathfrak{p} = g \in G = I(\mathcal{C})/H$.

$$\begin{aligned} \sum_{\chi} \log(L(s,\chi)) &\sim \sum_{\chi, g \in G} \chi(g) \left[\sum_{\mathfrak{p}} \frac{1}{(N\mathfrak{p})^s}\right] \\ &= |G| \sum_{\mathfrak{p} \in H} \frac{1}{(N\mathfrak{p})^s} \end{aligned}$$

On the other hand, $L(s,\chi) = (s-1)^{m(\chi)}.f_\chi(s)$

$$\begin{aligned}\log(L(s,\chi)) &\sim -m(\chi)\log\frac{1}{s-1}\\ \sum\log(L(s,\chi)) &\sim \left[1-\sum_{\chi\neq 1}m(\chi)\right]\log\frac{1}{s-1}\end{aligned}$$

So we get

$$\frac{\left[1-\sum_{\chi\neq 1}m(\chi)\right]\log\frac{1}{s-1}}{|G|} \sim \sum_{\mathfrak{p}\in H}\frac{1}{(N\mathfrak{p})^s}$$

Note that all primes $\mathfrak{q}$ in K which are of degree 1 over k have the property $\mathfrak{p} = \mathfrak{q}\bigcap O_K$ belongs to the norm from K to k. Hence,

$$\begin{aligned}\frac{\left[1-\sum_{\chi\neq 1}m(\chi)\right]\log\frac{1}{s-1}}{|G|} &\geq \frac{1}{[K:k]}\sum_{\mathfrak{q}\text{ of degree }1}\frac{1}{(N\mathfrak{p})^s}\\ &\sim \frac{1}{[K:k]}\zeta_K(s)\\ &\sim \frac{1}{[K:k]}\log\frac{1}{s-1}\end{aligned}$$

which implies

$$1 \geq 1-\sum m(\chi) \geq \frac{|G|}{[K:k]}$$

$[K:k] \geq |G| = |\frac{I(\mathcal{C})}{PN}|$ i.e. order of $\left|\frac{I_k(\mathcal{C})}{P_{\mathcal{C}}.N_k^K(I_K(\mathcal{C}))}\right| \leq [K:k]$. Further we get $m(\chi) = 0\ \forall\chi \neq 1$. $\square$

Corollary 27.3. *For $\chi \neq 1$ the function $L(1,\chi) \neq 1$.*

Corollary 27.4 (Density Theorem)**.** *There are positive density of primes in an arithmetic progression. i.e.*

$$\sum_{\mathfrak{p}\in\mathfrak{a}_0}\frac{1}{(N\mathfrak{p})^s} \sim \frac{1}{[I(\mathcal{C}):P_{\mathcal{C}}]}\log\frac{1}{s-1}$$

where $\mathfrak{a}_0 \in I(\mathcal{C})/P_{\mathcal{C}}$.

Proof : We have

$$\begin{aligned}\log(L(s,\chi)) &\sim \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s} \\ &= \sum_{\mathfrak{a}} \chi(\mathfrak{a}) \sum_{\mathfrak{p}\in\mathfrak{a}} \frac{1}{(N\mathfrak{p})^s}\end{aligned}$$

Then,

$$\begin{aligned}\sum_{\chi} \chi(\mathfrak{a}_0^{-1}) \log(L(s,\chi)) &= \sum_{\chi}\sum_{\mathfrak{a}} \chi(\mathfrak{a}\mathfrak{a}_0^{-1}) \sum_{\mathfrak{p}\in\mathfrak{a}} \frac{1}{(N\mathfrak{p})^s} \\ &= [I(\mathcal{C}) : P_{\mathcal{C}}] \sum_{\mathfrak{p}\in\mathfrak{a}_0} \frac{1}{(N\mathfrak{p})^s}\end{aligned}$$

Hence,

$$\begin{aligned}\log \zeta_K(s) &= [I(\mathcal{C}) : P_{\mathcal{C}}] \sum_{\mathfrak{p}\in\mathfrak{a}_0} \frac{1}{(N\mathfrak{p})^s} \\ \log \frac{1}{s-1} &= [I(\mathcal{C}) : P_{\mathcal{C}}] \sum_{\mathfrak{p}\in\mathfrak{a}_0} \frac{1}{(N\mathfrak{p})^s}\end{aligned}$$

□

Proof of the index inequality in the other direction needs some algebraic preleminaries taken up in the next section.

28 Euler characteristic of a group G

Let $G = \mathbb{Z}/n$. Let A be an abelian group which is $\mathbb{Z}/n$-module. Let us denote the generator of $\mathbb{Z}/n$ as σ. Then we define cohomology and Tate

cohomology as follows,

$$\begin{aligned} H^0(G,A) &= A^G, \text{ the zeroth cohomology} \\ \widehat{H^0}(G,A) &= \frac{A^G}{(1+\sigma+\sigma^2+...+\sigma^{n-1})A}, \text{ the zeroth Tate cohomology} \\ H^1(G,A) &= \frac{ker(1+\sigma+\sigma^2+...+\sigma^{n-1}) : A \longrightarrow A}{(1-\sigma)A}, \text{ the first cohomology} \end{aligned}$$

Definition. *The Euler characteristic of A is defined by,*

$$\chi(A) = \frac{\#(\widehat{H^0}(G,A))}{\#(H^1(G,A))}$$

if orders make sense, i.e. the orders of both $\widehat{H^0}(G,A)$ and $(H^1(G,A)$ are finite.

Lemma 28.1. *1. If*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

is an exact sequence of $\mathbb{Z}/n$ modules, then whenever two of $\chi(A), \chi(B), \chi(C)$ make sense, so does the third one and $\chi(B) = \chi(A)\chi(C)$.

2. *$\chi(A) = 1$ for A finite.*

3. *$\chi(\mathbb{Z}) = n$ as $\widehat{H^0}(\mathbb{Z}/n, \mathbb{Z}) = \mathbb{Z}/n$ and $H^1(\mathbb{Z}/n, \mathbb{Z}) = 0$.*

Lemma 28.2. *Let K be a degree n cyclic extension of a local field k. Then,*

1. *$\chi(K^*) = [K : k]$.*

2. *$\chi(U_K) = 1$. where U_K denotes units in O_K.*

3. *$[U_K : NmU_K] = e$ where e is the ramification index.*

Proof :

1. Since $\chi(K^*) = \frac{\#\widehat{H^0}}{\#H^1}$, by Hilbert Theorem 90, $H^1 = 0$ (for any cyclic extensions). Hence $\chi(K^*) = \#\widehat{H^0} = [k^* : NmK^*]$.

2. Let us look at the following exact sequence of $\mathbb{Z}/n$ modules.

$$1 \longrightarrow U_K \longrightarrow K^* \longrightarrow \mathbb{Z} \longrightarrow 0$$

hence, $\chi(K^*) = \chi(U_K)\chi(\mathbb{Z}) = [K : k]\chi(U_K)$. Thus it suffices to prove that $\chi(U_K) = 1$.

By the exp map there exists an isomorphism of a subgroup of K of finite index which is isomorphic to a subgroup of O_k of finite index. Thus $\chi(O_K) = \chi(O_k)$. By normal basis theorem O_K has a subgroup of finite index which is free of rank 1 as an $O_k[\mathbb{Z}/n]$ module. Therefore

$$\chi(O_K) = \chi(O_k[\mathbb{Z}/n]) = \chi(Ind_{\{e\}}^{\mathbb{Z}/n} O_k)$$

We use Shapiro's lemma: for a subgroup H of G we have $H^i(H, B) = H^i(G, Ind_H^G B)$. We get $\chi(O_k) = \chi_{\{e\}}(O_k) = 1$.

3. Let us look at the following diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & k^* & \longrightarrow & K^* & \xrightarrow{x \mapsto \frac{x}{\sigma x}} & K^1 & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & U_k & \longrightarrow & U_K & \longrightarrow & U_K^1 & \longrightarrow & 1 \end{array}$$

where K^1 is set of norm 1 elements in K^*. Which implies that $\mathbb{Z}/e\mathbb{Z} \cong K^*/k^*U_K \cong K^1/U_K^1$.

$\chi(U_K) = 1 = \frac{\widehat{H^0}(U_K)}{H^1(U_K)} = \frac{[U_k : NmU_K]}{[U_K^1 : \{\frac{x}{\sigma x} | x \in U_K\}]}$

Observe that $U_K^1 = K^1$ thus $[U_k : NmU_K] = e$ and $[k^* : NmK^*] = [K : k]$ for cyclic extensions of local fields.□

29 Index calculation $[\mathbb{J}_k : k^* N_k^K \mathbb{J}_K]$

Theorem 29.1. *If K is a cyclic extension of degree n of a number field k then $[\mathbb{J}_k : k^* N_k^K \mathbb{J}_K]$ has order n.*

The proof depends on the universal norm index inequality proved earlier. Let S be the finite set of places of k containing all the archmedian places of k. Let S_K denotes the set of places of K (Galois extension of k) lying over the places S of k. To each place w in S_K define a symbol X_w. Let $E = \mathbb{Q}^n$ be the free $\mathbb{Q}$ module on the symbols X_w. Observe that E is a module for $Gal(K/k)$. Let M be any $Gal(K/k)$ -invariant lattice in $E \bigotimes \mathbb{R}$.

Theorem 29.2. *There exists a lattice $M' \subset M$ with basis τ_w such that $\sigma\tau_w = \tau_{\sigma w}$ $\forall w \in S_K, \sigma \in Gal(K/k)$.*

This amounts to the following lemma in group theory.

Lemma 29.1. *Let G be a group. If V_1 and V_2 are two finite dimensional $\mathbb{Q}$ vector spaces which are G modules and if $V_1 \bigotimes \mathbb{R} \cong V_2 \bigotimes \mathbb{R}$ as G modules then $V_1 \cong V_2$ as G modules.*

Proof : $X = \mathrm{Hom}_{\mathbb{Q}[G]}(V_1, V_2)$ is a vector space over $\mathbb{Q}$ such that $X \bigotimes \mathbb{R} = \mathrm{Hom}_{\mathbb{R}[G]}(V_1 \bigotimes \mathbb{R}, V_2 \bigotimes \mathbb{R})$. Therefore if $\mathrm{Hom}_{\mathbb{R}[G]}(V_1 \bigotimes \mathbb{R}, V_2 \bigotimes \mathbb{R}) \neq 0$ then so is $\mathrm{Hom}_{\mathbb{Q}[G]}(V_1, V_2)$. Further one observes that if $p(x)$ is a polynomial on a vector space X defined over $\mathbb{Q}$ such that $p(x)$ is trivial on $X(\mathbb{Q})$ then $p(x) \equiv 0$. $\square$

Corollary 29.1. *In the setting of above theorem we get,*

$$\chi(M) = \frac{\#\widehat{H^0}(G, M)}{\#H^1(G, M)} = \chi(M') = \prod_{v \in S} N_v$$

where N_v is the order of the decomposition subgroup at the places $v \in S$.

Proof : Since $M' = \bigoplus_v \left(Ind_{G_v}^G \mathbb{Z}\right)$ hence,

$$\begin{aligned}\chi(M') &= \prod_v \chi(Ind_{G_v}^G \mathbb{Z}) \\ &= \prod_v \chi(G_{v'}\mathbb{Z}) \\ &= \prod_v N_v \quad \square\end{aligned}$$

Corollary 29.2. *Let K_S be the set of S units in K, i.e. $w(x) = 0 \forall w \notin S_K$ then*

$$\chi(K_S) = \frac{\prod N_v}{[K:k]}$$

Proof : We look at the map

$$\begin{aligned}K_S &\longrightarrow E \bigotimes \mathbb{R} \\ x &\longmapsto \sum_{w \in S_K} \log |x|_w . X_w\end{aligned}$$

Dirichlet unit theorem says that image of K_S is a lattice in hyperplane in $E \bigotimes \mathbb{R}$ defined by $\sum X_w = 0$. Therefore

$$\chi(K_S)\chi(\mathbb{Z}) = \chi(M) = \chi(M') = \prod N_v$$

Thus $\chi(K_S) = \frac{\prod N_v}{[K:k]}$. $\square$

We continue the proof of theorem 29.1 as,

$$\begin{aligned}\chi(\mathbb{J}_K) &= \frac{\#\widehat{H^0}(Gal, \mathbb{J}_K)}{\#H^1(Gal, \mathbb{J}_K)} \\ &= \#\widehat{H^0}(Gal, \mathbb{J}_K) \quad (Hilbert\ 90) \\ &= [\mathbb{J}_k : Nm\mathbb{J}_K]\end{aligned}$$

So $\chi(\mathbb{J}_K/K^*) = [\mathbb{J}_k : k^* Nm\mathbb{J}_K]$. Hence $\frac{\mathbb{J}_K}{K^*} = \frac{\prod O_v^* \cdot \prod_{v \in S} k_v^*}{K_S}$. This completes the proof of $[\mathbb{J}_k : k^* Nm\mathbb{J}_K] = [K:k]$.

Artin Reciprocity Theorem :

This is true for all cyclotomic extensions of $\mathbb{Q}$ i.e. for all extensions K of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_n)$.

The Artin reciprocity is also true for relative cyclotomic extensions i.e. for K a extension of k such that $K \subset k(\zeta_n)$.