Algebraic Number Theory

Lectured by Professor Anthony Scholl
Typed by David Kurniadi Angdinata

Lent 2020

Syllabus

Contents

1 Absolute values and places **3**
1.1 Absolute values . . . 3
1.2 Places . . . 4
1.3 Extensions of places . . . 5

2 Number fields **6**
2.1 Dedekind domains . . . 6
2.2 Places of number fields . . . 8
2.3 Extensions of places of number fields . . . 9

3 Different and discriminant **10**
3.1 Discriminant . . . 10
3.2 Different . . . 12

4 Example: quadratic fields **14**
4.1 Discriminant and different . . . 14
4.2 Decomposition of primes . . . 14

5 Example: cyclotomic fields **15**
5.1 Cyclotomic fields . . . 15
5.2 Quadratic reciprocity . . . 16

6 Ideles and adeles **17**
6.1 Adeles . . . 17
6.2 Ideles . . . 19

7 Geometry of numbers **21**
7.1 Minkowski's theorem . . . 21
7.2 Compactness of $\mathcal{C}_K^1$ . . . 22
7.3 Finiteness of $\mathrm{Cl}\,(K)$ and S-unit theorem . . . 23
7.4 Strong approximation theorem . . . 25

8 Idele class group and class field theory **26**
8.1 Artin reciprocity law . . . 26
8.2 Finite quotients of $\mathcal{C}_K$ . . . 27
8.3 Uniqueness of $\mathrm{Art}_{L/K}$ . . . 29
8.4 Norm functoriality . . . 30
8.5 Existence theorem . . . 30
8.6 Relation with local class field theory . . . 31
8.7 Hilbert class field . . . 31
8.8 Another example . . . 32
8.9 Comparing $\mathcal{C}_K$ and $\mathrm{Gal}\left(K^{\mathrm{ab}}/K\right)$ . . . 33

9 ζ-functions and L-functions **34**
9.1 Riemann ζ-function . . . 34
9.2 Dedekind ζ-function . . . 35
9.3 Local Fourier analysis . . . 36
9.4 Local ζ-integrals . . . 39
9.5 Global Fourier analysis . . . 40
9.6 Global ζ-integrals . . . 41

1 Absolute values and places

1.1 Absolute values

Lecture 1 Thursday 21/01/21

Let K be a field. Recall that an **absolute value (AV)** on K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that for all $x, y \in K$,

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

Also assume

4. there exists $x \in K$ such that $|x| \neq 0, 1$.

This excludes the trivial AV

$$|x| = \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases}.$$

An AV is a **non-archimedean** if

3^{NA}. $|x + y| \leq \max(|x|, |y|)$,

and **archimedean** otherwise. An AV determines a metric $\mathrm{d}(x, y) = |x - y|$ which makes K a **topological field**, so $+$, $\times$, and $(\cdot)^{-1}$ are continuous.

Remark. It is convenient to weaken 3 to

$3'$. there exists $\alpha > 0$ such that for all x and y, $|x + y|^\alpha \leq |x|^\alpha + |y|^\alpha$.

For non-archimedean AV, makes no difference. Does mean that if $|\cdot|$ is an AV, then so is $|\cdot|^\alpha$ for any $\alpha > 0$. The point is that we want the function $z \mapsto z\overline{z}$ on $\mathbb{C}$ to be an AV. Explain why later.

Let us suppose $|\cdot|$ is a non-archimedean AV. Then

$$R = \{x \in K \mid |x| \leq 1\}$$

is a subring of K. It is a **local ring** with maximal ideal

$$\mathfrak{m}_R = \{|x| < 1\}.$$

It is a **valuation ring** of K, so if $x \in K \setminus R$ then $x^{-1} \in R$.

Lemma 1.1. *R is a maximal subring of K.*

Proof. Let $x \in K \setminus R$. Then $|x| > 1$. Then if $y \in R$, there exists $n \geq 0$ such that $|yx^{-n}| = |y| / |x|^n \leq 1$, that is $y \in x^n R$ for $n \gg 0$. So $R[x] = K$, hence R is maximal. ☐

Remark. There is a general notion of valuation, not necessarily $\mathbb{R}$-valued, seen in algebraic geometry. The valuations we are considering here are rank one valuations, and they have this maximality property.

AVs $|\cdot|$ and $|\cdot|'$ are **equivalent** if there exists $\alpha > 0$ such that $|\cdot|' = |\cdot|^\alpha$.

Proposition 1.2. *The following are equivalent.*

- *$|\cdot|$ and $|\cdot|'$ are equivalent.*
- *for all $x, y \in K$, $|x| \leq |y|$ if and only if $|x|' \leq |y|'$.*
- *for all $x, y \in K$, $|x| < |y|$ if and only if $|x|' < |y|'$.*

Proof. See local fields. ☐

A corollary is if $|\cdot|$ and $|\cdot|'$ are non-archimedean AVs with valuation rings R and R', then $|\cdot|$ and $|\cdot|'$ are equivalent if and only if $R = R'$, if and only if $R \subset R'$, by 1.1.

Equivalent AVs define equivalent metrics on K, hence the completion of K with respect to $|\cdot|$ depends only on the equivalence class of $|\cdot|$. Inequivalent AVs determine independent topologies, in the following sense.

Proposition 1.3 (Weak approximation)**.** *Let $|\cdot|_i$ for $1 \le i \le n$ be pairwise inequivalent AVs on K, let $a_1, \dots, a_n \in K$, and let $\delta > 0$. Then there exists $x \in K$ such that for all i, $|x - a_i|_i < \delta$.*

Proof. Suppose $z_j \in K$ such that $|z_j|_j > 1$ and $|z_j|_i < 1$ for all $i \ne j$. Then $\left|z_j^N / \left(z_j^N + 1\right)\right|_i \to 0$ as $N \to \infty$ if $i \ne j$ but $\left|z_j^N / \left(z_j^N + 1\right) - 1\right|_j = \left|1 / \left(z_j^N + 1\right)\right|_j \to 0$. So

$$x = \sum_j a_j \frac{z_j^N}{z_j^N + 1}$$

works if N is sufficiently large. So it is enough to find z_j, and by symmetry take $j = 1$. Induction on n.

$n = 1$. Trivial.

$n > 1$. Suppose have y with $|y|_1 > 1$ and $|y|_2, \dots, |y|_{n-1} < 1$. If $|y|_n < 1$, finished. Otherwise, pick $w \in K$ with $|w|_1 > 1 > |w|_n$, such as by 1.2. If $|y|_n = 1$, then $z = y^N w$ works, for N sufficiently large. If $|y|_n > 1$, then $z = y^N w / \left(y^N + 1\right)$ works, for N sufficiently large.

□

Remark. If $K = \mathbb{Q}$ and $|\cdot|_1, \dots, |\cdot|_n$ are p_i-adic AVs for distinct primes p_i, and $a_i \in \mathbb{Z}$, then weak approximation says that for all $n_i \ge 1$, there exists $x \in \mathbb{Q}$, which is a p_i-adic integer for all $i \in \{1, \dots, n\}$ and $x \equiv a_i \mod p_i^{n_i}$. This of course follows from CRT, which guarantees there exists $x \in \mathbb{Z}$ satisfying this.

1.2 Places

Definition. A **place** of K is an equivalence class of AVs on K.

Example. If $K = \mathbb{Q}$, by Ostrowski's theorem, every AV on $\mathbb{Q}$ is equivalent to one of

- a p-adic AV $|\cdot|_p$ for p prime, or
- a Euclidean AV $|\cdot|_\infty$.

So places of $\mathbb{Q}$ are in bijection with $\{\text{primes}\} \cup \{\infty\}$. We will usually simply denote the places of $\mathbb{Q}$ by $\{2, 3, \dots, \infty\} = \{p \le \infty\}$.

Notation. Let

- V_K be the places of K,
- $\mathrm{V}_{K,\infty}$ be the places given by archimedean AVs, the **infinite places**, and
- $\mathrm{V}_{K,\mathrm{f}}$ be the places given by non-archimedean AVs, the **finite places**.

Often use letters v and w, decorated suitably, to denote places. If $v \in \mathrm{V}_K$, then K_v will denote the completion. If $v : K^\times \to \mathbb{R}$ is a valuation, will also use v to denote the corresponding place, that is the class of AVs $x \mapsto r^{-v(x)}$ for $r > 1$.

Can restate weak approximation in terms of places.

Proposition 1.4. *Let $v_1, \dots, v_n$ be distinct places of K. Then the image of the diagonal inclusion*

$$K \hookrightarrow \prod_{1 \le i \le n} K_{v_i}$$

is dense, for the product topology.

1.3 Extensions of places

Let L/K be finite separable, and let v and w be places of K and L respectively. Say w **lies over**, or **divides**, v, denoted $w \mid v$, if $v = w|_K$ is the restriction of w to K. Then there exists a unique continuous $K_v \hookrightarrow L_w$ extending $K \hookrightarrow L$.

Proposition 1.5. *There is a unique isomorphism of topological rings mapping*

$$\begin{array}{ccc} L \otimes_K K_v & \longrightarrow & \prod_{w \in \mathrm{V}_L,\ w \mid v} L_w \\ x \otimes y & \longmapsto & (xy)_w \end{array}.$$

In the local fields course, proved this for finite places of number fields.

Proof. Let $L = K(a)$, and let $f \in K[T]$ be the minimal polynomial, which is separable. Factor $f = \prod_i g_i$ for $g_i \in K_v[T]$ irreducible and distinct. Let $L_i = K_v[T] / \langle g_i \rangle$. Then $L \otimes_K K_v = K_v[T] / \langle f \rangle \xrightarrow{\sim} \prod_i L_i$ by CRT. Let $w \mid v$, inducing $\iota_w : L \hookrightarrow L_w$. Let $g_w \in K_v[T]$ be the minimal polynomial of $\iota_w(a)$ over K_v. Then $g_w \mid f$ so $g_w \in \{g_i\}$ and $L_w = K_v(\iota_w(a))$ is some L_i. Conversely, K_v is complete and L_i/K_v is finite, so there exists a unique extension of v to L_i, so there is a bijection $\{g_i\} \leftrightarrow \{w \mid v\}$, and thus

$$L \otimes_K K_v \cong \prod_w L_w.$$

Use that both sides are finite-dimensional normed K_v-spaces. For the left hand side, choose a basis of L/K for $L \otimes_K K_v \cong K_v^{[L:K]}$ with norm $\|(x_i)\| = \sup_i |x_i|_v$, where $|\cdot|_v$ is an AV in class of v satisfying triangle inequality. For the right hand side, $\|(y_w)\| = \sup_w |y_w|_w$, where $|\cdot|_w$ is the AV in class of w extending $|\cdot|_v$. A fact is that any two norms on a finite-dimensional vector space over a field complete with respect to an AV are equivalent. For local fields, exactly the same proof as for $\mathbb{R}$, and in general not much harder. See Cassels and Fröhlich chapter II, section 8. $\square$

Corollary 1.6.

- $\{w \mid v\}$ *is finite, non-empty, and*

$$\sum_{w \mid v} [L_w : K_v] = [L : K].$$

- *For all* $x \in L$,

$$\mathrm{N}_{L/K}(x) = \prod_{w \mid v} \mathrm{N}_{L_w/K_v}(x), \qquad \mathrm{Tr}_{L/K}(x) = \sum_{w \mid v} \mathrm{Tr}_{L_w/K_v}(x).$$

Let L/K be a finite Galois extension with $G = \mathrm{Gal}(L/K)$. Then G acts on places w of L lying over a given place v of K. If $|\cdot|$ is an AV on L, then for all $g \in G$, the map $x \mapsto |g^{-1}(x)|$ is an AV on L, agreeing with $|\cdot|$ on K. So this defines a left action of G on $\{w \mid v\}$ by $g(w) = w \circ g^{-1}$. If $w = \mathrm{v}_\mathfrak{p}$ for a prime $\mathfrak{p}$ in a Dedekind domain, then $g(w) = \mathrm{v}_{g(\mathfrak{p})}$. Lecture 2 Saturday 23/01/21

Definition. Define the **decomposition group** D_w or G_w to be the stabiliser of w in G.

If $g \in G_w$, then it is continuous for the topology induced by w on L, so extends to an automorphism of L_w, the completion. Then $G_w \hookrightarrow \mathrm{Aut}(L_w/K_v)$, by continuity, so $\#G_w \le [L_w : K_v]$, and

$$\#G = (G : G_w)\#G_w \le (G : G_w)[L_w : K_v] = \sum_{g \in G/G_w} \left[L_{g(w)} : K_v\right] \le \sum_{w' \mid v} [L_{w'} : K_v] = [L : K] = \#G,$$

by 1.6. So have equality, hence $[L_w : K_v] = \#G_w$, and so L_w/K_v is Galois with group $\mathrm{Gal}(L_w/K_v) \xrightarrow{\sim} G_w \subset G$, and G acts transitively on places over v.

Notation. Suppose v is discrete valuation of L, so a finite place, and the valuation ring is a DVR. Then so is any $w \mid v$, and define $\mathrm{f}(w \mid v) = \mathrm{f}_{L_w/K_v}$ to be the degree of residue class extension and $\mathrm{e}(w \mid v)$ to be the ramification degree, and

$$[L_w : K_v] = \mathrm{e}(w \mid v)\,\mathrm{f}(w \mid v).$$

2 Number fields

Remark. A lot of theory applies to other global fields, that is **function fields** $K/\mathbb{F}_p(t)$ that are finite extensions. These are less interesting, at least to number theorists, since there are no infinite places.

2.1 Dedekind domains

Let K be a **number field**, a finite extension of $\mathbb{Q}$, with **ring of integers** $\mathcal{O}_K$, the integral closure of $\mathbb{Z}$ in K. A basic property is that $\mathcal{O}_K$ is a Dedekind domain, that is

1. Noetherian, in fact, by finiteness of integral closure, $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module,
2. integrally closed in K, by definition, and
3. every non-zero prime ideal is maximal, so Krull dimension at most one.

The following are basic results about Dedekind domains.

Theorem 2.1.

1. *A local domain is Dedekind if and only if it is a DVR.*
2. *For a domain R, the following are equivalent.*
   (a) *R is Dedekind.*
   (b) *R is Noetherian and for all non-zero prime $\mathfrak{p} \subset R$, $R_{\mathfrak{p}}$ is a DVR.*
   (c) *Every fractional ideal of R is invertible.*
3. *A Dedekind domain with only finitely many prime ideals, so **semi-local**, is a PID.*

A **fractional ideal** of R is a non-zero R-submodule $I \subset K$ such that for some $0 \neq x \in R$, $xI \subset R$ is an ideal, and I is **invertible** if there exists a fractional ideal I^{-1} such that $II^{-1} = R$.

Proof.

1. A DVR is a local PID. Proved in local fields. The forward direction is the hardest part.
2. Let $K = \operatorname{Frac} R$.

$(a) \implies (b)$. Enough to check [1] that properties 1 to 3 are preserved under localisation, then use part 1.

$(b) \implies (c)$. To prove (c), may assume $I \subset R$ is an ideal. Let

$$I^{-1} = \{x \in K \mid xI \subset R\}.$$

If $0 \neq y \in I$, then $R \subset I^{-1} \subset y^{-1}R$, so I^{-1} is a fractional ideal and $I^{-1}I \subset R$. Let $\mathfrak{p} \subset R$ be prime, so $R_{\mathfrak{p}}$ is a DVR. It suffices to prove $I^{-1}I \not\subset \mathfrak{p}$. Let $I = \langle a_1, \dots, a_n \rangle$ for $a_i \in R$. Without loss of generality, $\mathrm{v}_{\mathfrak{p}}(a_1) \le \mathrm{v}_{\mathfrak{p}}(a_i)$ for all i. Then $IR_{\mathfrak{p}} = a_1 R_{\mathfrak{p}}$, so for all i, $a_i/a_1 = x_i/y_i \in R_{\mathfrak{p}}$ for $x_i \in R$ and $y_i \in R \setminus \mathfrak{p}$. Then $y = \prod_i y_i \notin \mathfrak{p}$ as $\mathfrak{p}$ is prime, and $ya_i/a_1 \in R$ for all i, so $y/a_1 \in I^{-1}$. Thus $y \in II^{-1} \setminus \mathfrak{p}$.

$(c) \implies (a)$. Check the following.

- R is Noetherian. Let $I \subset R$ be an ideal. Then $II^{-1} = R$, so $1 = \sum_{i=1}^{n} a_i b_i$ for $a_i \in I$ and $b_i \in I^{-1}$. Let $I' = \langle a_1, \dots, a_n \rangle \subset I$. Then $I'I^{-1} = R = II^{-1}$, so $I' = I$. So I is finitely generated.
- R is integrally closed. Let $x \in K$, integral over R. Then $I = R[x] = \sum_{0 \le i < d} Rx^i \subset K$, where d is the degree of the polynomial of integral independence, is a fractional ideal. Obviously $I^2 = I$, so $I = I^2 I^{-1} = II^{-1} = R$, that is $x \in R$.
- Every non-zero prime is maximal. Let $\{0\} \neq \mathfrak{q} \subset \mathfrak{p} \subsetneq R$ for $\mathfrak{p}$ and $\mathfrak{q}$ prime. Then $R \subsetneq \mathfrak{p}^{-1} \subset \mathfrak{q}^{-1}$, so $\mathfrak{q} \subsetneq \mathfrak{p}^{-1}\mathfrak{q} \subset R$, and $\mathfrak{p}\left(\mathfrak{p}^{-1}\mathfrak{q}\right) = \mathfrak{q}$, so as $\mathfrak{q}$ is prime and $\mathfrak{p}^{-1}\mathfrak{q} \not\subset \mathfrak{q}$, so $\mathfrak{p} \subset \mathfrak{q}$, that is $\mathfrak{p} = \mathfrak{q}$.

[1] Exercise

3. Let R be semi-local Dedekind with non-zero primes $\mathfrak{p}_1, \dots, \mathfrak{p}_n$. Choose $x \in R$ with $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$ and $x \notin \mathfrak{p}_2, \dots, \mathfrak{p}_n$. Then $\mathfrak{p}_1 = \langle x \rangle$, and every ideal is a product of powers of $\{\mathfrak{p}_i\}$, by below, so R is a PID.

□

Theorem 2.2. *Let R be Dedekind. Then*

1. *the group of fractional ideals is freely generated by the non-zero prime ideals, and*

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(I)}, \qquad \mathrm{v}_{\mathfrak{p}}(I) = \inf \{ \mathrm{v}_{\mathfrak{p}}(x) \mid x \in I \},$$

2. *if $(R : I) < \infty$ for all $I \neq \{0\}$, then for all I and J,*

$$(R : IJ) = (R : I)(R : J).$$

Proof.

1. If $I \neq R$, then $I \subset \mathfrak{p}$ for some prime ideal $\mathfrak{p}$. Then $I = \mathfrak{p} I'$ where $I' = I \mathfrak{p}^{-1} \supsetneq I$ then by Noetherian induction, using the ascending chain condition on ideals, I is a product of powers of prime ideals, $I = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}}$. Then get the same for fractional ideals $J = x^{-1} I$. Consider the homomorphisms

$$\begin{array}{ccc} \{\text{fractional ideals of } R\} & \longrightarrow & \{\text{fractional ideals of } R_{\mathfrak{p}}\} \\ I & \longmapsto & I R_{\mathfrak{p}} \end{array}, \qquad \begin{array}{ccc} \{\text{fractional ideals of } R_{\mathfrak{p}}\} & \longrightarrow & \mathbb{Z} \\ \langle \pi^n \rangle & \longmapsto & n \end{array}.$$

The composition is $I \mapsto \mathrm{v}_{\mathfrak{p}}(I)$, and if $\mathfrak{q} \neq \mathfrak{p}$ then $\mathrm{v}_{\mathfrak{p}}(\mathfrak{q}) = 0$. So

$$\begin{array}{cccc} (\mathrm{v}_{\mathfrak{p}})_{\mathfrak{p}} & : & \{\text{fractional ideals of } R\} & \longrightarrow & \bigoplus_{\mathfrak{p}} \mathbb{Z} \\ & & \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}} & \longmapsto & (a_{\mathfrak{p}})_{\mathfrak{p}} \end{array}.$$

So $a_{\mathfrak{p}}$ are unique and $(\mathrm{v}_{\mathfrak{p}})_{\mathfrak{p}}$ is an isomorphism. Lecture 3 Tuesday 26/01/21

2. By unique factorisation of ideals in 1,

$$\prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}} \cap \prod_{\mathfrak{p}} \mathfrak{p}^{b_{\mathfrak{p}}} = \prod_{\mathfrak{p}} \mathfrak{p}^{\max(a_{\mathfrak{p}}, b_{\mathfrak{p}})},$$

so if $I + J = R$, then $IJ = I \cap J$, so by CRT, $R/IJ \cong R/I \times R/J$ so the result holds if $I + J = R$. So reduced to showing that $\left(R : \mathfrak{p}^{n+1}\right) = (R : \mathfrak{p})(R : \mathfrak{p}^n)$. Now $R/\mathfrak{p}^n \cong R_{\mathfrak{p}}/\mathfrak{p}^n R_{\mathfrak{p}}$, so without loss of generality, R is local, so a DVR, $\mathfrak{p} = \langle \pi \rangle$, and

$$\cdot \pi : R / \langle \pi^n \rangle \xrightarrow{\sim} \langle \pi \rangle / \left\langle \pi^{n+1} \right\rangle,$$

hence $\left(R : \mathfrak{p}^{n+1}\right) = (R : \mathfrak{p}) \left(\mathfrak{p} : \mathfrak{p}^{n+1}\right) = (R : \mathfrak{p})(R : \mathfrak{p}^n)$.

□

The quotient group

$$\mathrm{Cl}\, R = \{\text{fractional ideals of } R\} / \left\{\text{principal fractional ideals } aR \text{ for } a \in K^\times\right\}$$

is the **class group** of R, or the **Picard group** $\mathrm{Pic}\, R$. If K is a number field, write $\mathrm{Cl}(K) = \mathrm{Cl}\, \mathcal{O}_K$, the **ideal class group** of K.

Fact. For a number field K, $\mathrm{Cl}(K)$ is finite.

2.2 Places of number fields

Recall that $\mathrm{V}_{\mathbb{Q}} = \{p \mid p \text{ prime}\} \cup \{\infty\}$. Let K be a number field. Let $\mathfrak{p} \subset \mathcal{O}_K$ be non-zero prime. Then $\mathfrak{p}$ determines a discrete valuation $\mathrm{v}_{\mathfrak{p}}$ of K and so a non-archimedean AV $|x|_{\mathfrak{p}} = r^{-\mathrm{v}_{\mathfrak{p}}(x)}$ for $r > 1$.

Theorem 2.3. *This gives a bijection*

$$\{\textit{non-zero primes of } \mathcal{O}_K\} \xrightarrow{\sim} \mathrm{V}_{K,\mathrm{f}}.$$

Proof. Let $\mathfrak{p} \neq \mathfrak{q}$. Then there exists $x \in \mathfrak{p} \setminus \mathfrak{q}$, and then $|x|_{\mathfrak{p}} < 1 = |x|_{\mathfrak{q}}$, so $|\cdot|_{\mathfrak{p}}$ and $|\cdot|_{\mathfrak{q}}$ are inequivalent, so the map is injective. Let $|\cdot|$ be a non-archimedean AV on K, with valuation ring $R = \{x \in K \mid |x| \le 1\}$. As $|\cdot|$ is non-archimedean, $\mathbb{Z} \subset R$, hence $R \supset \mathcal{O}_K$, as R is integrally closed, and so $R \supset \mathcal{O}_{K,\mathfrak{p}}$ for some prime $\mathfrak{p} = \mathfrak{m}_R \cap \mathcal{O}_K$. Thus $R = \mathcal{O}_{K,\mathfrak{p}}$, since by 1.1 $\mathcal{O}_{K,\mathfrak{p}}$ is a maximal subring of K, so $|\cdot|$ and $|\cdot|_{\mathfrak{p}}$ are equivalent. ☐

Notation. If $v \in \mathrm{V}_{K,\mathrm{f}}$, then

- $\mathfrak{p}_v$ is the corresponding prime ideal of $\mathcal{O}_K$,
- K_v is a complete discretely valued field, the completion of K,
- $\mathcal{O}_v = \mathcal{O}_{K_v} \subset K_v$ is the valuation ring, not to be confused with $\mathcal{O}_{K,\mathfrak{p}_v}$,
- $\pi_v \in \mathcal{O}_v$ is any generator of the maximal ideal, the **uniformiser**, often assuming $\pi_v \in K$,
- $v : K^\times \twoheadrightarrow \mathbb{Z}$ is the **normalised discrete valuation** such that $v(\pi_v) = 1$,
- $\kappa_v = \mathcal{O}_K/\mathfrak{p}_v \cong \mathcal{O}_v/\langle \pi_v \rangle$ is finite of order $\mathrm{q}_v = p^{\mathrm{f}_v}$ for a prime p such that $v \mid p$, and
- $|x|_v = \mathrm{q}_v^{-v(x)}$ is the **normalised AV**, so $|\pi_v|_v = 1/\mathrm{q}_v$.

Recall that if L/K is a finite separable field extension and v is a place of K, then $L \otimes_K K_v \cong \prod_{w \mid v} L_w$. There is a unique infinite place ∞ of $\mathbb{Q}$ and $\mathbb{Q}_\infty = \mathbb{R}$. So

$$K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \prod_{v \in \mathrm{V}_{K,\infty}} K_v.$$

Each K_v is a finite extension of $\mathbb{R}$, so either $K_v = \mathbb{R}$, and v is **real**, or $K_v \cong \mathbb{C}$, and v is **complex**. In the second case, as $K \subset K_v$ is dense, $K \not\subset \mathbb{R}$. On the other hand, by Galois theory, $\Sigma_K = \{\text{homomorphisms } \sigma : K \hookrightarrow \mathbb{C}\}$ has order $n = [K : \mathbb{Q}]$ and there is an isomorphism

$$\begin{array}{ccc} K \otimes_{\mathbb{Q}} \mathbb{C} & \longrightarrow & \prod_{\sigma \in \Sigma_K} \mathbb{C} \\ x \otimes z & \longmapsto & (\sigma(x) z)_\sigma \end{array}. \qquad (1)$$

Complex conjugation acts on both sides by $x \otimes z \mapsto x \otimes \overline{z}$ and $(z_\sigma)_\sigma \mapsto (\overline{z_{\overline{\sigma}}})_\sigma$. Let

$$\sigma_1, \dots, \sigma_{\mathrm{r}_1} : K \hookrightarrow \mathbb{R}, \qquad \sigma_{\mathrm{r}_1+1} = \overline{\sigma_{\mathrm{r}_1+\mathrm{r}_2+1}}, \dots, \sigma_{\mathrm{r}_1+\mathrm{r}_2} = \overline{\sigma_{\mathrm{r}_1+2\mathrm{r}_2}} : K \hookrightarrow \mathbb{C}, \qquad \mathrm{r}_1 + 2\mathrm{r}_2 = n.$$

Then taking fixed points under complex conjugation of (1),

$$K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \prod_{\sigma \text{ real}} \mathbb{R} \times \prod_{(\sigma,\overline{\sigma}),\ \sigma \neq \overline{\sigma}} \{(z, \overline{z}) \in \mathbb{C} \times \mathbb{C}\} \cong \mathbb{R}^{\mathrm{r}_1} \times \mathbb{C}^{\mathrm{r}_2}.$$

Therefore the following holds.

Theorem 2.4. *There is a bijection*

$$\begin{array}{ccc} \Sigma_K / (\sigma \sim \overline{\sigma}) & \longrightarrow & \mathrm{V}_{K,\infty} \\ \sigma & \longmapsto & \textit{class of AV } |\sigma(\cdot)| \textit{ in } \mathbb{R} \textit{ or } \mathbb{C} \end{array}.$$

Notation. Define
$$K_\infty = K \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{v \in \mathrm{V}_{K,\infty}} K_v \cong \mathbb{R}^{\{\text{real } v\}} \times \mathbb{C}^{\{\text{complex } v\}},$$
where for v complex, $K_v \cong \mathbb{C}$ is well-defined up to complex conjugation. For normalised AVs,

- v real corresponds to $\sigma : K \hookrightarrow \mathbb{R}$ and $|x|_v = |\sigma(x)|$ is the Euclidean AV, and
- v complex corresponds to $\sigma \neq \overline{\sigma} : K \hookrightarrow \mathbb{C}$ and $|x|_v = \sigma(x)\overline{\sigma}(x) = |\sigma(x)|^2$ is the square of modulus.

2.3 Extensions of places of number fields

Let L/K be an extension of number fields, and let $w \mid v$. If v is finite, L_w/K_v is a finite extension of non-archimedean local fields and $[L_w : K_v] = \mathrm{e}(w \mid v)\,\mathrm{f}(w \mid v)$. If v is infinite,
$$L_w/K_v \cong \begin{cases} \mathbb{R}/\mathbb{R} & \mathrm{f} = \mathrm{e} = 1 \\ \mathbb{C}/\mathbb{C} & \mathrm{f} = \mathrm{e} = 1 \\ \mathbb{C}/\mathbb{R} & \mathrm{e} = 2,\ \mathrm{f} = 1 \end{cases}.$$

Lecture 4 Thursday 28/01/21

Proposition 2.5. *Let $x \in L$ and $v \in \mathrm{V}_K$. Then*
$$\left|\mathrm{N}_{L/K}(x)\right|_v = \prod_{w \mid v} |x|_w.$$

Proof. $\mathrm{N}_{L/K}(x) = \prod_{w \mid v} \mathrm{N}_{L_w/K_v}(x)$ so it is enough to show $\left|\mathrm{N}_{L_w/K_v}(x)\right|_v = |x|_w$. If v is finite, it is enough to take $x = \pi_w \in L$, and
$$\left|\mathrm{N}_{L_w/K_v}(\pi_w)\right|_v = \left|u\pi_v^{\mathrm{f}(w \mid v)}\right|_v = \mathrm{q}_v^{-\mathrm{f}(w \mid v)} = \mathrm{q}_w^{-1} = |\pi_w|_w, \qquad u \in \mathcal{O}_{K_v}^\times.$$
If v is infinite, need only consider $L_w/K_v \cong \mathbb{C}/\mathbb{R}$ and $\mathrm{N}_{\mathbb{C}/\mathbb{R}}(z) = z\overline{z}$. □

Theorem 2.6 (Product formula)**.** *Let $x \in K^\times$. Then $|x|_v = 1$ for all but finitely many v and*
$$\prod_{v \in \mathrm{V}_K} |x|_v = 1.$$

Proof. Let $x = a/b$ for $a, b \in \mathcal{O}_K \setminus \{0\}$. Then
$$\{v \in \mathrm{V}_K \mid |x|_v \neq 1\} \subset \mathrm{V}_{K,\infty} \cup \{v \in \mathrm{V}_{K,\mathrm{f}} \mid v(a) > 0 \text{ or } v(b) > 0\}$$
is a finite set. Now
$$\prod_{v \in \mathrm{V}_K} |x|_v = \prod_{p \le \infty} \prod_{v \mid p} |x|_v = \prod_{p \le \infty} \left|\mathrm{N}_{K/\mathbb{Q}}(x)\right|_p.$$
So it is enough to prove for $K = \mathbb{Q}$, and by multiplicativity, reduce to

- $x = q$ prime, where
$$|q|_p = \begin{cases} \frac{1}{q} & p = q \\ 1 & p \neq q, \infty \\ q & p = \infty \end{cases},$$
- $x = -1$, where $|-1|_p = 1$ for all $p \le \infty$.

□

Remark.

- $\mathbb{R}$, with standard measure $\mathrm{d}x$, transforms under $a \in \mathbb{R}^\times$ by $\mathrm{d}(ax) = |a|\,\mathrm{d}x$.
- $\mathbb{C}$, with standard measure $\mathrm{d}x\mathrm{d}y$, transforms under $a \in \mathbb{C}^\times$ by $\mathrm{d}(ax)\,\mathrm{d}(ay) = |a|^2\,\mathrm{d}x\mathrm{d}y$, with the normalised AV on $\mathbb{C}$.

Fact. On K_v, for any v, there is a translation-invariant measure, the Haar measure, $\mathrm{d}_v\,x$, and for all $a \in K_v^\times$, $\mathrm{d}_v\,(ax) = |a|_v\,\mathrm{d}_v\,x$ where $|\cdot|_v$ is the normalised AV.

3 Different and discriminant

3.1 Discriminant

Let $R \subset S$ be rings, commutative with unity, such that S is a free R-module of finite rank $n \geq 1$. Then we have a trace map given by

$$\begin{array}{rcccl} \mathrm{Tr}_{S/R} & : & S & \longrightarrow & R \\ & & x & \longmapsto & \mathrm{Tr}\left(y \mapsto xy\right) \end{array},$$

the trace of the R-linear map $S \to S \cong R^n$. If $x_1, \dots, x_n \in S$, define

$$\mathrm{disc}_{S/R}\left(x_i\right) = \mathrm{disc}\left(x_i\right) = \det\left(\mathrm{Tr}_{S/R}\left(x_i x_j\right)\right) \in R.$$

If $y_i = \sum_{j=1}^n r_{ji} x_j$ for $r_{ji} \in R$, then $\mathrm{Tr}_{S/R}\left(y_i y_j\right) = \sum_{k,l} r_{ki} r_{lj} \mathrm{Tr}_{S/R}\left(x_k x_l\right)$, so

$$\mathrm{disc}\left(y_i\right) = \det\left(r_{ij}\right)^2 \mathrm{disc}\left(x_i\right). \tag{2}$$

Definition. Let $S = \bigoplus_{i=1}^n R e_i$. Then the **discriminant**

$$\mathrm{disc}\left(S/R\right) = \mathrm{disc}_{S/R}\left(e_i\right) R \subset R$$

is an ideal of R, independent of the basis by (2).

The following are obvious properties.

- If $S = S_1 \times S_2$ for S_i free over R, then
$$\mathrm{disc}\left(S/R\right) = \mathrm{disc}\left(S_1/R\right) \mathrm{disc}\left(S_2/R\right).$$
- If $f : R \to R'$ is a ring homomorphism, then
$$\mathrm{disc}\left(S \otimes_R R'/R'\right) = f\left(\mathrm{disc}\left(S/R\right)\right) R'.$$
- If R is a field, then $\mathrm{disc}\left(S/R\right) = R$ or $\mathrm{disc}\left(S/R\right) = \{0\}$ and $\mathrm{disc}\left(S/R\right) = R$ if and only if the R-bilinear form
$$\begin{array}{rcl} S \times S & \longrightarrow & R \\ (x, y) & \longmapsto & \mathrm{Tr}_{S/R}\left(xy\right) \end{array}$$
is non-degenerate, that is there is a duality of the R-vector space S with itself.

By field theory, if L/K is a finite field extension, then $\mathrm{disc}\left(L/K\right) = K$ if and only if the trace form is non-degenerate, if and only if there exists $x \in L$ with $\mathrm{Tr}_{L/K}\left(x\right) \neq 0$, if and only if L/K is separable. More generally is the following.

Theorem 3.1. *Let k be a field, and let A be a finite-dimensional k-algebra. Then $\mathrm{disc}\left(A/k\right) \neq 0$, so $\mathrm{disc}\left(A/k\right) = k$, if and only if $A = \prod_i K_i$ for K_i/k a finite separable field extension.*

Proof. Write $A = \prod_{i=1}^m A_i$ where A_i are indecomposable k-algebras, so A_i is local. So may assume A is local with maximal ideal $\mathfrak{m}$. If $\mathfrak{m} = 0$, that is A is a field, reduced to the previous statement. If not, then every element of $\mathfrak{m}$ is nilpotent, since $\dim_k A < \infty$. So there exists $x \in \mathfrak{m} \setminus \{0\}$ nilpotent. So the endomorphism $y \mapsto xy$ of A is nilpotent and for all $r \in A$, so is $y \mapsto \left(rx\right) y$, so for all $r \in A$, $\mathrm{Tr}_{A/k}\left(rx\right) = 0$. So the trace form is degenerate, and the discriminant is zero. See Atiyah-Macdonald chapter on Artinian rings for an explanation of $A = \prod_i A_i$. ☐

Lecture 5 Saturday 30/01/21

Let R be a Dedekind domain, let $K = \mathrm{Frac}\, R$, let L/K be finite separable, and let S be the integral closure of R in L. Say S/R is an **extension of Dedekind domains**. Then S is a finitely generated R-module, but need not be free.

Proposition 3.2. *S is **locally free** R-module of rank $n = [L : K]$, that is for all $\mathfrak{p} \subset R$, $S_\mathfrak{p} \cong R_\mathfrak{p}^n$.*

Proof. $S \subset L$ so S is torsion-free, hence so is $S_\mathfrak{p}$, and $R_\mathfrak{p}$ is a PID, so $S_\mathfrak{p}$ is free, clearly of rank $\dim_K L = n$. ☐

Lemma 3.3. *If $x \in S$, then $\mathrm{Tr}_{L/K}(x) \in R$.*

Proof. If R is local, then S is a free R-module so $\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{S \otimes_R K/K}(x \otimes 1) = \mathrm{Tr}_{S/R}(x) \in R$. So in general, for all $0 \neq \mathfrak{p} \subset R$, $y = \mathrm{Tr}_{L/K}(x) \in R_\mathfrak{p}$ and

$$\bigcap_\mathfrak{p} R_\mathfrak{p} = \{x \in K \mid \forall \mathfrak{p},\ \mathrm{v}_\mathfrak{p}(x) \geq 0\} = R.$$

□

Then there are two equivalent definitions of $\mathrm{disc}(S/R)$.

Definition. $\mathrm{disc}(S/R)$ is defined to be the ideal of R generated by

$$\left\{\mathrm{disc}_{L/K}(x_1, \dots, x_n) \mid x_1, \dots, x_n \in S\right\}.$$

If S/R is free, this gives the previous definition. As $S \otimes_R K = L$ is separable over K, $\mathrm{disc}(L/K) = K \neq 0$ and so $\mathrm{disc}(S/R) \neq 0$. This is how we prove that S/R is finitely generated.

Proposition 3.4. $\mathrm{disc}(S/R) R_\mathfrak{p} = \mathrm{disc}(S_\mathfrak{p}/R_\mathfrak{p})$ *for all* $\mathfrak{p}$.

Proof. Claim there exist $x_1, \dots, x_n \in S$ which is an $R_\mathfrak{p}$-basis for $S_\mathfrak{p}$. Certainly there exist $e_1, \dots, e_n \in S_\mathfrak{p}$ which is an $R_\mathfrak{p}$-basis. Let

$$\mathcal{Q} = \{\text{primes } \mathfrak{q} \subset S \mid \exists i,\ \mathrm{v}_\mathfrak{q}(e_i) < 0\}$$

be a finite set. By CRT, there exist $a_i \in S$ such that $\mathrm{v}_\mathfrak{q}(a_i) + \mathrm{v}_\mathfrak{q}(e_i) \geq 0$ for all $\mathfrak{q} \in \mathcal{Q}$ and $a_i - 1 \in \mathfrak{p}S$. Then $x_i = a_i e_i \in S$ and $x_i \equiv e_i \mod \mathfrak{p}S$. So (x_i) is an $R/\mathfrak{p}$-basis for $S/\mathfrak{p}S = S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}$, so (x_i) is an $R_\mathfrak{p}$-basis for $S_\mathfrak{p}$. Thus $\mathrm{disc}(S_\mathfrak{p}/R_\mathfrak{p}) = \mathrm{disc}(x_i) R_\mathfrak{p}$, and $\mathrm{disc}(x_i) \in \mathrm{disc}(S/R)$. So $\mathrm{disc}(S_\mathfrak{p}/R_\mathfrak{p}) \subset \mathrm{disc}(S/R) R_\mathfrak{p}$ and the other inclusion is obvious. □

There is an alternative definition of $\mathrm{disc}(S/R)$. If $x_1, \dots, x_n \in S$ is a K-basis for L, then $\mathrm{disc}_{L/K}(x_i) \neq 0$. Let

$$\mathcal{P} = \left\{\mathfrak{p} \subset R \mid \mathrm{v}_\mathfrak{p}\left(\mathrm{disc}_{L/K}(x_i)\right) > 0\right\}$$

be a finite set. So for all $\mathfrak{p} \notin \mathcal{P}$, $\mathrm{disc}(S_\mathfrak{p}/R_\mathfrak{p}) = R_\mathfrak{p}$.

Definition. Define

$$\mathrm{disc}(S/R) = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\mathrm{disc}(S_\mathfrak{p}/R_\mathfrak{p}))},$$

which is equivalent by 3.4 to the previous definition.

Theorem 3.5. $\mathrm{v}_\mathfrak{p}(\mathrm{disc}(S/R)) = 0$ *if and only if* $\mathfrak{p}$ *is unramified in* S *and for all* $\mathfrak{q} \subset S$ *over* $\mathfrak{p}$*, the residue field extension* $(S/\mathfrak{q}) / (R/\mathfrak{p})$ *is separable.*

Proof. May assume R is local, so S is free over R. Have $\mathfrak{p}S = \prod_\mathfrak{q} \mathfrak{q}^{e_\mathfrak{q}}$, so

$$S \otimes_R (R/\mathfrak{p}) \cong S/\mathfrak{p}S \cong \prod_\mathfrak{q} S/\mathfrak{q}^{e_\mathfrak{q}}.$$

So $\mathrm{v}_\mathfrak{p}(\mathrm{disc}(S/R)) = 0$ if and only if $\mathrm{disc}((S/\mathfrak{p}S) / (R/\mathfrak{p})) = R/\mathfrak{p}$, if and only if each $S/\mathfrak{q}^{e_\mathfrak{q}}$ is a finite separable field extension of $R/\mathfrak{p}$ by 3.1, if and only if for all $\mathfrak{q}$, $e_\mathfrak{q} = 1$ and $(S/\mathfrak{q}) / (R/\mathfrak{p})$ is separable. □

Corollary 3.6. *In an extension S/R of Dedekind domains, only finitely many primes are ramified, just the* $\mathfrak{p}$ *such that* $\mathrm{v}_\mathfrak{p}(\mathrm{disc}(S/R)) > 0$.

Proposition 3.7. *Let* $\mathfrak{p} \subset R$*. Then*

$$\mathrm{v}_\mathfrak{p}(\mathrm{disc}(S/R)) = \sum_{\mathfrak{q} \supset \mathfrak{p}} \mathrm{v}_\mathfrak{p}\left(\mathrm{disc}\left(\widehat{S_\mathfrak{q}}/\widehat{R_\mathfrak{p}}\right)\right).$$

Proof. By 3.4 may assume R is local, so S is a free R-module, and $S \otimes_R \widehat{R} \cong \prod_{\mathfrak{q} \subset S} \widehat{S_\mathfrak{q}}$ so

$$\mathrm{v}_\mathfrak{p}(\mathrm{disc}(S/R)) = \mathrm{v}_\mathfrak{p}\left(\mathrm{disc}\left(S \otimes_R \widehat{R}/\widehat{R}\right)\right) = \sum_\mathfrak{q} \mathrm{v}_\mathfrak{p}\left(\mathrm{disc}\left(\widehat{S_\mathfrak{q}}/\widehat{R}\right)\right).$$

□

3.2 Different

There is a finer invariant of ramification.

Definition. The **inverse different** $\mathcal{D}_{S/R}^{-1}$ of an extension S/R of Dedekind domains is

$$\mathcal{D}_{S/R}^{-1} = \left\{x \in L \mid \forall y \in S,\ \mathrm{Tr}_{L/K}(xy) \in R\right\}.$$

This is the dual of S with respect to the trace form $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$, which is non-degenerate and clearly an S-submodule of L. If $\bigoplus_{i=1}^n Rx_i \subset S$, let (y_i) be the dual basis to (x_i) for the trace form, that is $\mathrm{Tr}_{L/K}(x_i y_j) = \delta_{ij}$. Then $S \subset \mathcal{D}_{S/R}^{-1} \subset \bigoplus_{i=1}^n Ry_i$, so $\mathcal{D}_{S/R}^{-1}$ is a fractional ideal, since it is finitely generated.

Definition. $\mathcal{D}_{S/R}$ is an ideal of S, the **different**.

Proposition 3.8.

1. *If $\mathfrak{p} \subset R$, then $\mathcal{D}_{S_\mathfrak{p}/R_\mathfrak{p}} = \mathcal{D}_{S/R} S_\mathfrak{p}$.*
2. $\mathrm{N}_{L/K}\left(\mathcal{D}_{S/R}\right) = \mathrm{disc}(S/R)$.
3. *Let $\mathfrak{q} \subset S$ lying over $\mathfrak{p} \subset R$. Then $\mathrm{v}_\mathfrak{q}\left(\mathcal{D}_{S/R}\right) = \mathrm{v}_\mathfrak{q}\left(\mathcal{D}_{\widehat{S_\mathfrak{q}}/\widehat{R_\mathfrak{p}}}\right)$.*

Proof.

1. Exercise. [2]
2. By 1 and 3.4, can suppose R is local. Then S is a PID by 2.1.3. So $\mathcal{D}_{S/R}^{-1} = x^{-1}S$ for some $0 \ne x \in S$. Let (e_i) be a basis for S over R. Then there exists a basis (e_i') for S over R such that $\mathrm{Tr}_{L/K}\left(e_i x^{-1} e_j'\right) = \delta_{ij}$. Let $x^{-1}e_j' = \sum_k b_{kj} e_k$ for $b_{kj} \in K$. Then

$$\langle 1 \rangle = \left\langle \det\left(\mathrm{Tr}_{L/K}\left(e_i x^{-1} e_j'\right)\right)\right\rangle = \left\langle \det\left(\mathrm{Tr}_{L/K}(e_i e_j)\right)\det(b_{ij})\right\rangle = \det(b_{ij})\,\mathrm{disc}(S/R).$$

But $\mathrm{N}_{L/K}\left(x^{-1}\right)$ is $\det(b_{ij})$ times some unit in R. So $\langle 1 \rangle = \left\langle \mathrm{N}_{L/K}\left(x^{-1}\right)\right\rangle \mathrm{disc}(S/R)$.

Lecture 6 Tuesday 02/02/21

3. Assume R is local and $\mathfrak{p} = \langle \pi_\mathfrak{p} \rangle$. Write $\widehat{K} = \mathrm{Frac}\,\widehat{R}$ and for $\mathfrak{q} = \langle \pi_\mathfrak{q} \rangle \subset S$ write $\widehat{L_\mathfrak{q}} = \mathrm{Frac}\,\widehat{S_\mathfrak{q}}$. So say

$$L \otimes_K \widehat{K} \supset S \otimes_R \widehat{R} \xrightarrow{\sim} \prod_\mathfrak{q} \widehat{S_\mathfrak{q}} \subset \prod_\mathfrak{q} \widehat{L_\mathfrak{q}},$$

and

$$\mathrm{Tr}_{L \otimes_K \widehat{K}/\widehat{K}}(x) = \sum_\mathfrak{q} \mathrm{Tr}_{\widehat{L_\mathfrak{q}}/\widehat{K}}(x). \tag{3}$$

Let $S = \bigoplus_{i=1}^n Rx_i$, and $\prod_\mathfrak{q} \pi_\mathfrak{q}^{-a_\mathfrak{q}} S = \mathcal{D}_{S/R}^{-1} = \bigoplus_{i=1}^n Ry_i$ for some $a_\mathfrak{q} \ge 0$ and $y_i \in L$, the dual basis to x_i. Then as $S \otimes_R \widehat{R} = \bigoplus_{i=1}^n \widehat{R}(x_i \otimes 1)$,

$$\begin{aligned}\mathcal{D}_{S \otimes_R \widehat{R}/\widehat{R}}^{-1} &= \left\{x \in L \otimes_K \widehat{K} \;\middle|\; \forall y \in S \otimes_R \widehat{R},\ \mathrm{Tr}_{L \otimes_K \widehat{K}/\widehat{K}}(xy) \in \widehat{R}\right\} \\ &= \bigoplus_{i=1}^n \widehat{R}(y_i \otimes 1) = \mathcal{D}_{S/R}^{-1}\left(S \otimes_R \widehat{R}\right) = \prod_\mathfrak{q} \pi_\mathfrak{q}^{-a_\mathfrak{q}}\left(S \otimes_R \widehat{R}\right) \subset L \otimes_K \widehat{K},\end{aligned}$$

since $\mathrm{Tr}_{L/K}(x_i y_j) = \delta_{ij}$ and trace commutes with base change. On the other hand, by (3) and the definitions

$$\mathcal{D}_{S \otimes_R \widehat{R}/\widehat{R}}^{-1} \cong \prod_\mathfrak{q} \mathcal{D}_{\widehat{S_\mathfrak{q}}/\widehat{R}}^{-1} \subset \prod_\mathfrak{q} \widehat{L_\mathfrak{q}},$$

so

$$\mathcal{D}_{\widehat{S_\mathfrak{q}}/\widehat{R}}^{-1} = \prod_{\mathfrak{q}'} \pi_{\mathfrak{q}'}^{-a_{\mathfrak{q}'}} \widehat{S_\mathfrak{q}} = \pi_\mathfrak{q}^{-a_\mathfrak{q}} \widehat{S_\mathfrak{q}},$$

as $\mathrm{v}_\mathfrak{q}(\pi_{\mathfrak{q}'}) = 0$ if $\mathfrak{q}' \ne \mathfrak{q}$.

∎

[2] Exercise: the same idea as 3.4

Use this to prove the following.

Theorem 3.9. *Assume all extensions of residue fields are separable. Let* $\mathfrak{p}S = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i} \subset S$*. Then*

1. $\mathfrak{q}_i \mid \mathcal{D}_{S/R}$ *if and only if* $e_i > 1$*, and*

2. $\mathfrak{q}_i^{e_i - 1} \mid \mathcal{D}_{S/R}$.

Proof. First assume R is complete local and $\mathfrak{p} = \langle \pi_R \rangle$. Then S is also local, and complete, with unique prime $\mathfrak{q} = \langle \pi_S \rangle$, so $g = 1$.

1. So $\mathcal{D}_{S/R} = \langle \pi_S \rangle^d$ for $d \geq 0$. By 3.8.2, $\operatorname{disc}(S/R) = \left\langle \mathrm{N}_{L/K}(\pi_S)^d \right\rangle = \langle \pi_R \rangle^{\mathrm{df}}$. So as $\mathrm{v}_{\mathfrak{p}}(\operatorname{disc}(S/R)) = 0$ if and only if $\mathfrak{p}$ is unramified by 3.5, get the first statement.

2. Claim $\operatorname{Tr}_{L/K}(\mathfrak{q}) \subset \mathfrak{p}$. Let $x \in \mathfrak{q}$. Then multiplication by x is a nilpotent endomorphism of $S \otimes_R (R/\mathfrak{p}) \cong S/\mathfrak{q}^{\mathrm{e}}$, so $\operatorname{Tr}_{S \otimes_R (R/\mathfrak{p})/(R/\mathfrak{p})}(x \otimes 1) = 0$, that is $\operatorname{Tr}_{L/K}(x) = \operatorname{Tr}_{S/R}(x) \in \mathfrak{p}$. Hence the claim. Therefore $\operatorname{Tr}_{L/K}\left(\mathfrak{q}^{1-\mathrm{e}}\right) = \operatorname{Tr}_{L/K}\left(\pi_R^{-1}\mathfrak{q}\right) \subset R$, so $\mathfrak{q}^{1-\mathrm{e}} \subset \mathcal{D}_{S/R}^{-1}$, that is $\mathfrak{q}^{\mathrm{e}-1} \mid \mathcal{D}_{S/R}$.

For the general case, apply the above to $\widehat{S_{\mathfrak{q}_i}}/\widehat{R_{\mathfrak{p}}}$ and use 3.8.3. ☐

Fact.

- If $\mathfrak{p} \nmid e_i$ then $\mathrm{v}_{\mathfrak{q}_i}\left(\mathcal{D}_{S/R}\right) = e_i - 1$. If $\mathfrak{p} \mid e_i$ then $\mathrm{v}_{\mathfrak{q}_i}\left(\mathcal{D}_{S/R}\right) \geq e_i$. More precisely, $\mathrm{v}_{\mathfrak{q}_i}\left(\mathcal{D}_{S/R}\right)$ is determined by the orders of the higher ramification groups, for a Galois closure of L/K. See for example Serre, Local fields, Chapter 4, Section 1, Proposition 4.

- If $S = R[x]$, and x has minimal polynomial $f \in R[T]$ then $\mathcal{D}_{S/R} = \langle f'(x) \rangle$ where f' is the derivative. See example sheet 1. This means that $\mathcal{D}_{S/R}$ is the annihilator of the cyclic S-module $\Omega_{S/R}$ of Kähler differentials, generated by $\mathrm{d}x$.

For an extension L/K of number fields write

$$\mathcal{D}_{L/K} = \mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K} \subset \mathcal{O}_L, \qquad \delta_{L/K} = \operatorname{disc}(\mathcal{O}_L/\mathcal{O}_K) \subset \mathcal{O}_K.$$

Remark. Let $K/\mathbb{Q}$, and let (e_i) be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Then $\delta_{K/\mathbb{Q}} \subset \mathbb{Z}$ is $\langle \operatorname{disc}(e_i) \rangle$ and if (e_i') is another basis such that $e_i' = \sum_{i,j} a_{ji} e_j$, then $\operatorname{disc}(e_i') = (\det(a_{ij}))^2 \operatorname{disc}(e_i) = \operatorname{disc}(e_i)$, since $\det(a_{ij}) = \pm 1$. So the integer $\operatorname{disc}(e_i)$ is independent of the basis, not just the ideal it generates. This is called the **absolute discriminant** $\mathrm{d}_K \in \mathbb{Z} \setminus \{0\}$ of K. The sign is significant.

Theorem 3.10 (Kummer-Dedekind criterion)**.** *Let S/R be an extension of Dedekind domains, and let $x \in S$ such that $L = K(x)$. Suppose $\mathfrak{p} \subset R$ such that $S_{\mathfrak{p}} = R_{\mathfrak{p}}[x]$. Let $g \in R[T]$ be the minimal polynomial of x and $g = \prod_i \overline{g_i}^{e_i} \in (R/\mathfrak{p})[T]$ the factorisation of reduction of g into powers of distinct monic irreducibles $\overline{g_i}$. Let $g_i \in R[T]$ be any monic lifting of $\overline{g_i}$ and $f_i = \deg g_i = \deg \overline{g_i}$. Then $\mathfrak{q}_i = \mathfrak{p}S + \langle g_i(x) \rangle \subset S$ is prime with*

$$[S/\mathfrak{q}_i : R/\mathfrak{p}] = f_i, \qquad \forall i \neq j, \ \mathfrak{q}_i \neq \mathfrak{q}_j, \qquad \mathfrak{p}S = \prod_i \mathfrak{q}_i^{e_i}.$$

Proof. Can assume R is local, so then $S = R[x]$. Set $\mathfrak{p} = \langle \pi \rangle$ and $R/\mathfrak{p} = \kappa$. Then $\mathfrak{q}_i$ is prime with residue degree f_i, since $S/\mathfrak{q}_i \cong \kappa[T] / \langle \overline{g_i} \rangle$, and $\overline{g_i}$ is irreducible of degree f_i. Claim that $\mathfrak{q}_i \neq \mathfrak{q}_j$. If $i \neq j$, there exist $a, b \in R[T]$ such that $\overline{a g_i} + \overline{b g_j} = 1 \in \kappa[T]$, so $1 = a g_i + b g_j + \pi c$ for some $c \in R[T]$, so $1 \in \langle \pi, g_i(x), g_j(x) \rangle = \mathfrak{q}_i + \mathfrak{q}_j$. Let $g = \prod_i g_i^{e_i} + \pi h$ for $h \in R[T]$. Then

$$\prod_i \mathfrak{q}_i^{e_i} = \prod_i \langle \pi, g_i(x) \rangle^{e_i} \subset \prod_i \langle \pi, g_i(x)^{e_i} \rangle \subset \left\langle \pi, \prod_i g_i(x)^{e_i} \right\rangle = \langle \pi, \pi h(x) \rangle \subset \mathfrak{p}S = \langle \pi \rangle.$$

Now $\dim_\kappa(S/\mathfrak{p}S) = n = [L : K]$, and

$$\dim_\kappa\left(S/\mathfrak{q}_i^{e_i}\right) = \sum_{j=0}^{e_i - 1} \dim_\kappa\left(\mathfrak{q}_i^j / \mathfrak{q}_i^{j+1}\right) = e_i \dim_\kappa(S/\mathfrak{q}_i) = e_i f_i,$$

so $\prod_i \mathfrak{q}_i^{e_i} \subset \mathfrak{p}S$ gives $\sum_i e_i f_i \geq n$. As $\sum_i e_i f_i = \sum_i e_i \deg \overline{g_i} = \deg \overline{g} = n$, have equality. ☐

4 Example: quadratic fields

Lecture 7 Thursday 04/02/21

Let $K = \mathbb{Q}\left(\sqrt{d}\right)$ for $d \in \mathbb{Q}^\times$ not a square. Multiplying d by a square, can assume $d \in \mathbb{Z} \setminus \{0, 1\}$ is squarefree. Then $\mathcal{O}_K \supset \mathbb{Z}\left[\sqrt{d}\right] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$.

4.1 Discriminant and different

Since $\mathrm{Tr}_{K/\mathbb{Q}}(1) = 2$ and $\mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{d}\right) = 0$, $\mathrm{disc}\left(1, \sqrt{d}\right) = 4d$, so either $\mathrm{d}_K = 4d$, and

$$\mathcal{O}_K = \mathbb{Z}\left[\sqrt{d}\right],$$

or $\mathrm{d}_K = d$, and $\left(\mathcal{O}_K : \mathbb{Z}\left[\sqrt{d}\right]\right) = 2$. This holds if and only if there exist $m, n \in \mathbb{Z}$ not both even with $\frac{m+n\sqrt{d}}{2} \in \mathcal{O}_K$, if and only if $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$ since obviously $\frac{1}{2}, \frac{\sqrt{d}}{2} \notin \mathcal{O}_K$, if and only if $d \equiv 1 \mod 4$ since the minimal polynomial of $\frac{1+\sqrt{d}}{2}$ is $\left(T - \frac{1}{2}\right)^2 - \frac{d}{4} = T^2 - T - \frac{d-1}{4}$, in which case

$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\tfrac{1+\sqrt{d}}{2} = \mathbb{Z}\left[\tfrac{1+\sqrt{d}}{2}\right].$$

The dual basis of $\left(1, \sqrt{d}\right)$ for the trace form is $\left(\frac{1}{2}, \frac{1}{2\sqrt{d}}\right)$, so

$$\mathcal{D}_{K/\mathbb{Q}} = \begin{cases} \left\langle 2\sqrt{d} \right\rangle & d \not\equiv 1 \mod 4 \\ \left\langle \sqrt{d} \right\rangle & d \equiv 1 \mod 4 \end{cases}.$$

4.2 Decomposition of primes

By Kummer-Dedekind.

- If $p \neq 2$ or $d \not\equiv 1 \mod 4$ then $p \nmid \left(\mathcal{O}_K : \mathbb{Z}\left[\sqrt{d}\right]\right)$. So applying the criterion to $T^2 - d$, see that
  - $\langle p \rangle = \mathfrak{p}^2$ is ramified if $p \mid d$, so $\mathfrak{p} = \left\langle p, \sqrt{d} \right\rangle$,
  - $\langle p \rangle = \mathfrak{p}$ is inert if $\left(\frac{d}{p}\right) = -1$, and
  - $\langle p \rangle = \mathfrak{p}\mathfrak{p}'$ is split if $\left(\frac{d}{p}\right) = 1$, so if $d \equiv a^2 \mod p$ then $\mathfrak{p} = \left\langle p, \sqrt{d} - a \right\rangle \neq \left\langle p, \sqrt{d} + a \right\rangle = \mathfrak{p}'$.
- The remaining case is $p = 2$ and $d \equiv 1 \mod 4$. Factoring $T^2 - T - \frac{d-1}{4}$ modulo two, get
  - $\langle 2 \rangle$ is inert if $d \equiv 5 \mod 8$, and
  - $\langle 2 \rangle = \mathfrak{p}\mathfrak{p}'$ is split if $d \equiv 1 \mod 8$ and $\mathfrak{p} = \left\langle 2, \frac{\sqrt{d}+1}{2} \right\rangle \neq \left\langle 2, \frac{\sqrt{d}-1}{2} \right\rangle = \mathfrak{p}'$.

Go through the calculations if you have not seen them before. [3]

[3] Exercise

5 Example: cyclotomic fields

Recall some Galois theory. Let $n > 1$, and let K be a field of characteristic zero or characteristic $p \nmid n$. Suppose $L = K(\zeta_n)$, where $\zeta_n \in L$ is a primitive n-th root of unity, that is $\zeta_n^m \neq 1$ for all $1 \leq m < n$. Equivalently, ζ_n is a root of the n-th cyclotomic polynomial $\Phi_n \in \mathbb{Z}[T]$ of degree $\phi(n)$, defined recursively by

$$T^n - 1 = \prod_{d \mid n} \Phi_d(T).$$

Then L/K is Galois, with abelian Galois group, and

$$\begin{array}{rcl} \mathrm{Gal}(L/K) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ g & \longmapsto & \text{unique } a \mod n \text{ such that } g(\zeta_n) = \zeta_n^a \end{array}.$$

is an injective homomorphism.

5.1 Cyclotomic fields

Theorem 5.1. *Let $L = \mathbb{Q}(\zeta_n)$. Then*

1. $\mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$,
2. *p ramifies in L if and only if $p \mid n$, and*
3. $\mathcal{O}_L = \mathbb{Z}[\zeta_n]$.

Remark. 1 if and only if Φ_n is irreducible over $\mathbb{Q}$, if and only if $[L : \mathbb{Q}] = \phi(n)$.

Proof. Let $n = p^r m$ for $r \geq 1$ and $p \nmid m$ prime. Let $\zeta_m = \zeta_n^{p^r}$ and $\zeta_{p^r} = \zeta_n^m$. Then there exist $a, b \in \mathbb{Z}$ such that $p^r a + mb = 1$, so $\zeta_n = \zeta_m^a \zeta_{p^r}^b$. Let $K = \mathbb{Q}(\zeta_m)$. Then $L = K(\zeta_{p^r})$. Will prove that

- Φ_{p^r} is irreducible over K,
- if $v \in \mathrm{V}_{K,\mathrm{f}}$ and $v \nmid p$ then v is unramified in L/K,
- if $v \mid p$ then v is totally ramified in L/K, and
- $\mathcal{O}_L = \mathcal{O}_K[\zeta_{p^r}]$.

This proves 5.1 by induction on n. For a place w of L, write $x_w \in L_w$ for the image of ζ_{p^r} under $L \hookrightarrow L_w$. Suppose $v \mid p$. By induction, p is unramified in $K/\mathbb{Q}$, so $v(p) = 1$. Then

$$\Phi_{p^r}(T+1) = \frac{(T+1)^{p^r} - 1}{(T+1)^{p^{r-1}} - 1}$$

is an Eisenstein polynomial in $\mathcal{O}_{K_v}[T]$. Indeed $\Phi_{p^r}(T+1) \equiv T^{p^{r-1}(p-1)} \mod p$, and the constant coefficient is p, so has valuation one. Then from local fields,

- Φ_{p^r} is irreducible over K_v, hence over K,
- L/K is totally ramified at v, and
- if w is the unique place of L over v, then $\mathcal{O}_{L_w} = \mathcal{O}_{K_v}[\pi_w]$ where $\pi_w = x_w - 1$ is the root of $\Phi_{p^r}(T+1)$ in L_w.

Now let $v \mid q \neq p$. Then Φ_{p^r} is separable modulo q. Have

$$K_v \otimes_K L \cong \prod_{w \mid v} L_w = \prod_{w \mid v} K_v(x_w).$$

Let $f_w \in \mathcal{O}_{K_v}[T]$ be the minimal polynomial of x_w over K_v. Then

- $\prod_{w \mid v} f_w = \Phi_{p^r}$, so the reduction of f_w at v is separable, hence L_w/K_v is unramified, and
- by local fields again, $\mathcal{O}_{L_w} = \mathcal{O}_{K_v}[x_w]$.

Thus for all $v \in \mathrm{V}_{K,\mathrm{f}}$,

$$\mathcal{O}_{K_v} \otimes_{\mathcal{O}_K} \mathcal{O}_K[\zeta_{p^r}] \cong \mathcal{O}_{K_v}[T] / \langle \Phi_{p^r} \rangle \cong \prod_{w \mid v} \mathcal{O}_{K_v}[T] / \langle f_w \rangle = \prod_{w \mid v} \mathcal{O}_{L_w} \cong \mathcal{O}_{K_v} \otimes_{\mathcal{O}_K} \mathcal{O}_L,$$

by CRT, so must have $\mathcal{O}_K[\zeta_{p^r}] = \mathcal{O}_L$. ☐

5.2 Quadratic reciprocity

Recall Frobenius elements. Let L/K be a Galois extension of number fields, let $w \mid v$ be finite places, and let $G = \mathrm{Gal}(L/W) \supset G_w \cong \mathrm{Gal}(L_w/K_v)$ be the decomposition group of w. Then

$$1 \to \mathrm{I}_w \to G_w \to \mathrm{Gal}(\ell_w/\kappa_v) \to 1,$$

where I_w is the inertia subgroup. Suppose w is unramified in L/K, if and only if v is unramified in L/K. Then $\mathrm{I}_w = \{1\}$. Define the **Frobenius** at w to be the unique element $\sigma_w \in G_w$ mapping to the generator $x \mapsto x^{\mathrm{q}_v}$ of $\mathrm{Gal}(\ell_w/\kappa_v)$. So $\mathrm{ord}\,\sigma_w = \mathrm{f}(w \mid v) = [\ell_w : \kappa_v] = [\ell_{w'} : \kappa_v]$ for any $w' \mid v$, as G acts transitively on $\{w'\}$. In particular, $\sigma_w = 1$ if and only if v splits completely in L/K, that is there exist $[L : K]$ places of L over v. Suppose G is abelian. Then G_w and σ_w are independent of w, so depends only on v.

Notation. $\sigma_v = \sigma_{L/K,v} = \sigma_w$ is the **arithmetic Frobenius** at v. There are other notations, such as $\phi_{L/K,v}$ or $(v, L/K)$, the **norm residue symbol**.

Remark. Let $L/F/K$ where L/K is abelian. Then $\sigma_{L/K}\big|_F = \sigma_{F/K}$ by definition.

Let $L = \mathbb{Q}(\zeta_n)$, let $K = \mathbb{Q}$, and let $n > 2$. Have an isomorphism

$$\begin{array}{cccc} \lambda & : & (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & \mathrm{Gal}(L/\mathbb{Q}) \\ & & a \mod n & \longmapsto & (\zeta_n \mapsto \zeta_n^a) \end{array}.$$

Claim that

$$\sigma_p = \sigma_{L/\mathbb{Q},p} = \lambda(p \mod n) = (\zeta_n \mapsto \zeta_n^p) \in \mathrm{Gal}(L/\mathbb{Q}),$$

if $p \nmid n$. Indeed, σ_p is characterised by for all $v \mid p$, σ_p induces $x \mapsto x^p$ on the residue field $\mathbb{Z}[\zeta_n]/\mathfrak{p}_v$, whereas $\lambda(p)$ induces $x \mapsto x^p$ over $\mathbb{Z}[\zeta_n]/\langle p \rangle$. Lecture 8 Saturday 06/02/21

Remark.

- These elements σ_p generate $\mathrm{Gal}(L/\mathbb{Q})$, since every integer prime to n is a product of $p \nmid n$, so gives, with some thought, another proof that $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
- If $\sigma : L \hookrightarrow \mathbb{C}$ is any embedding, then $\overline{\sigma(\zeta_n)} = \sigma(\zeta_n^{-1})$. So $\lambda(-1 \mod n)$ is complex conjugation, for any $\sigma : L \hookrightarrow \mathbb{C}$.

Specialise to the case $n = q > 2$ is prime. Then $\mathrm{Gal}(L/\mathbb{Q}) = (\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic of order $q-1$, so has a unique index two subgroup $H \cong \left((\mathbb{Z}/q\mathbb{Z})^\times\right)^2$. Let $K = L^H$ be a quadratic extension of $\mathbb{Q}$. Every $p \ne q$ is unramified in L, hence also in K. So $K = \mathbb{Q}(\sqrt{\pm q})$, and as $\langle 2 \rangle$ is unramified in K, must have

$$K = \mathbb{Q}\left(\sqrt{q^*}\right), \qquad q^* = \begin{cases} q & q \equiv 1 \mod 4 \\ -q & q \equiv 3 \mod 4 \end{cases}, \qquad \mathrm{d}_K = q^*.$$

Now let $p \ne q$ be an odd prime. Then

$$\sigma_{K/\mathbb{Q},p} = 1 \qquad \iff \qquad \sigma_{L/\mathbb{Q},p} = \lambda(p) \in H \qquad \iff \qquad \left(\frac{p}{q}\right) = 1.$$

But

$$\sigma_{K/\mathbb{Q},p} = 1 \qquad \iff \qquad p \text{ splits completely in } K \qquad \iff \qquad \left(\frac{q^*}{p}\right) = 1.$$

That is, $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$. Combine with $\left(\frac{-1}{q}\right) = (-1)^{(p-1)/2}$ to get the quadratic reciprocity law. In algebraic number theory, quadratic reciprocity says that splitting of p in $K/\mathbb{Q}$ depends only on the congruence class of p modulo something. Class field theory tells us that a similar thing holds for any abelian extension of number fields, since there is a law describing the decomposition of primes in an abelian extension which is just a congruence condition.

6 Ideles and adeles

To study congruences modulo p^n for $n \geq 1$ Hensel introduced $\mathbb{Z}_p$ and $\mathbb{Q}_p$ such that $\mathbb{Q} \hookrightarrow \mathbb{Z}_p$. For congruences to arbitrary moduli, or to study local-global problems in general, it would be nice to simultaneously embed $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ for all $p \leq \infty$, which are locally compact. The first guess is $\mathbb{Q} \hookrightarrow \prod_{p \leq \infty} \mathbb{Q}_p$, but this product is not nice, for example not locally compact. Better is to notice that if $x \in \mathbb{Q}$, then the image of x lies in $\mathbb{Z}_p$ for all but finitely many p. So Chevalley introduced a small product with better properties, for any number field K, the ring of adeles or valuation vectors $\mathbb{A}_K$ of K and the group of ideles $\mathcal{J}_K = \mathbb{A}_K^\times$ of K. These are topological rings and groups respectively. They are highly disconnected, that is have plenty of open subgroups. Open subgroups are closed, so if $H \subset G$ is an open subgroup, then G/H is discrete, that is $G = \bigsqcup_x xH$ is a topological disjoint union.

6.1 Adeles

Let K be a number field, let $\mathrm{V}_K = \mathrm{V}_{K,\infty} \sqcup \mathrm{V}_{K,\mathrm{f}}$, and let K_v be its completions. If $v \in \mathrm{V}_{K,\mathrm{f}}$, have $\mathcal{O}_v = \mathcal{O}_{K_v} = \{x \mid |x|_v \leq 1\} \subset K_v$.

Definition. The **adele ring** of K is

$$\mathbb{A}_K = \left\{ (x_v) \in \prod_{v \in \mathrm{V}_K} K_v \ \middle|\ \text{for all but finitely many } v,\ x_v \in \mathcal{O}_v \right\} = \bigcup_{\text{finite } S \subset \mathrm{V}_{K,\mathrm{f}}} \mathrm{U}_{K,S} \subset \prod_{v \in \mathrm{V}_K} K_v,$$

where

$$\mathrm{U}_{K,S} = \prod_{v \in \mathrm{V}_{K,\infty}} K_v \times \prod_{v \in S} K_v \times \prod_{v \in \mathrm{V}_{K,\mathrm{f}} \setminus S} \mathcal{O}_v.$$

Notation. Let

$$K_\infty = \prod_{v \in \mathrm{V}_{K,\infty}} K_v = K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{\mathrm{r}_1} \times \mathbb{C}^{\mathrm{r}_2}.$$

Then $\mathbb{A}_K$ is a ring. The topology on $\mathbb{A}_K$ is generated by all open $V \subset \mathrm{U}_{K,S}$ as S varies, and where $\mathrm{U}_{K,S}$ has the product topology, so

$$V = \prod_{v \in S} X_v \times \prod_{v \notin S} \mathcal{O}_{K_v},$$

where S is finite, containing $\mathrm{V}_{K,\infty}$, and X_v is open in K_v. This means in particular that every $\mathrm{U}_{K,S} \subset \mathbb{A}_K$ is open, so

$$\mathrm{U}_{K,\emptyset} = K_\infty \times \prod_{v \in \mathrm{V}_{K,\mathrm{f}}} \mathcal{O}_v = K_\infty \times \widehat{\mathcal{O}_K},$$

where $\widehat{\mathcal{O}_K}$ is the profinite completion, is open and has the product topology. This completely determines the topology on $\mathbb{A}_K$. See example sheet 1 exercise 1(ii).

Example. Let $K = \mathbb{Q}$. Then

$$\mathbb{A}_{\mathbb{Q}} = \mathbb{R} \times \left\{ (x_p)_p \in \prod_{p < \infty} \mathbb{Q}_p \ \middle|\ \text{for all but finitely many } p,\ x_p \in \mathbb{Z}_p \right\}.$$

So, letting $m \in \mathbb{Z}_{>0}$ be the product of the denominators p^i of x_p see that $m\,(x_p)_p \in \prod_{p<\infty} \mathbb{Z}_p = \widehat{\mathbb{Z}}$, that is $(x_p)_p \in (1/m)\,\widehat{\mathbb{Z}} \subset \prod_p \mathbb{Q}_p$. Let [4]

$$\widehat{\mathbb{Q}} = \bigcup_{m \geq 1} \frac{1}{m} \widehat{\mathbb{Z}} \cong \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Then $\mathbb{A}_{\mathbb{Q}} = \mathbb{R} \times \widehat{\mathbb{Q}}$.

[4] Exercise: easy

Proposition 6.1. *$\mathbb{A}_K$ is Hausdorff and locally compact, so every point has a compact neighbourhood.*

Proof. $\mathrm{U}_{K,\emptyset}$ is Hausdorff, and is locally compact, since K_∞ is locally compact and $\widehat{\mathcal{O}_K}$ is compact, and it is an open neighbourhood of zero. So by translation, $\mathbb{A}_K$ is Hausdorff and locally compact. ☐

There is a diagonal embedding $K \hookrightarrow \mathbb{A}_K$.

Proposition 6.2. *K is discrete in $\mathbb{A}_K$.*

Proof. Find a neighbourhood of zero containing only $0 \in K$. Let

$$U = \left\{ x = (x_v) \in \mathbb{A}_K \;\middle|\; \begin{array}{l} \forall v \in \mathrm{V}_{K,\mathrm{f}},\ \left|x_v\right|_v \le 1 \\ \forall v \in \mathrm{V}_{K,\infty},\ \left|x_v\right|_v < 1 \end{array} \right\}.$$

Then $U \subset \mathbb{A}_K$ is open. If $x \in K \cap U$, then $\left|x_v\right|_v \le 1$ for all $v \nmid \infty$ implies that $x \in \mathcal{O}_K$, and $\left|x_v\right|_v < 1$ for all $v \mid \infty$ implies that $\left|\mathrm{N}_{K/\mathbb{Q}}(x)\right| < 1$, that is $x = 0$. So zero is isolated in K. Thus K is discrete. ☐

Let L/K be an extension of number fields. For all $v \in \mathrm{V}_K$, $K_v \hookrightarrow \prod_{w \mid v} L_w$ induces an inclusion of rings $\mathbb{A}_K \hookrightarrow \mathbb{A}_L$ visibly continuous. Lecture 9 Tuesday 09/02/21

Proposition 6.3. *Let $(a_1, \dots, a_n)$ be a K-basis for L. Consider*

$$\begin{array}{ccccc} \mathbb{A}_K^n & \xrightarrow{f} & \mathbb{A}_K \otimes_K L & \xrightarrow{g} & \mathbb{A}_L \\ \left(x^{(i)}\right)_{1 \le i \le n} & \longmapsto & \sum_i x^{(i)} \otimes a_i & \longmapsto & \sum_i a_i x^{(i)} \end{array},$$

viewing $x^{(i)} \in \mathbb{A}_K \hookrightarrow \mathbb{A}_L$ as above. Then g is a ring isomorphism, f is an $\mathbb{A}_K$-module isomorphism, and $g \circ f$ is a homeomorphism. This then defines a unique topology on $\mathbb{A}_K \otimes_K L$ such that g is an isomorphism of topological rings.

Proof. Since $L = \bigoplus_i K a_i \cong K^n$, f is an $\mathbb{A}_K$-module isomorphism. By definition, g is a ring homomorphism. So it suffices to prove $g \circ f$ is bijective, and that it maps $X^n = \left(K_\infty \times \widehat{\mathcal{O}_K}\right)^n$ homeomorphically to an open subgroup of $\mathbb{A}_L$. Note that multiplication by any $x \in K^\times$ is a self-homeomorphism of $\mathbb{A}_K$ with itself, since the inverse is multiplication by x^{-1}. Similarly for $\mathbb{A}_L$. So may replace (a_i) by non-zero K-multiples, so without loss of generality, $a_i \in \mathcal{O}_L$. Let

$$S = \left\{ v \in \mathrm{V}_{K,\mathrm{f}} \;\middle|\; v\left(\left(\mathcal{O}_L : \sum_i a_i \mathcal{O}_K\right)\right) > 0 \right\}$$

be a finite subset of $\mathrm{V}_{K,\mathrm{f}}$. Then for all $v \in \mathrm{V}_{K,\mathrm{f}} \setminus S$,

$$(a_i) : \mathcal{O}_{K_v}^n \xrightarrow{\sim} \mathcal{O}_{K_v} \otimes_{\mathcal{O}_K} \mathcal{O}_L \cong \prod_{w \mid v} \mathcal{O}_{L_w},$$

and for all $v \in S$, $\sum_i a_i \mathcal{O}_{K_v} = M_v$ is an open $\mathcal{O}_{K_v}$-submodule of $\prod_{w \mid v} \mathcal{O}_{L_w}$. Then

$$g \circ f : \left(K_\infty \times \widehat{\mathcal{O}_K}\right)^n \xrightarrow{\sim} L_\infty \times \prod_{v \notin S} \prod_{w \mid v} \mathcal{O}_{L_w} \times \prod_{v \in S} M_v$$

is a homeomorphism onto an open subgroup in $\mathbb{A}_L$. Moreover, for any finite $S' \supset S \cup \mathrm{V}_{K,\infty}$,

$$g \circ f : \mathrm{U}_{K,S'} = \left(\prod_{v \in S'} K_v \times \prod_{v \notin S'} \mathcal{O}_{K_v}\right)^n \xrightarrow{\sim} \prod_{w \mid v \in S'} L_w \times \prod_{w \mid v \notin S'} \mathcal{O}_{L_w}.$$

So $g \circ f$ is bijective. ☐

In particular, $\mathbb{A}_K = \mathbb{A}_\mathbb{Q} \otimes_\mathbb{Q} K$.

Corollary 6.4. *$\mathbb{A}_L$ is a free $\mathbb{A}_K$-module of rank $[L:K]$, and the diagram*

$$\begin{tikzcd} \prod_{w \mid v} L_w \arrow[r, hook] \arrow[d, "\sum_w \mathrm{Tr}_{L_w/K_v}"] & \mathbb{A}_L \arrow[d, "\mathrm{Tr}_{\mathbb{A}_L/\mathbb{A}_K}"] & \mathbb{A}_K \otimes_K L \arrow[l, "\sim"'] \arrow[d, "\mathrm{id} \otimes \mathrm{Tr}_{L/K}"] & L \arrow[l, hook'] \arrow[d, "\mathrm{Tr}_{L/K}"] \\ K_v \arrow[r, hook] & \mathbb{A}_K & \mathbb{A}_K \otimes_K K \arrow[l, "\sim"] & K \arrow[l, hook'] \end{tikzcd}$$

commutes, where the left hand inclusions are

$$(x_w)_{w \mid v} \mapsto (y_w), \qquad y_w = \begin{cases} x_w & w \mid v \\ 0 & \text{otherwise} \end{cases}.$$

Proof. Exercise. [5] ◻

Theorem 6.5. *$\mathbb{A}_K/K$ is compact Hausdorff.*

Proof. Since K is closed in $\mathbb{A}_K$ and $\mathbb{A}_K$ is Hausdorff, $\mathbb{A}_K/K$ is Hausdorff. By 6.3, $\mathbb{A}_K/K \cong (\mathbb{A}_\mathbb{Q}/\mathbb{Q})^{[K:\mathbb{Q}]}$ as topological groups, so may assume $K = \mathbb{Q}$. Let $X = [0,1] \times \widehat{\mathbb{Z}} \subset \mathbb{A}_\mathbb{Q}$. Then X is compact. So it is enough to show that $X + \mathbb{Q} = \mathbb{A}_\mathbb{Q}$, as then $X \twoheadrightarrow \mathbb{A}_\mathbb{Q}/\mathbb{Q}$. Let $x = (x_p)_{p \le \infty} \in \mathbb{A}_\mathbb{Q}$. Let

$$S = \{p < \infty \mid x_p \notin \mathbb{Z}_p\}$$

be a finite set. There exists $r_p \in \mathbb{Z}[1/p]$ such that $x_p - r_p \in \mathbb{Z}_p$ for all $p \in S$. Let $r = \sum_{p \in S} r_p \in \mathbb{Q}$. For all $p < \infty$, $x_p - r \in \mathbb{Z}_p$, that is $x - r \in \mathbb{R} \times \widehat{\mathbb{Z}}$, and then for suitable $m \in \mathbb{Z}$, $x - (r+m) \in [0,1] \times \widehat{\mathbb{Z}}$. ◻

From 6.3 also get $\mathbb{A}_K = K_\infty \times \widehat{K}$ where

$$\widehat{K} = \widehat{\mathcal{O}_K} \otimes_\mathbb{Z} \mathbb{Q} = \widehat{\mathcal{O}_K} \otimes_{\mathcal{O}_K} K,$$

where $\widehat{\mathcal{O}_K} \cong \prod_\mathfrak{p} \widehat{\mathcal{O}_{K,\mathfrak{p}}} = \prod_{v \nmid \infty} \mathcal{O}_{K_v}$ is the profinite completion of $\mathcal{O}_K$.

6.2 Ideles

Definition. The **idele group** of K is the group of units of $\mathbb{A}_K$,

$$\mathcal{J}_K = \mathbb{A}_K^\times = \left\{ (x_v) \in \prod_{v \in \mathrm{V}_K} K_v^\times \;\middle|\; \text{for all but finitely many finite } v,\ x_v \in \mathcal{O}_v^\times \right\} = \bigcup_{\text{finite } S \subset \mathrm{V}_{K,\mathrm{f}}} \mathcal{J}_{K,S},$$

where

$$\mathcal{J}_{K,S} = K_\infty^\times \times \prod_{v \in S} K_v^\times \times \prod_{v \in \mathrm{V}_{K,\mathrm{f}} \setminus S} \mathcal{O}_v^\times.$$

The topology on $\mathcal{J}_K$ is generated by open subsets of $\mathcal{J}_{K,S}$, as S varies, and $\mathcal{J}_{K,S}$ is given the product topology. In particular, $K_\infty^\times \times \prod_{v \nmid \infty} \mathcal{O}_v^\times$ is an open subgroup, and has the product topology.

Remark. $\mathcal{J}_K \hookrightarrow \mathbb{A}_K$ is continuous, by the definitions, but is not a homeomorphism onto its image, since $x \mapsto x^{-1}$ on $\mathbb{A}_K^\times$ is not continuous for the $\mathbb{A}_K$-topology, by example sheet 1 exercise 8, but

$$\begin{array}{rcl} \mathcal{J}_K & \longrightarrow & \mathbb{A}_K \times \mathbb{A}_K \\ x & \longmapsto & (x, x^{-1}) \end{array}$$

is a homeomorphism of $\mathcal{J}_K$ onto the closed subset $\{xy = 1\} \subset \mathbb{A}_K^2$. In geometry, $\mathrm{GL}_n K \subset \mathbb{A}^{n^2}$ and

$$\begin{array}{rcl} \mathrm{GL}_n K & \longrightarrow & \mathbb{A}^{n^2+1} \\ (a_{ij}) & \longmapsto & \left(a_{ij}, \det(a_{ij})^{-1}\right) \end{array}$$

has closed image.

Then $K^\times \hookrightarrow \mathcal{J}_K$ since if $x \in K^\times$ then $|x|_v = 1$ for all but finitely many v. The image is discrete, since $\mathcal{J}_K \hookrightarrow \mathbb{A}_K$ is continuous and $K \subset \mathbb{A}_K$ is discrete.

[5] Exercise

Lecture 10 Thursday 11/02/21

Definition. The **idele class group** of K is

$$\mathcal{C}_K = \mathcal{J}_K / K^\times.$$

This is a Hausdorff and locally compact topological group. There are two important homomorphisms.

Definition. Let $x = (x_v) \in \mathcal{J}_K$. Then for all v, $|x_v|_v \neq 0$, and for all but finitely many v, $|x_v|_v = 1$. So can define the **idele norm** homomorphism

$$\begin{array}{cccc} |\cdot|_{\mathbb{A}} & : & \mathcal{J}_K & \longrightarrow & \mathbb{R}_{>0} \\ & & (x_v) & \longmapsto & \prod_{v \in \mathrm{V}_K} |x_v|_v \end{array},$$

This is continuous, since the restriction to $\mathcal{J}_{K,S}$ is $\prod_v |\cdot|_v : \mathcal{J}_{K,S} \to \prod_{v \in S \cup \mathrm{V}_{K,\infty}} K_v^\times \to \mathbb{R}_{>0}$. Clearly $|\cdot|_{\mathbb{A}}$ is surjective, since $K_\infty^\times \subset \mathcal{J}_K$. A key fact is that for all $x \in K^\times$, $|x|_{\mathbb{A}} = 1$ by the product formula, so $|\cdot|_{\mathbb{A}} : \mathcal{J}_K \to \mathcal{C}_K \to \mathbb{R}_{>0}$.

Definition. Let

$$\mathcal{J}_K^1 = \{x \in \mathcal{J}_K \mid |x|_{\mathbb{A}} = 1\}, \qquad \mathcal{C}_K^1 = \mathcal{J}_K^1 / K^\times.$$

Proposition 6.6.

$$\mathcal{J}_K \cong \mathcal{J}_K^1 \times \mathbb{R}_{>0}, \qquad \mathcal{C}_K \cong \mathcal{C}_K^1 \times \mathbb{R}_{>0}.$$

Proof. Have $|\cdot|_{\mathbb{A}} : \mathcal{J}_K \twoheadrightarrow \mathbb{R}_{>0}$. Consider

$$\begin{array}{cccc} \mathrm{i} & : & \mathbb{R}_{>0} & \longrightarrow & K_\infty^\times \subset \mathcal{J}_K \\ & & x & \longmapsto & \left(x^{\frac{1}{n}}\right)_{v \mid \infty} \end{array}.$$

Because $|x|_v$ is the Euclidean AV if v is real and the square of modulus if v is complex, this homomorphism is a right inverse to $|\cdot|_{\mathbb{A}}$. So defines a splitting $\mathcal{J}_K \cong \mathcal{J}_K^1 \times \mathbb{R}_{>0}$. As $\mathrm{i}(\mathbb{R}_{>0}) \cap K^\times = \{1\}$, also have $\mathcal{C}_K \cong \mathcal{C}_K^1 \times \mathbb{R}_{>0}$. ☐

Recall $\mathfrak{p}_v$ is the prime ideal corresponding to a finite place v. Write v also for the corresponding normalised discrete valuation.

Definition. Let

$$\mathrm{I}(K) = \{\text{group of fractional ideals of } K\} \cong \{\text{free abelian group generated by } \mathrm{V}_{K,\mathrm{f}}\}.$$

The **content map** is

$$\begin{array}{cccc} \mathrm{c} & : & \mathcal{J}_K & \longrightarrow & \mathrm{I}(K) \\ & & (x_v) & \longmapsto & \prod_{v \in \mathrm{V}_{K,\mathrm{f}}} \mathfrak{p}_v^{v(x_v)} \end{array}.$$

This is a continuous homomorphism, for the discrete topology on $\mathrm{I}(K)$, since $\ker \mathrm{c} = \mathcal{J}_{K,\emptyset} = K_\infty^\times \times \prod_{v \nmid \infty} \mathcal{O}_v^\times$ is open. If $x \in K^\times$ then $\mathrm{c}(x)$ is the principal fractional ideal $\langle x \rangle$. So c descends to a homomorphism

$$\mathrm{c} : \mathcal{C}_K = \mathcal{J}_K / K^\times \to \mathrm{Cl}(K) = \mathrm{I}(K) / \mathrm{P}(K),$$

where $\mathrm{P}(K)$ is the group of principal fractional ideals. The image of the inclusion $K^\times \hookrightarrow \mathcal{J}_K$ is called the **subgroup of principal ideles**. Then c is clearly surjective, since $v : K_v^\times \twoheadrightarrow \mathbb{Z}$. So $\mathcal{C}_K \twoheadrightarrow \mathrm{Cl}(K)$. As $\mathrm{c} \circ \mathrm{i} : \mathbb{R}_{>0} \to \mathrm{Cl}(K)$ is zero, have a continuous surjection $\mathcal{C}_K^1 \twoheadrightarrow \mathrm{Cl}(K)$. Now prove that $\mathcal{C}_K^1 = \mathcal{J}_K^1 / K^\times$ is compact. A corollary is that $\mathrm{Cl}(K)$ is finite, since compact and discrete. The following is a variant.

Definition. Let $S \subset \mathrm{V}_{K,\mathrm{f}}$ be a finite subset, and let

$$\mathrm{I}^S(K) = \{\text{fractional ideals prime to } S\} = \{I \mid \forall v \in S,\ v(I) = 0\}.$$

Define

$$\begin{array}{cccc} \mathrm{c}^S & : & \mathcal{J}_K & \longrightarrow & \mathrm{I}^S(K) \\ & & (x_v) & \longmapsto & \prod_{v \in \mathrm{V}_{K,\mathrm{f}} \setminus S} \mathfrak{p}_v^{v(x_v)} \end{array}.$$

This will be useful later on.

7 Geometry of numbers

7.1 Minkowski's theorem

Classically, embed

$$\sigma : K \hookrightarrow K_\infty = \prod_{v|\infty} K_v \cong \mathbb{R}^{\mathrm{r}_1} \times \mathbb{C}^{\mathrm{r}_2} \cong \mathbb{R}^n,$$

and study the image $\sigma(I) \subset \mathbb{R}^n$ for I a fractional ideal.

Definition. Let U be a finite-dimensional real vector space. A **lattice** $\Lambda \subset U$ is a discrete subgroup such that U/Λ is compact.

Proposition 7.1. *A subgroup $\Lambda \subset U$ is a lattice if and only if $\Lambda = \bigoplus_{1 \le i \le n} \mathbb{Z} e_i$, where (e_i) is an $\mathbb{R}$-basis for U where $n = \dim_{\mathbb{R}} U$.*

Proof. Example sheet. ☐

Theorem 7.2 (Minkowski's theorem)**.** *Let $\Lambda \subset \mathbb{R}^n$ be a lattice, and let $\mu_\Lambda = \mathrm{meas}(\mathbb{R}^n/\Lambda)$, the **covolume** of Λ. Let $X \subset \mathbb{R}^n$ be a compact subset, which is*

- *convex, that is if $t \in [0,1]$ and $x, y \in X$ then $tx + (1-t)y \in X$, and*
- *symmetric about the origin, that is if $x \in X$ then $-x \in X$.*

If $\mathrm{meas}(X) > 2^n \mu_\Lambda$, then $X \cap \Lambda \neq \{0\}$.

Remark. $\mathbb{R}^n$ has a Lebesgue measure, and $\mathrm{meas}(X)$ is the measure of X. The Lebesgue measure defines a measure on $\mathbb{R}^n/\Lambda$, and μ_Λ is the measure of $\mathbb{R}^n/\Lambda$. Naively, if $\Lambda = \bigoplus_i \mathbb{Z} e_i$ for (e_i) linearly independent over $\mathbb{R}$ and $\mathcal{P} = \{\sum_i x_i e_i \mid 0 \le x_i < 1\}$, then $\mathcal{P}$ is a set of coset representatives for $\Lambda \subset \mathbb{R}^n$, and $\mu_\Lambda = \mathrm{meas}(\mathcal{P}) = |\det(e_{ij})|$, which is independent of the basis.

Proof. Let $\pi : \mathbb{R}^n \to \mathbb{R}^n/2\Lambda$. Then

$$\mathrm{meas}(\pi(X)) \le \mathrm{meas}(\mathbb{R}^n/2\Lambda) = 2^n \mathrm{meas}(\mathbb{R}^n/\Lambda) < \mathrm{meas}(X).$$

So $X \to \pi(X)$ is not one-to-one, so there exists $x \neq y$ in X such that $x - y = 2\lambda \in 2\Lambda$. Then $0 \neq \lambda = (x-y)/2 = \frac{1}{2}x + \frac{1}{2}(-y) \in X$ as $-y \in X$, by symmetry, and X is convex. ☐

Theorem 7.3. *There exists a constant $\mathrm{r}_K > 0$ such that, if $(d_v)_{v \in K}$ are positive reals with*

- *$d_v \in |K_v^\times|_v = \{|x|_v \mid x \in K_v^\times\} \subset \mathbb{R}_{>0}$ for all v,*
- *$d_v = 1$ for all but finitely many v, and*
- *$\prod_{v \in \mathrm{V}_K} d_v > \mathrm{r}_K$,*

then $\{x \in K \mid \forall v,\ |x|_v \le d_v\} \neq \{0\}$.

Proof. For $v \nmid \infty$, write $d_v = \mathrm{q}_v^{-n_v}$ for $n_v \in \mathbb{Z}$. Let

$$I = \{x \in K \mid \forall v \nmid \infty,\ |x|_v \le d_v\} = \prod_v \mathfrak{p}_v^{n_v}$$

be a fractional ideal of K. Then $mI \subset \mathcal{O}_K$ for $m > 0$, so

$$\mu_{\sigma(I)} = m^{-n} \mu_{\sigma(mI)} = m^{-n} \mu_{\sigma(\mathcal{O}_K)} (\sigma(\mathcal{O}_K) : \sigma(mI)) = m^{-n} \mu_{\sigma(\mathcal{O}_K)} \mathrm{N}(mI) = \mu_{\sigma(\mathcal{O}_K)} \prod_v \mathrm{q}_v^{n_v}, \tag{4}$$

and $\sigma(I)$ is a lattice in $\mathbb{R}^n$, by the non-vanishing of the discriminant. Let

$$X = \left\{ x \in \prod_{v \in \infty} K_v \cong \mathbb{R}^n \;\middle|\; \forall v,\ |x_v|_v \le d_v \right\} = \prod_{v \text{ real}} [-d_v, d_v] \times \prod_{v \text{ complex}} \left\{ |z|^2 \le d_v \right\} \subset K_\infty \cong \mathbb{R}^{\mathrm{r}_1} \times \mathbb{C}^{\mathrm{r}_2}.$$

This is convex, compact, symmetric, and

$$\operatorname{meas}(X) = 2^{\mathrm{r}_1}\pi^{\mathrm{r}_2}\prod_{v\mid\infty} d_v > 2^n \prod_{v\nmid\infty} d_v^{-1}\mu_{\sigma(\mathcal{O}_K)} = 2^n\mu_{\sigma(I)},$$

by (4), provided

$$\prod_v d_v > \mathrm{r}_K = \left(\frac{4}{\pi}\right)^{\mathrm{r}_2}\mu_{\sigma(\mathcal{O}_K)} = \left(\frac{2}{\pi}\right)^{\mathrm{r}_2}\left|\mathrm{d}_K\right|^{\frac{1}{2}}.$$

Then applying 7.2, $X \cap \sigma(I) \ne \{0\}$ and any $x \in X \cap \sigma(I)$ has $|x|_v \le d_v$ for all v. □

This is the translation of a classical result that if $0 \ne I$ is an ideal then there exists $x \in I \setminus \{0\}$ such that $\left|\mathrm{N}_{K/\mathbb{Q}}(x)\right| < \mathrm{r}_K\mathrm{N}(I)$.

Lecture 11
Saturday
13/02/21

Remark. Used Minkowski's theorem, with convex symmetric set $X = [-d_v, d_v]^{\mathrm{r}_1} \times \left\{|z|^2 \le d_v\right\}^{\mathrm{r}_2}$ and obtained $\mathrm{r}_K = \left(\frac{4}{\pi}\right)^{\mathrm{r}_2}\mu_{\sigma(\mathcal{O}_K)}$. Using better chosen X, can get a better bound, the Minkowski bound c_K, which is useful for computation.

7.2 Compactness of $\mathcal{C}_K^1$

Recall $K^\times \subset \mathcal{J}_K^1 = \ker\left(|\cdot|_{\mathbb{A}} : \mathcal{J}_K \to \mathbb{R}_{>0}\right)$ is discrete. Based on 7.3 and the following.

Proposition 7.4. *Let $\rho_v > 0$ for $v \in \mathrm{V}_K$, with $\rho_v = 1$ for all but finitely many v. Then*

$$X = \left\{x \in \mathcal{J}_K^1 \;\middle|\; \forall v,\ |x_v|_v \le \rho_v\right\}$$

is compact.

This is false for $\mathcal{J}_K$. Note that $|x_v|_v \le \rho_v$ for all v defines a compact subset of $\mathbb{A}_K$.

Proof. Let $R = \prod_v \rho_v$, and let

$$S = \mathrm{V}_{K,\infty} \cup \{v \mid \rho_v \ne 1\} \cup \{v \in \mathrm{V}_{K,\mathrm{f}} \mid \mathrm{q}_v \le R\}$$

be a finite set of places, since the last set is contained in $\{v \mid p \mid p \le R\}$, which is finite. If $v \notin S$, and $x \in X$, since $\rho_v = 1$,

$$1 \ge |x_v|_v = \prod_{w \ne v} |x_w|_w^{-1} \ge \prod_{w \ne v} \rho_w^{-1} = R^{-1}.$$

As $\mathrm{q}_v > R$, this forces $|x_v|_v = 1$. So $X = X' \times \prod_{v \notin S}\mathcal{O}_v^\times$, where

$$X' = \left\{(x_v) \in \prod_{v\in S} K_v^\times \;\middle|\; \prod_{v \in S}|x_v|_v = 1,\ \forall v \in S,\ |x_v|_v \le \rho_v\right\},$$

which is a closed subset of

$$X'' = \left\{(x_v) \in \prod_{v \in S} K_v^\times \;\middle|\; \forall v \in S,\ \frac{\rho_v}{R} \le |x_v|_v \le \rho_v\right\},$$

which is compact. So X' is compact, hence so is X, since $\prod_{v\notin S}\mathcal{O}_v^\times$ is compact. □

Theorem 7.5. *$\mathcal{C}_K^1 = \mathcal{J}_K^1/K^\times$ is compact.*

Proof. Let r_K be as in 7.3. Pick any $y \in \mathcal{J}_K$ with $|y|_{\mathbb{A}} > \mathrm{r}_K$, and let

$$X = \left\{x \in \mathcal{J}_K^1 \;\middle|\; \forall v \in \mathrm{V}_K,\ |x_v|_v \le |y_v|_v\right\},$$

which is compact by 7.4. Show that

$$\mathcal{J}_K^1 = K^\times X = \left\{ax \;\middle|\; a \in K^\times,\ x \in X\right\}.$$

Let $z \in \mathcal{J}_K^1$. Then $\prod_v |y_v z_v|_v = |y|_{\mathbb{A}} > \mathrm{r}_K$. So by 7.3, there exists $b \in K^\times$ such that for all $v \in \mathrm{V}_K$, $|b|_v \le |y_v z_v|_v$. Therefore $bz^{-1} \in X$, that is $z^{-1} \in b^{-1}X \subset K^\times X$. □

7.3 Finiteness of $\mathrm{Cl}(K)$ and S-unit theorem

The following are two corollaries.

Corollary 7.6. *The ideal class group* $\mathrm{Cl}(K)$ *is finite.*

Proof. $\mathcal{C}_K^1 \twoheadrightarrow \mathrm{Cl}(K)$ by the content map, which is continuous, so $\mathrm{Cl}(K)$ is discrete and compact, therefore finite. ☐

Corollary 7.7 (S-unit theorem)**.** *Let* $S \subset \mathrm{V}_{K,\mathrm{f}}$ *be finite, possibly empty, and let*

$$\mathcal{O}_{K,S} = \{x \in K \mid \forall v \in \mathrm{V}_{K,\mathrm{f}} \setminus S,\ |x|_v \le 1\}$$

be the ***S-integers*** *of* K*, sometimes written* $\mathcal{O}_K[1/S]$*. Then*

$$\mathcal{O}_{K,S}^\times = \mu(K) \times \mathbb{Z}^{\mathrm{r}_1+\mathrm{r}_2-1+\#S},$$

where $\mu(K) = \{$*roots of unity in* $K\}$ *is finite.*

The case $S = \emptyset$ is Dirichlet's unit theorem,

$$\mathcal{O}_K^\times = \mu(K) \times \mathbb{Z}^{\mathrm{r}_1+\mathrm{r}_2-1}.$$

Proof.

- First explain the proof for $S = \emptyset$. Recall

$$\mathcal{J}_{K,\emptyset} = K_\infty^\times \times \prod_{v \nmid \infty} \mathcal{O}_v^\times \supset \mathcal{J}_{K,\emptyset}^1 = K_\infty^{\times,1} \times \prod_{v\nmid\infty} \mathcal{O}_v^\times, \qquad K_\infty^{\times,1} = \left\{ (x_v) \in K_\infty^\times \;\middle|\; \prod_{v\mid\infty} |x_v|_v = 1 \right\}.$$

  Then $\mathcal{J}_{K,\emptyset} \cap K^\times = \mathcal{J}_{K,\emptyset}^1 \cap K^\times = \mathcal{O}_K^\times$ is discrete in $\mathcal{J}_{K,\emptyset}^1$ and by 7.5, the closed $\mathcal{J}_{K,\emptyset}^1 / \mathcal{O}_K^\times \subset \mathcal{C}_K^1$ is compact. Let

$$\begin{array}{cccc} \lambda & : & \mathcal{J}_{K,\emptyset} & \longrightarrow & \mathcal{L}_K = \prod_{v\mid\infty} \mathbb{R} \cong \mathbb{R}^{\mathrm{r}_1+\mathrm{r}_2} \\ & & (x_v)_v & \longmapsto & (\log|x_v|_v)_v \end{array}$$

  be the **logarithm map**, such that

$$\lambda\left(\mathcal{J}_{K,\emptyset}^1\right) \subset \mathcal{L}_K^0 = \left\{ (l_v) \in \mathcal{L}_K \;\middle|\; \sum_v l_v = 0 \right\}.$$

  Then

$$\ker\lambda = \{(x_v) \in \mathcal{J}_K \mid \forall v,\ |x_v|_v = 1\} = \{\pm 1\}^{\mathrm{r}_1} \times \mathrm{U}(1)^{\mathrm{r}_2} \times \prod_{v\nmid\infty} \mathcal{O}_v^\times, \qquad \mathrm{U}(1) = \{z \in \mathbb{C} \mid |z| = 1\}$$

  is compact. So $\ker\lambda \cap \mathcal{O}_K^\times$ is discrete and compact, hence finite. Obviously $\mu(K) \subset \ker\lambda$, so $\mu(K)$ is finite and equals $\ker\lambda \cap \mathcal{O}_K^\times$. Next, show $\lambda\left(\mathcal{O}_K^\times\right) \subset \mathcal{L}_K^0 \cong \mathbb{R}^{\mathrm{r}_1+\mathrm{r}_2-1}$ is a lattice. Then we get

$$1 \to \mu(K) \to \mathcal{O}_K^\times \to \lambda\left(\mathcal{O}_K^\times\right) \cong \mathbb{Z}^{\mathrm{r}_1+\mathrm{r}_2-1} \to 0,$$

  which gives 7.7. Now

$$\begin{array}{ccc} \mathcal{J}_{K,\emptyset} & \cong & \prod_{v\mid\infty} \mathbb{R}_{>0} \times \ker\lambda \\ \Big\downarrow{\scriptstyle\lambda} & & \Big\downarrow{\scriptstyle\pi_1} \\ \mathcal{L}_K & \xleftarrow[\log]{\sim} & \prod_{v\mid\infty} \mathbb{R}_{>0} \end{array},$$

where $\mathbb{R}_{>0} \hookrightarrow K_v^\times \subset \mathbb{C}^\times$ for all $v \mid \infty$. Hence λ has the property that for all compact Y in its target, $\lambda^{-1}(Y)$ is compact, so λ is a proper map. A simple fact is if $f : X \to Y$ is a continuous proper map of topological spaces, with Y locally compact and Hausdorff, then if $Z \subset X$ is discrete then $f(Z)$ is discrete. [6] Hence $\lambda\left(\mathcal{O}_K^\times\right) \subset \mathcal{L}_K^0$ is discrete. Finally,

$$\lambda : \mathcal{J}_{K,\emptyset}^1 / \mathcal{O}_K^\times \twoheadrightarrow \mathcal{L}_K^0 / \lambda\left(\mathcal{O}_K^\times\right),$$

so $\mathcal{L}_K^0 / \lambda(\mathcal{O}_K)$ is compact, by 7.5. Thus $\lambda(\mathcal{O}_K)$ is a lattice. Lecture 12 Tuesday 16/02/21

- For the general case, the difference is mainly notational. Let $S_\infty = S \cup \mathrm{V}_{K,\infty}$, so

$$\mathcal{J}_{K,S} = \prod_{v \in S_\infty} K_v^\times \times \prod_{v \notin S_\infty} \mathcal{O}_v^\times, \qquad \mathcal{L}_{K,S} = \prod_{v \mid \infty} \mathbb{R} \times \prod_{v \in S} \log \mathrm{q}_v \mathbb{Z} \cong \mathbb{R}^{\mathrm{r}_1 + \mathrm{r}_2} \times \mathbb{Z}^{\# S}.$$

Let

$$\begin{array}{rccc} \lambda_S & : & \mathcal{J}_{K,S} & \longrightarrow & \mathcal{L}_{K,S} \\ & & (x_v)_v & \longmapsto & (\log|x_v|_v)_{v \in S_\infty} \end{array}$$

be the S**-logarithm map**, such that

$$\lambda_S\left(\mathcal{J}_{K,S}^1\right) \subset \mathcal{L}_{K,S}^0 = \left\{ (l_v) \in \mathcal{L}_{K,S} \;\middle|\; \sum_v l_v = 0 \right\}.$$

Note that $\mathcal{L}_{K,S}^0 \cong \mathbb{R}^{\mathrm{r}_1 + \mathrm{r}_2 - 1} \times \mathbb{Z}^{\# S}$ since

$$\begin{tikzcd} \mathcal{L}_{K,S}^0 \arrow[r, two heads, "\pi_2"] & \prod_{v \in S} \log \mathrm{q}_v \mathbb{Z} \arrow[d, phantom, "\cong" rotate=90] \\ & \mathbb{Z}^{\# S} \arrow[ul, dashed] \end{tikzcd}$$

is surjective with kernel $\mathbb{R}^{\mathrm{r}_1 + \mathrm{r}_2 - 1}$, so there exists a splitting as $\mathbb{Z}^{\# S}$ is free. Then

$$\ker \lambda_S \cong \{\pm 1\}^{\mathrm{r}_1} \times \mathrm{U}(1)^{\mathrm{r}_2} \times \prod_{v \in \mathrm{V}_{K,\mathrm{f}}} \mathcal{O}_v^\times,$$

as before, and

$$\mathcal{J}_{K,S} = \prod_{v \mid \infty} \mathbb{R}_{>0} \times \prod_{v \in S} \langle \pi_v \rangle \times \ker \lambda_S \cong \prod_{v \mid \infty} \mathbb{R}_{>0} \times \mathbb{Z}^{\# S} \times \ker \lambda_S,$$

where $\pi_v \in K_v^\times$ such that $v(\pi_v) = 1$, so λ_S is proper and surjective, so $\mathcal{J}_{K,S} \cap K^\times = \mathcal{J}_{K,S}^1 \cap K^\times = \mathcal{O}_{K,S}^\times$ is discrete and closed in $\mathcal{J}_{K,S}^1$. As before, $\ker \lambda_S \cap \mathcal{O}_{K,S}^\times = \mu(K)$, since it is discrete and compact, and $\lambda_S\left(\mathcal{O}_{K,S}^\times\right) \subset \mathcal{L}_{K,S}^0$ is discrete and cocompact. Then prove that if $G \cong \mathbb{R}^m \times \mathbb{Z}^{\# S} \supset H$ is a discrete and cocompact subgroup then $H \cong \mathbb{Z}^{m + \# S}$. [7] Then

$$1 \to \mu(K) \to \mathcal{O}_{K,S}^\times \to \lambda_S\left(\mathcal{O}_{K,S}^\times\right) \cong \mathbb{Z}^{\mathrm{r}_1 + \mathrm{r}_2 - 1 + \# S} \to 0,$$

and so done.

$\square$

Let $T \subset \mathrm{V}_K$ be finite, not necessarily containing $\mathrm{V}_{K,\infty}$. What can we say about the group

$$\left\{ x \in K^\times \;\middle|\; \forall v \notin T,\ |x|_v = 1 \right\}?$$

The answer is non-trivial and depends on K. See example sheet.

[6] Exercise: a hint is to take a compact neighbourhood V of some $f(z)$ for $z \in Z$ and use compactness of $f^{-1}(V)$

[7] Exercise

7.4 Strong approximation theorem

Earlier, weak approximation implies that K is dense in any finite product of K_v's. Also, $K \hookrightarrow \mathbb{A}_K$ is discrete.

Theorem 7.8 (Strong approximation). *Let $T \subset \mathrm{V}_K$ be finite, and set*

$$\mathbb{A}_K^T = \left\{ x = (x_v) \in \prod_{v \notin T} K_v \;\middle|\; \text{for all but finitely many } v,\ |x_v|_v \le 1 \right\},$$

so $\mathbb{A}_K = \prod_{v \in T} K_v \times \mathbb{A}_K^T$, with the adelic topology. Then if $T \ne \emptyset$, then K is dense in $\mathbb{A}_K^T$.

There are various ways to rewrite this.

- If $T \ne \emptyset$, then $K + \prod_{v \in T} K_v$ is dense in $\mathbb{A}_K$, where $K \hookrightarrow \mathbb{A}_K$ is the diagonal inclusion and $K_v \subset \mathbb{A}_K$ by
$$y \mapsto (x_w), \qquad x_w = \begin{cases} y & w = v \\ 0 & w \ne v \end{cases}.$$

It is enough to prove 7.8 for $T = \{v_0\}$. Will actually prove the following.

- Let $S \subset \mathrm{V}_K$ be finite such that $v_0 \notin S$, let $y_v \in K_v$ for all $v \in S$, and let $\epsilon > 0$. Then there exists $x \in K$ such that
  - for all $v \in S$, $|x - y_v|_v \le \epsilon$, and
  - for all $v \notin S$ such that $v \ne v_0$, $|x|_v \le 1$.

Take $y \in \mathbb{A}_K$ with component y_v at $v \in S$ and zero elsewhere. This is equivalent to strong approximation for $T = \{v_0\}$, by definition of the topology.

Proof. Free to enlarge S. Then by the proof of compactness of $\mathbb{A}_K/K$, there exists $R > 0$ such that if

$$X = \left\{ (x_v) \in \mathbb{A}_K \;\middle|\; \begin{array}{l} \forall v \in S,\ |x_v|_v \le R \\ \forall v \notin S,\ |x_v|_v \le 1 \end{array} \right\},$$

then $X + K = \mathbb{A}_K$. For example, assume $S \supset \mathrm{V}_{K,\infty}$ and let $\mathcal{O}_K = \bigoplus_i \mathbb{Z} e_i$, then $\mathbb{A}_K = \bigoplus_i \mathbb{A}_{\mathbb{Q}} e_i$ and $\mathbb{A}_{\mathbb{Q}} = [0,1] \times \widehat{\mathbb{Z}} + \mathbb{Q}$. Claim that there exists $z \in K \setminus \{0\}$ such that

$$|z|_v \le \begin{cases} \dfrac{\epsilon}{R} & v \in S \\ 1 & v \notin S,\ v \ne v_0 \end{cases}.$$

Apply Minkowski 7.3 with

- $d_v = 1$ for all $v \notin S \cup \{v_0\}$,
- $d_v \le \epsilon / R$ for all $v \in S$, and
- $d_{v_0} > \mathrm{r}_K \left(\prod_{v \in S} d_v \right)^{-1}$.

This defines a box in $\mathbb{A}_K$ whose intersection with K is not $\{0\}$, since $\prod_v d_v > \mathrm{r}_K$. Now write $z^{-1} y = a + t$ for $a \in X$ and $t \in K$. Then $x = zt = y - za$ has

$$|x - y_v|_v = |zt - y_v|_v = |z a_v|_v \le \begin{cases} \dfrac{\epsilon}{R} \cdot R = \epsilon & v \in S \\ 1 \cdot 1 = 1 & v \notin S,\ v \ne v_0 \end{cases},$$

so done. ☐

In the special case $T = \mathrm{V}_{K,\infty}$, $\mathbb{A}_K^T$ are the finite adeles. Then 7.8 says

$$K \hookrightarrow \mathbb{A}_K^T = \widehat{K} = \widehat{\mathcal{O}_K} \otimes_{\mathbb{Z}} \mathbb{Q}$$

is dense, which is equivalent to the density of

$$\mathcal{O}_K \hookrightarrow \widehat{\mathcal{O}_K} = \prod_{v \nmid \infty} \mathcal{O}_{K_v} = \prod_{v \nmid \infty} \varprojlim_r \mathcal{O}_K / \mathfrak{p}_v^r \cong \varprojlim_{I \subset \mathcal{O}_K} \mathcal{O}_K / I,$$

by CRT. So strong approximation is a generalisation of CRT.

8 Idele class group and class field theory

Lecture 13 Thursday 18/02/21

Recall if $L = \mathbb{Q}(\zeta_m)$, then there is an isomorphism

$$\begin{array}{rcl} \mathrm{Gal}(L/\mathbb{Q}) & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^\times \\ \sigma_p & \longmapsto & p \mod m \end{array}, \qquad p \nmid m,$$

given by the action on ζ_m. In particular, σ_p depends only on the congruence class of $p \mod m$, which implies quadratic reciprocity. As σ_p determines the decomposition of $\langle p\rangle$ in L, since $\mathrm{f}(v \mid p) = \mathrm{ord}\,\mathrm{D}_v = \mathrm{ord}\,\sigma_p$, this says that the decomposition of $\langle p\rangle$ in L depends only on $p \mod m$. A consequence is if $g \in \mathrm{Gal}(L/\mathbb{Q})$, then there exist infinitely many p such that $g = \sigma_p$, by Dirichlet's theorem on primes in arithmetic progressions. The following is a general problem. Let L/K be a Galois extension of number fields, and let v be a finite place of K, unramified in L. Then

$$\Sigma_v = \{\sigma_w \mid w \in \mathrm{V}_{L,\mathrm{f}},\ w \mid v\}$$

is a conjugacy class in $G = \mathrm{Gal}(L/K)$, and Σ_v describes the decomposition of v in L.

- How does Σ_v depend on v?
- Can it be any conjugacy class in G?

For the first question, do not know the answer for general L/K. This is non-abelian class field theory or the Langlands programme. The second question is answered by the Chebotarev density theorem in the 1920s. Let $C \subset G$ be a conjugacy class. Then there exist infinitely many v for which $C = \Sigma_v$.

Example. Let $C = \{1\}$. There exist infinitely many v such that $\Sigma_v = \{1\}$, that is such that v splits completely in L/K.

Class field theory answers the first question completely for L/K abelian.

8.1 Artin reciprocity law

Theorem (Artin reciprocity law)**.** *Let L/K be an abelian extension of number fields. Then there exists a unique continuous homomorphism*

$$\mathrm{Art}_{L/K} : \mathcal{C}_K = \mathcal{J}_K/K^\times \to \mathrm{Gal}(L/K),$$

such that for all unramified $v \in \mathrm{V}_{K,\mathrm{f}}$,

$$\begin{array}{rcrcl} \mathrm{Art}_{L/K} & : & K_v^\times \hookrightarrow \mathcal{C}_K & \longrightarrow & \mathrm{Gal}(L/K) \\ & & x & \longmapsto & \sigma_v^{-v(x)} \end{array}.$$

Moreover, $\mathrm{Art}_{L/K}$ *is surjective with kernel* $K^\times \mathrm{N}_{L/K}(\mathcal{J}_L)$.

How does this generalise the cyclotomic theory? Since $\mathbb{C}^\times$ is connected, the only open subgroup is $\mathbb{C}^\times$, and the only open subgroups of $\mathbb{R}^\times$ are $\mathbb{R}^\times$ and $\mathbb{R}_{>0}$. Then $\ker \mathrm{Art}_{L/K}$ is open, so contains some $K^\times U$, where

$$U = \prod_{v \text{ complex}} K_v^\times \times \prod_{v \text{ real}} \mathbb{R}_{>0} \times \prod_{v \in S} U_v \times \prod_{v \in \mathrm{V}_{K,\mathrm{f}} \setminus S} \mathcal{O}_v^\times, \qquad U_v = \left\{x \in \mathcal{O}_v^\times \mid v(x-1) \ge m_v\right\}, \qquad m_v > 0,$$

where say S contains all ramified places. If $w \notin S$ is unramified,

$$\mathrm{Art}_{L/K} : K^\times\left(\dots, 1, 1, \pi_w^{-1}, 1, 1, \dots\right) = K^\times(\dots, \pi_w, \pi_w, 1, \pi_w, \pi_w, \dots) \mapsto \sigma_w,$$

where $\pi_w \in \mathcal{O}_K$ such that $w(\pi_w) = 1$ is a uniformiser at w. So if

1. $\sigma(\pi_w) > 0$ for all $\sigma : K \hookrightarrow \mathbb{R}$,
2. $v(\pi_w - 1) \ge m_v$ for all $v \in S$, and
3. $\pi_w \in \mathcal{O}_v^\times$ for all $v \notin S$ such that $v \ne w$,

which are congruence conditions on w, then $\sigma_w = 1$. In particular, if $\mathfrak{p}_w = \langle \pi_w\rangle$ is principal, then 3 is automatic. So just a congruence condition on π_w modulo some ideal divisible only by primes in S, and positivity.

Example. Let $L = \mathbb{Q}(\zeta_m)/K = \mathbb{Q}$. Then

$$\begin{tikzcd}
\left(\mathbb{R}^\times \times \widehat{\mathbb{Q}}^\times\right)/\mathbb{Q}^\times \arrow[d, phantom, "\wr"] & \left(\mathbb{R}^\times \times \widehat{\mathbb{Z}}^\times\right)/\{\pm 1\} \arrow[l, "\sim"'] \arrow[d, phantom, "\wr"] & \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times \arrow[l, "\sim"'] \arrow[r] \arrow[d] & \prod_{q \mid m} \mathbb{Z}_q^\times \arrow[d] \\
\mathcal{J}_{\mathbb{Q}}/\mathbb{Q}^\times \arrow[dr, dashed] & \mathcal{J}_{\mathbb{Q},\emptyset}/\{\pm 1\} \arrow[l, "\sim"] & (\mathbb{Z}/m\mathbb{Z})^\times \arrow[dl, "\sim"] & \prod_{q \mid m} \left(\mathbb{Z}_q/q\mathbb{Z}_q\right)^\times \arrow[l, "\sim"] \\
& \mathrm{Gal}(L/\mathbb{Q}) & &
\end{tikzcd}.$$

Claim this is $\mathrm{Art}_{L/\mathbb{Q}}$. Let $\mathbb{Q}^\times\left(\dots, 1, 1, p^{-1}, 1, 1, \dots\right) = \mathbb{Q}^\times(\dots, p, p, 1, p, p, \dots) \in \mathcal{J}_{\mathbb{Q}}/\mathbb{Q}^\times$ for $p \nmid m$. Then

$$\begin{array}{ccccccc} \mathcal{J}_{\mathbb{Q}}/\mathbb{Q}^\times & \longleftarrow & \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^\times & \longrightarrow & \mathrm{Gal}(L/\mathbb{Q}) \\ \mathbb{Q}^\times(\dots, p, p, 1, p, p, \dots) & \longleftarrow\!\shortmid & (\dots, p, p, 1, p, p, \dots) & \longmapsto & p \mod m & \longmapsto & \sigma_p \end{array}.$$

So via $\mathcal{J}_{\mathbb{Q}}/\mathbb{Q}^\times \cong \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times$, $\mathrm{Art}_{L/\mathbb{Q}}$ is just the cyclotomic map.

8.2 Finite quotients of $\mathcal{C}_K$

Proposition 8.1. *Let G be a discrete group.*

1. *Any continuous homomorphism $\alpha : \mathcal{C}_K \to G$ has finite image.*
2. *There is a bijection*

$$\left\{ \begin{array}{c} \text{continuous homomorphisms} \\ \alpha : \mathcal{J}_K \to G \end{array} \right\} \qquad \leftrightsquigarrow \qquad \left\{ \begin{array}{c} \text{families } \left(\alpha_v : K_v^\times \to G\right)_{v \in \mathrm{V}_K} \\ \text{such that } \alpha_v\left(\mathcal{O}_v^\times\right) = \{1\} \\ \text{for all but finitely many } v \in \mathrm{V}_{K,\mathrm{f}} \end{array} \right\}.$$

Notation. $\alpha_v : K_v^\times \to G$ is **unramified** if $\alpha_v\left(\mathcal{O}_v^\times\right) = \{1\}$. See local class field theory, where $\mathcal{O}_v^\times$ corresponds to the inertia.

Proof.

1. $\mathcal{J}_K \cong \mathbb{R}_{>0} \times \mathcal{J}_K^1$, and $\alpha(\mathbb{R}_{>0}) = \{1\}$ so $\alpha(\mathcal{C}_K) = \alpha\left(\mathcal{C}_K^1\right)$, which is compact and discrete so finite.
2. The subgroup
$$\bigoplus_v K_v^\times = \{(x_v) \mid x_v = 1 \text{ for all but finitely many } v\} \subset \mathcal{J}_K$$
is dense, since $\bigoplus_v \mathcal{O}_v^\times \subset \prod_v \mathcal{O}_v^\times$ is dense for the product topology. So a continuous $\alpha : \mathcal{J}_K \to G$ is determined by its restrictions $\alpha_v = \alpha|_{K_v^\times} : K_v^\times \to G$. As $\ker \alpha$ is open, $\alpha_v\left(\mathcal{O}_v^\times\right) = \{1\}$ for all but finitely many v. So have $\{\alpha\} \hookrightarrow \{(\alpha_v)_v\}$. Conversely, if $(\alpha_v : K_v^\times \to G)_v$ is such a family, then $\alpha((x_v)) = \prod_v \alpha_v(x_v)$ is a finite product for any $(x_v) \in \mathcal{J}_K$, as $x_v \in \mathcal{O}_v^\times$ and $\alpha_v\left(\mathcal{O}_v^\times\right) = \{1\}$ for all but finitely many v, and defines a continuous homomorphism $\alpha : \mathcal{J}_K \to G$.

∎

Lecture 14 Saturday 20/02/21

Proposition 8.2. *Let $\alpha, \alpha' : \mathcal{C}_K \to G$ be continuous homomorphisms, where G is finite, unramified at all $v \in \mathrm{V}_{K,\mathrm{f}} \setminus S$, where S is finite. Then if $\alpha_v = \alpha'_v$ for all $v \notin S$ such that v is finite, that is $\alpha_v(\pi_v) = \alpha'_v(\pi_v)$, have $\alpha = \alpha'$.*

Proof. Look at α/α', so without loss of generality $\alpha' = 1$. Then $\alpha : \mathcal{J}_K/K^\times \to G$ satisfies for all $v \in \mathrm{V}_{K,\mathrm{f}} \setminus S$, $\alpha_v = 1$. Let $w \in S_\infty = \mathrm{V}_{K,\infty} \cup S$ and $y \in K_w^\times$. Then by weak approximation, for any $\epsilon > 0$, there exists $x \in K^\times$ such that $|x - y|_w < \epsilon$ and $|x - 1|_v < \epsilon$ for all $v \in S_\infty \setminus \{w\}$. Hence $\alpha_v(x) = 1$ for all $v \in S_\infty \setminus \{w\}$, so $\alpha_v(x) = 1$ for all $v \neq w$. Since $\alpha(K^\times) = 1$, $\alpha_w(x) = 1$, so $\alpha_w(y) = 1$. So $\alpha_w = 1$, so $\alpha = 1$. ∎

Definition. A **modulus** is a finite formal sum

$$\mathfrak{m} = \sum_{v \in \mathrm{V}_K} \mathrm{m}_v (v), \qquad \mathrm{m}_v \geq 0.$$

The **support** and **finite support** of $\mathfrak{m}$ are

$$\operatorname{supp} \mathfrak{m} = \{v \in \mathrm{V}_K \mid \mathrm{m}_v > 0\}, \qquad \operatorname{supp}_{\mathrm{f}} \mathfrak{m} = \operatorname{supp} \mathfrak{m} \cap \mathrm{V}_{K,\mathrm{f}}.$$

We may use also $\mathfrak{m}_{\mathrm{f}} = \sum_{v \in \mathrm{V}_{K,\mathrm{f}}} \mathrm{m}_v (v)$, the finite part of $\mathfrak{m}$, can think of as an ideal of $\mathcal{O}_K$. Define

$$\mathrm{U}_{K,\mathfrak{m}} = \prod_{v \in \mathrm{V}_K} \mathrm{U}_v^{\mathrm{m}_v}, \qquad K_v^\times \supset \mathrm{U}_v^m = \begin{cases} \mathcal{O}_v^\times & v \in \mathrm{V}_{K,\mathrm{f}}, \ m = 0 \\ 1 + \pi_v^m \mathcal{O}_v & v \in \mathrm{V}_{K,\mathrm{f}}, \ m > 0 \\ \mathbb{R}^\times & v \text{ real}, \ m = 0 \\ \mathbb{R}_{>0} & v \text{ real}, \ m > 0 \\ \mathbb{C}^\times & v \text{ complex} \end{cases}.$$

Note that in the definition of the modulus, we may as well forget about v complex, and for v real, take $\mathrm{m}_v \in \{0, 1\}$. Then $\mathrm{U}_{K,\mathfrak{m}} \subset \mathcal{J}_K$ is an open subgroup, and every open subgroup of $\mathcal{J}_K$ contains some $\mathrm{U}_{K,\mathfrak{m}}$.

Proposition 8.3. *$\mathcal{J}_K / K^\times \mathrm{U}_{K,\mathfrak{m}}$ is finite.*

Proof. $\mathcal{J}_K / K^\times \to \mathcal{J}_K / K^\times \mathrm{U}_{K,\mathfrak{m}}$ with discrete image, since $\mathrm{U}_{K,\mathfrak{m}}$ is open. So by 8.1.1, the image is finite. ☐

So every finite quotient of $\mathcal{C}_K$ is a quotient of some $\mathcal{J}_K / K^\times \mathrm{U}_{K,\mathfrak{m}}$.

Definition. The **ray class group** of K modulo $\mathfrak{m}$ is

$$\mathrm{Cl}_{\mathfrak{m}} (K) = \mathcal{J}_K / K^\times \mathrm{U}_{K,\mathfrak{m}}.$$

Example. If $\mathfrak{m} = 0$, then $\mathrm{U}_{K,\mathfrak{m}} = \ker \mathrm{c}$, where $\mathrm{c} : \mathcal{J}_K \to \mathrm{I}(K)$ is the content map, and $\mathrm{Cl}_{\mathfrak{m}}(K) = \mathrm{Cl}(K)$.

Now relate to ideals.

Notation. Let $x \in K^\times$. Write $x \equiv 1 \mod^* \mathfrak{m}$ if

- for all $v \in \operatorname{supp}_{\mathrm{f}} \mathfrak{m}$, $v(x - 1) \geq \mathrm{m}_v$, and
- for all real $v \in \operatorname{supp} \mathfrak{m}$, $x \in (K_v^\times)^+ = \mathbb{R}_{>0}$.

Let

$$\begin{aligned} K_{\mathfrak{m}}^\times &= \left\{x \in K^\times \;\middle|\; x \equiv 1 \mod^* \mathfrak{m}\right\}, \\ \mathrm{I}_{\mathfrak{m}}(K) &= \{\text{fractional ideals prime to } \operatorname{supp}_{\mathrm{f}} \mathfrak{m}\} \cong \{\text{free abelian group on } \mathrm{V}_{K,\mathrm{f}} \setminus \operatorname{supp}_{\mathrm{f}} \mathfrak{m}\}, \\ \mathrm{P}_{\mathfrak{m}}(K) &= \left\{x\mathcal{O}_K \;\middle|\; x \in K_{\mathfrak{m}}^\times\right\} \subset \mathrm{I}_{\mathfrak{m}}(K). \end{aligned}$$

Theorem 8.4.

$$\mathrm{Cl}_{\mathfrak{m}}(K) \cong \mathrm{I}_{\mathfrak{m}}(K) / \mathrm{P}_{\mathfrak{m}}(K).$$

Example. Assume K has real places, and let $\mathfrak{m} = \sum_{v \text{ real}} (v)$. Then $\mathrm{I}_{\mathfrak{m}}(K) = \mathrm{I}(K)$ and $\mathrm{P}_{\mathfrak{m}}(K)$ is the group of principal fractional ideals $x\mathcal{O}_K$ where x is **totally positive**, that is for all $\sigma : K \hookrightarrow \mathbb{R}$, $\sigma(x) > 0$. Then $\mathrm{Cl}_{\mathfrak{m}}(K)$ is called the **narrow ideal class group** of K, also written $\mathrm{Cl}^+(K)$. Obviously $\mathrm{Cl}^+(K) \twoheadrightarrow \mathrm{Cl}(K)$ with kernel killed by two.

Precisely is the following.

Theorem 8.5. *Let $S \subset \mathrm{V}_{K,\mathrm{f}}$ be finite, containing* $\operatorname{supp}_{\mathrm{f}} \mathfrak{m}$*. Then there exists a unique continuous homomorphism*

$$\alpha = (\alpha_v) : \mathcal{J}_K / K^\times \to \mathrm{I}_{\mathfrak{m}}(K) / \mathrm{P}_{\mathfrak{m}}(K),$$

such that for all $v \in \mathrm{V}_{K,\mathrm{f}} \setminus S$, $\alpha_v(\mathcal{O}_v^\times) = \{1\}$ and $\alpha_v(\pi_v) \in \mathfrak{p}_v^{-1}$. Moreover, α induces an isomorphism

$$\mathcal{J}_K / K^\times \mathrm{U}_{K,\mathfrak{m}} \xrightarrow{\sim} \mathrm{I}_{\mathfrak{m}}(K) / \mathrm{P}_{\mathfrak{m}}(K).$$

Proof. By 8.2, α is unique. For existence, let

$$\mathcal{J}_{K,\mathfrak{m}} = \{(x_v) \in \mathcal{J}_K \mid \forall v \in \operatorname{supp}\mathfrak{m},\ x_v \in \mathrm{U}_v^{\mathrm{m}_v}\},$$

the open subgroup generated by $\mathrm{U}_{K,\mathfrak{m}}$ and $\{K_v^\times \mid v \notin \operatorname{supp}\mathfrak{m}\}$. Then by weak approximation, $K^\times \mathcal{J}_{K,\mathfrak{m}} = \mathcal{J}_K$, and by definition, $K_\mathfrak{m}^\times = K^\times \cap \mathcal{J}_{K,\mathfrak{m}}$, so

$$\iota : \mathcal{J}_K / K^\times \mathrm{U}_{K,\mathfrak{m}} \xleftarrow{\sim} \mathcal{J}_{K,\mathfrak{m}} / K_\mathfrak{m}^\times \mathrm{U}_{K,\mathfrak{m}}.$$

Also, there is an isomorphism

$$\begin{array}{cccc} \mathrm{c}^S & : & \mathcal{J}_{K,\mathfrak{m}} / \mathrm{U}_{K,\mathfrak{m}} & \longrightarrow & \mathrm{I}_\mathfrak{m}(K) \\ & & (x_v) & \longmapsto & \prod_{v \in \mathrm{V}_{K,\mathrm{f}},\ v \notin \operatorname{supp}_{\mathrm{f}} \mathfrak{m}} \mathfrak{p}_v^{v(x_v)} \end{array}.$$

Then

$$\mathcal{J}_K / K^\times \mathrm{U}_{K,\mathfrak{m}} \xleftarrow{\iota} \mathcal{J}_{K,\mathfrak{m}} / K_\mathfrak{m}^\times \mathrm{U}_{K,\mathfrak{m}} \xrightarrow{\mathrm{c}^S} \mathrm{I}_\mathfrak{m}(K) / \mathrm{P}_\mathfrak{m}(K),$$

and this is the map $x \mapsto \alpha\left(x^{-1}\right)$. □

Remark. The isomorphism $\mathcal{J}_K / K^\times \mathrm{U}_{K,\mathfrak{m}} \to \mathrm{I}_\mathfrak{m}(K) / \mathrm{P}_\mathfrak{m}(K)$ is not induced by the S-content map $\mathcal{J}_K \to \mathrm{I}_\mathfrak{m}(K)$ but only on the subgroup $\mathcal{J}_{K,\mathfrak{m}}$. Fröhlich called this the **fundamental mistake of class field theory**.

Example. Let $K = \mathbb{Q}$, let $m > 1$, and let $\mathfrak{m} = (m)\infty = \sum_{p \mid m} \mathrm{v}_p(m)(p) + (\infty)$. If $I \in \mathrm{I}_\mathfrak{m}(\mathbb{Q})$, then $I = (a/b)\mathbb{Z}$ for unique positive coprime $a, b \in \mathbb{Z}$ with $(ab, m) = 1$. Set

$$\begin{array}{cccc} \Theta & : & \mathrm{I}_\mathfrak{m}(\mathbb{Q}) & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^\times \\ & & I & \longmapsto & \dfrac{a}{b} \mod m \end{array}.$$

This clearly defines an isomorphism such that

$$\begin{tikzcd} p\mathbb{Z} \in \mathrm{I}_\mathfrak{m}(\mathbb{Q}) / \mathrm{P}_\mathfrak{m}(\mathbb{Q}) \arrow[r, "\Theta", "\sim"'] & (\mathbb{Z}/m\mathbb{Z})^\times \ni p \mod m \\ \mathbb{Q}^\times \left(\dots, 1, 1, p^{-1}, 1, 1, \dots\right) \in \mathcal{J}_\mathbb{Q} / \mathbb{Q}^\times \arrow[u, "\alpha"] \arrow[r, "\sim"] & \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times \ni (\dots, p, p, 1, p, p, \dots) \arrow[u] \end{tikzcd}$$

commutes.

This is the reason for using $\mathfrak{p}_v^{-1}$, and σ_v^{-1} in the reciprocity law, since it means that for $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, recover the usual map $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$. Older treatments of class field theory use σ_v and end up with the inverse of the usual map. Another reason is that the inverse $\mathrm{Fr}_v = \mathrm{F}_v = \sigma_v^{-1}$, the so-called **geometric Frobenius**, is what occurs naturally in algebraic geometry. The modern normalisation of class field theory maps a uniformiser at an unramified v to the geometric Frobenius σ_v^{-1}.

8.3 Uniqueness of $\mathrm{Art}_{L/K}$

Lecture 15 Tuesday 23/02/21

By 8.2, $\mathrm{Art}_{L/K}$ is unique. A consequence is if L'/K' is an abelian extension, and have isomorphisms

$$\begin{tikzcd} L \arrow[r, "\widetilde{\tau}", "\sim"'] & L' \\ K \arrow[u] \arrow[r, "\sim", "\tau"'] & K' \arrow[u] \end{tikzcd},$$

then get isomorphisms

$$\begin{array}{cccc} \tau & : & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(L'/K') \\ & & g & \longmapsto & \widetilde{\tau} \circ g \circ \widetilde{\tau}^{-1} \end{array}.$$

As extensions are abelian, any other $\widetilde{\tau}'$ with $\widetilde{\tau}'|_K = \tau$ is $\widetilde{\tau}' = \widetilde{\tau} \circ h$ for $h \in \mathrm{Gal}(L/K)$, so $\widetilde{\tau}' \circ g \circ \widetilde{\tau}'^{-1} = \widetilde{\tau} \circ h \circ g \circ h^{-1} \circ \widetilde{\tau}^{-1} = \widetilde{\tau} \circ g \circ \widetilde{\tau}^{-1}$. So this isomorphism depends only on τ. Then

$$\begin{tikzcd} \mathcal{C}_K \arrow[r, "\mathrm{Art}_{L/K}"] \arrow[d, "\tau"', "\sim"] & \mathrm{Gal}(L/K) \arrow[d, "\sim"', "\tau"] \\ \mathcal{C}_{K'} \arrow[r, "\mathrm{Art}_{L'/K'}"'] & \mathrm{Gal}(L'/K') \end{tikzcd}$$

commutes, by uniqueness. This sort of argument is often called **transport of structure**.

Example. Suppose $L/K/F$ is Galois such that L/K is abelian and K/F is Galois. Take $\tau = g \in \mathrm{Gal}(K/F)$. As L/K is abelian, $\mathrm{Gal}(K/F)$ acts by conjugation on $\mathrm{Gal}(L/K)$. Let $K = K'$ and $L = L'$. Then

$$\mathrm{Art}_{L/K}(gx) = g \circ \mathrm{Art}_{L/K}(x) \circ g^{-1}, \qquad g \in \mathrm{Gal}(K/F), \qquad x \in \mathcal{C}_K. \tag{5}$$

8.4 Norm functoriality

Proposition 8.6. *Suppose L/K and L'/K' are abelian such that $L \subset L'$ and $K \subset K'$. Then*

$$\begin{tikzcd} \mathrm{Gal}(L'/K') \arrow[r, "g \mapsto g|_L"] & \mathrm{Gal}(L/K) \\ \mathcal{C}_{K'} \arrow[u, "\mathrm{Art}_{L'/K'}"] \arrow[r, "\mathrm{N}_{K'/K}"'] & \mathcal{C}_K \arrow[u, "\mathrm{Art}_{L/K}"'] \end{tikzcd}$$

commutes.

Proof. It is enough to check for $\pi_w \in K_w'^{\times} \subset \mathcal{C}_{K'}$ for w outside a finite set. Assume w is unramified in L'/K' such that $w \mid v \in \mathrm{V}_{K,\mathrm{f}}$ where v is unramified in L/K. If $\sigma_w \in \mathrm{D}_w \subset \mathrm{Gal}(L'/K')$, then

$$\sigma_w|_L = (x \mapsto x^{\mathrm{q}_w})|_L = (x \mapsto x^{\mathrm{q}_v})^{\mathrm{f}(w|v)} = \sigma_v^{\mathrm{f}(w|v)}.$$

If $\pi_w \in K_w'^{\times}$ is a uniformiser, then

$$\mathrm{N}_{K_w'/K_v}(\pi_w) = u\pi_v^{\mathrm{f}(w|v)}, \qquad u \in \mathcal{O}_{K_v}^{\times},$$

since $\pi_v^{[K_w':K_v]} = \mathrm{N}_{K_w'/K_v}(\pi_v)$ and $\pi_v = u\pi_w^{\mathrm{e}(w|v)}$. ☐

Example. A special case is $K' = L = L'$. Then $1 = \mathrm{Art}_{L/L}(x) = \mathrm{Art}_{L/K}(\mathrm{N}_{L/K}(x))$ for $x \in \mathcal{J}_L$, so

$$\mathrm{N}_{L/K}(\mathcal{J}_L) \subset \ker \mathrm{Art}_{L/K}.$$

8.5 Existence theorem

By the reciprocity law, there is a map from abelian extensions of K to finite quotients of $\mathcal{C}_K$.

Theorem (Existence theorem)**.** *Let $U \subset \mathcal{J}_K$ be an open subgroup. Then there exists an abelian extension L/K with*

$$\ker \mathrm{Art}_{L/K} = UK^{\times}.$$

Combining with the reciprocity law,

$$\varprojlim_{\text{open subgroups } U \subset \mathcal{J}_K} \mathcal{J}_K/K^{\times}U \xrightarrow{\sim} \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right).$$

In particular, if $\mathfrak{m}$ is a modulus, and $U = \mathrm{U}_{K,\mathfrak{m}}$, there is a corresponding abelian extension of K, called the **ray class field**.

Example. Let $K = \mathbb{Q}$ with $\mathfrak{m} = (m)\infty$. Then the ray class field is $\mathbb{Q}(\zeta_m)$. So should think of ray class fields as analogues of cyclotomic fields. Maybe later will discuss ray class fields for $\mathbb{Q}\left(\sqrt{-d}\right)$, which correspond to elliptic curves.

8.6 Relation with local class field theory

Let L/K be abelian, let $v \in \mathrm{V}_K$, and let $w \mid v$. Then

$$\begin{array}{ccc} \mathcal{J}_K/K^\times & \xrightarrow{\mathrm{Art}_{L/K}} & \mathrm{Gal}\left(L/K\right) \\ \big\uparrow & & \cup \\ K_v^\times & \xrightarrow[\psi_v]{} & \mathrm{D}_v = \mathrm{Gal}\left(L_w/K_v\right) \end{array}.$$

Indeed, in the proof of the reciprocity law, it is usual to start with local Artin maps ψ_v.

Example. Let $v \mid \infty$.

- If $K_v = L_w$, then $\psi_v = 1$.
- If $K_v = \mathbb{R}$ and $L_w \cong \mathbb{C}$, then $\psi_v = \mathrm{sign} : \mathbb{R}^\times \to \{\pm 1\} \cong \mathrm{Gal}\left(L_w/K_v\right)$ with kernel $\mathbb{R}_{>0} = \mathrm{N}_{\mathbb{C}/\mathbb{R}}\left(\mathbb{C}^\times\right)$.

The (ψ_v) combine to give

$$\begin{array}{ccc} \mathcal{J}_K/\mathrm{N}_{L/K}\left(\mathcal{J}_L\right) & \xrightarrow{\mathrm{Art}_{L/K}} & \mathrm{Gal}\left(L/K\right) \\ \sim\big\uparrow & & \cup \\ \bigoplus_v K_v^\times/\mathrm{N}_{L_w/K_v}\left(L_w^\times\right) & \xrightarrow[\sim]{} & \bigoplus_v \mathrm{D}_v \end{array}.$$

So the fact that $\mathrm{Art}_{L/K}\left(K^\times\right) = \{1\}$, the hard part of the reciprocity law, is equivalent to knowing the relations between the various $\mathrm{D}_v \subset \mathrm{Gal}\left(L/K\right)$. Why are ideles better than ideals?

- Ideals only will tell you about relations between D_v for v unramified.
- Need ideles to understand properly ramification.

8.7 Hilbert class field

Let K be arbitrary with modulus $\mathfrak{m} = 0$. Then $\mathrm{Cl}_{\mathfrak{m}}\left(K\right) = \mathrm{Cl}\left(K\right)$. By the existence theorem, there is a corresponding abelian extension H/K, the **Hilbert class field**, with

$$\mathrm{Art}_{H/K} : \mathrm{Cl}\left(K\right) \xrightarrow{\sim} \mathrm{Gal}\left(H/K\right).$$

Then H/K satisfies the following.

- It is abelian.
- For all $v \in \mathrm{V}_{K,\mathrm{f}}$, it is unramified at v, since $\mathcal{O}_v^\times \subset \mathrm{U}_{K,\mathfrak{m}}$ for all v.
- At an infinite place v, $\mathrm{U}_{K,\mathfrak{m}} \supset K_v^\times$, so the local decomposition group at v is trivial, that is if v is a real place of K, then if $w \mid v$ then w is also real.

Thus H/K is unramified at all places of K, and H is the maximal extension with these properties.

Example. Let $K = \mathbb{Q}\left(\sqrt{-23}\right)$, so $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$. By a standard computation, $\mathrm{Cl}\left(K\right) \cong \mathbb{Z}/3\mathbb{Z}$ is generated by $[\mathfrak{p}]$ for $\mathfrak{p} = \left\langle 2, \frac{1+\sqrt{-23}}{2}\right\rangle$. Let $\tau \in \mathrm{Gal}\left(K/\mathbb{Q}\right)$ be complex conjugation. Then $\tau\left(\mathfrak{p}\right) = \left\langle 2, \frac{1-\sqrt{-23}}{2}\right\rangle$ and $\mathfrak{p} \cdot \tau\left(\mathfrak{p}\right) = \langle 2\rangle$, that is $\tau\left([\mathfrak{p}]\right) = [\mathfrak{p}]^{-1}$, so τ acts as -1 on $\mathrm{Cl}\left(K\right)$. Let H be the Hilbert class field of K, which is the maximal abelian extension of K which is unramified at all $v \in \mathrm{V}_{K,\mathrm{f}}$, that is $\delta_{H/K} = \mathcal{O}_K$. Then $[H : K] = 3$ and Galois. By (5) above, τ acts as -1 on $\mathrm{Gal}\left(H/K\right)$, so $H/\mathbb{Q}$ is an $\mathcal{S}_3$-extension. Show that H is the splitting field of $f = T^3 - T + 1$ with discriminant -23. [8]

[8] Exercise

8.8 Another example

Lecture 16 Thursday 25/02/21

The following arose in a research problem.

Proposition 8.7. *There is no $\mathcal{S}_3$-extension $L/\mathbb{Q}$, so Galois with group $\mathcal{S}_3$, which is unramified outside $2, 7, \infty$, with quadratic subfield $K = \mathbb{Q}\left(\sqrt{-7}\right)$ or $K = \mathbb{Q}\left(\sqrt{2}\right)$.*

Proof. Let

$$\mathrm{Art}_{L/K} : \mathcal{J}_K/K^\times \twoheadrightarrow \mathrm{Gal}\left(L/K\right) \cong \mathbb{Z}/3\mathbb{Z}.$$

The condition that $L/\mathbb{Q}$ is Galois with group $\mathcal{S}_3$ is

$$\mathrm{Art}_{L/K}\left(\tau\left(x\right)\right) = \mathrm{Art}_{L/K}\left(x^{-1}\right),$$

by (5), since $\mathrm{Gal}\left(K/\mathbb{Q}\right) = \langle\tau\rangle$ acts on $\mathrm{Gal}\left(L/K\right)$ by conjugation non-trivially. For both $\mathbb{Q}\left(\sqrt{-7}\right)$ and $\mathbb{Q}\left(\sqrt{2}\right)$, $\mathrm{Cl}\left(K\right) = 1$. So

$$\mathcal{J}_K/K^\times \xleftarrow{\sim} \mathcal{J}_{K,\emptyset}/\mathcal{O}_K^\times = \left(K_\infty^\times \times \widehat{\mathcal{O}_K}^\times\right)/\mathcal{O}_K^\times.$$

Then $\mathrm{Art}_{L/K} : K_\infty^\times = \left(\mathbb{R}^\times\right)^{\mathrm{r}_1} \times \left(\mathbb{C}^\times\right)^{\mathrm{r}_2} \hookrightarrow \mathcal{J}_{K,\emptyset} \to \mathbb{Z}/3\mathbb{Z}$ is trivial on $\mathbb{C}^\times$ and $\mathbb{R}_{>0}$, and even on $\mathbb{R}^\times$, since there is no non-zero continuous homomorphism $\mathbb{R}^\times \to \mathbb{Z}/3\mathbb{Z}$. So $\mathrm{Art}_{L/K}$ factors through $\widehat{\mathcal{O}_K}^\times/\mathcal{O}_K$, and since L/K is unramified at $v \nmid 14$, factors further by

$$\begin{tikzcd}
\mathcal{J}_K/K^\times \cong \mathcal{J}_{K,\emptyset}/\mathcal{O}_K^\times \arrow[r] \arrow[d, two heads, "\mathrm{Art}_{L/K}"'] & \widehat{\mathcal{O}_K}^\times/\mathcal{O}_K^\times \arrow[d] \\
\mathrm{Gal}\left(L/K\right) \cong \mathbb{Z}/3\mathbb{Z} & \left(\prod_{v \mid 14} \mathcal{O}_v^\times\right)/\mathcal{O}_K^\times \arrow[l, two heads, "\psi"]
\end{tikzcd},$$

since $\mathrm{Art}_{L/K}\left(\mathcal{O}_v^\times\right) = 1$ for all $v \nmid 14$. Thus

$$\psi \circ \tau = -\psi. \qquad (6)$$

- Let $K = \mathbb{Q}\left(\sqrt{-7}\right)$, so $\mathcal{O}_K^\times = \{\pm 1\}$.
  - Since $-7 \equiv 1 \mod 8$, 2 splits in K, so $\prod_{v \mid 2} \mathcal{O}_v^\times = \mathbb{Z}_2^\times \times \mathbb{Z}_2^\times$ is a pro-2 group, so $\psi\left(\prod_{v \mid 2} \mathcal{O}_v^\times\right) = 0$.
  - 7 ramifies, so if $v \mid 7$, then $\mathcal{O}_v^\times = \mathbb{F}_7^\times \times \left(1 + \pi_v\mathcal{O}_v\right)$, where $\mathbb{F}_7^\times$ is the Teichmüller and $1 + \pi_v\mathcal{O}_v$ is a pro-7 group.

  So ψ factors through $\mathbb{F}_7^\times$, and $\tau \in \mathrm{Gal}\left(K/\mathbb{Q}\right)$ acts trivially on $\mathbb{F}_7$. So by (6), there is no possible ψ. There does exist a ψ with $\psi \circ \tau = \psi$, unique up to inverse, corresponding to an abelian $L/\mathbb{Q}$, which has to be $\mathbb{Q}\left(\zeta_7\right)$.
- Let $K = \mathbb{Q}\left(\sqrt{2}\right)$, so $\mathcal{O}_K^\times = \left\langle -1, \epsilon = 1 + \sqrt{2}\right\rangle$.
  - 2 ramifies, so if $v \mid 2$, then $\mathcal{O}_v^\times = 1 + \pi_v\mathcal{O}_v$ is a pro-2 group and $\psi\left(\mathcal{O}_v^\times\right) = 0$.
  - Since $7 = \left(3 + \sqrt{2}\right)\left(3 - \sqrt{2}\right)$, $\prod_{v \mid 7} \mathcal{O}_v^\times = \mathbb{Z}_7^\times \times \mathbb{Z}_7^\times \cong \mathbb{F}_7^\times \times \mathbb{F}_7^\times \times \left(1 + 7\mathbb{Z}_7\right)^2$, where $1 + 7\mathbb{Z}_7$ is a pro-7 group, so $\psi\left(1 + 7\mathbb{Z}_7\right) = 0$.

  So ψ factors through $\psi : \left(\mathbb{F}_7^\times \times \mathbb{F}_7^\times\right)/\mathcal{O}_K^\times \twoheadrightarrow \mathbb{Z}/3\mathbb{Z}$. Then $\tau : (x, y) \mapsto (y, x)$, so

  $$\psi\left(x, x\right) = 0, \qquad (7)$$

  by (6). Now

  $$\epsilon = 1 + \sqrt{2} \equiv \begin{cases} -2 & \mod 3 + \sqrt{2} \\ 4 & \mod 3 - \sqrt{2} \end{cases},$$

  that is $\psi\left(-2, 4\right) = 0$. By this and (7), $\psi = 0$.

∎

8.9 Comparing $\mathcal{C}_K$ and $\mathrm{Gal}\left(K^{\mathrm{ab}}/K\right)$

Fix $K \subset \overline{\mathbb{Q}}$. Let

$$\mathrm{Art}_K : \mathcal{C}_K \to \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right) = \varprojlim_{\text{finite abelian } K \subset L \subset \overline{\mathbb{Q}}} \mathrm{Gal}\left(L/K\right),$$

where K^{ab} is the **maximal abelian extension** of K in $\overline{\mathbb{Q}}$, the union of all finite abelian L/K, so $\mathrm{Gal}\left(K^{\mathrm{ab}}/K\right)$ is profinite. As $\mathcal{C}_K^1 \twoheadrightarrow \mathrm{Gal}\left(L/K\right)$ for all L and $\mathcal{C}_K^1$ is compact, $\mathcal{C}_K^1 \twoheadrightarrow \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right)$, since the image is dense and compact. The existence theorem is equivalent to the statement that $\mathrm{Gal}\left(K^{\mathrm{ab}}/K\right)$ is the maximal profinite quotient of $\mathcal{C}_K$, or of $\mathcal{C}_K^1$. There is a diagram

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{J}_{K,\emptyset}/\mathcal{O}_K^\times \arrow[r] \arrow[d, two heads] & \mathcal{C}_K \arrow[r, "c"] \arrow[d, two heads, "\mathrm{Art}_K"'] & \mathrm{Cl}\left(K\right) \arrow[r] \arrow[d, "\sim"] & 1 \\
1 \arrow[r] & \mathrm{Gal}\left(K^{\mathrm{ab}}/H\right) \arrow[r] & \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right) \arrow[r] & \mathrm{Gal}\left(H/K\right) \arrow[r] & 1
\end{tikzcd},$$

where H is the Hilbert class field. What is the kernel of the vertical maps?

- If $K = \mathbb{Q}$, then
$$\mathrm{Art}_{\mathbb{Q}} : \mathcal{C}_{\mathbb{Q}} \cong \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times \twoheadrightarrow \widehat{\mathbb{Z}}^\times = \mathrm{Gal}\left(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}\right).$$
- If $K = \mathbb{Q}\left(\sqrt{-d}\right)$, then $\mu\left(K\right)$ is finite, so the maximal profinite quotient is
$$\mathrm{Art}_K : \mathcal{J}_{K,\emptyset}/\mathcal{O}_K^\times \cong \left(\mathbb{C}^\times \times \widehat{\mathcal{O}_K}^\times\right)/\mu\left(K\right) \twoheadrightarrow \widehat{\mathcal{O}_K}^\times/\mu\left(K\right) = \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right).$$
- Let $K = \mathbb{Q}\left(\sqrt{2}\right)$, so $\mathrm{Cl}\left(K\right) = 1$ and $\mathcal{O}_K^\times = \left\langle -1, \epsilon = 1 + \sqrt{2}\right\rangle$. Then $\mathrm{N}_{K/\mathbb{Q}}\left(\epsilon\right) = -1$ and ϵ has signature $(1, -1)$. Let $\epsilon_+ = \epsilon^2$ be the least totally positive unit. Then the maximal profinite quotient is
$$\begin{array}{ccccc}
\mathcal{C}_K = \mathcal{J}_{K,\emptyset}/\mathcal{O}_K^\times & \xleftarrow{\sim} & \left(\mathbb{R}_{>0}^2 \times \widehat{\mathcal{O}_K}^\times\right)/\left\langle \epsilon_+ \right\rangle & & \\
\cup & & & & \\
\mathcal{C}_K^1 = \mathcal{J}_{K,\emptyset}^1/\mathcal{O}_K^\times & \xleftarrow[\sim]{} & \left(\mathbb{R}_{>0} \times \widehat{\mathcal{O}_K}^\times\right)/\left\langle \epsilon_+ \right\rangle & \underset{\mathrm{Art}_K^1}{\twoheadrightarrow} & \widehat{\mathcal{O}_K}^\times/\overline{\left\langle \epsilon_+ \right\rangle} = \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right)
\end{array}.$$
If $G = \varprojlim_i G_i$ is a profinite group and $g \in G$, there exists a unique continuous $\phi : \widehat{\mathbb{Z}} \to G$ such that $\phi\left(1\right) = g$.[9] So have
$$\begin{array}{ccc}
\widehat{\mathbb{Z}} & \longrightarrow & \overline{\left\langle \epsilon_+ \right\rangle} \subset \widehat{\mathcal{O}_K}^\times \\
1 & \longmapsto & \epsilon_+
\end{array}.$$
One can show that $\widehat{\mathbb{Z}} \xrightarrow{\sim} \overline{\left\langle \epsilon_+ \right\rangle}$, so there is an isomorphism
$$\ker \mathrm{Art}_K^1 = \left(\mathbb{R}_{>0} \times \overline{\left\langle \epsilon_+ \right\rangle}\right)/\left\langle \epsilon_+ \right\rangle \cong \left(\mathbb{R} \times \widehat{\mathbb{Z}}\right)/\mathbb{Z} = \mathbb{A}_{\mathbb{Q}}/\mathbb{Q},$$
where $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is compact and connected, that is have
$$1 \to \mathbb{A}_{\mathbb{Q}}/\mathbb{Q} \to \mathcal{C}_K^1 \to \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right) \to 1.$$
- For general K, what happens is that
$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{C}_K^0 & \longrightarrow & \mathcal{C}_K & \xrightarrow{\mathrm{Art}_K} & \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right) & \longrightarrow & 1 \\
& & \wr\!\wr & & \cup & & \cup & & \\
1 & \longrightarrow & \mathcal{C}_K^0 & \longrightarrow & \mathcal{J}_{K,\emptyset}/\mathcal{O}_K^\times & \longrightarrow & \mathrm{Gal}\left(K^{\mathrm{ab}}/H\right) & \longrightarrow & 1 \\
& & & & & & \wr\!\wr & & \\
& & & & & & \left(\{\pm 1\}^{r_1} \times \widehat{\mathcal{O}_K}^\times\right)/\overline{\mathcal{O}_K^\times} & &
\end{array},$$
where the maximal connected subgroup of $\mathcal{C}_K$, the closure of $\mathbb{R}_{>0}^{r_1} \times \left(\mathbb{C}^\times\right)^{r_2}$, is
$$\mathcal{C}_K^0 \cong \mathbb{R}_{>0} \times \mathrm{U}\left(1\right)^{r_2} \times \left(\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}\right)^{r_1 + r_2 - 1}.$$

[9] Exercise: easy

9 ζ-functions and L-functions

9.1 Riemann ζ-function

Lecture 17 Saturday 27/02/21

The **Riemann ζ-function** is

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}, \qquad s \in \mathbb{C}, \qquad \Re s > 1,$$

by unique factorisation in $\mathbb{Z}$. Define

$$\mathrm{Z}(s) = \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s).$$

Theorem 9.1.

$$\mathrm{Z}(s) = \mathrm{Z}(1-s),$$

with analytic continuation to $\mathbb{C}$ except for simple poles at $s = 0, 1$ with residues ± 1.

Proof. There are three steps.

Step 1. The **Mellin transform** of $\frac{1}{2}(\Theta(y) - 1)$ is

$$\mathrm{Z}(2s) = \pi^{-s} \sum_{n \geq 1} \frac{1}{n^{2s}} \int_0^\infty e^{-t} t^{s-1} \, \mathrm{d}t = \int_0^\infty \sum_{n=1}^\infty e^{-\pi n^2 y} y^{s-1} \, \mathrm{d}y = \int_0^\infty \frac{1}{2}(\Theta(y) - 1) \frac{y^s}{y} \, \mathrm{d}y,$$

where Θ is the **theta function**

$$\Theta(y) = \sum_{n=-\infty}^\infty e^{-\pi n^2 y}.$$

Step 2. If $f : \mathbb{R} \to \mathbb{C}$ is nice, then the **Poisson summation formula** is

$$\sum_{n=-\infty}^\infty f(n) = \sum_{n=-\infty}^\infty \widehat{f}(n),$$

where $\widehat{f}$ is the **Fourier transform**

$$\widehat{f}(u) = \int_{-\infty}^\infty e^{-2\pi i u x} f(x) \, \mathrm{d}x.$$

Take $f(x) = e^{-\pi x^2 y}$. Then $\widehat{f}(u) = y^{-1/2} e^{\pi u^2 / y}$, so $\Theta(y) = y^{-1/2} \Theta(1/y)$.

Step 3. In step 1, split

$$\int_0^\infty \frac{1}{2}(\Theta(y) - 1) \frac{y^s}{y} \, \mathrm{d}y = \int_1^\infty \frac{1}{2}(\Theta(y) - 1) \frac{y^s}{y} \, \mathrm{d}y + \int_0^1 \frac{1}{2}(\Theta(y) - 1) \frac{y^s}{y} \, \mathrm{d}y,$$

and in the second term, use step 2 to make into

$$\int_0^1 \frac{1}{2}(\Theta(y) - 1) \frac{y^s}{y} \, \mathrm{d}y = \int_1^\infty \frac{1}{2}\left(\Theta\left(\frac{1}{y}\right) - 1\right) \frac{y^{-s}}{y} \, \mathrm{d}y,$$

by $y \mapsto 1/y$. Get that

$$\mathrm{Z}(2s) = \frac{1}{2} \int_1^\infty (\Theta(y) - 1)\left(y^s + y^{\frac{1}{2} - s}\right) \frac{1}{y} \, \mathrm{d}y + \frac{1}{2s-1} - \frac{1}{2s},$$

where the first term is an entire function of s since $\Theta(y) - 1 \to 0$ rapidly as $y \to \infty$, so $\mathrm{Z}(2s) = \mathrm{Z}(1-2s)$.

$\square$

9.2 Dedekind ζ-function

Let K be a number field. The **Dedekind ζ-function of K** is

$$\zeta_K(s) = \sum_{0 \neq \mathfrak{a} \subset \mathcal{O}_K \text{ ideals}} \frac{1}{\mathrm{N}(\mathfrak{a})^s}.$$

Proposition 9.2 (Euler product)**.**

$$\zeta_K(s) = \prod_{v \in \mathrm{V}_{K,\mathrm{f}}} \frac{1}{1 - \mathrm{q}_v^{-s}},$$

absolutely convergent for $\Re s > 1$.

Proof. Formally, if $\mathfrak{a} \subset \mathcal{O}_K$ such that $\mathfrak{a} = \prod_v \mathfrak{p}_v^{n_v}$ then $\mathrm{N}(\mathfrak{a})^{-s} = \prod_v \mathrm{q}_v^{-n_v s}$, so

$$\zeta_K(s) = \prod_v \left(1 + \mathrm{q}_v^{-s} + \dots\right) = \prod_v \frac{1}{1 - \mathrm{q}_v^{-s}}.$$

Now $\#\{v \mid p\} \le n = [K : \mathbb{Q}]$, and if $v \mid p$ then $\mathrm{q}_v \ge p$, so the product converges by comparison with $\prod_p \left(1 - p^{-s}\right)^{-n} = \zeta(s)^n$. ☐

The $1/\left(1 - \mathrm{q}_v^{-s}\right)$ are **Euler factors at** v. Define

$$\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right), \qquad \Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s} \Gamma(s),$$

the Euler factors for the infinite places, and

$$\mathrm{Z}_K(s) = |\mathrm{d}_K|^{\frac{s}{2}} \Gamma_{\mathbb{R}}(s)^{\mathrm{r}_1} \Gamma_{\mathbb{C}}(s)^{\mathrm{r}_2} \zeta_K(s).$$

The following is a generalisation of 9.1.

Theorem 9.3.

1. $\mathrm{Z}_K(s)$ *has an analytic continuation to* $\mathbb{C}$*, apart from simple poles at* $s = 0, 1$*, and*

$$\mathrm{Z}_K(1 - s) = \mathrm{Z}_K(s).$$

2. $\zeta_K(s)$ *has a simple zero of order* $r = \mathrm{r}_1 + \mathrm{r}_2 - 1$ *at* $s = 0$*, and*

$$\lim_{s \to 0} \frac{1}{s^r} \zeta_K(s) = -\frac{\mathrm{h}_K \mathrm{R}_K}{\mathrm{w}_K}, \tag{8}$$

the ***analytic class number formula****.*

Here, $\mathrm{h}_K = \#\,\mathrm{Cl}(K)$ is the class number, $\mathrm{w}_K = \#\mu(K)$ is the number of roots of unity in K, and R_K is the **regulator** of K. If $\epsilon_1, \dots, \epsilon_r$ are generators for $\mathcal{O}_K^\times/\mu(K) \cong \mathbb{Z}^r$, by the unit theorem, R_K is the absolute value of any $(r \times r)$-minor of the matrix

$$\left(\log|\epsilon_j|_v\right)_{1 \le j \le r,\ v \in \mathrm{V}_{K,\infty}}.$$

Note that by the product formula, the sum of the columns of this matrix is zero, so minors are equal up to sign. Then $\mathrm{R}_K \neq 0$ by the proof of the unit theorem. More usual to write (8) at $s = 1$ but more complicated.

Example. If $K = \mathbb{Q}$, then $\zeta(0) = -\frac{1}{2}$.

There are two ways to prove this.

- Hecke, using theta functions.
- Tate, using adeles. Generalises much more easily to other L-functions, such as L-functions of characters of $\mathcal{C}_K$.

Tate's proof is an adelic version of 9.1. The idea is to first interpret $\zeta_K(s)$, or $Z_K(s)$, as an adelic integral. Assuming we know how to integrate on $\mathbb{Q}_p$,

$$\int_{\mathbb{Z}_p \setminus \{0\}} |x|_p^{s-1} \, \mathrm{d}x = \sum_{n \geq 0} \int_{p^n \mathbb{Z}_p \setminus p^{n+1} \mathbb{Z}_p} p^{-n(s-1)} \, \mathrm{d}x = \sum_{n \geq 0} p^{-n(s-1)} \operatorname{meas}\left(p^n \mathbb{Z}_p \setminus p^{n+1} \mathbb{Z}_p\right).$$

Then

$$\mathbb{Z}_p = \bigsqcup_{a=0}^{p^n-1} a + p^n \mathbb{Z}_p, \qquad \operatorname{meas}(a + p^n \mathbb{Z}_p) = \frac{1}{p^n} \operatorname{meas}(\mathbb{Z}_p),$$

so

$$\int_{\mathbb{Z}_p \setminus \{0\}} |x|_p^{s-1} \, \mathrm{d}x = \sum_{n \geq 0} p^{-n(s-1)} \left(\frac{1}{p^n} - \frac{1}{p^{n+1}}\right) \operatorname{meas}(\mathbb{Z}_p) = \left(1 - p^{-1}\right) \operatorname{meas}(\mathbb{Z}_p) \frac{1}{1 - p^{-s}},$$

where $1/(1-p^{-s})$ is the Euler factor at p in $\zeta(s)$. Suggests that $\zeta(s)$ is a product of p-adic integrals, an adelic integral.

- The Γ-factor will be an integral at an infinite place.
- Have to normalise measure to get $1/(1-p^{-s})$ for almost all p.
- The functional equation will come from a Fourier transform.

9.3 Local Fourier analysis

On $\mathbb{R}$,

$$\widehat{f}(y) = \int_{-\infty}^{\infty} e^{-2\pi i x y} f(x) \, \mathrm{d}x,$$

which has three ingredients. Define $\widehat{f}$ replacing $\mathbb{R}$ by any local field F, of characteristic zero.

Definition. The **additive character** is a continuous $1 \neq \psi : F \to \mathrm{U}(1) = \{|z| = 1\} \subset \mathbb{C}^\times$.

- If $F = \mathbb{R}$, then $\psi(x) = e^{-2\pi i x}$.
- If $F = \mathbb{C}$, then $\psi(z) = e^{-2\pi i (z + \overline{z})}$.
- Let $F/\mathbb{Q}_p$ be finite. Since $\mathbb{Q}_p = \mathbb{Z}[1/p] + \mathbb{Z}_p$, define

$$\begin{array}{cccc} \psi_p & : & \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & \mathrm{U}(1) \\ & & x & \longmapsto & e^{2\pi i y} \end{array}, \qquad y \in \mathbb{Z}\left[\frac{1}{p}\right], \qquad x - y \in \mathbb{Z}_p,$$

  which is well-defined. Let $\psi = \psi_p \circ \mathrm{Tr}_{F/\mathbb{Q}_p} : F \to \mathrm{U}(1)$.

Why the sign in the case $F/\mathbb{R}$? If $x \in \mathbb{Q}$, then $\psi_\infty(x) \prod_p \psi_p(x) = 1$. Lecture 18 Tuesday 02/03/21

Definition. The **Haar measure** $\mathrm{d}_F\, x$ is translation-invariant.

- If $F = \mathbb{R}$, then $\mathrm{d}_F\, x$ is the usual Lebesgue measure $\mathrm{d}x$.
- If $F = \mathbb{C}$, then $\mathrm{d}_F\, z = 2\mathrm{d}x\mathrm{d}y$ for $z = x + iy$, which is twice the Lebesgue measure.
- Let $F/\mathbb{Q}_p$. Our functions will be locally constant, that is sums of multiples of characteristic functions of $a + \pi^n \mathcal{O}_F$ for $a \in F$ and $n \in \mathbb{Z}$. If $n \geq 0$, then $\mathcal{O}_F = \bigsqcup_a a + \pi^n \mathcal{O}_F$ is a disjoint union of q^n cosets, so

$$\operatorname{meas}(a + \pi^n \mathcal{O}_F) = \operatorname{meas}(\pi^n \mathcal{O}_F) = \frac{1}{q^n} \operatorname{meas}(\mathcal{O}_F),$$

  and will normalise $\operatorname{meas}(\mathcal{O}_F) = q^{-\delta/2}$ where $\delta = \delta_{F/\mathbb{Q}_p} = \mathrm{v}\left(\mathcal{D}_{F/\mathbb{Q}_p}\right)$, that is

$$\int_F \mathbb{1}_{a + \pi^n \mathcal{O}_F} \, \mathrm{d}_F\, x = \operatorname{meas}(a + \pi^n \mathcal{O}_F) = q^{-n - \frac{\delta}{2}}.$$

In each case, $\mathrm{d}_F(ax) = |a|_F \, \mathrm{d}_F\, x$ for $a \in F^\times$.

Definition. The class of functions to integrate is the **Schwartz space** $\mathcal{S}(F)$.

- If $F = \mathbb{R}$, then
$$\mathcal{S}(F) = \left\{ \mathrm{C}^\infty\text{-functions } f : F \to \mathbb{C} \;\middle|\; \forall n \ge 0,\ \forall \alpha \in \mathbb{N},\ \lim_{|x| \to \infty} \left(|x|^n \left| \frac{\mathrm{d}^\alpha f}{\mathrm{d} x^\alpha} \right| \right) = 0 \right\}.$$
For example, $e^{-c|x|^2}$ for $c > 0$.
- If $F = \mathbb{C}$, then
$$\mathcal{S}(F) = \left\{ \mathrm{C}^\infty\text{-functions } f : F \to \mathbb{C} \;\middle|\; \forall n \ge 0,\ \forall \alpha \in \mathbb{N}^2,\ \lim_{|z| \to \infty} \left(|z|^n \left| \frac{\partial^\alpha f}{\partial x^{\alpha_1} \partial y^{\alpha_2}} \right| \right) = 0 \right\}.$$
- If $F / \mathbb{Q}_p$, then
$$\begin{aligned} \mathcal{S}(F) &= \{\text{locally constant } f : F \to \mathbb{C} \text{ of compact support}\} \\ &= \{\text{span of characteristic functions } \mathbb{1}_{a + \pi^n \mathcal{O}_F}\}. \end{aligned}$$

If $f \in \mathcal{S}(F)$, write
$$\int_F f(x) \, \mathrm{d}_F x$$
for the integral. If $F / \mathbb{Q}_p$ and $f = \mathbb{1}_{a + \pi^n \mathcal{O}_F}$, then
$$\int_F f(x) \, \mathrm{d}_F x = \operatorname{meas}(a + \pi^n \mathcal{O}_F),$$
that is p-adic integrals are basically just finite sums. Also write
$$\int_U f(x) \, \mathrm{d}_F x = \int_F \mathbb{1}_U f(x) \, \mathrm{d}_F x,$$
for $U \subset F$ compact open.

Lemma 9.4. *Let $F / \mathbb{Q}_p$, and let $\mathfrak{a} \subset F$ be a fractional ideal. Then*
$$\int_{\mathfrak{a}} \psi(x) \, \mathrm{d}_F x = \int_F \mathbb{1}_{\mathfrak{a}} \psi(x) \, \mathrm{d}_F x = \begin{cases} \operatorname{meas}(\mathfrak{a}) & \mathfrak{a} \subset \mathcal{D}_{F/\mathbb{Q}_p}^{-1} \\ 0 & \textit{otherwise} \end{cases},$$
where $\mathbb{1}_{\mathfrak{a}} \psi \in \mathcal{S}(F)$.

Proof.

- If $\mathfrak{a} \subset \mathcal{D}_{F/\mathbb{Q}_p}^{-1}$, then $\operatorname{Tr}_{F/\mathbb{Q}_p}(\mathfrak{a}) \subset \mathbb{Z}_p$ so $\psi|_{\mathfrak{a}} = 1$, as $\psi_p|_{\mathbb{Z}_p} = 1$.
- If $\mathfrak{a} \not\subset \mathcal{D}_{F/\mathbb{Q}_p}^{-1}$, there exists $x \in \mathfrak{a}$ such that $\operatorname{Tr}_{F/\mathbb{Q}_p}(x) \notin \mathbb{Z}_p$, so $\psi(x) \ne 1$. As $x + \mathfrak{a} = \mathfrak{a}$, and $\mathrm{d}_F(x + y) = \mathrm{d}_F y$,
$$\int_{\mathfrak{a}} \psi(y) \, \mathrm{d}_F y = \int_{\mathfrak{a}} \psi(x + y) \, \mathrm{d}_F y = \psi(x) \int_{\mathfrak{a}} \psi(y) \, \mathrm{d}_F y,$$
so the integral is zero.

$\square$

Compare to
$$\sum_{g \in G} \chi(g) = \begin{cases} \# G & g = e \\ 0 & \text{otherwise} \end{cases},$$
for G finite abelian.

Definition. Let $f \in \mathcal{S}(F)$. Define the **Fourier transform**
$$\widehat{f}(y) = \int_F \psi(xy) f(x) \, \mathrm{d}_F x,$$
where $\psi(xy) f(x) \in \mathcal{S}(F)$.

Proposition 9.5.

1. *If $F = \mathbb{R}$ and $f(x) = e^{-\pi x^2}$, then $\widehat{f} = f$.*
2. *If $F = \mathbb{C}$ and $f(z) = \frac{1}{\pi} e^{-2\pi z \overline{z}}$, then $\widehat{f} = f$.*
3. *If $F/\mathbb{Q}_p$ and $f = \mathbb{1}_{\pi^n \mathcal{O}_F}$, then*
$$\widehat{f} = q^{-n-\frac{\delta}{2}} \mathbb{1}_{\pi^{-n} \mathcal{D}_{F/\mathbb{Q}_p}^{-1}} = q^{-n-\frac{\delta}{2}} \mathbb{1}_{\pi^{-n-\delta} \mathcal{O}_F}.$$

Proof.

1. Changing the contour of f,
$$\widehat{f}(y) = \int_{-\infty}^{\infty} e^{-2\pi i x y - \pi x^2} \, \mathrm{d}x = e^{-\pi y^2} \int_{-\infty}^{\infty} e^{-\pi (x+iy)^2} \, \mathrm{d}x = e^{-\pi y^2} \int_{-\infty}^{\infty} e^{-\pi x^2} \, \mathrm{d}x = e^{-\pi y^2}.$$
2. Exercise. [10]
3. By 9.4,
$$\widehat{f}(y) = \int_{\pi^n \mathcal{O}_F} \psi(xy) \, \mathrm{d}_F \, x = \begin{cases} \mathrm{meas}(\pi^n \mathcal{O}_F) & y \in \pi^{-n} \mathcal{D}_{F/\mathbb{Q}_p}^{-1} \\ 0 & y \notin \pi^{-n} \mathcal{D}_{F/\mathbb{Q}_p}^{-1} \end{cases},$$
which gives the answer.

□

Fact. If $f \in \mathcal{S}(F)$, then $\widehat{f} \in \mathcal{S}(F)$.

- For $F/\mathbb{R}$, this is standard analysis, using $\widehat{f^{(n)}}(y) = (2\pi i y)^n \widehat{f}(y)$.
- For $F/\mathbb{Q}_p$, this is an exercise in sheet 3.

Proposition 9.6 (Inversion formula)**.**
$$\widehat{\widehat{f}}(x) = f(-x).$$

Proof.

- For $F = \mathbb{R}$, this is standard analysis.
- For $F = \mathbb{C}$, notice that if $f(z) = f(x+iy) = g(x,y)$, then $\widehat{f}(w) = \widehat{f}(u+iv) = 2\widehat{g}(2u, -2v)$ since $zw + \overline{zw} = 2(ux - vy)$, so $\widehat{\widehat{f}}(z) = f(-z)$ easily.
- For $F/\mathbb{Q}_p$, if $f = \mathbb{1}_{\mathcal{O}_F}$, then
$$\widehat{\widehat{f}} = q^{-\frac{\delta}{2}} \widehat{\mathbb{1}_{\mathcal{D}_{F/\mathbb{Q}_p}^{-1}}} = q^{-\frac{\delta}{2}} q^{\delta - \frac{\delta}{2}} \mathbb{1}_{\mathcal{O}_F},$$
by 9.5.3 twice. [11]

□

This explains the choice of constants in $\mathrm{d}_F \, x$, a **self-dual** Haar measure, otherwise we would get $\widehat{\widehat{f}}(x) = cf(-x)$.

Lemma 9.7. *Let $c \in F^\times$, and let $g(x) = f(cx)$. Then*
$$\widehat{g}(y) = |c|_F^{-1} \widehat{f}(c^{-1} y).$$

Proof. By $x = c^{-1} t$,
$$\widehat{g}(y) = \int_F \psi(xy) f(cx) \, \mathrm{d}_F \, x = \int_F \psi(c^{-1} t y) f(t) \, \mathrm{d}_F (c^{-1} t) = |c|_F^{-1} \int_F \psi(t c^{-1} y) f(t) \, \mathrm{d}_F \, t = |c|_F^{-1} \widehat{f}(c^{-1} y).$$

□

[10] Exercise
[11] Exercise: the rest is in example sheet

9.4 Local ζ-integrals

Lecture 19 Thursday 04/03/21

Definition. Define the **Haar measure** $\mathrm{d}_F^\times x$ **on the multiplicative group** $F^\times$ by

$$\mathrm{d}_F^\times x = \begin{cases} \dfrac{1}{|x|_F} \mathrm{d}_F x & F/\mathbb{R} \\ \dfrac{q^{\frac{\delta}{2}}}{1-q^{-1}} \dfrac{1}{|x|_F} \mathrm{d}_F x & F/\mathbb{Q}_p \end{cases},$$

where q is the residue field order and $\delta = \mathrm{v}\left(\mathcal{D}_{F/\mathbb{Q}_p}\right)$.

Since $\mathrm{d}_F(ax) = |a|_F \mathrm{d}_F x$, $\mathrm{d}_F^\times (ax) = \mathrm{d}_F^\times x$. If $F/\mathbb{Q}_p$, then

$$\operatorname{meas} \mathcal{O}_F^\times = \int_{\mathcal{O}_F^\times} \mathrm{d}_F^\times x = \frac{q^{\frac{\delta}{2}}}{1-q^{-1}} \int_{\mathcal{O}_F \setminus \pi \mathcal{O}_F} \mathrm{d}_F x = \frac{q^{\frac{\delta}{2}}}{1-q^{-1}} \left(q^{-\frac{\delta}{2}} - q^{-1-\frac{\delta}{2}}\right) = 1.$$

This is the reason to normalise in this way.

Definition. Let $f \in \mathcal{S}(F)$, and let $s \in \mathbb{C}$. Define **local ζ-integrals**, or **local Euler factors**,

$$\zeta(f,s) = \int_{F^\times} f(x) |x|_F^s \, \mathrm{d}_F^\times x = c \lim_{\epsilon \to 0} \int_{\left\{x \in F \mid |x|_F \geq \epsilon\right\}} f(x) |x|_F^{s-1} \, \mathrm{d}_F x, \qquad c = \begin{cases} 1 & F/\mathbb{R} \\ \dfrac{q^{\frac{\delta}{2}}}{1-q^{-1}} & F/\mathbb{Q}_p \end{cases}.$$

If $F/\mathbb{Q}_p$, this is just a finite sum. Since f is continuous and tends rapidly to zero as $|x|_F \to \infty$ if $F/\mathbb{R}$ and has compact support if $F/\mathbb{Q}_p$, the limit exists for $\Re s \geq 1$.

Proposition 9.8.

1. *If $F = \mathbb{R}$ and $f(x) = e^{-\pi x^2}$, then $\zeta(f,s) = \Gamma_{\mathbb{R}}(s)$.*
2. *If $F = \mathbb{C}$ and $f(z) = \frac{1}{\pi} e^{-2\pi z \overline{z}}$, then $\zeta(f,s) = \Gamma_{\mathbb{C}}(s)$.*
3. *If $F/\mathbb{Q}_p$ and $f = \mathbb{1}_{\pi^n \mathcal{O}_F}$, then*
$$\zeta(f,s) = \frac{q^{-ns}}{1-q^{-s}}.$$

Recall

$$\Gamma(s) = \int_0^\infty e^{-t} \frac{t^s}{t} \, \mathrm{d}t, \qquad \Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right), \qquad \Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s} \Gamma(s).$$

Proof.

1. Follows from the definition of $\Gamma(s)$ after a change of variables.
2. Follows from the definition of $\Gamma(s)$ after a change of variables and polar coordinates.
3.

$$\begin{aligned} \zeta\left(\mathbb{1}_{\pi^n \mathcal{O}_F}, s\right) &= \int_{\pi^n \mathcal{O}_F \setminus \{0\}} |x|_F^s \, \mathrm{d}_F^\times x = \sum_{m=n}^\infty \int_{\pi^m \mathcal{O}_F \setminus \pi^{m+1} \mathcal{O}_F} \frac{q^{-ms}}{q^{-m}} \frac{q^{\frac{\delta}{2}}}{1-q^{-1}} \, \mathrm{d}_F x \\ &= \sum_{m=n}^\infty q^{m(1-s)+\frac{\delta}{2}} \frac{1}{1-q^{-1}} \operatorname{meas}\left(\pi^m \mathcal{O}_F \setminus \pi^{m+1} \mathcal{O}_F\right) \\ &= \sum_{m=n}^\infty q^{m(1-s)+\frac{\delta}{2}} \frac{1}{1-q^{-1}} q^{-\frac{\delta}{2}} \left(\frac{1}{q^m} - \frac{1}{q^{m+1}}\right) = \sum_{m=n}^\infty q^{-ms} = \frac{q^{-ns}}{1-q^{-s}}. \end{aligned}$$

$\square$

Example. $\zeta\left(\mathbb{1}_{\mathcal{O}_F}, s\right) = 1/\left(1-q^{-s}\right)$.

A variant is to also consider, for a continuous homomorphism $\chi : F^\times \to \mathbb{C}^\times$,

$$\zeta\left(\chi, f, s\right) = \int_{F^\times} f\left(x\right)\chi\left(x\right)|x|_F^s \ \mathrm{d}_F^\times x,$$

defined as a limit in the same way.

9.5 Global Fourier analysis

Let K be a number field with completions K_v, and let $\psi_v : K_v \to \mathrm{U}\left(1\right)$, $\mathrm{d}_v\, x$, $\mathrm{d}_v^\times\, x$, $\mathcal{S}\left(K_v\right)$, and δ_v be the objects defined above for $F = K_v$. Let

$$\mathrm{V}_{K,\mathrm{r}} = \left\{v \in \mathrm{V}_{K,\mathrm{f}} \mid v \text{ ramified in } F/\mathbb{Q}_p\right\} = \left\{v \in \mathrm{V}_{K,\mathrm{f}} \mid \delta_v \neq 0\right\}.$$

Then

$$\mathbb{A}_K = \bigcup_S \left(\prod_{v\in S} K_v \times \prod_{v\notin S} \mathcal{O}_v\right),$$

where $S \subset \mathrm{V}_K$ is finite containing $\mathrm{V}_{K,\infty}$.

Definition. Let $f_v \in \mathcal{S}\left(K_v\right)$ for $v \in \mathrm{V}_K$ such that for all but finitely many $v \in \mathrm{V}_{K,\mathrm{f}}$, $f_v = \mathbb{1}_{\mathcal{O}_v}$. Then if $x = \left(x_v\right) \in \mathbb{A}_K$, for all but finitely many v, $f_v\left(x_v\right) = 1$. So can define

$$f\left(x\right) = \prod_{v\in \mathrm{V}_K} f_v\left(x_v\right),$$

and write $f = \prod_v f_v$, or better, $f = \bigotimes_v f_v$. Then the **global Schwartz space** $\mathcal{S}\left(\mathbb{A}_K\right)$ is the space of finite linear combinations of f of this type.

Definition. Let $f = \bigotimes_v f_v \in \mathcal{S}\left(\mathbb{A}_K\right)$ where $f_v = \mathbb{1}_{\mathcal{O}_v}$ for all $v \notin S$ for a finite set $S \supset \mathrm{V}_{K,\infty} \cup \mathrm{V}_{K,\mathrm{r}}$. Then $f = 0$ outside $\prod_{v\in S} K_v \times \prod_{v\notin S} \mathcal{O}_v$ and can define the **global integral**

$$\int_{\mathbb{A}_K} f\left(x\right)\ \mathrm{d}_{\mathbb{A}}\, x = \prod_v \int_{K_v} f_v\left(x\right)\ \mathrm{d}_v\, x = \prod_{v\in S}\int_{K_v} f_v\left(x\right)\ \mathrm{d}_v\, x,$$

since if $v \notin S$,

$$\int_{K_v} f_v\left(x\right)\ \mathrm{d}_v\, x = \int_{\mathcal{O}_v} \mathrm{d}_v\, x = 1.$$

Definition. Let the **global additive character** be

$$\psi_{\mathbb{A}} = \prod_v \psi_v \quad : \quad \begin{array}{ccc} \mathbb{A}_K & \longrightarrow & \mathrm{U}\left(1\right) \\ \left(x_v\right) & \longmapsto & \prod_v \psi_v\left(x_v\right) \end{array},$$

which is a finite product, since for all but finitely many $v \in \mathrm{V}_{K,\mathrm{f}}$, $x_v \in \mathcal{O}_v$ so $\psi_v\left(x_v\right) = \psi_p\left(\mathrm{Tr}_{K_v/\mathbb{Q}_p}\left(x_v\right)\right) = 1$.

Proposition 9.9. *$\psi_{\mathbb{A}}$ is continuous, and $\psi_{\mathbb{A}}\left(x\right) = 1$ if $x \in K$.*

Proof. Take a finite $S \supset \mathrm{V}_{K,\infty}$. The restriction of $\psi_{\mathbb{A}}$ to $\prod_{v\in S} K_v \times \prod_{v\notin S} \mathcal{O}_v$ factors through $\prod_{v\in S}\psi_v : \prod_{v\in S} K_v \to \mathrm{U}\left(1\right)$, which is continuous. Now $\psi_{\mathbb{A}}\left(x\right) = \psi_{\mathbb{A}_{\mathbb{Q}}}\left(\mathrm{Tr}_{K/\mathbb{Q}}\left(x\right)\right)$, as $\mathrm{Tr}_{K/\mathbb{Q}}\left(x\right) = \sum_{v\mid p}\mathrm{Tr}_{K_v/\mathbb{Q}_p}\left(x\right)$ for all $p \leq \infty$, so it is enough to consider $K = \mathbb{Q}$. Write $x \in \mathbb{Q}$ as partial fractions $x = \sum_i y_i/p_i^{k_i}$ for $y_i \in \mathbb{Z}$ and $k_i \geq 0$. Then $\psi_{p_i}\left(x\right) = e^{2\pi i y_i/p_i^{k_i}}$ as for $j \neq i$, $y_j/p_j^{k_j} \in \mathbb{Z}_{p_i}$, and $\psi_p\left(x\right) = 1$ if $p \notin \left\{p_i\right\}$. Thus $\prod_{p<\infty}\psi_p\left(x\right) = e^{2\pi i x} = \psi_\infty\left(x\right)^{-1}$. ☐

Definition. Define the **global Fourier transform** of $f \in \mathcal{S}\left(\mathbb{A}_K\right)$ as

$$\widehat{f}\left(y\right) = \int_{\mathbb{A}_K}\psi_{\mathbb{A}}\left(xy\right) f\left(x\right)\ \mathrm{d}_{\mathbb{A}}\, x = \prod_v \widehat{f}_v\left(y_v\right), \qquad f = \bigotimes_v f_v.$$

Note that for all but finitely many v, $f_v = \mathbb{1}_{\mathcal{O}_v} = \widehat{f}_v$.

9.6 Global ζ-integrals

Definition. Let $f = \bigotimes_v f_v \in \mathcal{S}(\mathbb{A}_K)$. Define the **global ζ-integral**

$$\zeta(f, s) = \int_{\mathcal{J}_K} f(x) |x|_{\mathbb{A}}^s \, \mathrm{d}_{\mathcal{J}} x = \prod_{v \in \mathrm{V}_K} \int_{K_v^\times} f_v(x) |x|_v^s \, \mathrm{d}_v^\times x = \prod_{v \in \mathrm{V}_K} \zeta(f_v, s),$$

which really is a genuine infinite product.

Lecture 20 Saturday 06/03/21

If $a \in \mathcal{J}_K$, then there is an isomorphism

$$\begin{array}{cccc} a & : & \mathbb{A}_K & \longrightarrow & \mathbb{A}_K \\ & & x & \longmapsto & ax \end{array},$$

so if $f \in \mathcal{S}(\mathbb{A}_K)$ then $f(ax) \in \mathcal{S}(\mathbb{A}_K)$. Then $\mathrm{d}_{\mathbb{A}}(ax) = |a|_{\mathbb{A}} \, \mathrm{d}_{\mathbb{A}} x$, since holds locally, and $\mathrm{d}_{\mathcal{J}}(ax) = \mathrm{d}_{\mathcal{J}} x$.

Proposition 9.10. *The product $\zeta(f, s)$ converges absolutely for $\Re s > 1$.*

Proof. Assume $f = \bigotimes_v f_v$ such that $f_v = \mathbb{1}_{\mathcal{O}_v}$ for all $v \notin S$. Then $\zeta(f_v, s) = 1/(1 - \mathrm{q}_v^{-s})$ for $v \notin S$, which gives convergence by 9.2, the product for $\zeta_K(s)$. $\square$

Theorem 9.11. *$\zeta(f, s)$ has a meromorphic continuation to $\mathbb{C}$, with at worst simple poles at $s = 0, 1$. Moreover,*

$$\zeta(f, s) = \zeta\left(\widehat{f}, 1 - s\right),$$

with

$$\operatorname{Res} \zeta(f, s) = \begin{cases} \widehat{f}(0) \kappa & s = 1 \\ -f(0) \kappa & s = 0 \end{cases}, \qquad \kappa = \operatorname{meas}\left(\mathcal{J}_K^1 / K^\times\right) > 0.$$

Let $n = [K : \mathbb{Q}]$. Then

$$\begin{array}{cccc} \mathrm{i} & : & \mathbb{R}_{>0} & \longrightarrow & K_\infty^\times = \prod_{v \mid \infty} K_v^\times \hookrightarrow \mathcal{J}_K \\ & & t & \longmapsto & \left(t^{\frac{1}{n}}\right)_v \end{array},$$

so $|\mathrm{i}(t)|_{\mathbb{A}} = t$. So there is an isomorphism

$$\begin{array}{ccc} \mathbb{R}_{>0} \times \mathcal{J}_K^1 & \longrightarrow & \mathcal{J}_K \\ (t, x) & \longmapsto & \mathrm{i}(t) x \end{array}.$$

Write t in place of $\mathrm{i}(t)$. Use this to define a measure $\mathrm{d}_{\mathcal{J}^1} x$ on $\mathcal{J}_K^1$ such that

$$\int_{\mathcal{J}_K} f(x) \, \mathrm{d}_{\mathcal{J}} x = \int_0^\infty \left(\int_{\mathcal{J}_K^1} f(tx) \, \mathrm{d}_{\mathcal{J}^1} x \right) \frac{1}{t} \, \mathrm{d}t. \tag{9}$$

The most concrete way to do this is to pick $\phi : \mathbb{R}_{>0} \to \mathbb{R}$, C^∞ of compact support such that

$$\int_0^\infty \frac{\phi(t)}{t} \, \mathrm{d}t = 1.$$

Given f on $\mathcal{J}_K^1$, let

$$\begin{array}{cccc} \widetilde{f_\phi} & : & \mathcal{J}_K & \longrightarrow & \mathbb{C} \\ & & tx & \longmapsto & \phi(t) f(x) \end{array},$$

and define

$$\int_{\mathcal{J}_K^1} f(x) \, \mathrm{d}_{\mathcal{J}^1} x = \int_{\mathcal{J}_K} \widetilde{f_\phi}(y) \, \mathrm{d}_{\mathcal{J}} y.$$

Lemma 9.12.

1. *This is independent of ϕ.*
2. *The identity* (9) *holds.*

Proof. If $y \in \mathcal{J}_K$ such that $y = tx$ for $t > 0$ and $x \in \mathcal{J}_K^1$, then $x = y / |y|_{\mathbb{A}}$ and $t = |y|_{\mathbb{A}}$.

1. So $\widetilde{f_\phi}(y) = \phi(|y|_{\mathbb{A}}) f(y/|y|_{\mathbb{A}})$. Putting $s' = |y|_{\mathbb{A}}$ and $y' = sy/s'$, so $|y'|_{\mathbb{A}} = s$,

$$\begin{aligned}
\int_{\mathcal{J}_K^1} f(x) \, \mathrm{d}_{\mathcal{J}^1} x &= \int_0^\infty \frac{\psi(s)}{s} \, \mathrm{d}s \int_{\mathcal{J}_K} \widetilde{f_\phi}(y) \, \mathrm{d}_{\mathcal{J}} y \\
&= \int_0^\infty \left(\int_{\mathcal{J}_K} \psi(s) \phi(|y|_{\mathbb{A}}) f\left(\frac{y}{|y|_{\mathbb{A}}} \right) \mathrm{d}_{\mathcal{J}} y \right) \frac{1}{s} \, \mathrm{d}s \\
&= \int_0^\infty \left(\int_{\mathcal{J}_K} \psi(|y'|_{\mathbb{A}}) \phi(s') f\left(\frac{y'}{|y'|_{\mathbb{A}}} \right) \mathrm{d}_{\mathcal{J}} y' \right) \frac{1}{s'} \, \mathrm{d}s' \\
&= \int_0^\infty \frac{\phi(s')}{s'} \, \mathrm{d}s' \int_{\mathcal{J}_K} \widetilde{f_\psi}(y) \, \mathrm{d}_{\mathcal{J}} y = \int_{\mathcal{J}_K^1} f(x) \, \mathrm{d}_{\mathcal{J}^1} x.
\end{aligned}$$

2. If $g_t(x) = f(tx)$, then $\widetilde{g_t}(y) = \phi(|y|_{\mathbb{A}}) f(ty/|y|_{\mathbb{A}})$, so putting $s = |y|_{\mathbb{A}}$ and $x = ty/s$,

$$\begin{aligned}
\int_0^\infty \left(\int_{\mathcal{J}_K^1} f(tx) \, \mathrm{d}_{\mathcal{J}^1} x \right) \frac{1}{t} \, \mathrm{d}t &= \int_0^\infty \left(\int_{\mathcal{J}_K} \phi(|y|_{\mathbb{A}}) f\left(\frac{ty}{|y|_{\mathbb{A}}} \right) \mathrm{d}_{\mathcal{J}} y \right) \frac{1}{s} \, \mathrm{d}s \\
&= \int_0^\infty \frac{\phi(s)}{s} \, \mathrm{d}s \int_{\mathcal{J}_K} f(x) \, \mathrm{d}_{\mathcal{J}} x = \int_{\mathcal{J}_K} f(x) \, \mathrm{d}_{\mathcal{J}} x.
\end{aligned}$$

□

So

$$\zeta(f, s) = \int_0^\infty \frac{\zeta_t(f, s)}{t} \, \mathrm{d}t, \qquad \zeta_t(f, s) = t^s \int_{\mathcal{J}_K^1} f(tx) \, \mathrm{d}_{\mathcal{J}^1} x.$$

Recall that $\mathcal{J}_K^1 / K^\times = \mathcal{C}_K^1$ is compact. Will show next time that there exists a **fundamental domain** $E \subset \mathcal{J}_K^1$ with $\operatorname{meas}(E) < \infty$ and $\overline{E}$ compact such that

$$\mathcal{J}_K^1 = \bigsqcup_{a \in K^\times} aE.$$

Let $\kappa = \operatorname{meas}(E)$.

Proposition 9.13 (Functional equation for ζ_t)**.**

$$\zeta_t(f, s) + \kappa f(0) t^s = \zeta_{\frac{1}{t}}\left(\widehat{f}, 1 - s \right) + \kappa \widehat{f}(0) t^{s-1}.$$

This is an analogue of the functional equation of $\Theta(t) = \sum_{n \in \mathbb{Z}} e^{-\pi n^2 t}$. The proof uses the following.

Theorem 9.14 (Poisson summation formula)**.** *Let $f \in \mathcal{S}(\mathbb{A}_K)$. Then*

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

and both sums are absolutely convergent.

Corollary 9.15. *Let $x \in \mathcal{J}_K$. Then*

$$\sum_{a \in K} f(xa) = |x|_{\mathbb{A}}^{-1} \sum_{a \in K} \widehat{f}\left(x^{-1} a \right).$$

Proof. Apply 9.14 to $f \circ x$ and use 9.7. □

Proof of 9.13. Write the integral over $\mathcal{J}_K^1$ as an integral over E of a sum over $K^\times$. By 9.15,

$$\begin{aligned}
\zeta_t(f,s) + \kappa f(0) t^s &= t^s \int_{\mathcal{J}_K^1} f(tx) \, \mathrm{d}_{\mathcal{J}^1} x \\
&= t^s \int_E \sum_{a \in K^\times} f(atx) \, \mathrm{d}_{\mathcal{J}^1} x + \kappa f(0) t^s = t^s \int_E \sum_{a \in K} f(atx) \, \mathrm{d}_{\mathcal{J}^1} x \\
&= t^s \int_E \sum_{a \in K} |tx|_{\mathbb{A}}^{-1} \widehat{f}\left(t^{-1}x^{-1}a\right) \, \mathrm{d}_{\mathcal{J}^1} x = t^{s-1} \int_E \sum_{a \in K^\times} \widehat{f}\left(t^{-1}x^{-1}a\right) \, \mathrm{d}_{\mathcal{J}^1} x + \kappa \widehat{f}(0) t^{s-1} \\
&= t^{s-1} \int_{\mathcal{J}_K^1} \widehat{f}\left(t^{-1}x^{-1}\right) \, \mathrm{d}_{\mathcal{J}^1} x + \kappa \widehat{f}(0) t^{s-1} = \zeta_{\frac{1}{t}}\left(\widehat{f}, 1-s\right) + \kappa \widehat{f}(0) t^{s-1},
\end{aligned}$$

since $|x|_{\mathbb{A}} = 1$ on E. $\square$

Proof of 9.11. Now, if $\Re s > 1$,

$$\begin{aligned}
\zeta(f,s) = \int_0^\infty \frac{\zeta_t(f,s)}{t} \, \mathrm{d}t &= \int_1^\infty \frac{\zeta_t(f,s)}{t} \, \mathrm{d}t + \int_0^1 \frac{\zeta_t(f,s)}{t} \, \mathrm{d}t = \int_1^\infty \frac{\zeta_t(f,s) + \zeta_{\frac{1}{t}}(f,s)}{t} \, \mathrm{d}t \\
&= \int_1^\infty \frac{\zeta_t(f,s) + \zeta_t\left(\widehat{f}, 1-s\right) - \kappa f(0) t^{-s} + \kappa \widehat{f}(0) t^{1-s}}{t} \, \mathrm{d}t \\
&= \int_1^\infty \frac{\zeta_t(f,s) + \zeta_t\left(\widehat{f}, 1-s\right)}{t} \, \mathrm{d}t + \kappa \left(\frac{\widehat{f}(0)}{s-1} - \frac{f(0)}{s}\right).
\end{aligned}$$

Now since $f(tx) \to 0$ rapidly as $t \to \infty$ as $f \in \mathcal{S}(\mathbb{A}_K)$, $\int_1^\infty (\zeta_t(f,s)/t) \, \mathrm{d}t$ is an entire function of $s \in \mathbb{C}$, which gives a meromorphic continuation of $\zeta(f,s)$ with poles at $s = 0, 1$, and $\zeta(f,s) = \zeta\left(\widehat{f}, 1-s\right)$. $\square$

Morally, $\zeta_t(f,s)$ is Θ deprived of the constant term.