

# Algebraic Number Theory

Lectured by Prof Tony Scholl  
Typed by David Kurniadi Angdinata

Lent 2021

**Syllabus**

# Contents

<b>1</b>	<b>Absolute values and places</b>	<b>3</b>
1.1	Absolute values . . . . .	3
1.2	Places . . . . .	4
<b>2</b>	<b>Number fields</b>	<b>6</b>
2.1	Dedekind domains . . . . .	6
2.2	Places of number fields . . . . .	8
<b>3</b>	<b>Different and discriminant</b>	<b>10</b>
3.1	Discriminant . . . . .	10
3.2	Different . . . . .	12
<b>4</b>	<b>Example: quadratic fields</b>	<b>14</b>
<b>5</b>	<b>Example: cyclotomic fields</b>	<b>15</b>
<b>6</b>	<b>Ideles and adeles</b>	<b>17</b>
6.1	Adeles . . . . .	17
6.2	Ideles . . . . .	19
<b>7</b>	<b>Geometry of numbers</b>	<b>21</b>
7.1	Minkowski's theorem . . . . .	21
7.2	Compactness of $\mathcal{C}_K^1$ . . . . .	22
7.3	Finiteness of $\text{Cl}(K)$ and $S$ -unit theorem . . . . .	23
7.4	Strong approximation theorem . . . . .	25
<b>8</b>	<b>Idele class group and class field theory</b>	<b>26</b>
8.1	Artin reciprocity law . . . . .	26
8.2	Finite quotients of $\mathcal{C}_K$ . . . . .	27
8.3	Specific open subgroups of $\mathcal{C}_K$ . . . . .	28
8.4	Properties of $\text{Art}_{L/K}$ . . . . .	29
8.5	Examples . . . . .	31
8.6	Comparing $\mathcal{C}_K$ and $\text{Gal}(K^{\text{ab}}/K)$ . . . . .	33
<b>9</b>	<b><math>\zeta</math>-functions</b>	<b>34</b>
9.1	Riemann $\zeta$ -function . . . . .	34
9.2	Dedekind $\zeta$ -function . . . . .	35
9.3	Local Fourier analysis . . . . .	36
9.4	Local Fourier transform . . . . .	38
9.5	Local $\zeta$ -integrals . . . . .	39
9.6	Global Fourier analysis . . . . .	40
9.7	Global $\zeta$ -integral . . . . .	41
9.8	Proof of Poisson summation formula . . . . .	44
9.9	Proof of functional equation and analytic class number formula . . . . .	45
9.10	Description of $E \subset \mathbb{J}_K^1$ . . . . .	47
<b>10</b>	<b>L-functions</b>	<b>48</b>
10.1	Hecke characters . . . . .	48
10.2	Hecke L-functions . . . . .	50
10.3	Global $\zeta$ -integral . . . . .	51
10.4	Artin L-functions* . . . . .	52

# 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  $|\cdot| : K \rightarrow \mathbb{R}_{\geq 0}$  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

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

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

**Remark.** It is convenient to weaken 3 to

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

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  $z \mapsto z\bar{z}$  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

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

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  $y \in K$ , 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.  $\square$

**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.  $\square$

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  $1 \leq i \leq n$  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  $i \neq j$ . Then  $|z_j^N / (z_j^N + 1)|_i \rightarrow 0$  as  $N \rightarrow \infty$  if  $i \neq j$  but  $|z_j^N / (z_j^N + 1)|_j = |1 / (z_j^N + 1)|_j \rightarrow 0$ . 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  $z = y^N w / (y^N + 1)$  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  $n_i \geq 1$ , there exists  $x \in \mathbb{Q}$ , which is a  $p_i$ -adic integer for all  $i \in \{1, \dots, n\}$  and  $x \equiv a_i \pmod{p_i^{n_i}}$ . 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  $\{2, 3, \dots, \infty\} = \{p \leq \infty\}$ .

**Notation.** Let

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

Often use letters  $v$  and  $w$ , decorated suitably, to denote places. If  $v \in V_K$ , then  $K_v$  will denote the completion. If  $v : K^\times \rightarrow \mathbb{R}$  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*

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

*is dense, for the product topology.*

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*

$$\begin{aligned} L \otimes_K K_v &\longrightarrow \prod_{w \in V_L, w|v} L_w \\ x \otimes y &\longmapsto (xy)_w \end{aligned}$$

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

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

For the topological isomorphism, 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

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

- For all  $x \in L$ ,

$$N_{L/K}(x) = \prod_{w|v} N_{L_w/K_v}(x), \quad \text{Tr}_{L/K}(x) = \sum_{w|v} \text{Tr}_{L_w/K_v}(x).$$

Let  $L/K$  be a finite Galois extension with  $G = \text{Gal}(L/K)$ . 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  $w = \mathfrak{p}_v$  for a prime  $\mathfrak{p}$  in a Dedekind domain, then  $g(w) = \mathfrak{p}_{g(\mathfrak{p})}$ .

**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  $G_w \hookrightarrow \text{Aut}(L_w/K_v)$ , by continuity, so  $\#G_w \leq [L_w : K_v]$ , and

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

by 1.6. So have equality, hence  $[L_w : K_v] = \#G_w$ , and so  $L_w/K_v$  is Galois with group  $\text{Gal}(L_w/K_v) \xrightarrow{\sim} G_w \subset G$ , 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  $f(w \mid v) = f_{L_w/K_v}$  to be the degree of residue class extension and  $e(w \mid v)$  to be the ramification degree. Then

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

Lecture 2  
Saturday  
23/01/21

## 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  $K = \text{Frac } R$ .
  - (a)  $\implies$  (b). Enough to check <sup>1</sup> 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,  $v_{\mathfrak{p}}(a_1) \leq v_{\mathfrak{p}}(a_i)$  for all  $i$ . Then  $IR_{\mathfrak{p}} = a_1R_{\mathfrak{p}}$ , 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  $I = R[x] = \sum_{0 \leq i < d} Rx^i \subset K$ , 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  $\mathfrak{p}(\mathfrak{p}^{-1}\mathfrak{q}) = \mathfrak{q}$ , so as  $\mathfrak{q}$  is prime and  $\mathfrak{p}^{-1}\mathfrak{q} \not\subset \mathfrak{q}$ , so  $\mathfrak{p} \subset \mathfrak{q}$ , that is  $\mathfrak{p} = \mathfrak{q}$ .

---

<sup>1</sup>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.  $\square$

**Theorem 2.2.** *Let  $R$  be Dedekind. Then*

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

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}, \quad v_{\mathfrak{p}}(I) = \inf \{v_{\mathfrak{p}}(x) \mid x \in I\},$$

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

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

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

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

So  $a_{\mathfrak{p}}$  are unique and  $(v_{\mathfrak{p}})_{\mathfrak{p}}$  is an isomorphism.

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

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

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

The quotient group

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

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

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

Lecture 3  
Tuesday  
26/01/21

## 2.2 Places of number fields

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

**Theorem 2.3.** *There is a bijection*

$$\begin{aligned} \{\text{non-zero primes of } \mathcal{O}_K\} &\longrightarrow V_{K,f} \\ \mathfrak{p} &\longmapsto |\cdot|_{\mathfrak{p}} \end{aligned}$$

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

**Notation.** If  $v \in V_{K,f}$ , 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  $\pi_v \in K$ ,
- $v : K^\times \rightarrow \mathbb{Z}$  is the **normalised discrete valuation** such that  $v(\pi_v) = 1$ ,
- $\kappa_v = \mathcal{O}_v / \mathfrak{p}_v \cong \mathcal{O}_v / \langle \pi_v \rangle$  is finite of order  $q_v = p^{f_v}$  for a prime  $p$  such that  $v \mid p$ , and
- $|x|_v = q_v^{-v(x)}$  is the **normalised AV**, so  $|\pi_v|_v = 1/q_v$ .

**Theorem 2.4.** *There is a bijection*

$$\begin{aligned} \{\text{homomorphisms } \sigma : K \hookrightarrow \mathbb{C}\} / (\sigma \sim \bar{\sigma}) &\longrightarrow V_{K,\infty} \\ \sigma &\longmapsto |\sigma(\cdot)| \end{aligned}$$

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

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

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, the group of homomorphisms  $\sigma : K \hookrightarrow \mathbb{C}$  has order  $n = [K : \mathbb{Q}]$  and there is an isomorphism

$$\begin{aligned} K \otimes_{\mathbb{Q}} \mathbb{C} &\longrightarrow \prod_{\sigma : K \hookrightarrow \mathbb{C}} \mathbb{C} \\ x \otimes z &\longmapsto (\sigma(x)z)_{\sigma} \end{aligned} \tag{1}$$

Complex conjugation acts on both sides of (1) by  $x \otimes z \mapsto x \otimes \bar{z}$  and  $(z_{\sigma})_{\sigma} \mapsto (\bar{z}_{\bar{\sigma}})_{\sigma}$ . Let

$$\sigma_1, \dots, \sigma_{r_1} : K \hookrightarrow \mathbb{R}, \quad \sigma_{r_1+1} = \overline{\sigma_{r_1+r_2+1}}, \dots, \sigma_{r_1+r_2} = \overline{\sigma_{r_1+2r_2}} : K \hookrightarrow \mathbb{C}, \quad r_1 + 2r_2 = n.$$

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

$$K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \prod_{\sigma \text{ real}} \mathbb{R} \times \prod_{(\sigma, \bar{\sigma}), \sigma \neq \bar{\sigma}} \{(z, \bar{z}) \in \mathbb{C} \times \mathbb{C}\} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

$\square$



**Notation.** Define

$$K_\infty = K \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{v \in V_{K,\infty}} K_v \cong \mathbb{R}^{\{\text{real } v\}} \times \mathbb{C}^{\{\text{complex } v\}},$$

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  $\sigma \neq \bar{\sigma} : K \hookrightarrow \mathbb{C}$  and  $|x|_v = \sigma(x) \bar{\sigma}(x) = |\sigma(x)|^2$  is the square of modulus.

Let  $L/K$  be an extension of number fields, and let  $w \mid v$ .

- If  $L_w/K_v$  is a finite extension of non-archimedean local fields  $[L_w : K_v] = e(w \mid v) f(w \mid v)$ .
- If  $L_w/K_v \cong \mathbb{R}/\mathbb{R}$  or  $L_w/K_v \cong \mathbb{C}/\mathbb{C}$ , then  $f = e = 1$ . If  $L_w/K_v \cong \mathbb{C}/\mathbb{R}$ , then  $v$  is ramified, and  $e = 2$  and  $f = 1$ . Neukirch has a different terminology.

**Proposition 2.5.** *Let  $x \in L$  and  $v \in V_K$ . Then*

$$|N_{L/K}(x)|_v = \prod_{w \mid v} |x|_w.$$

*Proof.*  $N_{L/K}(x) = \prod_{w \mid v} N_{L_w/K_v}(x)$  so it is enough to show  $|N_{L_w/K_v}(x)|_v = |x|_w$ . If  $v$  is finite, it is enough to take  $x = \pi_w \in L$ , and

$$|N_{L_w/K_v}(\pi_w)|_v = |u \pi_v^{f(w|v)}|_v = q_v^{-f(w|v)} = q_w^{-1} = |\pi_w|_w, \quad u \in \mathcal{O}_{K_v}^\times.$$

If  $v$  is infinite, need only consider  $L_w/K_v \cong \mathbb{C}/\mathbb{R}$  and  $N_{\mathbb{C}/\mathbb{R}}(z) = z\bar{z}$ . □

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

$$\prod_{v \in V_K} |x|_v = 1.$$

*Proof.* Let  $x = a/b$  for  $a, b \in \mathcal{O}_K \setminus \{0\}$ . Then

$$\{v \in V_K \mid |x|_v \neq 1\} \subset V_{K,\infty} \cup \{v \in V_{K,f} \mid v(a) > 0 \text{ or } v(b) > 0\}$$

is a finite set. Now

$$\prod_{v \in V_K} |x|_v = \prod_{p \leq \infty} \prod_{v \mid p} |x|_v = \prod_{p \leq \infty} |N_{K/\mathbb{Q}}(x)|_p.$$

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  $p \leq \infty$ . □

**Remark.**

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

**Fact.** On  $K_v$ , for any  $v$ , there is a translation-invariant measure, the Haar measure,  $d_v x$ , and for all  $a \in K_v^\times$ ,  $d_v(ax) = |a|_v d_v x$  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

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

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

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

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

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

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

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

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

$$\mathrm{disc}(S/R) = \mathrm{disc}(S_1/R) \mathrm{disc}(S_2/R).$$

- If  $f : R \rightarrow R'$  is a ring homomorphism, then

$$\mathrm{disc}(S \otimes_R R'/R') = f(\mathrm{disc}(S/R)) R'.$$

- If  $R$  is a field, then  $\mathrm{disc}(S/R) = R$  or  $\mathrm{disc}(S/R) = 0$ , and  $\mathrm{disc}(S/R) = R$  if and only if the  $R$ -bilinear form

$$\begin{aligned} S \times S &\longrightarrow R \\ (x, y) &\longmapsto \mathrm{Tr}_{S/R}(xy) \end{aligned}$$

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  $\mathrm{disc}(L/K) = K$  if and only if the trace form is non-degenerate, if and only if there exists  $x \in L$  with  $\mathrm{Tr}_{L/K}(x) \neq 0$ , 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  $\mathrm{disc}(A/k) \neq 0$ , so  $\mathrm{disc}(A/k) = k$ , 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  $y \mapsto (rx)y$ , so for all  $r \in A$ ,  $\mathrm{Tr}_{A/k}(rx) = 0$ . So the trace form is degenerate, and the discriminant is zero. See Atiyah-Macdonald chapter on Artinian rings for an explanation of  $A = \prod_i A_i$ .  $\square$

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  $\dim_K L = n$ .  $\square$

Lecture 5  
Saturday  
30/01/21

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

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

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

□

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

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

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

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

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

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

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

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

$$\mathcal{P} = \{\mathfrak{p} \subset R \mid v_{\mathfrak{p}}(\text{disc}_{L/K}(x_i)) > 0\}$$

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

**Definition.** Define

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

which is equivalent by 3.4 to the previous definition.

**Theorem 3.5.**  $v_{\mathfrak{p}}(\text{disc}(S/R)) = 0$  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  $v_{\mathfrak{p}}(\text{disc}(S/R)) = 0$  if and only if  $\text{disc}((S/\mathfrak{p}S)/(R/\mathfrak{p})) = R/\mathfrak{p}$ , 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  $v_{\mathfrak{p}}(\text{disc}(S/R)) > 0$ .*

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

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

*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

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

□

### 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

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

This is the dual of  $S$  with respect to the trace form  $(x, y) \mapsto \operatorname{Tr}_{L/K}(xy)$ , 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  $\operatorname{Tr}_{L/K}(x_i y_j) = \delta_{ij}$ . 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.  $N_{L/K}(\mathcal{D}_{S/R}) = \operatorname{disc}(S/R)$ .
3. Let  $\mathfrak{q} \subset S$  lying over  $\mathfrak{p} \subset R$ . Then  $v_{\mathfrak{q}}(\mathcal{D}_{S/R}) = v_{\mathfrak{q}}(\mathcal{D}_{\widehat{S_{\mathfrak{q}}}/\widehat{R_{\mathfrak{p}}}})$ .

*Proof.*

1. Exercise. <sup>2</sup>
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  $0 \neq x \in S$ . Let  $(e_i)$  be a basis for  $S$  over  $R$ . Then there exists a basis  $(e'_i)$  for  $S$  over  $R$  such that  $\operatorname{Tr}_{L/K}(e_i x^{-1} e'_j) = \delta_{ij}$ . Let  $x^{-1} e'_j = \sum_k b_{kj} e_k$  for  $b_{kj} \in K$ . Then

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

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

3. Assume  $R$  is local and  $\mathfrak{p} = \langle \pi_{\mathfrak{p}} \rangle$ . Write  $\widehat{K} = \operatorname{Frac} \widehat{R}$  and for  $\mathfrak{q} = \langle \pi_{\mathfrak{q}} \rangle \subset S$  write  $\widehat{L}_{\mathfrak{q}} = \operatorname{Frac} \widehat{S_{\mathfrak{q}}}$ . 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

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

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

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

since  $\operatorname{Tr}_{L/K}(x_i y_j) = \delta_{ij}$  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  $v_{\mathfrak{q}}(\pi_{\mathfrak{q}'}) = 0$  if  $\mathfrak{q}' \neq \mathfrak{q}$ .

□

<sup>2</sup>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  $\mathfrak{q}_i \mid \mathcal{D}_{S/R}$  if and only if  $e_i > 1$ , and  $\mathfrak{q}_i^{e_i-1} \mid \mathcal{D}_{S/R}$ .*

*Proof.* First assume  $R$  is complete local and  $\mathfrak{p} = \langle \pi_{\mathfrak{p}} \rangle$ . Then  $S$  is also local, and complete, with unique prime  $\mathfrak{q} = \langle \pi_{\mathfrak{q}} \rangle$ , so  $g = 1$ . So  $\mathcal{D}_{S/R} = \langle \pi_{\mathfrak{q}} \rangle^d$  for  $d \geq 0$ . By 3.8.2,  $\text{disc}(S/R) = \langle N_{L/K}(\pi_{\mathfrak{q}})^d \rangle = \langle \pi_{\mathfrak{p}} \rangle^{\text{df}}$ . So as  $v_{\mathfrak{p}}(\text{disc}(S/R)) = 0$  if and only if  $\mathfrak{p}$  is unramified by 3.5, get the first statement. For the second, claim  $\text{Tr}_{L/K}(\mathfrak{q}) \subset \mathfrak{p}$ . Let  $x \in \mathfrak{q}$ . Then multiplication by  $x$  is a nilpotent endomorphism of  $S \otimes_R (R/\mathfrak{p}) \cong S/\mathfrak{q}^e$ , so  $\text{Tr}_{S \otimes_R (R/\mathfrak{p})/(R/\mathfrak{p})}(x \otimes 1) = 0$ , that is  $\text{Tr}_{L/K}(x) = \text{Tr}_{S/R}(x) \in \mathfrak{p}$ . Hence the claim. Therefore  $\text{Tr}_{L/K}(\mathfrak{q}^{1-e}) = \text{Tr}_{L/K}(\pi_{\mathfrak{p}}^{-1} \mathfrak{q}) \subset R$ , so  $\mathfrak{q}^{1-e} \subset \mathcal{D}_{S/R}^{-1}$ , that is  $\mathfrak{q}^{e-1} \mid \mathcal{D}_{S/R}$ . For the general case, apply the above to  $\widehat{S_{\mathfrak{q}_i}}/\widehat{R_{\mathfrak{p}}}$  and use 3.8.3.  $\square$

**Fact.**

- If  $\mathfrak{p} \nmid e_i$  then  $v_{\mathfrak{q}_i}(\mathcal{D}_{S/R}) = e_i - 1$ . If  $\mathfrak{p} \mid e_i$  then  $v_{\mathfrak{q}_i}(\mathcal{D}_{S/R}) \geq e_i$ . More precisely,  $v_{\mathfrak{q}_i}(\mathcal{D}_{S/R})$  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  $dx$ .

For an extension  $L/K$  of number fields write

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

**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  $\langle \text{disc}(e_i) \rangle$  and if  $(e'_i)$  is another basis such that  $e'_i = \sum_{j,i} a_{ji} e_j$ , then  $\text{disc}(e'_i) = (\det(a_{ij}))^2 \text{disc}(e_i) = \text{disc}(e_i)$ , since  $\det(a_{ij}) = \pm 1$ . So the integer  $\text{disc}(e_i)$  is independent of the basis, not just the ideal it generates. This is called the **absolute discriminant**  $d_K \in \mathbb{Z} \setminus \{0\}$  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  $[S/\mathfrak{q}_i : R/\mathfrak{p}] = f_i$ , if  $i \neq j$  then  $\mathfrak{q}_i \neq \mathfrak{q}_j$ , and  $\mathfrak{p}S = \prod_i \mathfrak{q}_i^{e_i}$ .*

*Proof.* Can assume  $R$  is local, so then  $S = R[x]$ . Set  $\mathfrak{p} = \langle \pi \rangle$  and  $R/\mathfrak{p} = \kappa$ .

- $\mathfrak{q}_i$  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  $f_i$ .
- If  $i \neq j$ , there exist  $a, b \in R[T]$  such that  $a\overline{g}_i + b\overline{g}_j = 1 \in \kappa[T]$ , so  $1 = ag_i + bg_j + \pi c$  for some  $c \in R[T]$ . Then  $1 \in \langle \pi, g_i(x), g_j(x) \rangle = \mathfrak{q}_i + \mathfrak{q}_j$ , so  $\mathfrak{q}_i \neq \mathfrak{q}_j$ .

Let  $g = \prod_i g_i^{e_i} + \pi h$  for  $h \in R[T]$ . Then

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

Now

$$\dim_{\kappa}(S/\mathfrak{p}S) = n = [L : K], \quad \dim_{\kappa}(S/\mathfrak{q}_i^{e_i}) = \sum_{j=0}^{e_i-1} \dim_{\kappa}(\mathfrak{q}_i^j/\mathfrak{q}_i^{j+1}) = e_i \dim_{\kappa}(S/\mathfrak{q}_i) = e_i f_i,$$

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.  $\square$

## 4 Example: quadratic fields

Lecture 7  
Thursday  
04/02/21

Let  $K = \mathbb{Q}(\sqrt{d})$  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

$$\mathcal{O}_K \supset \mathbb{Z}[\sqrt{d}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}.$$

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

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

or  $d_K = d$ , and  $(\mathcal{O}_K : \mathbb{Z}[\sqrt{d}]) = 2$ . 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  $d \equiv 1 \pmod{4}$  since the minimal polynomial of  $\frac{1+\sqrt{d}}{2}$  is  $(T - \frac{1}{2})^2 - \frac{d}{4} = T^2 - T - \frac{d-1}{4}$ , in which case

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

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

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

Decomposition of primes by Kummer-Dedekind.

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

Go through the calculations if you have not seen them before. <sup>3</sup>

---

<sup>3</sup>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,  $\zeta_n$  is a root of the  $n$ -th cyclotomic polynomial  $\Phi_n \in \mathbb{Z}[T]$  of degree  $\phi(n)$ , defined recursively by

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

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

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

is an injective homomorphism.

**Theorem 5.1.** *Let  $L = \mathbb{Q}(\zeta_n)$  for  $n$  odd or  $4 \mid n$ . Then*

1.  $\text{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$ ,
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  $\Phi_n$  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, so  $r \geq 2$  if  $p = 2$ . 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

- $\Phi_{p^r}$  is irreducible over  $K$ ,
- if  $v \in V_{K,f}$  and  $v \nmid p$  then  $v$  is unramified in  $L/K$ ,
- if  $v \mid p$  then  $v$  is totally ramified in  $L/K$ , since  $p^r \geq 3$  so  $L \neq K$ , 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  $\zeta_{p^r}$  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  $\Phi_{p^r}(T+1) \equiv T^{p^{r-1}(p-1)} \pmod p$ , and the constant coefficient is  $p$ , so has valuation one. Then from local fields,

- $\Phi_{p^r}$  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  $v \nmid p$ . Then  $\Phi_{p^r}$  is separable modulo  $q$ . Have

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

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

- $\prod_{w|v} f_w = \Phi_{p^r}$ , 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  $v \in V_{K,f}$ ,

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

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

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

$$1 \rightarrow I_w \rightarrow G_w \rightarrow \text{Gal}(\ell_w/\kappa_v) \rightarrow 1,$$

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  $I_w = 1$ . Define the **Frobenius** at  $w$  to be the unique element  $\sigma_w \in G_w$  mapping to the generator  $x \mapsto x^{q_v}$  of  $\text{Gal}(\ell_w/\kappa_v)$ . So  $\text{ord } \sigma_w = f(w | v) = [\ell_w : \kappa_v] = [\ell_{w'} : \kappa_v]$  for any  $w' | v$ , 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  $\sigma_w$  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  $\sigma_{L/K}|_F = \sigma_{F/K}$  by definition.

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

$$\begin{aligned} \lambda &: (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \text{Gal}(L/\mathbb{Q}) \\ a \pmod n &\longmapsto (\zeta_n \mapsto \zeta_n^a). \end{aligned}$$

Claim that if  $p \nmid n$ ,

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

Indeed,  $\sigma_p$  is characterised by for all  $v | p$ ,  $\sigma_p$  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  $\mathbb{Z}[\zeta_n]/\langle p \rangle$ .

**Remark.**

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

Specialise to the case  $n = q > 2$  is prime. Then  $\text{Gal}(L/\mathbb{Q}) = (\mathbb{Z}/q\mathbb{Z})^\times$  is cyclic of order  $q - 1$ , so has a unique index two subgroup  $H \cong ((\mathbb{Z}/q\mathbb{Z})^\times)^2$ . Let  $K = L^H$  be a quadratic extension of  $\mathbb{Q}$ . Every  $p \neq q$  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

$$K = \mathbb{Q}(\sqrt{q^*}), \quad q^* = \begin{cases} q & q \equiv 1 \pmod 4 \\ -q & q \equiv 3 \pmod 4 \end{cases}, \quad d_K = q^*.$$

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

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

But

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

That is,  $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$ . Combine with  $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$  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  $\mathbb{J}_K = \mathbb{A}_K^\times$  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  $V_K = V_{K,\infty} \sqcup V_{K,f}$ , and let  $K_v$  be its completions. If  $v \in V_{K,f}$ , have  $\mathcal{O}_v = \mathcal{O}_{K_v} = \{x \mid |x|_v \leq 1\} \subset K_v$ .

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

$$\mathbb{A}_K = \left\{ (x_v) \in \prod_{v \in V_K} K_v \mid \text{for all but finitely many } v, x_v \in \mathcal{O}_v \right\} = \bigcup_{\text{finite } S \subset V_{K,f}} U_{K,S} \subset \prod_{v \in V_K} K_v,$$

where

$$U_{K,S} = \prod_{v \in V_{K,\infty}} K_v \times \prod_{v \in S} K_v \times \prod_{v \in V_{K,f} \setminus S} \mathcal{O}_v.$$

**Notation.** Let

$$K_\infty = \prod_{v \in V_{K,\infty}} K_v = K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

Then  $\mathbb{A}_K$  is a ring. The topology on  $\mathbb{A}_K$  is generated by all open  $V \subset U_{K,S}$  as  $S$  varies, and where  $U_{K,S}$  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  $V_{K,\infty}$ , and  $X_v$  is open in  $K_v$ . This means in particular that every  $U_{K,S} \subset \mathbb{A}_K$  is open, so

$$U_{K,\emptyset} = K_\infty \times \prod_{v \in V_{K,f}} \mathcal{O}_v = K_\infty \times \widehat{\mathcal{O}_K},$$

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

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

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 <sup>4</sup>

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

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

---

<sup>4</sup>Exercise: easy

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

*Proof.*  $\mathbb{U}_{K,\emptyset}$  is Hausdorff, and is locally compact, since  $K_\infty$  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.  $\square$

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

$$U = \left\{ x = (x_v) \in \mathbb{A}_K \mid \begin{array}{l} \forall v \in V_{K,f}, |x_v|_v \leq 1 \\ \forall v \in V_{K,\infty}, |x_v|_v < 1 \end{array} \right\}.$$

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

Let  $L/K$  be an extension of number fields. For all  $v \in V_K$ ,  $K_v \hookrightarrow \prod_{w|v} L_w$  induces an inclusion of rings  $\mathbb{A}_K \hookrightarrow \mathbb{A}_L$  visibly continuous.

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

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

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  $X^n = (K_\infty \times \widehat{\mathcal{O}_K})^n$  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

$$S = \left\{ v \in V_{K,f} \mid v \left( \left( \mathcal{O}_L : \sum_i a_i \mathcal{O}_K \right) \right) > 0 \right\}$$

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

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

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  $\prod_{w|v} \mathcal{O}_{L_w}$ . Then

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

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

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

So  $g \circ f$  is bijective.  $\square$

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

Lecture 9  
Tuesday  
09/02/21

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

$$\begin{array}{ccccccc} \prod_{w|v} L_w & \hookrightarrow & \mathbb{A}_L & \xleftarrow{\sim} & \mathbb{A}_K \otimes_K L & \longleftrightarrow & L \\ \downarrow \sum_w \text{Tr}_{L_w/K_v} & & \downarrow \text{Tr}_{\mathbb{A}_L/\mathbb{A}_K} & & \downarrow \text{id} \otimes \text{Tr}_{L/K} & & \downarrow \text{Tr}_{L/K} \\ K_v & \hookrightarrow & \mathbb{A}_K & \xleftarrow{\sim} & \mathbb{A}_K \otimes_K K & \longleftrightarrow & K \end{array}$$

commutes, where the left hand inclusions are

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

*Proof.* Exercise. <sup>5</sup> □

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

*Proof.* Since  $K$  is discrete in  $\mathbb{A}_K$  and  $\mathbb{A}_K$  is Hausdorff,  $K$  is closed in  $\mathbb{A}_K$ , so  $\mathbb{A}_K/K$  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  $X \rightarrow \mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ . Let  $x = (x_p)_{p \leq \infty} \in \mathbb{A}_{\mathbb{Q}}$ . 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  $\mathbb{A}_K$ ,

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

where

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

The topology on  $\mathbb{J}_K$  is generated by open subsets of  $\mathbb{J}_{K, S}$ , as  $S$  varies, and  $\mathbb{J}_{K, S}$  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.**  $\mathbb{J}_K \hookrightarrow \mathbb{A}_K$  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

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

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

$$\begin{aligned} \text{GL}_n K &\longrightarrow \mathbb{A}^{n^2+1} \\ (a_{ij}) &\longmapsto (a_{ij}, \det(a_{ij})^{-1}) \end{aligned}$$

has closed image.

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

<sup>5</sup>Exercise

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

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

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

**Definition.** Let  $x = (x_v) \in \mathbb{J}_K$ . 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

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

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

**Definition.** Let

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

**Proposition 6.6.**

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

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

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

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  $\mathbb{J}_K \cong \mathbb{J}_K^1 \times \mathbb{R}_{>0}$ . As  $i(\mathbb{R}_{>0}) \cap K^\times = 1$ , also have  $\mathcal{C}_K \cong \mathcal{C}_K^1 \times \mathbb{R}_{>0}$ .  $\square$

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

**Definition.** The **content map** is

$$\begin{aligned} c : \mathbb{J}_K &\longrightarrow I(K) \\ (x_v) &\longmapsto \prod_{v \in V_{K,f}} \mathfrak{p}_v^{v(x_v)}, \end{aligned}$$

where

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

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

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

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

**Definition.** Let  $S \subset V_{K,f}$  be a finite subset. Define

$$\begin{aligned} c^S : \mathbb{J}_K &\longrightarrow I^S(K) \\ (x_v) &\longmapsto \prod_{v \in V_{K,f} \setminus S} \mathfrak{p}_v^{v(x_v)}, \end{aligned}$$

where

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

This will be useful later on.

## 7 Geometry of numbers

### 7.1 Minkowski's theorem

Classically, embed

$$\sigma : K \hookrightarrow K_\infty = \prod_{v|\infty} K_v \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n,$$

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  $U/\Lambda$  is compact.

**Proposition 7.1.** *A subgroup  $\Lambda \subset U$  is a lattice if and only if  $\Lambda = \bigoplus_{1 \leq i \leq n} \mathbb{Z}e_i$ , 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  $\mu_\Lambda = \text{meas}(\mathbb{R}^n/\Lambda)$ , the **covolume** of  $\Lambda$ . 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  $\text{meas}(X) > 2^n \mu_\Lambda$ , then  $X \cap \Lambda \neq \{0\}$ .*

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

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

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

So  $X \rightarrow \pi(X)$  is not one-to-one, so there exist  $x \neq y$  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  $r_K > 0$  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
- $\prod_{v \in \mathbb{V}_K} d_v > r_K$ ,

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

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

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

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

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

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

$$X = \left\{ x \in \prod_{v|\infty} K_v \cong \mathbb{R}^n \mid \forall v, |x|_v \leq d_v \right\} = \prod_{v \text{ real}} [-d_v, d_v] \times \prod_{v \text{ complex}} \{|z|^2 \leq d_v\} \subset K_\infty \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

This is convex, compact, symmetric, and

$$\text{meas}(X) = 2^{r_1} \pi^{r_2} \prod_{v|\infty} d_v > 2^n \prod_{v \nmid \infty} d_v^{-1} \mu_{\sigma(\mathcal{O}_K)} = 2^n \mu_{\sigma(I)},$$

by (4), provided

$$\prod_v d_v > r_K = \left(\frac{4}{\pi}\right)^{r_2} \mu_{\sigma(\mathcal{O}_K)} = \left(\frac{2}{\pi}\right)^{r_2} |\text{d}_K|^{\frac{1}{2}}.$$

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

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

**Remark.** Used Minkowski's theorem, with convex symmetric set  $X = [-d_v, d_v]^{r_1} \times \{|z|^2 \leq d_v\}^{r_2}$  and obtained  $r_K = \left(\frac{4}{\pi}\right)^{r_2} \mu_{\sigma(\mathcal{O}_K)}$ . Using better chosen  $X$ , can get a better bound, the Minkowski bound  $c_K$ , which is useful for computation.

Lecture 11  
Saturday  
13/02/21

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

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

**Proposition 7.4.** *Let  $\rho_v > 0$  for  $v \in V_K$ , with  $\rho_v = 1$  for all but finitely many  $v$ . Then*

$$X = \{x \in \mathbb{J}_K^1 \mid \forall v, |x_v|_v \leq \rho_v\}$$

*is compact.*

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

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

$$S = V_{K,\infty} \cup \{v \mid \rho_v \neq 1\} \cup \{v \in V_{K,f} \mid q_v \leq R\}$$

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

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

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

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

which is a closed subset of

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

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

**Theorem 7.5.**  $\mathcal{C}_K^1$  is compact.

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

$$X = \{x \in \mathbb{J}_K^1 \mid \forall v \in V_K, |x_v|_v \leq |y_v|_v\},$$

which is compact by 7.4. Show that

$$\mathbb{J}_K^1 = K^\times X = \{ax \mid a \in K^\times, x \in X\}.$$

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

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

The following are two corollaries.

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

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

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

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

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

$$\mathcal{O}_{K,S}^\times = \mu(K) \times \mathbb{Z}^{r_1+r_2-1+\#S},$$

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

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

$$\mathcal{O}_K^\times = \mu(K) \times \mathbb{Z}^{r_1+r_2-1}.$$

*Proof.*

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

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

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

$$\begin{aligned} \lambda : \mathbb{J}_{K,\emptyset} &\longrightarrow \mathcal{L}_K = \prod_{v \mid \infty} \mathbb{R} \cong \mathbb{R}^{r_1+r_2} \\ (x_v)_v &\longmapsto (\log |x_v|_v)_v \end{aligned}$$

be the **logarithm map**, such that

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

Then

$$\ker \lambda = \{(x_v) \in \mathbb{J}_K \mid \forall v, |x_v|_v = 1\} = \{\pm 1\}^{r_1} \times \text{U}(1)^{r_2} \times \prod_{v \nmid \infty} \mathcal{O}_v^\times, \quad \text{U}(1) = \{z \in \mathbb{C} \mid |z| = 1\}$$

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  $\lambda(\mathcal{O}_K^\times) \subset \mathcal{L}_K^0 \cong \mathbb{R}^{r_1+r_2-1}$  is a lattice. Then we get

$$1 \rightarrow \mu(K) \rightarrow \mathcal{O}_K^\times \rightarrow \lambda(\mathcal{O}_K^\times) \cong \mathbb{Z}^{r_1+r_2-1} \rightarrow 0,$$

which gives 7.7. Now

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

where  $\mathbb{R}_{>0} \hookrightarrow K_v^\times \subset \mathbb{C}^\times$  for all  $v \mid \infty$ . Hence  $\lambda$  has the property that for all compact  $Y$  in its target,  $\lambda^{-1}(Y)$  is compact, so  $\lambda$  is a **proper** map. A simple fact is if  $f : X \rightarrow Y$  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.<sup>6</sup> Hence  $\lambda(\mathcal{O}_K^\times) \subset \mathcal{L}_K^0$  is discrete. Finally,

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

so  $\mathcal{L}_K^0 / \lambda(\mathcal{O}_K^\times)$  is compact, by 7.5. Thus  $\lambda(\mathcal{O}_K^\times)$  is a lattice.

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

$$\mathbb{J}_{K,S} = \prod_{v \in S_\infty} K_v^\times \times \prod_{v \notin S_\infty} \mathcal{O}_v^\times, \quad \mathcal{L}_{K,S} = \prod_{v \mid \infty} \mathbb{R} \times \prod_{v \in S} \log q_v \mathbb{Z} \cong \mathbb{R}^{r_1+r_2} \times \mathbb{Z}^{\#S}.$$

Let

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

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

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

Note that  $\mathcal{L}_{K,S}^0 \cong \mathbb{R}^{r_1+r_2-1} \times \mathbb{Z}^{\#S}$  since

$$\begin{array}{ccc} \mathcal{L}_{K,S}^0 & \xrightarrow{\pi_2} & \prod_{v \in S} \log q_v \mathbb{Z} \\ & \nwarrow & \uparrow \mathbb{R} \\ & & \mathbb{Z}^{\#S} \end{array}$$

is surjective with kernel  $\mathbb{R}^{r_1+r_2-1}$ , so there exists a splitting as  $\mathbb{Z}^{\#S}$  is free. Then

$$\ker \lambda_S \cong \{\pm 1\}^{r_1} \times \mathbb{U}(1)^{r_2} \times \prod_{v \nmid \infty} \mathcal{O}_v^\times,$$

as before, and

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

where  $\pi_v \in K_v^\times$  such that  $v(\pi_v) = 1$ , so  $\lambda_S$  is proper and surjective. Then  $\mathbb{J}_{K,S} \cap K^\times = \mathbb{J}_{K,S}^1 \cap K^\times = \mathcal{O}_{K,S}^\times$  is discrete and closed in  $\mathbb{J}_{K,S}^1$ . As before,  $\ker \lambda_S \cap \mathcal{O}_{K,S}^\times = \mu(K)$ , since it is discrete and compact, and  $\lambda_S(\mathcal{O}_{K,S}^\times) \subset \mathcal{L}_{K,S}^0$  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  $H \cong \mathbb{Z}^{m+\#S}$ .<sup>7</sup> Then

$$1 \rightarrow \mu(K) \rightarrow \mathcal{O}_{K,S}^\times \rightarrow \lambda_S(\mathcal{O}_{K,S}^\times) \cong \mathbb{Z}^{r_1+r_2-1+\#S} \rightarrow 0,$$

and so done. □

Let  $T \subset V_K$  be finite, not necessarily containing  $V_{K,\infty}$ . What can we say about the group

$$\{x \in K^\times \mid \forall v \notin T, |x|_v = 1\}?$$

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

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

<sup>7</sup>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  $T \subset V_K$  be finite, and set*

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

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

There are various ways to rewrite this.

- If  $T \neq \emptyset$ , 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

$$y \mapsto (x_w), \quad x_w = \begin{cases} y & w = v \\ 0 & w \neq v \end{cases}.$$

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

- Let  $S \subset V_K$  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  $v \in S$ ,  $|x - y_v|_v \leq \epsilon$ , and
  - for all  $v \notin S$  such that  $v \neq v_0$ ,  $|x|_v \leq 1$ .

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

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

then  $X + K = \mathbb{A}_K$ . For example, assume  $S \supset V_{K,\infty}$  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

$$|z|_v \leq \begin{cases} \frac{\epsilon}{R} & v \in S \\ 1 & v \notin S, v \neq v_0 \end{cases}.$$

Apply Minkowski 7.3 with

- $d_v = 1$  for all  $v \notin S \cup \{v_0\}$ ,
- $d_v \leq \epsilon/R$  for all  $v \in S$ , and
- $d_{v_0} > r_K (\prod_{v \in S} d_v)^{-1}$ .

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

$$|x - y_v|_v = |zt - y_v|_v = |za_v|_v \leq \begin{cases} \frac{\epsilon}{R} \cdot R = \epsilon & v \in S \\ 1 \cdot 1 = 1 & v \notin S, v \neq v_0 \end{cases},$$

so done. □

A special case is  $T = V_{K,\infty}$ , so  $\mathbb{A}_K^T$  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

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

$$\begin{aligned} \text{Gal}(L/\mathbb{Q}) &\longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \\ \sigma_p &\longmapsto p \pmod{m}, \quad p \nmid m, \end{aligned}$$

given by the action on  $\zeta_m$ . In particular,  $\sigma_p$  depends only on the congruence class of  $p \pmod{m}$ , which implies quadratic reciprocity. As  $\sigma_p$  determines the decomposition of  $\langle p \rangle$  in  $L$ , since  $f(v|p) = \text{ord } D_v = \text{ord } \sigma_p$ , this says that the decomposition of  $\langle p \rangle$  in  $L$  depends only on  $p \pmod{m}$ . A consequence is if  $g \in \text{Gal}(L/\mathbb{Q})$ , 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

$$\Sigma_v = \{\sigma_w \mid w \in V_{L,f}, w|v\}$$

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

- How does  $\Sigma_v$  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 in the 1920s.

**Theorem** (Chebotarev density theorem). *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*

$$\text{Art}_{L/K} : \mathcal{C}_K \rightarrow \text{Gal}(L/K),$$

*such that for all unramified  $v \in V_{K,f}$  in  $L/K$ ,*

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

*Moreover,  $\text{Art}_{L/K}$  is surjective with kernel  $K^\times N_{L/K}(\mathbb{J}_L)$ .*

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  $\ker \text{Art}_{L/K}$  is open, so contains some  $K^\times U$ , where

$$U = \prod_{v \text{ complex}} \mathbb{C}^\times \times \prod_{v \text{ real}} \mathbb{R}_{>0} \times \prod_{v \in S} U_v \times \prod_{v \in V_{K,f} \setminus S} \mathcal{O}_v^\times, \quad U_v = \{x \in \mathcal{O}_v^\times \mid v(x-1) \geq m_v\}, \quad m_v > 0,$$

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

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

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

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

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  $\pi_w$  modulo some ideal divisible only by primes in  $S$ , and positivity.

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

$$\begin{array}{ccccc}
 (\mathbb{R}^\times \times \widehat{\mathbb{Q}}^\times) / \mathbb{Q}^\times & \xleftarrow{\sim} & (\mathbb{R}^\times \times \widehat{\mathbb{Z}}^\times) / \{\pm 1\} & \xleftarrow{\sim} & \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times & \longrightarrow & \prod_{q|m} \mathbb{Z}_q^\times \\
 \downarrow \mathbb{R} & & \downarrow \mathbb{R} & & \downarrow & & \downarrow \\
 \mathcal{C}_{\mathbb{Q}} & \xleftarrow{\sim} & \mathbb{J}_{\mathbb{Q}, \emptyset} / \{\pm 1\} & & (\mathbb{Z}/m\mathbb{Z})^\times & \xleftarrow{\sim} & \prod_{q|m} (\mathbb{Z}_q/q\mathbb{Z}_q)^\times \\
 & \searrow & & \swarrow & & & \\
 & & \text{Gal}(L/\mathbb{Q}) & & & & 
 \end{array}$$

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

$$\begin{array}{ccccccc}
 \mathcal{C}_{\mathbb{Q}} & \xleftarrow{\sim} & \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^\times & \longrightarrow & \text{Gal}(L/\mathbb{Q}) \\
 \mathbb{Q}^\times(\dots, p, p, 1, p, p, \dots) & \xleftarrow{\sim} & (\dots, p, p, 1, p, p, \dots) & \mapsto & p \pmod m & \mapsto & \sigma_p
 \end{array}$$

So via  $\mathcal{C}_{\mathbb{Q}} \cong \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times$ ,  $\text{Art}_{L/\mathbb{Q}}$  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  $\alpha : \mathcal{C}_K \rightarrow G$  has finite image.*
2. *There is a bijection*

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

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

*Proof.*

1.  $\mathbb{J}_K \cong \mathbb{R}_{>0} \times \mathbb{J}_K^1$ , and  $\alpha(\mathbb{R}_{>0}) = 1$  so  $\alpha(\mathcal{C}_K) = \alpha(\mathcal{C}_K^1)$ , which is compact and discrete so finite.
2. The subgroup

$$\bigoplus_v K_v^\times = \{(x_v) \mid x_v = 1 \text{ for all but finitely many } v\} \subset \mathbb{J}_K$$

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  $\alpha : \mathbb{J}_K \rightarrow G$  is determined by its restrictions  $\alpha_v = \alpha|_{K_v^\times} : K_v^\times \rightarrow G$ . As  $\ker \alpha$  is open,  $\alpha_v(\mathcal{O}_v^\times) = 1$  for all but finitely many  $v$ . So have  $\{\alpha\} \hookrightarrow \{(\alpha_v)_v\}$ . Conversely, if  $(\alpha_v : K_v^\times \rightarrow G)_v$  is such a family, then  $\alpha((x_v)) = \prod_v \alpha_v(x_v)$  is a finite product for any  $(x_v) \in \mathbb{J}_K$ , as  $x_v \in \mathcal{O}_v^\times$  and  $\alpha_v(\mathcal{O}_v^\times) = 1$  for all but finitely many  $v$ , and defines a continuous homomorphism  $\alpha : \mathbb{J}_K \rightarrow G$ . □

**Proposition 8.2.** *Let  $\alpha, \alpha' : \mathcal{C}_K \rightarrow G$  be continuous homomorphisms, where  $G$  is finite, unramified at all  $v \in V_{K,f} \setminus S$ , 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  $\alpha/\alpha'$ , so without loss of generality  $\alpha' = 1$ . Then  $\alpha : \mathcal{C}_K \rightarrow G$  satisfies for all  $v \in V_{K,f} \setminus S$ ,  $\alpha_v = 1$ . Let  $w \in S_\infty = V_{K,\infty} \cup S$  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  $\alpha = 1$ . □

Lecture 14  
Saturday  
20/02/21

### 8.3 Specific open subgroups of $\mathcal{C}_K$

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

$$\mathfrak{m} = \sum_{v \in V_K} m_v(v), \quad m_v \geq 0.$$

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

$$\text{supp } \mathfrak{m} = \{v \in V_K \mid m_v > 0\}, \quad \text{supp}_f \mathfrak{m} = \text{supp } \mathfrak{m} \cap V_{K,f}.$$

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

$$U_{K,\mathfrak{m}} = \prod_{v \in V_K} U_v^{m_v}, \quad K_v^\times \supset U_v^m = \begin{cases} \mathcal{O}_v^\times & v \in V_{K,f}, m = 0 \\ 1 + \pi_v^m \mathcal{O}_v & v \in V_{K,f}, m > 0 \\ \mathbb{R}^\times & v \text{ real}, m = 0 \\ \mathbb{R}_{>0} & v \text{ real}, m > 0 \\ \mathbb{C}^\times & v \text{ complex} \end{cases}.$$

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

**Proposition 8.3.**  $\mathcal{C}_K/U_{K,\mathfrak{m}}$  is finite.

*Proof.*  $\mathcal{C}_K \rightarrow \mathcal{C}_K/U_{K,\mathfrak{m}}$  with discrete image, since  $U_{K,\mathfrak{m}}$  is open. So by 8.1.1, the image is finite.  $\square$

So every finite quotient of  $\mathcal{C}_K$  is a quotient of some  $\mathcal{C}_K/U_{K,\mathfrak{m}}$ .

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

$$\text{Cl}_\mathfrak{m}(K) = \mathcal{C}_K/U_{K,\mathfrak{m}}.$$

**Example.** If  $\mathfrak{m} = 0$ , then  $U_{K,\mathfrak{m}} = \ker c$ , where  $c : \mathbb{J}_K \rightarrow I(K)$  is the content map, and  $\text{Cl}_\mathfrak{m}(K) = \text{Cl}(K)$ .

Now relate to ideals.

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

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

Let

$$\begin{aligned} K_\mathfrak{m}^\times &= \{x \in K^\times \mid x \equiv 1 \pmod{\mathfrak{m}^*}\}, \\ I_\mathfrak{m}(K) &= \{\text{fractional ideals prime to } \text{supp}_f \mathfrak{m}\} \cong \{\text{free abelian group on } V_{K,f} \setminus \text{supp}_f \mathfrak{m}\}, \\ P_\mathfrak{m}(K) &= \{x\mathcal{O}_K \mid x \in K_\mathfrak{m}^\times\} \subset I_\mathfrak{m}(K). \end{aligned}$$

**Theorem 8.4.**

$$\text{Cl}_\mathfrak{m}(K) \cong I_\mathfrak{m}(K)/P_\mathfrak{m}(K).$$

**Example.** Assume  $K$  has real places, and let  $\mathfrak{m} = \sum_{v \text{ real}} (v)$ . Then  $I_\mathfrak{m}(K) = I(K)$  and  $P_\mathfrak{m}(K)$  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  $\text{Cl}_\mathfrak{m}(K)$  is called the **narrow ideal class group** of  $K$ , also written  $\text{Cl}^+(K)$ . Obviously  $\text{Cl}^+(K) \twoheadrightarrow \text{Cl}(K)$  with kernel killed by two.

Precisely is the following.

**Theorem 8.5.** Let  $S \subset V_{K,f}$  be finite, containing  $\text{supp}_f \mathfrak{m}$ . Then there exists a unique continuous homomorphism

$$\alpha = (\alpha_v) : \mathcal{C}_K \rightarrow I_\mathfrak{m}(K)/P_\mathfrak{m}(K),$$

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

$$\mathcal{C}_K/U_{K,\mathfrak{m}} \xrightarrow{\sim} I_\mathfrak{m}(K)/P_\mathfrak{m}(K).$$

*Proof.* By 8.2,  $\alpha$  is unique. For existence, let

$$\mathbb{J}_{K,\mathfrak{m}} = \{(x_v) \in \mathbb{J}_K \mid \forall v \in \text{supp } \mathfrak{m}, x_v \in U_v^{\mathfrak{m}_v}\},$$

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

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

Also, there is an isomorphism

$$\begin{aligned} c^S &: \mathbb{J}_{K,\mathfrak{m}} / U_{K,\mathfrak{m}} \longrightarrow I_\mathfrak{m}(K) \\ (x_v) &\longmapsto \prod_{v \in V_{K,f}, v \notin \text{supp } \mathfrak{m}} \mathfrak{p}_v^{v(x_v)}. \end{aligned}$$

Then

$$\mathcal{C}_K / U_{K,\mathfrak{m}} \xleftarrow{\iota} \mathbb{J}_{K,\mathfrak{m}} / K_\mathfrak{m}^\times U_{K,\mathfrak{m}} \xrightarrow{c^S} I_\mathfrak{m}(K) / P_\mathfrak{m}(K),$$

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

**Remark.** The isomorphism  $\mathcal{C}_K / U_{K,\mathfrak{m}} \rightarrow I_\mathfrak{m}(K) / P_\mathfrak{m}(K)$  is not induced by the  $S$ -content map  $\mathbb{J}_K \rightarrow I_\mathfrak{m}(K)$  but only on the subgroup  $\mathbb{J}_{K,\mathfrak{m}}$ . Fröhlich called this the **fundamental mistake of class field theory**.

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

$$\begin{aligned} \Theta &: I_\mathfrak{m}(\mathbb{Q}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \\ I &\longmapsto \frac{a}{b} \pmod{m}. \end{aligned}$$

This clearly defines an isomorphism such that

$$\begin{array}{ccc} p\mathbb{Z} \in I_\mathfrak{m}(\mathbb{Q}) / P_\mathfrak{m}(\mathbb{Q}) & \xrightarrow[\sim]{\Theta} & (\mathbb{Z}/m\mathbb{Z})^\times \ni p \pmod{m} \\ \alpha \uparrow & & \uparrow \\ \mathbb{Q}^\times (\dots, 1, 1, p^{-1}, 1, 1, \dots) \in \mathcal{C}_\mathbb{Q} & \xrightarrow{\sim} & \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times \ni (\dots, p, p, 1, p, p, \dots) \end{array}$$

commutes.

This is the reason for using  $\mathfrak{p}_v^{-1}$ , and  $\sigma_v^{-1}$  in the reciprocity law, since it means that for  $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ , recover the usual map  $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ . Older treatments of class field theory use  $\sigma_v$  and end up with the inverse of the usual map. Another reason is that the inverse  $\text{Fr}_v = \sigma_v^{-1}$ , 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  $\sigma_v^{-1}$ .

## 8.4 Properties of $\text{Art}_{L/K}$

**Corollary 8.6** (Uniqueness).  $\text{Art}_{L/K}$  is unique.

*Proof.* By 8.2.  $\square$

A consequence is if  $L'/K'$  is an abelian extension, and have isomorphisms

$$\begin{array}{ccc} L & \xrightarrow[\sim]{\tilde{\tau}} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow[\tau]{\sim} & K' \end{array},$$

then get isomorphisms

$$\begin{aligned} \tau &: \text{Gal}(L/K) \longrightarrow \text{Gal}(L'/K') \\ g &\longmapsto \tilde{\tau} \circ g \circ \tilde{\tau}^{-1}. \end{aligned}$$

Lecture 15  
Tuesday  
23/02/21

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

$$\begin{array}{ccc} \mathcal{C}_K & \xrightarrow{\text{Art}_{L/K}} & \text{Gal}(L/K) \\ \tau \downarrow \sim & & \sim \downarrow \tau \\ \mathcal{C}_{K'} & \xrightarrow{\text{Art}_{L'/K'}} & \text{Gal}(L'/K') \end{array}$$

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  $\tau = g \in \text{Gal}(K/F)$ . As  $L/K$  is abelian,  $\text{Gal}(K/F)$  acts by conjugation on  $\text{Gal}(L/K)$ . Let  $K = K'$  and  $L = L'$ . Then

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

**Proposition 8.7** (Norm functoriality). *Suppose  $L/K$  and  $L'/K'$  are abelian such that  $L \subset L'$  and  $K \subset K'$ . Then*

$$\begin{array}{ccc} \mathcal{C}_{K'} & \xrightarrow{\text{Art}_{L'/K'}} & \text{Gal}(L'/K') \\ \text{N}_{K'/K} \downarrow & & \downarrow g \mapsto g|_L \\ \mathcal{C}_K & \xrightarrow{\text{Art}_{L/K}} & \text{Gal}(L/K) \end{array}$$

*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  $w \mid v \in V_{K,f}$  where  $v$  is unramified in  $L/K$ . If  $\sigma_w \in D_w \subset \text{Gal}(L'/K')$ , then

$$\sigma_w|_L = (x \mapsto x^{q_w})|_L = (x \mapsto x^{q_v})^{f(w|v)} = \sigma_v^{f(w|v)}.$$

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

$$\text{N}_{K'_w/K_v}(\pi_w) = u\pi_v^{f(w|v)}, \quad u \in \mathcal{O}_{K_v}^{\times},$$

since  $\pi_v^{[K'_w:K_v]} = \text{N}_{K'_w/K_v}(\pi_v)$  and  $\pi_v = u\pi_w^{e(w|v)}$ . □

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

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

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

**Theorem 8.8** (Existence theorem). *Let  $U \subset \mathbb{J}_K$  be an open subgroup. Then there exists an abelian extension  $L/K$  with*

$$\ker \text{Art}_{L/K} = K^{\times}U.$$

Combining with the reciprocity law,

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

In particular, if  $\mathfrak{m}$  is a modulus, and  $U = U_{K,\mathfrak{m}}$ , 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  $\mathbb{Q}(\sqrt{-d})$ , which correspond to elliptic curves.

**Theorem 8.9** (Relation with local class field theory). *Let  $L/K$  be abelian, let  $v \in V_K$ , and let  $w \mid v$ . Then*

$$\begin{array}{ccc} \mathcal{C}_K & \xrightarrow{\text{Art}_{L/K}} & \text{Gal}(L/K) \\ \uparrow & & \cup \\ K_v^\times & \xrightarrow{\psi_v} & D_v = \text{Gal}(L_w/K_v) \end{array}.$$

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

**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  $\psi_v = \text{sign} : \mathbb{R}^\times \rightarrow \{\pm 1\} \cong \text{Gal}(L_w/K_v)$  with kernel  $\mathbb{R}_{>0} = N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times)$ .

The  $(\psi_v)$  combine to give

$$\begin{array}{ccc} \mathbb{J}_K / N_{L/K}(\mathbb{J}_L) & \xrightarrow{\text{Art}_{L/K}} & \text{Gal}(L/K) \\ \sim \uparrow & & \uparrow D_v \subset \text{Gal}(L/K) \\ \bigoplus_v K_v^\times / N_{L_w/K_v}(L_w^\times) & \xrightarrow{\sim} & \bigoplus_v D_v \end{array}.$$

So the fact that  $\text{Art}_{L/K}(K^\times) = 1$ , the hard part of the reciprocity law, is equivalent to knowing the relations between the various  $D_v \subset \text{Gal}(L/K)$ . 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.

## 8.5 Examples

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

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

Then  $H/K$  satisfies the following.

- It is abelian.
- For all  $v \in V_{K,f}$ , it is unramified at  $v$ , since  $\mathcal{O}_v^\times \subset U_{K,\mathfrak{m}}$  for all  $v$ .
- At an infinite place  $v$ ,  $K_v^\times \subset U_{K,\mathfrak{m}}$ , 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  $K = \mathbb{Q}(\sqrt{-23})$ , so  $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$ . By a standard computation,  $\text{Cl}(K) \cong \mathbb{Z}/3\mathbb{Z}$  is generated by  $[\mathfrak{p}]$  for  $\mathfrak{p} = \left\langle 2, \frac{1+\sqrt{-23}}{2} \right\rangle$ . Let  $\tau \in \text{Gal}(K/\mathbb{Q})$  be complex conjugation. Then  $\tau(\mathfrak{p}) = \left\langle 2, \frac{1-\sqrt{-23}}{2} \right\rangle$  and  $\mathfrak{p} \cdot \tau(\mathfrak{p}) = \langle 2 \rangle$ , that is  $\tau([\mathfrak{p}]) = [\mathfrak{p}]^{-1}$ , so  $\tau$  acts as  $-1$  on  $\text{Cl}(K)$ . Let  $H$  be the Hilbert class field of  $K$ , which is the maximal abelian extension of  $K$  which is unramified at all  $v \in V_{K,f}$ , that is  $\delta_{H/K} = \mathcal{O}_K$ . Then  $[H : K] = 3$  and Galois. By (5) above,  $\tau$  acts as  $-1$  on  $\text{Gal}(H/K)$ , 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  $-23$ .<sup>8</sup>

<sup>8</sup>Exercise

The following arose in a research problem.

**Proposition 8.10.** *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  $K = \mathbb{Q}(\sqrt{-7})$  or  $K = \mathbb{Q}(\sqrt{2})$ .*

*Proof.* Let

$$\mathrm{Art}_{L/K} : \mathcal{C}_K \rightarrow \mathrm{Gal}(L/K) \cong \mathbb{Z}/3\mathbb{Z}.$$

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

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

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

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

Then  $\mathrm{Art}_{L/K} : K_\infty^\times = (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \hookrightarrow \mathbb{J}_{K,\emptyset} \rightarrow \mathbb{Z}/3\mathbb{Z}$  is trivial on  $\mathbb{C}^\times$  and  $\mathbb{R}_{>0}$ , and even on  $\mathbb{R}^\times$ , since there is no non-zero continuous homomorphism  $\mathbb{R}^\times \rightarrow \mathbb{Z}/3\mathbb{Z}$ . So  $\mathrm{Art}_{L/K}$  factors through  $\widehat{\mathcal{O}_K}^\times/\mathcal{O}_K^\times$ , and since  $L/K$  is unramified at  $v \nmid 14$ , factors further by

$$\begin{array}{ccc} \mathcal{C}_K \cong \mathbb{J}_{K,\emptyset}/\mathcal{O}_K^\times & \longrightarrow & \widehat{\mathcal{O}_K}^\times/\mathcal{O}_K^\times \\ \mathrm{Art}_{L/K} \downarrow & & \downarrow \\ \mathrm{Gal}(L/K) \cong \mathbb{Z}/3\mathbb{Z} & \xleftarrow[\psi]{} & \left(\prod_{v \nmid 14} \mathcal{O}_v^\times\right)/\mathcal{O}_K^\times \end{array},$$

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

$$\psi \circ \tau = -\psi. \tag{6}$$

- Let  $K = \mathbb{Q}(\sqrt{-7})$ , so  $\mathcal{O}_K^\times = \{\pm 1\}$ .

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

So  $\psi$  factors through  $\mathbb{F}_7^\times$ , and  $\tau \in \mathrm{Gal}(K/\mathbb{Q})$  acts trivially on  $\mathbb{F}_7$ . So by (6), there is no possible  $\psi$ . There does exist a  $\psi$  with  $\psi \circ \tau = \psi$ , unique up to inverse, corresponding to an abelian  $L/\mathbb{Q}$ , which has to be  $\mathbb{Q}(\zeta_7)$ .

- Let  $K = \mathbb{Q}(\sqrt{2})$ , so  $\mathcal{O}_K^\times = \langle -1, \epsilon = 1 + \sqrt{2} \rangle$ .

- 2 ramifies, so if  $v \mid 2$ , then  $\mathcal{O}_v^\times = 1 + \pi_v \mathcal{O}_v$  is a pro-2 group and  $\psi(\mathcal{O}_v^\times) = 0$ .
- Since  $7 = (3 + \sqrt{2})(3 - \sqrt{2})$ ,  $\prod_{v|7} \mathcal{O}_v^\times = \mathbb{Z}_7^\times \times \mathbb{Z}_7^\times \cong \mathbb{F}_7^\times \times \mathbb{F}_7^\times \times (1 + 7\mathbb{Z}_7)^2$ , where  $1 + 7\mathbb{Z}_7$  is a pro-7 group, so  $\psi(1 + 7\mathbb{Z}_7) = 0$ .

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

$$\psi(x, x) = 0, \tag{7}$$

by (6). Now

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

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

□



## 8.6 Comparing $\mathcal{C}_K$ and $\text{Gal}(K^{\text{ab}}/K)$

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

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

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

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathbb{J}_{K,\emptyset}/\mathcal{O}_K^\times & \longrightarrow & \mathcal{C}_K & \xrightarrow{\text{c}} & \text{Cl}(K) \longrightarrow 1 \\ & & \downarrow & & \downarrow \text{Art}_K & & \downarrow \sim \\ 1 & \longrightarrow & \text{Gal}(K^{\text{ab}}/H) & \longrightarrow & \text{Gal}(K^{\text{ab}}/K) & \longrightarrow & \text{Gal}(H/K) \longrightarrow 1 \end{array},$$

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

- If  $K = \mathbb{Q}$ , then

$$\text{Art}_{\mathbb{Q}} : \mathcal{C}_{\mathbb{Q}} \cong \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times \twoheadrightarrow \widehat{\mathbb{Z}}^\times = \text{Gal}(\mathbb{Q}^{\text{ab}}/\mathbb{Q}).$$

- If  $K = \mathbb{Q}(\sqrt{-d})$ , then  $\mu(K)$  is finite, so the maximal profinite quotient is

$$\text{Art}_K : \mathbb{J}_{K,\emptyset}/\mathcal{O}_K^\times \cong (\mathbb{C}^\times \times \widehat{\mathcal{O}_K^\times}) / \mu(K) \twoheadrightarrow \widehat{\mathcal{O}_K^\times} / \mu(K) = \text{Gal}(K^{\text{ab}}/K).$$

- Let  $K = \mathbb{Q}(\sqrt{2})$ , so  $\text{Cl}(K) = 1$  and  $\mathcal{O}_K^\times = \langle -1, \epsilon = 1 + \sqrt{2} \rangle$ . Then  $N_{K/\mathbb{Q}}(\epsilon) = -1$  and  $\epsilon$  has signature  $(1, -1)$ . Let  $\epsilon_+ = \epsilon^2$  be the least totally positive unit. Then the maximal profinite quotient is

$$\begin{array}{c} \mathcal{C}_K = \mathbb{J}_{K,\emptyset}/\mathcal{O}_K^\times \xleftarrow{\sim} (\mathbb{R}_{>0}^2 \times \widehat{\mathcal{O}_K^\times}) / \langle \epsilon_+ \rangle \\ \cup \\ \mathcal{C}_K^1 = \mathbb{J}_{K,\emptyset}^1/\mathcal{O}_K^\times \xleftarrow{\sim} (\mathbb{R}_{>0} \times \widehat{\mathcal{O}_K^\times}) / \langle \epsilon_+ \rangle \xrightarrow{\text{Art}_K^1} \widehat{\mathcal{O}_K^\times} / \overline{\langle \epsilon_+ \rangle} = \text{Gal}(K^{\text{ab}}/K) \end{array}.$$

If  $G = \varprojlim_i G_i$  is a profinite group and  $g \in G$ , there exists a unique continuous  $\phi : \widehat{\mathbb{Z}} \rightarrow G$  such that  $\phi(1) = g$ .<sup>9</sup> So have

$$\begin{array}{ccc} \widehat{\mathbb{Z}} & \longrightarrow & \overline{\langle \epsilon_+ \rangle} \subset \widehat{\mathcal{O}_K^\times} \\ 1 & \longmapsto & \epsilon_+ \end{array}.$$

One can show that  $\widehat{\mathbb{Z}} \xrightarrow{\sim} \overline{\langle \epsilon_+ \rangle}$ , so there is an isomorphism

$$\ker \text{Art}_K^1 = (\mathbb{R}_{>0} \times \overline{\langle \epsilon_+ \rangle}) / \langle \epsilon_+ \rangle \cong (\mathbb{R} \times \widehat{\mathbb{Z}}) / \mathbb{Z} = \mathbb{A}_{\mathbb{Q}}/\mathbb{Q},$$

where  $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$  is compact and connected, that is have

$$1 \rightarrow \mathbb{A}_{\mathbb{Q}}/\mathbb{Q} \rightarrow \mathcal{C}_K^1 \rightarrow \text{Gal}(K^{\text{ab}}/K) \rightarrow 1.$$

- For general  $K$ , what happens is that

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathcal{C}_K^\circ & \longrightarrow & \mathcal{C}_K & \xrightarrow{\text{Art}_K} & \text{Gal}(K^{\text{ab}}/K) \longrightarrow 1 \\ & & \downarrow \mathbb{R} & & \downarrow \cup & & \downarrow \cup \\ 1 & \longrightarrow & \mathcal{C}_K^\circ & \longrightarrow & \mathbb{J}_{K,\emptyset}/\mathcal{O}_K^\times & \longrightarrow & \text{Gal}(K^{\text{ab}}/H) \longrightarrow 1 \\ & & & & & & \downarrow \mathbb{R} \\ & & & & & & (\{\pm 1\}^{r_1} \times \widehat{\mathcal{O}_K^\times}) / \overline{\mathcal{O}_K^\times} \end{array},$$

where the maximal connected subgroup of  $\mathcal{C}_K$ , the closure of  $\mathbb{R}_{>0}^{r_1} \times (\mathbb{C}^\times)^{r_2}$ , is

$$\mathcal{C}_K^\circ \cong \mathbb{R}_{>0} \times \text{U}(1)^{r_2} \times (\mathbb{A}_{\mathbb{Q}}/\mathbb{Q})^{r_1+r_2-1}.$$

<sup>9</sup>Exercise: easy

## 9 $\zeta$ -functions

### 9.1 Riemann $\zeta$ -function

The **Riemann  $\zeta$ -function** is

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

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

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

**Theorem 9.1** (Functional equation for Riemann  $\zeta$ -function).

$$Z(s) = Z(1-s),$$

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

*Proof.* There are three steps.

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

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

where  $\Theta$  is the **theta function**

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

Step 2. If  $f : \mathbb{R} \rightarrow \mathbb{C}$  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**

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

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

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

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

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

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

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

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

□

## 9.2 Dedekind $\zeta$ -function

Let  $K$  be a number field. The **Dedekind  $\zeta$ -function of  $K$**  is

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

**Proposition 9.2** (Euler product).

$$\zeta_K(s) = \prod_{v \in V_{K,f}} \frac{1}{1 - q_v^{-s}},$$

absolutely convergent for  $\operatorname{Re} s > 1$ .

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

$$\zeta_K(s) = \prod_v (1 + q_v^{-s} + \dots) = \prod_v \frac{1}{1 - q_v^{-s}}.$$

Now  $\#\{v \mid p\} \leq n = [K : \mathbb{Q}]$ , and if  $v \mid p$  then  $q_v \geq p$ , so the product converges by comparison with  $\prod_p (1 - p^{-s})^{-n} = \zeta(s)^n$ .  $\square$

The  $1/(1 - q_v^{-s})$  are **Euler factors at  $v$** . Define

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

the **Euler factors for the infinite places**, and

$$Z_K(s) = |d_K|^{\frac{s}{2}} \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2} \zeta_K(s).$$

The following is a generalisation of 9.1.

**Theorem 9.3.**

1. (Functional equation for Dedekind  $\zeta$ -function)  $Z_K(s)$  has an analytic continuation to  $\mathbb{C}$ , apart from simple poles at  $s = 0, 1$ , and

$$Z_K(1-s) = Z_K(s).$$

2. (Analytic class number formula)  $\zeta_K(s)$  has a zero of order  $r = r_1 + r_2 - 1$  at  $s = 0$ , and

$$\lim_{s \rightarrow 0} \frac{1}{s^r} \zeta_K(s) = -\frac{h_K R_K}{w_K}. \quad (8)$$

Here,  $h_K = \#\operatorname{Cl}(K)$  is the class number,  $w_K = \#\mu(K)$  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

$$(\log|\epsilon_j|_v)_{1 \leq j \leq r, v \in V_{K,\infty}}.$$

Note that by the product formula, the sum of the columns of this matrix is zero, so minors are equal up to sign. Then  $R_K \neq 0$  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  $\mathbb{Q}_p$ ,

$$\int_{\mathbb{Z}_p \setminus \{0\}} |x|_p^{s-1} dx = \sum_{n \geq 0} \int_{p^n \mathbb{Z}_p \setminus p^{n+1} \mathbb{Z}_p} p^{-n(s-1)} dx = \sum_{n \geq 0} p^{-n(s-1)} \text{meas}(p^n \mathbb{Z}_p \setminus p^{n+1} \mathbb{Z}_p).$$

Then

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

so

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

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 over all  $p$ , an adelic integral.

- The  $\Gamma$ -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  $\mathbb{R}$ ,

$$\hat{f}(y) = \int_{-\infty}^{\infty} e^{-2\pi i x y} f(x) dx,$$

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

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

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

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

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

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

**Definition.** The **Haar measure**  $d_F x$  is translation-invariant.

- If  $F = \mathbb{R}$ , then  $d_F x$  is the usual Lebesgue measure  $dx$ .
- If  $F = \mathbb{C}$ , then  $d_F z = 2dx dy$  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

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

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

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

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

Lecture 18  
Tuesday  
02/03/21

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

- If  $F = \mathbb{R}$ , then

$$\mathcal{S}(F) = \left\{ C^\infty\text{-functions } f : F \rightarrow \mathbb{C} \mid \forall n \geq 0, \forall \alpha \in \mathbb{N}, \lim_{|x| \rightarrow \infty} \left( |x|^n \left| \frac{d^\alpha f}{dx^\alpha} \right| \right) = 0 \right\}.$$

For example,  $e^{-c|x|^2}$  for  $c > 0$ .

- If  $F = \mathbb{C}$ , then

$$\mathcal{S}(F) = \left\{ C^\infty\text{-functions } f : F \rightarrow \mathbb{C} \mid \forall n \geq 0, \forall \alpha \in \mathbb{N}^2, \lim_{|z| \rightarrow \infty} \left( |z|^n \left| \frac{\partial^\alpha f}{\partial x^{\alpha_1} \partial y^{\alpha_2}} \right| \right) = 0 \right\}.$$

- If  $F/\mathbb{Q}_p$ , then

$$\begin{aligned} \mathcal{S}(F) &= \{\text{locally constant } f : F \rightarrow \mathbb{C} \text{ of compact support}\} \\ &= \{\text{span of characteristic functions } \mathbb{1}_{a+\pi^n \mathcal{O}_F}\}. \end{aligned}$$

If  $f \in \mathcal{S}(F)$ , write

$$\int_F f(x) \, d_F x$$

for the integral. If  $F/\mathbb{Q}_p$  and  $f = \mathbb{1}_{a+\pi^n \mathcal{O}_F}$ , then

$$\int_F f(x) \, d_F x = \text{meas}(a + \pi^n \mathcal{O}_F),$$

that is  $p$ -adic integrals are basically just finite sums. Also write

$$\int_U f(x) \, d_F x = \int_F \mathbb{1}_U f(x) \, d_F x,$$

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

$$\int_{\mathfrak{a}} \psi(x) \, d_F x = \int_F \mathbb{1}_{\mathfrak{a}} \psi(x) \, d_F x = \begin{cases} \text{meas}(\mathfrak{a}) & \mathfrak{a} \subset \mathcal{D}_{F/\mathbb{Q}_p}^{-1} \\ 0 & \text{otherwise} \end{cases},$$

where  $\mathbb{1}_{\mathfrak{a}} \psi \in \mathcal{S}(F)$ .

*Proof.*

- If  $\mathfrak{a} \subset \mathcal{D}_{F/\mathbb{Q}_p}^{-1}$ , then  $\text{Tr}_{F/\mathbb{Q}_p}(\mathfrak{a}) \subset \mathbb{Z}_p$  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  $\text{Tr}_{F/\mathbb{Q}_p}(x) \notin \mathbb{Z}_p$ , so  $\psi(x) \neq 1$ . As  $x + \mathfrak{a} = \mathfrak{a}$ , and  $d_F(x+y) = d_F y$ ,

$$\int_{\mathfrak{a}} \psi(y) \, d_F y = \int_{\mathfrak{a}} \psi(x+y) \, d_F y = \psi(x) \int_{\mathfrak{a}} \psi(y) \, d_F y,$$

so the integral is zero.

□

Compare to

$$\sum_{g \in G} \chi(g) = \begin{cases} \#G & g = e \\ 0 & \text{otherwise} \end{cases},$$

for  $G$  finite abelian.

## 9.4 Local Fourier transform

**Definition.** Let  $f \in \mathcal{S}(F)$ . Define the **Fourier transform**

$$\widehat{f}(y) = \int_F \psi(xy) f(x) \, d_F x,$$

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  $f(z) = \frac{1}{\pi} e^{-2\pi z \bar{z}}$ , 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  $f$ ,

$$\widehat{f}(y) = \int_{-\infty}^{\infty} e^{-2\pi i xy - \pi x^2} \, dx = e^{-\pi y^2} \int_{-\infty}^{\infty} e^{-\pi(x+iy)^2} \, dx = e^{-\pi y^2} \int_{-\infty}^{\infty} e^{-\pi x^2} \, dx = e^{-\pi y^2}.$$

2. Exercise. <sup>10</sup>

3. By 9.4,

$$\widehat{f}(y) = \int_{\pi^n \mathcal{O}_F} \psi(xy) \, d_F x = \begin{cases} \text{meas}(\pi^n \mathcal{O}_F) & y \in \pi^{-n} \mathcal{D}_{F/\mathbb{Q}_p}^{-1} \\ 0 & y \notin \pi^{-n} \mathcal{D}_{F/\mathbb{Q}_p}^{-1} \end{cases},$$

which gives the answer. □

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

- For  $F/\mathbb{R}$ , this is standard analysis, using  $\widehat{\widehat{f^{(n)}}}(y) = (2\pi i y)^n \widehat{f}(y)$ .
- 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  $zw + \bar{z}\bar{w} = 2(ux - vy)$ , 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. <sup>11</sup> □

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

<sup>10</sup>Exercise

<sup>11</sup>Exercise: the rest is in example sheet

**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  $x = c^{-1}t$ ,

$$\widehat{g}(y) = \int_F \psi(xy) f(cx) \, d_F x = \int_F \psi(c^{-1}ty) f(t) \, d_F(c^{-1}t) = |c|_F^{-1} \int_F \psi(tc^{-1}y) f(t) \, d_F t = |c|_F^{-1} \widehat{f}(c^{-1}y).$$

□

## 9.5 Local $\zeta$ -integrals

**Definition.** Define the **Haar measure**  $d_F^\times x$  on the multiplicative group  $F^\times$  by

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

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

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

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

This is the reason to normalise in this way.

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

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

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

**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  $f(z) = \frac{1}{\pi} e^{-2\pi z \bar{z}}$ , 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

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

*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.

Lecture 19  
Thursday  
04/03/21

3.

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

□

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

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

$$\zeta(f, \chi, s) = \int_{F^\times} f(x) \chi(x) |x|_F^s \, d_F^\times x,$$

defined as a limit in the same way.

## 9.6 Global Fourier analysis

Let  $K$  be a number field with completions  $K_v$ , and let  $\psi_v : K_v \rightarrow \mathbb{U}(1)$ ,  $d_v x$ ,  $d_v^\times x$ ,  $\mathcal{S}(K_v)$ , and  $\delta_v$  be the objects defined above for  $F = K_v$ . Let

$$V_{K,r} = \{v \in V_{K,f} \mid v \text{ ramified in } F/\mathbb{Q}_p\} = \{v \in V_{K,f} \mid \delta_v \neq 0\}.$$

Then

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

where  $S \subset V_K$  is finite containing  $V_{K,\infty}$ .

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

$$f(x) = \prod_{v \in V_K} f_v(x_v),$$

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

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

$$\int_{\mathbb{A}_K} f(x) \, d_{\mathbb{A}} x = \prod_v \int_{K_v} f_v(x) \, d_v x = \prod_{v \in S} \int_{K_v} f_v(x) \, d_v x,$$

since if  $v \notin S$ ,

$$\int_{K_v} f_v(x) \, d_v x = \int_{\mathcal{O}_v} d_v x = 1.$$

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

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

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



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

*Proof.* Take a finite  $S \supset V_{K,\infty}$ . The restriction of  $\psi_{\mathbb{A}}$  to  $\prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_v$  factors through  $\prod_{v \in S} \psi_v : \prod_{v \in S} K_v \rightarrow \mathbb{U}(1)$ , which is continuous. Now  $\psi_{\mathbb{A}}(x) = \psi_{\mathbb{A}_{\mathbb{Q}}}(\text{Tr}_{K/\mathbb{Q}}(x))$ , as  $\text{Tr}_{K/\mathbb{Q}}(x) = \sum_{v|p} \text{Tr}_{K_v/\mathbb{Q}_p}(x)$  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  $\psi_{p_i}(x) = e^{2\pi i y_i/p_i^{k_i}}$  as for  $j \neq i$ ,  $y_j/p_j^{k_j} \in \mathbb{Z}_{p_i}$ , and  $\psi_p(x) = 1$  if  $p \notin \{p_i\}$ . Thus  $\prod_{p < \infty} \psi_p(x) = e^{2\pi i x} = \psi_{\infty}(x)^{-1}$ .  $\square$

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

$$\widehat{f}(y) = \int_{\mathbb{A}_K} \psi_{\mathbb{A}}(xy) f(x) d_{\mathbb{A}} x = \prod_v \widehat{f}_v(y_v), \quad f = \bigotimes_v f_v.$$

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

## 9.7 Global $\zeta$ -integral

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

$$\zeta(f, s) = \int_{\mathbb{J}_K} f(x) |x|_{\mathbb{A}}^s d_{\mathbb{J}} x = \prod_{v \in V_K} \int_{K_v^{\times}} f_v(x) |x|_v^s d_v^{\times} x = \prod_{v \in V_K} \zeta(f_v, s),$$

which really is a genuine infinite product.

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

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

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

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

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

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

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

with

$$\text{Res}_s \zeta(f, s) = \begin{cases} \widehat{f}(0) \kappa & s = 1 \\ -f(0) \kappa & s = 0 \end{cases}, \quad \kappa = \text{meas}(\mathcal{C}_K^1) > 0.$$

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

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

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

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

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

$$\int_{\mathbb{J}_K} f(x) d_{\mathbb{J}} x = \int_0^{\infty} \left( \int_{\mathbb{J}_K^1} f(tx) d_{\mathbb{J}^1} x \right) \frac{1}{t} dt. \quad (9)$$

Lecture 20  
Saturday  
06/03/21

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

$$\int_0^\infty \frac{\phi(t)}{t} dt = 1.$$

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

$$\begin{aligned} \widetilde{f}_\phi &: \mathbb{J}_K \longrightarrow \mathbb{C} \\ tx &\longmapsto \phi(t) f(x), \end{aligned}$$

and define

$$\int_{\mathbb{J}_K^1} f(x) d_{\mathbb{J}^1} x = \int_{\mathbb{J}_K} \widetilde{f}_\phi(y) d_{\mathbb{J}} y.$$

**Lemma 9.12.**

1. This is independent of  $\phi$ .
2. The identity (9) holds.

*Proof.* If  $y \in \mathbb{J}_K$  such that  $y = tx$  for  $t > 0$  and  $x \in \mathbb{J}_K^1$ , 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  $|y'|_{\mathbb{A}} = s$ ,

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

We need to check the homomorphism

$$\begin{aligned} \lambda &: \mathbb{R}_{>0} \times \mathbb{J}_K \longrightarrow \mathbb{R}_{>0} \times \mathbb{J}_K \\ (s, y) &\longmapsto (s', y') \end{aligned}$$

is measure-preserving. Since  $|t|_{\mathbb{A}} = t$ ,  $\lambda^2 : (s, y) \mapsto (s, y)$ , that is  $\lambda^2 = \text{id}$ . The Haar measure is unique up to a constant, so

$$\lambda : d_{\mathbb{J}} y \times \frac{1}{s} ds \mapsto c d_{\mathbb{J}} y \times \frac{1}{s} ds, \quad c > 0,$$

so since  $c^2 = 1$ ,  $c = 1$ . If you like, it is easy to reduce to the computation just on  $K_\infty^\times$ .

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  $x = ty/s$ ,

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

□

So

$$\zeta(f, s) = \int_0^\infty \frac{\zeta_t(f, s)}{t} dt, \quad \zeta_t(f, s) = t^s \int_{\mathbb{J}_K^1} f(tx) d_{\mathbb{J}^1} x.$$

Recall that  $C_K^1$  is compact. Will show next time that there exists  $E \subset \mathbb{J}_K^1$ , the **fundamental domain**, with  $\text{meas}(E) < \infty$  and  $\overline{E}$  compact such that

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

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

**Proposition 9.13** (Functional equation for  $\zeta_t(f, s)$ ).

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

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  $x \in \mathbb{J}_K$ . Then*

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

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

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

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

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

*Proof of 9.11.* Now, if  $\operatorname{Re} s > 1$ ,

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

Say  $f \in \mathcal{S}(\mathbb{A}_K)$  such that  $f = f_\infty f^\infty$  for  $f_\infty = \bigotimes_{v|\infty} f_v \in \mathcal{S}(K_\infty)$  and  $f^\infty = \bigotimes_{v \nmid \infty} f_v \in \mathcal{S}(\widehat{K})$ , which has compact support. So if  $x \in \mathbb{J}_K^1$  and  $f^\infty(x) \neq 0$ , then there exists a finite  $S \subset V_{K,f}$  such that if  $v \in V_{K,f} \setminus S$  then  $f_v = \mathbb{1}_{\mathcal{O}_v}$  so  $|x_v|_v \leq 1$ , and if  $v \in S$  then  $|x_v|_v \leq c_v$ . As  $\prod_v |x_v|_v = |x|_{\mathbb{A}} = 1$ ,  $\prod_{v|\infty} |x_v|_v \geq c = \prod_{v \nmid \infty} c_v > 0$ , and

$$\int_{\mathbb{J}_K^1} f(tx) \, d_{\mathbb{J}^1} x \leq c \int_{\prod_{v|\infty} |x_v|_v \geq c'} f_\infty(tx) \, d^\times x = c \int_{\prod_{v|\infty} |x_v|_v \geq tc'} f_\infty(x) \, d^\times x \rightarrow 0$$

rapidly as  $t \rightarrow \infty$ , so  $\zeta_t(f, s)$  is rapidly decreasing, as  $t \rightarrow \infty$ . That implies that

$$\int_1^\infty \frac{\zeta_t(f, s)}{t} \, dt = \lim_{T \rightarrow \infty} \int_1^T \frac{\zeta_t(f, s)}{t} \, dt,$$

with uniform limit for  $\sigma_1 \leq \operatorname{Re} s \leq \sigma_2$ , is an analytic function for all  $s \in \mathbb{C}$ , which gives a meromorphic continuation of  $\zeta(f, s)$  with poles at  $s = 0, 1$ , and  $\zeta(f, s) = \zeta(\widehat{f}, 1-s)$ . □

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

## 9.8 Proof of Poisson summation formula

Lecture 21  
Tuesday  
09/03/21

Start off with the classical Poisson formula.

- If  $f \in \mathcal{S}(\mathbb{R})$ , then

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

since  $g(x) = \sum_{m \in \mathbb{Z}} f(x+m) : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{C}$  has Fourier expansion  $g(x) = \sum_{n \in \mathbb{Z}} c_n e^{2\pi i n x}$  with

$$c_n = \int_0^1 e^{-2\pi i n x} g(x) dx = \int_0^1 \sum_{m \in \mathbb{Z}} e^{-2\pi i n x} f(x+m) dx = \int_{-\infty}^{\infty} e^{-2\pi i n x} f(x) dx = \widehat{f}(n),$$

so

$$\sum_m f(m) = g(0) = \sum_n c_n = \sum_n \widehat{f}(n).$$

Similarly for  $f \in \mathcal{S}(\mathbb{R}^k)$ ,

$$\sum_{m \in \mathbb{Z}^k} f(m) = \sum_{n \in \mathbb{Z}^k} \widehat{f}(n),$$

by the same proof.

One method is abstract Fourier analysis.

- Let  $G$  be a locally compact abelian group, and let  $H$  be a countable discrete subgroup such that  $G/H$  is compact. If  $f$  is a nice function on  $G$ , then

$$\begin{aligned} \widehat{f} : \widehat{G} = \text{Hom}_{\text{cts}}(G, \mathbb{U}(1)) &\longrightarrow \mathbb{C} \\ \chi &\longmapsto \int_G \chi(x) f(x) dx. \end{aligned}$$

Then  $\widehat{G/H}$  is discrete, and

$$\sum_{h \in H} f(h) = \sum_{\chi \in \widehat{G/H}} \widehat{f}(\chi) \text{meas}(G/H)^{-1},$$

with proof the same as for  $(\mathbb{R}, \mathbb{Z})$ . Apply with  $G = \mathbb{A}_K$  and  $H = K$ , where  $G \cong \widehat{G}$ , via  $\psi_{\mathbb{A}}$ , and  $\widehat{G/H} \cong H$ .

The following is a more basic proof.

*Proof of 9.14.*

- Let  $V$  be a real vector space with  $\dim V < \infty$  and  $dx$  an invariant measure, let  $\Lambda \subset V$  be a lattice with  $\mu = \text{meas}(V/\Lambda) < \infty$ , and let

$$V' = \text{Hom}(V, \mathbb{R}) \supset \Lambda' = \text{Hom}(\Lambda, \mathbb{Z}) = \{y \in V' \mid \forall x \in \Lambda, \langle x, y \rangle \in \mathbb{Z}\}.$$

If  $f \in \mathcal{S}(V)$ , then  $\widehat{f} \in \mathcal{S}(V')$  and

$$\widehat{f}(y) = \int_V e^{-2\pi i \langle x, y \rangle} dx.$$

Then

$$\sum_{x \in \Lambda} f(x) = \mu^{-1} \sum_{y \in \Lambda'} \widehat{f}(y),$$

since scaling  $dx$ , may assume  $\mu = 1$ , then fix  $\mathbb{Z}^k \xrightarrow{\sim} \Lambda$ , so  $\mathbb{R}^k \cong V \cong V'$  and this reduces to the previous Poisson summation for  $(\mathbb{R}^k, \mathbb{Z}^k)$ .

- A special case is a fractional ideal  $\mathfrak{a} \subset K$ . Suppose  $f \in \mathcal{S}(\mathbb{A}_K)$  such that  $f = f_\infty \otimes f_{\mathfrak{a}}$  for  $f_\infty \in \mathcal{S}(K_\infty)$  and  $f_{\mathfrak{a}} : \widehat{K} \rightarrow \mathbb{C}$  the characteristic function of  $\widehat{\mathfrak{a}\mathcal{O}_K} = \prod_{v \nmid \infty} \mathfrak{a}\mathcal{O}_v \subset \prod_{v \nmid \infty} K_v$ . Then

$$\widehat{f} = \widehat{f_\infty} \otimes |\mathrm{d}_K|^{-\frac{1}{2}} \mathrm{N}(\mathfrak{a})^{-1} f_{\mathfrak{b}}, \quad \mathfrak{b} = \mathcal{D}_{K/\mathbb{Q}}^{-1} \mathfrak{a}^{-1},$$

by the local computation of  $\widehat{\mathbb{1}_{\pi^n \mathcal{O}_F}}$ . Now  $\sigma : \mathfrak{a} \hookrightarrow K_\infty$ . On  $K_\infty$  we have the trace form  $\mathrm{Tr}_{K_\infty/\mathbb{R}}(xy)$  identifying  $K_\infty$  with its dual, and by definition of  $\mathcal{D}_{K/\mathbb{Q}}$ , the dual of  $\mathfrak{a}$  is  $\mathfrak{b}$ . Moreover, the covolume of  $\sigma(\mathfrak{a})$  is  $|\mathrm{d}_K|^{1/2} \mathrm{N}(\mathfrak{a})$ . So

$$\sum_{x \in K} f(x) = \sum_{x \in \mathfrak{a}} f_\infty(x) = |\mathrm{d}_K|^{-\frac{1}{2}} \mathrm{N}(\mathfrak{a})^{-1} \sum_{y \in \mathfrak{b}} \widehat{f_\infty}(y) = \sum_{y \in \mathfrak{b}} \widehat{f}(y),$$

by the Poisson summation for lattices.

- For the general case, every element of  $\mathcal{S}(\mathbb{A}_K)$  is a sum of functions  $g(x) = f(x+a)$  where  $f = f_\infty \otimes f_{\mathfrak{a}}$  as above and  $a \in \widehat{K}$ . By strong approximation, may assume  $a \in K$ . Then

$$\widehat{g}(y) = \int_{\mathbb{A}_K} \psi_{\mathbb{A}}(xy) f(x+a) \mathrm{d}_{\mathbb{A}} x = \psi_{\mathbb{A}}(ay)^{-1} \widehat{f}(y),$$

and by the previous,

$$\sum_{x \in K} g(x) = \sum_{x \in K} f(x) = \sum_{y \in K} \widehat{f}(y) = \sum_{y \in K} \psi_{\mathbb{A}}(ay) \widehat{g}(y) = \sum_{y \in K} \widehat{g}(y),$$

as  $\psi_{\mathbb{A}}|_K = 1$ .

□

## 9.9 Proof of functional equation and analytic class number formula

Now use the functional equation of  $\zeta(f, s)$  to deduce the same for  $\zeta_K(s)$ .

*Proof of 9.3.1.* Choose

$$f_v = \begin{cases} e^{-\pi x^2} & v \text{ real} \\ \frac{1}{\pi} e^{-2\pi z \bar{z}} & v \text{ complex} \\ \mathbb{1}_{\mathcal{O}_v} & v \text{ finite} \end{cases}, \quad \widehat{f}_v = \begin{cases} e^{-\pi x^2} & v \text{ real} \\ \frac{1}{\pi} e^{-2\pi z \bar{z}} & v \text{ complex} \\ q_v^{-\frac{\delta_v}{2}} \mathbb{1}_{\mathcal{D}_{K_v/\mathbb{Q}_p}^{-1}} & v \text{ finite} \end{cases},$$

by 9.5. By 9.8,

$$\zeta(f, s) = \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2} \prod_{v \nmid \infty} \frac{1}{1 - q_v^{-s}}.$$

If  $v \mid \infty$ , then  $\zeta(\widehat{f}_v, 1-s) = \zeta(f_v, 1-s)$ . If  $v$  is finite,

$$\zeta(\widehat{f}_v, 1-s) = q_v^{-\frac{\delta_v}{2}} \frac{q_v^{\delta_v(1-s)}}{1 - q_v^{-(1-s)}} = q_v^{\delta_v(\frac{1}{2}-s)} \zeta(f_v, 1-s).$$

Thus

$$Z_K(s) = |\mathrm{d}_K|^{\frac{s}{2}} \zeta(f, s) = |\mathrm{d}_K|^{\frac{s}{2}} \zeta(\widehat{f}, 1-s) = |\mathrm{d}_K|^{\frac{s}{2} + (\frac{1}{2}-s)} \zeta(f, 1-s) = Z_K(1-s),$$

giving all of 9.3.1. □

For part 2, have to compute  $\kappa = \text{meas}(\mathcal{C}_K^1)$ .

**Theorem 9.16.**

$$\kappa = \frac{2^{r_1} (2\pi)^{r_2} h_K R_K}{w_K}.$$

*Proof.* Replacing  $\mathbb{J}_K^1$  by  $\mathbb{J}_K = \mathbb{J}_K^1 \times \mathfrak{i}(\mathbb{R}_{>0})$ , by 9.12.2,

$$\begin{aligned} \text{meas}(\mathcal{C}_K^1) &= \text{meas}(\mathcal{C}_K^1 \times \mathbb{R}_{>0} / \langle e \rangle) & \int_1^e \frac{1}{t} dt &= 1 \\ &= \text{meas}(\mathcal{C}_K / \langle \mathfrak{i}(e) \rangle) & d_{\mathbb{J}} x &= d_{\mathbb{J}^1} y \times \frac{1}{t} dt \\ &= h_K \text{meas}(\mathbb{J}_{K,\emptyset} / \mathcal{O}_K^\times \langle \mathfrak{i}(e) \rangle) & 1 &\rightarrow \mathbb{J}_{K,\emptyset} / \mathcal{O}_K^\times \rightarrow \mathcal{C}_K \rightarrow \text{Cl}(K) \rightarrow 1 \\ &= \frac{h_K}{w_K} \text{meas}(\mathbb{J}_{K,\emptyset} / \langle \epsilon_1, \dots, \epsilon_r, \mathfrak{i}(e) \rangle) & \mathcal{O}_K^\times &= \mu(K) \times \langle \epsilon_1, \dots, \epsilon_r \rangle \\ &= \frac{h_K}{w_K} \text{meas}(K_\infty^\times / \langle \epsilon_1, \dots, \epsilon_r, \mathfrak{i}(e) \rangle) & \text{meas}(\widehat{\mathcal{O}_K^\times}) &= \prod_{v \nmid \infty} \text{meas}(\mathcal{O}_v^\times) = 1. \end{aligned}$$

Let  $K_\infty = \prod_{v|\infty} K_v^\times$ .

- If  $v$  is real, there is an isomorphism

$$\begin{aligned} K_v^\times = \mathbb{R}^\times &\longrightarrow \{\pm 1\} \times \mathbb{R} \\ x &\longmapsto (\text{sign } x, \log|x|_v) , \\ d_v^\times x &\longmapsto \mu \times dy \end{aligned}$$

where  $\mu$  is the counting measure.

- If  $v$  is complex, there is an isomorphism

$$\begin{aligned} K_v^\times \cong \mathbb{C}^\times &\longrightarrow \text{U}(1) \times \mathbb{R} \\ z = re^{i\theta} &\longmapsto (e^{i\theta}, 2 \log r) . \\ d_v^\times z = \frac{1}{|z|_v} d_{\mathbb{C}} z = \frac{1}{r^2} 2r dr d\theta &\longmapsto d\theta \times dr \end{aligned}$$

Then

$$\begin{array}{ccccccc} 1 & \longrightarrow & \{\pm 1\}^{r_1} \times \text{U}(1)^{r_2} & \longrightarrow & K_\infty^\times & \xrightarrow{\lambda = (\log|\cdot|_v)_v} & \mathcal{L}_K \longrightarrow 0 \\ & & \downarrow \mathbb{R} & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \{\pm 1\}^{r_1} \times \text{U}(1)^{r_2} & \longrightarrow & K_\infty^\times / \langle \epsilon_1, \dots, \epsilon_r, \mathfrak{i}(e) \rangle & \xrightarrow{\lambda} & \mathcal{L}_K / \Lambda \longrightarrow 0 \end{array},$$

where  $\Lambda = \langle \lambda(\epsilon_1), \dots, \lambda(\epsilon_r), \lambda(\mathfrak{i}(e)) \rangle \subset \mathcal{L}_K$  is a lattice, by the unit theorem, and

$$\lambda(\mathfrak{i}(e)) = \left( \log \left| e^{\frac{1}{n}} \right|_v \right)_v = \left( \frac{e_v}{n} \right)_v, \quad e_v = \begin{cases} 1 & v \text{ real} \\ 2 & v \text{ complex} \end{cases}.$$

Then

$$\text{meas}(\{\pm 1\}^{r_1} \times \text{U}(1)^{r_2}) = 2^{r_1} (2\pi)^{r_2},$$

and  $\text{meas}(\mathcal{L}_K / \Lambda)$  is the absolute value of the determinant of the  $(r+1) \times (r+1)$  matrix with rows

$$\left( \frac{e_v}{n}, \log|\epsilon_1|_v, \dots, \log|\epsilon_r|_v \right), \quad v \in V_{K,\infty}.$$

The sum of the rows is  $(1, 0, \dots, 0)$ , as  $|\epsilon_j|_{\mathbb{A}} = 1$ . So the determinant, up to  $\pm 1$ , is any  $(r \times r)$ -minor of the matrix  $(\log|\epsilon_j|_v)_{j,v}$ , so

$$\text{meas}(\mathcal{L}_K / \Lambda) = R_K.$$

□

*Proof of 9.3.2.* Since  $f_{\mathbb{C}}(z) = \frac{1}{\pi} e^{-2\pi z \bar{z}}$ ,

$$-\pi^{-r_2} \kappa = -f(0) \kappa = \text{Res}_{s=0} \zeta(f, s) = \text{Res}_{s=0} Z_K(s) = \lim_{s \rightarrow 0} s \left( \frac{2}{s} \right)^{r_1+r_2} \zeta_K(s),$$

as  $\Gamma_{\mathbb{R}}(s) \sim 2/s \sim \Gamma_{\mathbb{C}}(s)$  since  $\Gamma(s) \sim 1/s$  at  $s = 0$ , so

$$\lim_{s \rightarrow 0} s^{-r} \zeta_K(s) = -2^{-r_1} (2\pi)^{-r_2} \kappa = -\frac{h_K R_K}{w_K}, \quad r = r_1 + r_2 - 1,$$

by 9.16. □

**Remark.** A criticism is that this method only tells us about  $\zeta_K(s)$ , as for almost all  $v$ ,  $f_v = \mathbb{1}_{\mathcal{O}_v}$  and  $\zeta(f_v, s) = 1/(1 - q_v^{-s})$ . Next is to generalise to L-functions.

### 9.10 Description of $E \subset \mathbb{J}_K^1$

After the proof, exhibit an explicit  $E \subset \mathbb{J}_K^1$  such that

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

Let  $y_1, \dots, y_h \in \mathbb{J}_K^1$ , where  $h = h_K = \# \text{Cl}(K)$ , be coset representatives for  $\mathbb{J}_{K, \emptyset}^1 / \mathcal{O}_K^\times \subset \mathcal{C}_K^1$ . We will find  $E_0 \subset \mathbb{J}_{K, \emptyset}^1$  such that

$$\mathbb{J}_{K, \emptyset}^1 = \bigsqcup_{a \in \mathcal{O}_K^\times} aE_0.$$

Then

$$E = \bigsqcup_{i=1}^h y_i E_0$$

will do. Let

$$\mathcal{P} = \left\{ \sum_{j=1}^r t_j \lambda(\epsilon_j) \mid t_j \in [0, 1] \right\} \subset \mathcal{L}_K^0$$

be a set of coset representatives for  $\langle \lambda(\epsilon_1), \dots, \lambda(\epsilon_r) \rangle \subset \mathcal{L}_K^0$ , so

$$E_1 = \lambda^{-1}(\mathcal{P}) \times \widehat{\mathcal{O}_K}^\times$$

is a set of coset representatives for  $\langle \epsilon_1, \dots, \epsilon_r \rangle$  in  $K_\infty^{\times, 1} \times \widehat{\mathcal{O}_K}^\times = \mathbb{J}_{K, \emptyset}^1$ . Let  $v_0 \in V_{K, \infty}$ , assumed complex if  $w_K > 2$ . Then

$$E_0 = \left\{ x \in E_1 \mid \arg x_{v_0} \in \left[ 0, \frac{2\pi}{w_K} \right) \right\},$$

and clear that this works. If  $v_0$  is real and  $w_K = 2$ , this says  $x_{v_0} > 0$ .

## 10 L-functions

**Example.** A **Dirichlet character** is a homomorphism  $\phi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ . The **Dirichlet L-series** is

$$L(\phi, s) = \sum_{n \geq 1, (n, N)=1} \frac{\phi(n)}{n^s} = \prod_{p \nmid N} \frac{1}{1 - \phi(p)p^{-s}},$$

which occurs in the theorem on primes in arithmetic progressions. Then get a continuous

$$\chi : \mathcal{C}_{\mathbb{Q}} \cong \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times \rightarrow \widehat{\mathbb{Z}}^\times \rightarrow \prod_{p \mid N} (\mathbb{Z}_p/N\mathbb{Z}_p)^\times \cong (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\phi} \mathbb{C}^\times,$$

**Exercise.**

$$\left\{ \begin{array}{c} \text{continuous } \chi : \mathcal{C}_{\mathbb{Q}} \rightarrow \mathbb{C}^\times \\ \text{of finite order} \end{array} \right\} \quad \rightsquigarrow \quad \left\{ \begin{array}{c} \text{Dirichlet characters } \phi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times \\ \text{which are primitive} \end{array} \right\},$$

where  $\phi$  is **primitive** if it does not factor

$$(\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\text{mod } M} (\mathbb{Z}/M\mathbb{Z})^\times \rightarrow \mathbb{C}^\times, \quad M \mid N, \quad M < N.$$

### 10.1 Hecke characters

**Definition.** An **idele class character**, or **Hecke character**, of  $K$  is a continuous homomorphism  $\chi : \mathcal{C}_K \rightarrow \mathbb{C}^\times$ .

Note that do not require  $|\chi| = 1$ . In Tate, these are called **quasi-characters**.

**Example.** A simple but important example is

$$\chi(x) = |x|_{\mathbb{A}}^s, \quad s \in \mathbb{C},$$

as  $|K^\times|_{\mathbb{A}} = 1$ . For  $K = \mathbb{Q}$ , every Hecke character is  $|\cdot|_{\mathbb{A}}^s$  times a finite order  $\chi$ . But for  $K \neq \mathbb{Q}$ , there exist lots of other interesting ones.

**Proposition 10.1.** *Let  $G$  be a profinite group. Then any continuous homomorphism  $\chi : G \rightarrow \mathbb{C}^\times$  has open kernel, so finite image, that is it is continuous for the discrete topology on  $\mathbb{C}^\times$ .*

*Proof.*  $\chi(G)$  is compact so  $\chi(G) \subset U(1)$ . Let

$$V = \left\{ e^{i\theta} \in U(1) \mid -\frac{\pi}{2} < \theta < \frac{\pi}{2} \right\} = U(1) \cap \{\operatorname{Re} z > 0\}.$$

Then  $\chi^{-1}(V) \subset G$  is an open neighbourhood of the identity, so contains an open subgroup  $H \subset G$ . Then  $\chi(H) \subset V \subset U(1)$  is a subgroup. But this implies  $\chi(H) = 1$ , since if  $1 \neq z \in U(1)$ , some integer power  $z^n$  has  $\operatorname{Re} z^n \leq 0$ .  $\square$

**Corollary 10.2.**

1. Let  $F/\mathbb{Q}_p$ , and let  $\chi : F^\times \rightarrow \mathbb{C}^\times$  be continuous. Then there exists  $n \geq 0$  such that  $\chi(x) = 1$  for all  $x \in (1 + \pi^n \mathcal{O}_F) \cap \mathcal{O}_F^\times$ . The least such  $n$  is the **conductor** of  $\chi$ .
2. Let  $\chi : \mathbb{J}_K \rightarrow \mathbb{C}^\times$  be a continuous homomorphism, and let  $\chi_v = \chi|_{K_v^\times} : K_v^\times \rightarrow \mathbb{C}^\times$ . Then,
  - (a) for all but finitely many  $v \in V_{K,f}$ ,  $\chi_v$  is unramified, that is  $\chi_v(\mathcal{O}_v^\times) = 1$ , and
  - (b)  $\chi(x) = \prod_{v \in V_K} \chi_v(x_v)$ , a finite product by (a), and conversely, if  $(\chi_v)$  is a family of continuous homomorphisms  $\chi_v : K_v^\times \rightarrow \mathbb{C}^\times$  satisfying (a), their product  $\chi(x) = \prod_v \chi_v(x_v)$  is a well-defined continuous homomorphism  $\mathbb{J}_K \rightarrow \mathbb{C}^\times$ .

Lecture 23  
Saturday  
13/03/21



*Proof.*

1. Apply 10.1 with  $G = \mathcal{O}_F^\times$ .
2.
  - (a) Apply 10.1 with  $G = \widehat{\mathcal{O}_K}^\times \subset \mathbb{J}_K$ . Then  $\chi = 1$  on an open subgroup of  $\widehat{\mathcal{O}_K}^\times = \prod_{v \nmid \infty} \mathcal{O}_v^\times$ , so  $\chi|_{\mathcal{O}_v^\times} = 1$  for all but finitely many  $v \in V_{K,f}$ .
  - (b) The same as 8.1.2, for  $\mathbb{J}_K \rightarrow \mathbb{C}^\times$  discrete.

□

So what is a continuous homomorphism  $F^\times \rightarrow \mathbb{C}^\times$ ?

- Let  $F/\mathbb{Q}_p$ . If  $\chi : F^\times \rightarrow \mathbb{C}^\times$  is unramified then it factors

$$F^\times \xrightarrow{|\cdot|_F} q^{\mathbb{Z}} \xrightarrow{q \mapsto q^s} \mathbb{C}^\times, \quad s \in \mathbb{C},$$

unique modulo  $(2\pi i / \log q) \mathbb{Z}$ , that is  $\chi(x) = |x|_F^s$ . In general,  $\chi_1(x) = \chi(x) / \chi(\pi)^{v(x)}$  factors

$$F^\times \rightarrow F^\times / \langle \pi \rangle \cong \mathcal{O}_F^\times \rightarrow \mathbb{C}^\times,$$

which has finite image by 10.2.1, and  $\chi/\chi_1$  is unramified as  $\chi|_{\mathcal{O}_F^\times} = \chi_1|_{\mathcal{O}_F^\times}$ , that is  $\chi = \chi_1|\cdot|_F^s$  and  $\chi_1(\pi) = 1$  has finite order.

- Let  $F/\mathbb{R}$ . Then

$$F^\times = \begin{cases} \{\pm 1\} \times \mathbb{R}_{>0} & F = \mathbb{R} \\ \mathbb{U}(1) \times \mathbb{R}_{>0} & F = \mathbb{C} \end{cases},$$

and <sup>12</sup>

$$\text{Hom}_{\text{cts}}(\mathbb{R}_{>0}, \mathbb{C}^\times) = \{x \mapsto x^s \mid s \in \mathbb{C}\} \cong \mathbb{C}.$$

So continuous homomorphisms  $\chi : F^\times \rightarrow \mathbb{C}^\times$  are

$$\chi = \begin{cases} x \mapsto |x|^s \text{ and } x \mapsto \text{sign } x |x|^s & F = \mathbb{R} \\ z \mapsto \left( \frac{z}{|z|^{\frac{1}{2}}} \right)^n |z|^s \text{ for } n \in \mathbb{Z} & F = \mathbb{C} \end{cases},$$

so  $\chi = \chi_1|\cdot|_F^s$  where  $\chi_1|_{\mathbb{R}_{>0}} = 1$ .

Globally is the following.

**Proposition 10.3.** *Let  $\chi : \mathcal{C}_K \rightarrow \mathbb{C}^\times$ . There exists a unique  $\chi = \chi_1|\cdot|_\mathbb{A}^s$  for  $s \in \mathbb{C}$  such that  $\chi_1|_{\mathbb{R}_{>0}} = 1$ . Moreover,  $\chi_1(\mathbb{J}_K) \subset \mathbb{U}(1)$ .*

*Proof.* There exists a unique  $s \in \mathbb{C}$  such that for all  $x \in \mathbb{R}_{>0} \subset \mathbb{J}_K$ ,  $\chi(x) = |x|^s = |x|_\mathbb{A}^s$ . Then  $\chi_1 = \chi|\cdot|_\mathbb{A}^{-s}$  is trivial on  $K^\times \mathbb{R}_{>0}$ . As  $\mathcal{C}_K/\mathbb{R}_{>0}$  is compact,  $\chi_1(\mathbb{J}_K) \subset \mathbb{U}(1)$ . □

The following is the relation between the local  $s_v$  and the global  $s$ .

**Proposition 10.4.** *Let  $\chi = \prod_v \chi_v : \mathcal{C}_K \rightarrow \mathbb{C}^\times$  such that  $\chi = \chi_1|\cdot|_\mathbb{A}^s$  and  $\chi_v = \chi_{v,1}|\cdot|_v^{s_v}$  as above. Then  $\text{Re } s = \text{Re } s_v$  for all  $v$ .*

*Proof.* Let  $x \in K_v^\times \subset \mathbb{J}_K$ . Then as  $|\chi_{v,1}| = 1$  and  $|\chi_1| = 1$ ,

$$|x|_v^{\text{Re } s_v} = |\chi_v(x)| = |\chi(x)| = |x|_\mathbb{A}^{\text{Re } s} = |x|_v^{\text{Re } s}.$$

□

Note that suppose  $s = 0$ , need not have  $s_v = 0$ , since if  $v$  is unramified,  $\chi_v(\pi_v) = q_v^{-s_v} \neq 1$ , usually.

<sup>12</sup>Exercise

## 10.2 Hecke L-functions

**Definition.** Let  $\chi = \prod_v \chi_v : \mathcal{C}_K \rightarrow \mathbb{C}^\times$  be a Hecke character, and let

$$S = V_{K,\infty} \cup \{v \in V_{K,f} \mid \chi_v \text{ is ramified}\}.$$

The **Hecke L-series** or **Hecke L-function** of  $\chi$  is

$$L(\chi, s) = \prod_{v \notin S} \frac{1}{1 - \chi_v(\pi_v) q_v^{-s}},$$

which does not depend on the choice of  $\pi_v$ .

**Remark.**

- If  $\chi = 1$ , then  $L(\chi, s) = \zeta_K(s)$ .
- If  $K = \mathbb{Q}$  and  $\chi|_{\mathbb{R}_{>0}} = 1$ , that is  $\chi$  is of finite order, then  $L(\chi, s)$  is a Dirichlet L-series.<sup>13</sup>
- If  $t \in \mathbb{C}$ , then  $L(\chi|\cdot|_{\mathbb{A}}^t, s) = L(\chi, s+t)$  as  $|\pi_v|_v = q_v^{-1}$ . So there is a redundancy in the definition. We can get all L-functions if either
  - restrict to  $s = 0$ , since  $L(\chi, s) = L(\chi|\cdot|_{\mathbb{A}}^s, 0)$ , or
  - restrict to  $\chi$  with  $\chi|_{\mathbb{R}_{>0}} = 1$ , using  $L(\chi|\cdot|_{\mathbb{A}}^t, s) = L(\chi, s+t)$ , in particular  $\chi$  is unitary.

Both are useful.

**Proposition 10.5.** *If  $\chi|_{\mathbb{R}_{>0}} = 1$ , and more generally, if  $|\chi| = 1$ , then  $L(\chi, s)$  converges absolutely for  $\operatorname{Re} s > 1$ .*

*Proof.* Since  $|\chi_v(\pi_v)| = 1$ , follows by comparison with  $\zeta_K(s)$ . □

The following is the main theorem.

**Theorem 10.6** (Functional equation for Hecke L-function). *Let  $\chi$  be a Hecke character.*

- *There exist  $a_v \in \mathbb{C}$  for  $v \in V_{K,\infty}$  and  $\epsilon(\chi, s) = AB^s$  for some  $A \in \mathbb{C}^\times$  and  $B > 0$  such that if*

$$\Lambda(\chi, s) = \prod_{v|\infty} \Gamma_{K_v}(s + a_v) L(\chi, s),$$

*then  $\Lambda(\chi, s)$  has a meromorphic continuation to  $\mathbb{C}$ , and*

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

*If  $\chi \neq |\cdot|_{\mathbb{A}}^t$  for some  $t \in \mathbb{C}$ , then  $\Lambda(\chi, s)$  is entire.*

•

$$\epsilon(\chi, s) = \prod_v \epsilon_v(\chi_v, s),$$

*where the **local  $\epsilon$ -factors** are  $\epsilon_v(\chi_v, s) = 1$  for all but finitely many  $v$ , and only depends on  $\chi_v$ .*

**Remark.** If  $\chi = |\cdot|_{\mathbb{A}}^t$ , then  $\Lambda(\chi, s) = Z_K(s+t)$  and we know the poles, and residues.

$K_v = \mathbb{R}$ . If  $\chi_v = |\cdot|_v^t$ , then  $a_v = t$  and  $\epsilon_v(\chi_v, s) = 1$ . If  $\chi_v = \operatorname{sign}|\cdot|_v^t$ , then  $a_v = t+1$  and  $\epsilon_v(\chi_v, s) = -i$ .

$K_v = \mathbb{C}$ . If  $\chi_v = \left(z/|z|_v^{1/2}\right)^n |z|_v^t$  for  $n \in \mathbb{Z}$ , then  $a_v = t + |n|/2$  and  $\epsilon_v(\chi_v, s) = i^{-|n|}$ .

---

<sup>13</sup>Exercise

$K_v/\mathbb{Q}_p$ . If  $\chi_v$  is unramified,

$$\epsilon_v(\chi_v, s) = \begin{cases} 1 & K_v/\mathbb{Q}_p \text{ is unramified, so } \delta_v = 0 \\ \delta_v \left(\frac{1}{2} - s\right)_{\chi_v(\pi_v)^{\delta_v}} & \text{in general} \end{cases}.$$

If  $\chi_v$  is ramified,

$$\epsilon_v(\chi_v, s) = \int_{K_v^\times} \chi_v(x)^{-1} |x|_v^{-s} \psi_v(x) \, d_v x = \sum_n \int_{\pi_v^{-n} \mathcal{O}_v^\times} \chi_v(x)^{-1} |x|_v^{-s} \psi_v(x) \, d_v x,$$

which is a Gauss sum, and in fact the integral is non-zero for only  $n = \delta_v + m_v$  where  $m_v$  is the conductor of  $\chi_v$ .

### 10.3 Global $\zeta$ -integral

**Definition.** Let  $f \in \mathcal{S}(\mathbb{A}_K)$ . Then

$$\zeta(f, \chi, s) = \int_{\mathbb{J}_K} f(x) \chi(x) |x|_{\mathbb{A}}^s \, d_{\mathbb{J}} x = \prod_v \int_{F^\times} f_v(x) \chi_v(x) |x|_v^s \, d_F^\times x = \prod_v \zeta_v(f_v, \chi_v, s), \quad f = \bigotimes_v f_v.$$

Can restrict to  $s = 0$  and changing  $\chi$ .

**Theorem 10.7** (Global functional equation for  $\zeta(f, \chi, s)$ ).

•

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

*meromorphic on  $\mathbb{C}$ .*

- If  $\chi \neq |\cdot|_{\mathbb{A}}^t$  for some  $t \in \mathbb{C}$ , then  $\zeta(f, \chi, s)$  is entire, so no poles.

*Proof.* Modify the proof of 9.11 to include  $\chi$ . Without loss of generality,  $\chi|_{\mathbb{R}_{>0}} = 1$ , by changing  $s$ . Replace  $\zeta_t(f, s)$  by

$$\begin{aligned} \zeta_t(f, \chi, s) &= t^s \int_{\mathbb{J}_K^1} f(tx) \chi(x) \, d_{\mathbb{J}^1} x = t^s \int_E \sum_{a \in K^\times} f(atx) \chi(x) \, d_{\mathbb{J}^1} x \\ &= t^s \int_E \sum_{a \in K} f(atx) \chi(x) \, d_{\mathbb{J}^1} x - f(0) t^s \int_E \chi(x) \, d_{\mathbb{J}^1} x, \end{aligned}$$

as  $\chi|_{K^\times} = 1$  and  $\mathbb{J}_K^1 = \bigsqcup_{a \in K^\times} aE$ .

- If  $\chi = 1$ , the latter integral is  $\kappa$  as before.
- If  $\chi \neq 1$ , choosing  $b \in E$  such that  $\chi(b) \neq 1$  and putting  $x \mapsto bx$ , the latter integral is zero.

Then apply the Poisson summation and the rest of the proof as for 9.11. □

To get the functional equation for  $\Lambda(\chi, s)$ , need a suitable  $f$ . The following is the nicest way to see this.

**Theorem 10.8** (Local functional equation for  $\zeta(f, \chi, s)$ ). *Let  $F$  be local, and let  $\chi : F^\times \rightarrow \mathbb{C}^\times$ . Then for all  $f \in \mathcal{S}(F)$ ,*

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

Here  $L$  and  $\epsilon$  are the local factors from above, so for  $F/\mathbb{R}$ , these are  $\Gamma_F(s + a_F)$ .

*Proof of 10.6.* Multiplying the local and global functional equations, get the functional equation for  $\Lambda(\chi, s)$ . □

Lecture 24  
Tuesday  
16/03/21

**Proposition 10.9.** *Let  $f, g \in \mathcal{S}(F)$ . Then*

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

*Proof.* Changing variables  $t' = x$ ,  $x' = t$ ,  $y' = ty/x$ , so  $x'/y' = x/y$  and  $yt = y't'$ ,

$$\begin{aligned} \zeta(f, \chi, s) \zeta(\widehat{g}, \chi^{-1}, 1-s) &= \int_{F^\times} \int_{F^\times} f(x) \widehat{g}(y) \chi\left(\frac{x}{y}\right) \left|\frac{x}{y}\right|_F^s |y|_F \, d_F^\times x \, d_F^\times y \\ &= c \int_F \int_{F^\times} \int_{F^\times} f(x) g(t) \psi(yt) \chi\left(\frac{x}{y}\right) \left|\frac{x}{y}\right|_F^s |yt|_F \, d_F^\times x \, d_F^\times y \, d_F^\times t \\ &= c \int_{F^\times} \int_{F^\times} \int_F f(t') g(x') \psi(y't') \chi\left(\frac{x'}{y'}\right) \left|\frac{x'}{y'}\right|_F^s |y't'|_F \, d_F^\times t' \, d_F^\times y' \, d_F^\times x' \\ &= \int_{F^\times} \int_{F^\times} \widehat{f}(y') g(x') \chi\left(\frac{x'}{y'}\right) \left|\frac{x'}{y'}\right|_F^s |y'|_F \, d_F^\times y' \, d_F^\times x' \\ &= \zeta(\widehat{f}, \chi^{-1}, 1-s) \zeta(g, \chi, s). \end{aligned}$$

□

*Proof of 10.8.*

- The independence of  $f$ , by 10.9.
- Just have to find a suitable  $f$ , depending on  $\chi$ , such that we can compute  $\zeta(f, \chi, s)$  and  $\zeta(\widehat{f}, \widehat{\chi}, 1-s)$ . For  $\chi = 1$  did earlier. For general  $\chi$ , see example sheet 4.

□

A special global case is when  $L(\chi^{-1}, s) = L(\chi, s+t)$ , such as  $\chi^2 = 1$ . More generally, there exists  $g \in \text{Aut}(K/\mathbb{Q})$  such that  $\chi^{-1} = (\chi \circ g)|\cdot|_{\mathbb{A}}^t$ . For an example, see example sheet 4, question 8. Then

$$\Lambda(\chi, s) = \epsilon(\chi, s) \Lambda(\chi, 1-s) = \epsilon(\chi, s) \epsilon(\chi, 1-s) \Lambda(\chi, s),$$

that is  $AB^s AB^{1-s} = 1$  so  $A^2 = B^{-1} > 0$ , so

$$\epsilon(\chi, s) = w(\chi) B^{s-\frac{1}{2}},$$

where  $w(\chi) \in \{\pm 1\}$  is the **root number** and

$$\Lambda\left(\chi, s + \frac{1}{2}\right) = w(\chi) B^s \Lambda\left(\chi, -s + \frac{1}{2}\right).$$

Thus  $w(\chi)$  determines the parity of the order of  $\Lambda(\chi, s)$  at  $s = \frac{1}{2}$ .

## 10.4 Artin L-functions\*

Let  $\chi : \mathcal{C}_K \rightarrow \mathbb{C}^\times$  be of finite order. Then by class field theory,  $\chi = \theta \circ \text{Art}_{L/K}$  for some abelian  $L/K$  and  $\theta : \text{Gal}(L/K) \hookrightarrow \mathbb{C}^\times$ . Then

$$L(\chi, s) = \prod_{v \notin S} \frac{1}{1 - \theta(\text{Fr}_v) q_v^{-s}},$$

where  $\text{Fr}_v$  is the geometric Frobenius. The local factor at  $v \mid \infty$  is

- $\Gamma_{\mathbb{C}}(s)$  if  $v$  is complex, and
- $\Gamma_{\mathbb{R}}(s)$  if  $\theta(c) = 1$  and  $\Gamma_{\mathbb{R}}(s+1)$  if  $\theta(c) = -1$  if  $v$  is real, where  $c$  is complex conjugation at  $v$ .

This suggests to try to define  $L(\rho, s)$  for any representation  $\rho : \text{Gal}(L/K) \rightarrow \text{GL } V$  for  $L/K$  Galois and  $V \cong \mathbb{C}^d$ . Thinking about  $\rho = \bigoplus_i \theta_i$  leads to the following.

**Definition.** The **Artin L-function** of  $\rho$  is

$$L(\rho, s) = \prod_{v \in V_{K, f}} L_v(\rho_v, s), \quad L_v(\rho_v, s) = L_v(\rho|_{D_v}, s) = \det \left( 1 - \rho(\text{Fr}_v) q_v^{-s} \mid V^{\rho(I_v)} \right)^{-1},$$

which is well-defined on  $V^{\rho(I_v)}$ .

- For  $v$  complex,  $L_v(\rho_v, s) = \Gamma_{\mathbb{C}}(s)^d$ .
- For  $v$  real,  $L_v(\rho_v, s) = \Gamma_{\mathbb{R}}(s)^{d^+} \Gamma_{\mathbb{R}}(s+1)^{d^-}$ , where  $d_{\pm} = \dim V^{\rho(c)=\pm 1}$ .

**Proposition 10.10.**

1.  $L(\rho_1 \oplus \rho_2, s) = L(\rho_1, s) L(\rho_2, s)$ .
2. If  $L/K_1/K$  and  $\rho_1 : \text{Gal}(L/K_1) \rightarrow \text{GL } V$ , then  $L(\rho_1, s) = L\left(\text{Ind}_{\text{Gal}(L/K_1)}^{\text{Gal}(L/K)} \rho_1, s\right)$ .

*Proof.*

1. Obvious.
2. It is easy to check locally. At  $v \mid \infty$ , this reduces to  $\Gamma_{\mathbb{R}}(s) \Gamma_{\mathbb{R}}(s+1) = \Gamma_{\mathbb{C}}(s)$ , which explains the normalisation of  $\Gamma_{\mathbb{C}}(s)$ .

□

**Theorem 10.11.**  $\Lambda(\rho, s) = \prod_v L(\rho_v, s)$  has a meromorphic continuation and a functional equation

$$\Lambda(\rho, s) = \epsilon(\rho, s) \Lambda(\rho^{\vee}, 1-s),$$

where  $\rho^{\vee}$  is the **contragredient representation**  $g \mapsto \rho(g^{-1})^{\top} \in \text{GL } V^*$ .

Proof by reduction to the abelian case.

**Theorem 10.12** (Brauer). *Let  $G$  be a finite group, and let  $\rho : G \rightarrow \text{GL}_d \mathbb{C}$ . Then there exist subgroups  $H_i \subset G$ , homomorphisms  $\chi_i : H_i \rightarrow \mathbb{C}^{\times}$ , and integers  $m_i$ , such that*

$$\text{Tr } \rho = \sum_i m_i \chi_i,$$

that is

$$\rho \oplus \sum_{m_i < 0} -m_i \chi_i = \sum_{m_i \geq 0} m_i \chi_i.$$

Then

$$L(\rho, s) = \prod_i L(\chi_i, s)^{m_i}.$$

Some  $m_i$  may be negative, so no control over poles.

**Conjecture 10.13** (Artin conjecture). *If  $\rho$  does not contain trivial representations, then  $L(\rho, s)$  is entire.*

Mostly still unsolved, now viewed as a problem in the Langlands programme, or non-abelian class field theory. The status is

- true if  $\dim V = 1$ , so Hecke L-functions, where  $\rho$  is  $\chi : \mathcal{C}_K \rightarrow \mathbb{C}^{\times}$ ,
- true if all  $m_i \geq 0$ , such as if  $G$  is a nilpotent group, and
- true if  $\dim V = 2$  and either
  - $\text{im } \rho \subset \text{GL}_2 \mathbb{C}$  is solvable, using automorphic base change, or
  - $K$  is totally real and  $\rho(c) \sim \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$  for all complex conjugations  $c \in \text{Gal}(L/K)$ , using the proof of Serre's conjecture and generalisations to totally real fields, that is lots of automorphic theory, modularity lifting theorems, etc,

where  $\rho$  is an automorphic representation  $\pi$  of  $\text{GL}_d \mathbb{A}_K$ .

Ignore the comment in Neukirch's book, where he says the conjecture is true for solvable extensions.