Algebraic Number Theory

Lectured by Professor Anthony Scholl
Typed by David Kurniadi Angdinata

Lent 2020

Syllabus

Contents

1 Absolute values and places

1.1 Absolute values

Lecture 1 Thursday 21/01/21

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

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

Also assume

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

This excludes the trivial AV

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

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

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

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

Remark. It is convenient to weaken 3 to

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

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

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

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

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

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

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

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

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

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

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

Proposition 1.2. *The following are equivalent.*

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

Proof. See local fields. □

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

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

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

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

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

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

$n = 1$. Trivial.

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

□

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

1.2 Places

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

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

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

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

Notation. Let

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

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

Can restate weak approximation in terms of places.

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

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

is dense, for the product topology.

1.3 Extensions of places

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

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

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

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

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

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

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

Corollary 1.6.

- $\{w \mid v\}$ *is finite, non-empty, and*
$$\sum_{w \mid v} [L_w : K_v] = [L : K].$$
- *For all* $x \in L$,
$$\mathrm{N}_{L/K}(x) = \prod_{w \mid v} \mathrm{N}_{L_w/K_v}(x), \qquad \mathrm{Tr}_{L/K}(x) = \sum_{w \mid v} \mathrm{Tr}_{L_w/K_v}(x).$$

Lecture 2 Saturday 23/01/21

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

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

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

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

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

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

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

2 Number fields

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

2.1 Dedekind domains

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

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

The following are basic results about Dedekind domains.

Theorem 2.1.

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

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

Proof.

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

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

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

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

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

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

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

[1] Exercise

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

$\square$

Theorem 2.2. *Let R be Dedekind. Then*

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

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

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

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

Proof.

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

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

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

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

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

2. By unique factorisation of ideals in 1,

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

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

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

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

$\square$

The quotient group

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

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

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

2.2 Places of number fields

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

Theorem 2.3. *This gives a bijection*

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

Proof. Let $\mathfrak{p} \neq \mathfrak{q}$. Then there exists $x \in \mathfrak{p} \setminus \mathfrak{q}$, and then $|x|_{\mathfrak{p}} < 1 = |x|_{\mathfrak{q}}$, so $|\cdot|_{\mathfrak{p}}$ and $|\cdot|_{\mathfrak{q}}$ are inequivalent, so the map is injective. Let $|\cdot|$ be a non-archimedean AV on K, with valuation ring $R = \{x \in K \mid |x| \leq 1\}$. 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. ☐

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

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

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

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

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

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

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

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

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

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

Therefore the following holds.

Theorem 2.4. *There is a bijection*

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

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

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

2.3 Extensions of places of number fields

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

Lecture 4 Thursday 28/01/21

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

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

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

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

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

☐

Remark.

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

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

3 Different and discriminant

3.1 Discriminant

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

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

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

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

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

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

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 $f : R \to R'$ 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

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

  is non-degenerate, that is there is a duality of the R-vector space S with itself.

By field theory, if L/K is a finite field extension, then $\mathrm{disc}(L/K) = K$ 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 $A = \prod_i A_i$. ☐

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. Lecture 5 Saturday 30/01/21

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

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

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

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

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

□

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

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

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

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

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

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

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

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

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

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

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

Definition. Define

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

which is equivalent by 3.4 to the previous definition.

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

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

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

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

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

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

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

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

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

□

3.2 Different

There is a finer invariant of ramification.

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

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

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

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

Proposition 3.8.

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

Proof.

1. Exercise. [2]
2. By 1 and 3.4, can suppose R is local. Then S is a PID by 2.1.3. So $\mathcal{D}_{S/R}^{-1} = x^{-1}S$ for some $0 \ne x \in S$. Let (e_i) be a basis for S over R. Then there exists a basis (e_i') for S over R such that $\mathrm{Tr}_{L/K}\left(e_i x^{-1} e_j'\right) = \delta_{ij}$. Let $x^{-1}e_j' = \sum_k b_{kj} e_k$ for $b_{kj} \in K$. Then
$$\langle 1 \rangle = \left\langle \det\left(\mathrm{Tr}_{L/K}\left(e_i x^{-1} e_j'\right)\right)\right\rangle = \left\langle \det\left(\mathrm{Tr}_{L/K}\left(e_i e_j\right)\right)\det\left(b_{ij}\right)\right\rangle = \det\left(b_{ij}\right)\mathrm{disc}\,(S/R).$$
But $\mathrm{N}_{L/K}\left(x^{-1}\right)$ is $\det\left(b_{ij}\right)$ times some unit in R. So $\langle 1 \rangle = \left\langle \mathrm{N}_{L/K}\left(x^{-1}\right)\right\rangle \mathrm{disc}\,(S/R)$. Lecture 6 Tuesday 02/02/21
3. Assume R is local and $\mathfrak{p} = \langle \pi_\mathfrak{p} \rangle$. Write $\widehat{K} = \mathrm{Frac}\,\widehat{R}$ and for $\mathfrak{q} = \langle \pi_\mathfrak{q} \rangle \subset S$ write $\widehat{L_\mathfrak{q}} = \mathrm{Frac}\,\widehat{S_\mathfrak{q}}$. So say
$$L \otimes_K \widehat{K} \supset S \otimes_R \widehat{R} \xrightarrow{\sim} \prod_\mathfrak{q} \widehat{S_\mathfrak{q}} \subset \prod_\mathfrak{q} \widehat{L_\mathfrak{q}},$$
and
$$\mathrm{Tr}_{L \otimes_K \widehat{K}/\widehat{K}}(x) = \sum_\mathfrak{q} \mathrm{Tr}_{\widehat{L_\mathfrak{q}}/\widehat{K}}(x). \qquad (3)$$
Let $S = \bigoplus_{i=1}^n Rx_i$, and $\prod_\mathfrak{q} \pi_\mathfrak{q}^{-a_\mathfrak{q}} S = \mathcal{D}_{S/R}^{-1} = \bigoplus_{i=1}^n Ry_i$ for some $a_\mathfrak{q} \ge 0$ and $y_i \in L$, the dual basis to x_i. Then as $S \otimes_R \widehat{R} = \bigoplus_{i=1}^n \widehat{R}\,(x_i \otimes 1)$,
$$\begin{aligned}\mathcal{D}_{S \otimes_R \widehat{R}/\widehat{R}}^{-1} &= \left\{x \in L \otimes_K \widehat{K} \;\middle|\; \forall y \in S \otimes_R \widehat{R},\ \mathrm{Tr}_{L \otimes_K \widehat{K}/\widehat{K}}(xy) \in \widehat{R}\right\} \\ &= \bigoplus_{i=1}^n \widehat{R}\,(y_i \otimes 1) = \mathcal{D}_{S/R}^{-1}\left(S \otimes_R \widehat{R}\right) = \prod_\mathfrak{q} \pi_\mathfrak{q}^{-a_\mathfrak{q}}\left(S \otimes_R \widehat{R}\right) \subset L \otimes_K \widehat{K},\end{aligned}$$
since $\mathrm{Tr}_{L/K}(x_i y_j) = \delta_{ij}$ and trace commutes with base change. On the other hand, by (3) and the definitions
$$\mathcal{D}_{S \otimes_R \widehat{R}/\widehat{R}}^{-1} \cong \prod_\mathfrak{q} \mathcal{D}_{\widehat{S_\mathfrak{q}}/\widehat{R}}^{-1} \subset \prod_\mathfrak{q} \widehat{L_\mathfrak{q}},$$
so
$$\mathcal{D}_{\widehat{S_\mathfrak{q}}/\widehat{R}}^{-1} = \prod_{\mathfrak{q}'} \pi_{\mathfrak{q}'}^{-a_{\mathfrak{q}'}} \widehat{S_\mathfrak{q}} = \pi_\mathfrak{q}^{-a_\mathfrak{q}} \widehat{S_\mathfrak{q}},$$
as $\mathrm{v}_\mathfrak{q}(\pi_{\mathfrak{q}'}) = 0$ if $\mathfrak{q}' \ne \mathfrak{q}$.

∎

[2] Exercise: the same idea as 3.4

Use this to prove the following.

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

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

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

1. So $\mathcal{D}_{S/R} = \langle \pi_S \rangle^d$ for $d \geq 0$. By 3.8.2, $\mathrm{disc}(S/R) = \left\langle \mathrm{N}_{L/K}(\pi_S)^d \right\rangle = \langle \pi_R \rangle^{\mathrm{df}}$. So as $\mathrm{v}_{\mathfrak{p}}(\mathrm{disc}(S/R)) = 0$ if and only if $\mathfrak{p}$ is unramified by 3.5, get the first statement.
2. Claim $\mathrm{Tr}_{L/K}(\mathfrak{q}) \subset \mathfrak{p}$. Let $x \in \mathfrak{q}$. Then multiplication by x is a nilpotent endomorphism of $S \otimes_R (R/\mathfrak{p}) \cong S/\mathfrak{q}^{\mathrm{e}}$, so $\mathrm{Tr}_{S \otimes_R (R/\mathfrak{p})/(R/\mathfrak{p})}(x \otimes 1) = 0$, that is $\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{S/R}(x) \in \mathfrak{p}$. Hence the claim. Therefore $\mathrm{Tr}_{L/K}\left(\mathfrak{q}^{1-\mathrm{e}}\right) = \mathrm{Tr}_{L/K}\left(\pi_R^{-1}\mathfrak{q}\right) \subset R$, so $\mathfrak{q}^{1-\mathrm{e}} \subset \mathcal{D}_{S/R}^{-1}$, that is $\mathfrak{q}^{\mathrm{e}-1} \mid \mathcal{D}_{S/R}$.

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

Fact.

- If $\mathfrak{p} \nmid e_i$ then $\mathrm{v}_{\mathfrak{q}_i}\left(\mathcal{D}_{S/R}\right) = e_i - 1$. If $\mathfrak{p} \mid e_i$ then $\mathrm{v}_{\mathfrak{q}_i}\left(\mathcal{D}_{S/R}\right) \geq e_i$. More precisely, $\mathrm{v}_{\mathfrak{q}_i}\left(\mathcal{D}_{S/R}\right)$ is determined by the orders of the higher ramification groups, for a Galois closure of L/K. See for example Serre, Local fields, Chapter 4, Section 1, Proposition 4.
- If $S = R[x]$, and x has minimal polynomial $f \in R[T]$ then $\mathcal{D}_{S/R} = \langle f'(x) \rangle$ where f' is the derivative. See example sheet 1. This means that $\mathcal{D}_{S/R}$ is the annihilator of the cyclic S-module $\Omega_{S/R}$ of Kähler differentials, generated by $\mathrm{d}x$.

For an extension L/K of number fields write

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

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

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

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

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

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

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

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

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

4 Examples

4.1 Quadratic fields

Lecture 7 Thursday 04/02/21

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

- Since $\mathrm{Tr}_{K/\mathbb{Q}}(1) = 2$ and $\mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{d}\right) = 0$, $\mathrm{disc}\left(1, \sqrt{d}\right) = 4d$, so
  - either $\mathrm{d}_K = 4d$, and $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{d}\right]$,
  - or $\mathrm{d}_K = d$, and $\left(\mathcal{O}_K : \mathbb{Z}\left[\sqrt{d}\right]\right) = 2$.

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

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

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

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

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

4.2 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 $\zeta_n^m \ne 1$ for all $1 \le m < n$. Equivalently, ζ_n is a root of the n-th cyclotomic polynomial $\Phi_n \in \mathbb{Z}[T]$ of degree $\phi(n)$, defined recursively by

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

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

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

is an injective homomorphism.

[3]Exercise

Theorem 4.1. *Let* $L = \mathbb{Q}(\zeta_n)$*. Then*

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

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

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

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

This proves 4.1 by induction on n. For a place w of L, write $x_w \in L_w$ for the image of ζ_{p^r} under $L \hookrightarrow L_w$. Suppose $v \mid p$. By induction, p is unramified in $K/\mathbb{Q}$, so $v(p) = 1$. Then

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

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

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

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

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

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

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

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

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

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

4.3 Frobenius elements

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

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

where I_w is the inertia subgroup. Suppose w is unramified in L/K, if and only if v is unramified in L/K. Then $\mathrm{I}_w = \{1\}$.

Definition. Define the **Frobenius** at w to be the unique element $\sigma_w \in G_w$ mapping to the generator $x \mapsto x^{\mathrm{q}_v}$ of $\mathrm{Gal}(\ell_w/\kappa_v)$.

So $\mathrm{ord}\,\sigma_w = \mathrm{f}(w \mid v) = [\ell_w : \kappa_v] = [\ell_{w'} : \kappa_v]$ for any $w' \mid v$, as G acts transitively on $\{w'\}$. In particular, $\sigma_w = 1$ if and only if v splits completely in L/K, that is there exist $[L : K]$ places of L over v. Suppose G is abelian. Then G_w and σ_w are independent of w, so depends only on v.

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

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

4.4 Quadratic reciprocity

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

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

Claim that

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

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

Remark.

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

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

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

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

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

But

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

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

5 Ideles and adeles

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

5.1 Adeles

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

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

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

where

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

Notation. Let

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

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

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

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

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

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

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

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

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

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

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

[4] Exercise: easy

Proposition 5.1. *$\mathbb{A}_K$ is Hausdorff and locally compact, so every point has a compact neighbourhood.*

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

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

Proposition 5.2. *K is discrete in $\mathbb{A}_K$.*

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

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

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

Lecture 9 Tuesday 09/02/21

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

Proposition 5.3. *Let $(a_1, \dots, a_n)$ be a K-basis for L. Consider*

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

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

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

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

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

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

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

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

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

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

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

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

Corollary 5.4. *$\mathbb{A}_L$ is a free $\mathbb{A}_K$-module of rank $[L:K]$, and the diagram*

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

commutes, where the left hand inclusions are

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

Proof. Exercise. [5] ☐

Theorem 5.5. *$\mathbb{A}_K/K$ is compact Hausdorff.*

Proof. Since K is closed in $\mathbb{A}_K$ and $\mathbb{A}_K$ is Hausdorff, $\mathbb{A}_K/K$ is Hausdorff. By 5.3, $\mathbb{A}_K/K \cong (\mathbb{A}_\mathbb{Q}/\mathbb{Q})^{[K:\mathbb{Q}]}$ as topological groups, so may assume $K = \mathbb{Q}$. Let $X = [0,1] \times \widehat{\mathbb{Z}} \subset \mathbb{A}_\mathbb{Q}$. Then X is compact. So it is enough to show that $X + \mathbb{Q} = \mathbb{A}_\mathbb{Q}$, as then $X \twoheadrightarrow \mathbb{A}_\mathbb{Q}/\mathbb{Q}$. Let $x = (x_p)_{p \le \infty} \in \mathbb{A}_\mathbb{Q}$. Let

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

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

From 5.3 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 $\mathcal{O}_K$.

5.2 Ideles

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

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

where

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

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

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

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

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

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

has closed image.

[5] Exercise

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

Lecture 10 Thursday 11/02/21

Definition. $\mathcal{C}_K = \mathcal{J}_K / K^\times$ is the **idele class group** of K.

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

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

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

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

Definition. Let

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

Proposition 5.6.

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

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

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

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

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

Definition. Let

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

The **content map** is

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

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

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

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

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

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

Define

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

This will be useful later on.

6 Geometry of numbers

6.1 Minkowski's theorem

Classically, embed

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

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

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

Proposition 6.1. *A subgroup $\Lambda \subset U$ is a lattice if and only if $\Lambda = \bigoplus_{1 \le i \le n} \mathbb{Z} e_i$, where (e_i) is an $\mathbb{R}$-basis for U where $n = \dim_{\mathbb{R}} U$.*

Proof. Example sheet. ☐

Theorem 6.2 (Minkowski's theorem)**.** *Let $\Lambda \subset \mathbb{R}^n$ be a lattice, and let $\mu_\Lambda = \mathrm{vol}(\mathbb{R}^n/\Lambda)$, the* ***covolume*** *of Λ. Let $X \subset \mathbb{R}^n$ be a compact subset, which is*

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

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

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

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

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

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

Theorem 6.3. *There exists a constant $\mathrm{r}_K > 0$ such that, if $(d_v)_{v \in K}$ are positive reals with*

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

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

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

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

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

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

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

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

This is convex, compact, symmetric, and

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

by (4), provided

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

Then applying 6.2, $X \cap \sigma(I) \neq \{0\}$ and any $x \in X \cap \sigma(I)$ has $|x|_v \leq d_v$ for all v. □

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 $\left|\mathrm{N}_{K/\mathbb{Q}}(x)\right| < \mathrm{r}_K\mathrm{N}(I)$.

Lecture 11 Saturday 13/02/21

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

6.2 Compactness of idele class group

Theorem 6.4. *$\mathcal{C}_K^1 = \mathcal{J}_K^1/K^\times$ is compact.*

Recall $K^\times \subset \mathcal{J}_K^1 = \ker\left(|\cdot|_{\mathbb{A}} : \mathcal{J}_K \to \mathbb{R}_{>0}\right)$ is discrete. Based on 6.3 and the following.

Proposition 6.5. *Let $\rho_v > 0$ for $v \in \mathrm{V}_K$, with $\rho_v = 1$ for all but finitely many v. Then*

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

is compact.

This is false for $\mathcal{J}_K$. 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

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

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

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

which is a closed subset of

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

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

Proof of 6.4. Let r_K be as in 6.3. Pick any $y \in \mathcal{J}_K$ with $|y|_{\mathbb{A}} > \mathrm{r}_K$, and let

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

which is compact by 6.5. Show that

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

Let $z \in \mathcal{J}_K^1$. Then $\prod_v |y_v z_v|_v = |y|_{\mathbb{A}} > \mathrm{r}_K$. So by 6.3, there exists $b \in K^\times$ such that for all $v \in \mathrm{V}_K$, $|b|_v \leq |y_v z_v|_v$. Therefore $bz^{-1} \in X$, that is $z^{-1} \in b^{-1}X \subset K^\times X$. □

6.3 Finiteness of ideal class group and S-unit theorem

The following are two corollaries.

Corollary 6.6. *The ideal class group* $\mathrm{Cl}(K)$ *is finite.*

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

Corollary 6.7 (S-unit theorem)**.** *Let* $S \subset \mathrm{V}_{K,\mathrm{f}}$ *be finite, possibly empty, and let*

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

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

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

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

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

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

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

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

Then $\mathcal{J}_{K,\emptyset} \cap K^\times = \mathcal{J}_{K,\emptyset}^1 \cap K^\times = \mathcal{O}_K^\times$ is discrete in $\mathcal{J}_{K,\emptyset}^1$ and by 6.4, the closed $\mathcal{J}_{K,\emptyset}^1/\mathcal{O}_K^\times \subset \mathcal{C}_K^1$ is compact. Let

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

be the **logarithm map**, such that

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

Then

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

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

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

which gives 6.7. Now

$$\begin{tikzcd} \mathcal{J}_{K,\emptyset} \arrow[r, phantom, "\cong"] \arrow[d, "\lambda"'] & \prod_{v \mid \infty} \mathbb{R}_{>0} \times \ker\lambda \arrow[d, "\pi_1"] \\ \mathcal{L}_K & \prod_{v \mid \infty} \mathbb{R}_{>0} \arrow[l, "\sim"', "\log"] \end{tikzcd},$$

where $\mathbb{R}_{>0} \hookrightarrow K_v^\times \subset \mathbb{C}^\times$ for all $v \mid \infty$. Hence λ has the property that for all compact Y in its target, $\lambda^{-1}(Y)$ is compact, so λ is a proper map. A simple fact is if $f : X \to Y$ is a continuous proper map of topological spaces, with Y locally compact and Hausdorff, then if $Z \subset X$ is discrete then $f(Z)$ is discrete. [6] Hence $\lambda(\mathcal{O}_K^\times) \subset \mathcal{L}_K^0$ is discrete. Finally, $\lambda : \mathcal{J}_{K,\emptyset}^1/\mathcal{O}_K^\times \twoheadrightarrow \mathcal{L}_K^0/\lambda(\mathcal{O}_K^\times)$, so $\mathcal{L}_K^0/\lambda(\mathcal{O}_K)$ is compact, by 6.4. Thus $\lambda(\mathcal{O}_K)$ is a lattice. ☐

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