

Algebraic Number Theory

Harry Armitage

February 15, 2021

Contents

1	Absolute Values and Places	2
1.1	Extensions and Places	3
2	Number Fields	5
2.1	Places of Number Fields	7
3	Different and Discriminant	9
3.1	Examples	13
6	Ideles and Adeles	16
6.1	Ideles	19
7	Geometry of Numbers	20

1 Absolute Values and Places

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

$$\text{i) } |x| = 0 \iff x = 0$$

$$\text{ii) } |xy| = |x||y|$$

$$\text{iii) } |x + y| \leq |x| + |y|$$

We will also assume that $|\cdot|$ is not trivial, i.e.

$$\text{iv) } \exists x \in K : |x| \neq 0, 1$$

An AV is *non-archimedean* if it satisfies

$$\text{iii-NA) } |x + y| \leq \max(|x|, |y|)$$

and *archimedean* otherwise.

An AV determines a metric $d(x, y) = |x - y|$ which makes K a *topological field*.

Remark It's convenient to weaken iii):

$$\text{iii') } \exists \alpha > 0 \text{ s.t. } \forall x, y, |x + y|^\alpha \leq |x|^\alpha + |y|^\alpha$$

For non-archimedean AVs, this makes no difference. What this does mean is that if $|\cdot|$ is an AV, then so is $|\cdot|^\alpha$ for any $\alpha > 0$. The point of this is that we want $z \mapsto z\bar{z}$ on \mathbb{C} to be an AV - we'll see why later.

Let's suppose $|\cdot|$ is a non-archimedean AV. Then $\{x \in K : |x| \leq 1\} = R$ is a subring of K . It is a local ring with unique maximal ideal $\{|x| < 1\} = \mathfrak{m}_R$.

It is a *valuation ring* of K (i.e. $x \in K \setminus R \implies x^{-1} \in R$).

Lemma 1.1. R is a maximal subring of K .

Proof. Let $x \in K \setminus R$, so $|x| > 1$. Then if $y \in K$, there is some $n \geq 0$ with $|yx^{-n}| = \frac{|y|}{|x|^n} \leq 1$. So $y \in x^n R$ for $n \gg 0$, and hence $R[x] = K$. Hence R is maximal. \square

There is a general notion of valuation (not nec. \mathbb{R} -valued). In the more general context, these valuations are called *rank 1 valuations*, and they have this maximality property.

We say two absolute values $|\cdot|$ and $|\cdot|'$ are *equivalent* if there is $\alpha > 0$ with $|\cdot|' = |\cdot|^\alpha$. This is an equivalence relation.

Proposition 1.2. *The following are equivalent:*

$$\text{i) } |\cdot|, |\cdot|' \text{ are equivalent.}$$

$$\text{ii) } |x| \leq |y| \iff |x|' \leq |y|'.$$

$$\text{iii) } |x| < |y| \iff |x|' < |y|'.$$

Proof. From local fields, or exercise. \square

Corollary 1.3. *Let $|\cdot|, |\cdot|'$ be non-archimedean AVs, with valuation rings R, R' . Then $|\cdot|, |\cdot|'$ are equivalent if and only if $R = R'$ if and only if $R \subset R'$.*

Equivalent AVs define equivalent metrics, hence the same topologies, 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 1.4 (Weak Approximation). *Let $|\cdot|_i$ for $1 \leq i \leq n$ be pairwise inequivalent AVs on K , and $a_1, \dots, a_n \in K$, $\delta > 0$.*

Then there is $x \in K$ 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 $|\frac{z_j^N}{z_j^N + 1}|_i \rightarrow 0$ as $N \rightarrow \infty$ if $i \neq j$, and to 1 if $i = j$.

So then $x = \sum a_j \frac{z_j^N}{z_j^N + 1}$ works for N sufficiently large. So it's enough to find z_j , and by symmetry take $j = 1$. We then induct on n . The case $n = 1$ is trivial.

Suppose we have y with $|y|_1 > 1$, and $|y|_2, \dots, |y|_{n-1} < 1$. If $|y|_n < 1$, we're finished, otherwise pick $w \in K$ with $|w|_1 > 1 > |w|_n$, by 1.2. If $|y|_n = 1$, then $z = y^N w$ works, and if $|y|_n > 1$, then $z = \frac{y^N w}{y^N + 1}$ works. \square

Remark. If $K = \mathbb{Q}$, $|\cdot|_1, \dots, |\cdot|_n$ are the 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 is $x \in \mathbb{Q}$ which is a p_i -adic integer for all i , and $x \equiv a_i \pmod{p_i^{n_i}}$ for all i . This is weaker than CRT, which guarantees $x \in \mathbb{Z}$.

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

Example $K = \mathbb{Q}$. *Ostrowski's Theorem* implies every AV on \mathbb{Q} is equivalent to one of $|\cdot|_p, |\cdot|_\infty$. So places of \mathbb{Q} are the primes, and ∞ . We write V_K for the set of places of K .

We write $V_{K,\infty}$ for the places given by archimedean AVs (the infinite places).

We write $V_{K,f}$ for the places given by non-archimedean AVs (the finite places).

We often use letters v, w denote places. Given $v \in V_K$, K_v will denote the completion of K at v . If $v : K^\times \rightarrow \mathbb{R}$ is a *valuation*, we will also use v to denote the corresponding place, i.e. the equivalence class of AVs $x \mapsto \gamma^{-v(x)}$.

We can restate the 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.

1.1 Extensions and Places

Let L/K be finite and separable, and let v, w be places of K, L respectively. Say w *lies over* or *divides* v (notation $w|v$) if v is the restriction of w to K .

Then there is a unique continuous $K_v \hookrightarrow L_w$ extending $K \hookrightarrow L$.

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

$$L \otimes_K K_v \xrightarrow{\sim} \prod_{w|v} L_w$$

mapping $x \otimes y$ to $(xy)_w$.

Proof. Both sides are finite dimensional normed K_v -vector spaces. The idea will be to choose a basis of L/K so that $L \otimes_K K_v \cong K_v^{[L:K]}$ (with the sup norm), and on the RHS we also use the sup norm. Then we use the fact that any 2 norms on a finite dimensional vector space over a field complete with respect to an absolute value are equivalent (see Cassels and Fröhlich, Ch. III, section 8).

Write $L = K(a)$ where $f \in K[T]$ is a minimal polynomial for a , and is separable. Factor $f = \prod g_i$ in K_v , so that the $g_i \in K_v[T]$ are irreducible and distinct.

Let $L_i = K_v[T]/(g_i)$. Then $L \otimes_K K_v = K_v[T]/(f) \cong \prod_i L_i$. Now let $w|v$, inducing $i_w : L \hookrightarrow L_w$. Let $g_w \in K_v[T]$ be the minimal polynomial of $i_w(a)$ over K_v . Then $g_w | f$, so g_w is one of the g_i s, and $L_w = K_v(i_w(a)) = L_i$.

Conversely, K_v is complete and L_i/K_v is finite, so there is a unique extension of v to L_i , and we get a bijection $\{g_i\} \leftrightarrow \{w|v\}$, and $L \otimes_K K_v \cong \prod L_w$. \square

Corollary 1.6.

1. $\{w|v\}$ is finite, nonempty, and $[L : K] = \sum_{w|v} [L_w : K_v]$
2. $\forall x \in K$,
 $N_{L/K}(x) = \prod_{w|v} N_{L_w/K_v}(x)$
 $\text{Tr}_{L/K}(x) = \sum_{w|v} \text{Tr}_{L_w/K_v}(x)$.

If L/K is Galois with Galois group G , then G acts on the places w of L lying over a given v : 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 , and hence gives a (left) action of G on $\{w|v\}$, $g(w) = w \circ g^{-1}$. If $w = v_P$ for a prime P , then $gw = v_{g(P)}$.

We define the **decomposition group** D_w or G_w to be the stabiliser of w . This action is transitive. If $g \in D_w$, then it is continuous for the topology induced by w on L , so it extends to an automorphism of L_w , the completion of L at w .

$$G \supset \text{Gal}(L_w/K_v) \supseteq D_w$$

Then we have

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

Hence equality holds throughout, and $G_w = \text{Gal}(L_w/K_v)$.

Suppose v is a **discrete valuation** of L , i.e. it is a finite place, and the valuation ring is a DVR. Then so is any $w|v$, and we define:

- $f(w|v)$, the degree of residue class extension, $= e_{L_w/K_v}$
- $e(w|v)$, the ramification degree

and $[L_w : K_v] = e(w|v)f(w|v)$.

2 Number Fields

A lot of this theory applies to other global fields, e.g. function fields. K will here be a number field (i.e. finite extension of the rationals) with ring of integers O_K . We have some basic properties:

- O_K is a **Dedekind domain**, i.e.
 1. Noetherian (in fact, O_K is a f.g. \mathbb{Z} -module).
 2. Integrally closed in K (by definition).
 3. Every non-zero prime ideal is maximal, so has Krull dimension ≤ 1 .

We have some 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 , TFAE:
 - (a) R is Dedekind.
 - (b) R is Noetherian and for every non-zero prime \mathfrak{p} , $R_{\mathfrak{p}}$ is a DVR.
 - (c) Every fractional ideal of R is invertible.
3. A Dedekind domain with only finitely many prime ideals (i.e. **semi-local**) is a PID.

Proof.

1. Proved in local fields, \implies is the hardest part.
2. Let $K = \text{Frac}(R)$. A fractional ideal of R is a non-zero R -submodule $I \subset K$ for some $0 \neq x \in R$ where $xI \subset R$ is an ideal. For (a) \implies (b) it is enough to check (exercise) that the basic properties are preserved under localisation.

For (b) \implies (c), I is invertible if there is a fractional ideal I^{-1} such that $II^{-1} = R$. To prove (c), we may assume $I \subset R$ is an ideal. Then let $I^{-1} = \{x \in K : xI \subset R\}$. If $0 \neq y \in I$, then $R \subset I^{-1} \subset y^{-1}R$, and so I^{-1} is a fractional ideal. Clearly $I^{-1}I \subset R$. Now let $P \subset R$ be prime - it is sufficient to show $I^{-1}I \not\subset P$. Let $I = (a_1, \dots, a_n)$. WLOG take $v_P(a_1) \leq v_P(a_i)$ for all $i > 1$. Then $IR_P = a_1R_P$, as R_P is a DVR.

Hence $a_i/a_1 = x_i/y_i \in R_P$ where $x_i \in R$, $y_i \in R \setminus P$. Then $y = \prod y_i \notin P$ as P is prime, and $ya_i/a_1 \in R$ for all i , and so $y/a_i \in I^{-1}$, so $y \in II^{-1} \setminus P$.

For (c) \implies (a), we check the properties. R is Noetherian - let $I \subset R$ be an ideal. Then $II^{-1} = R \implies 1 = \sum_{i=1}^n a_i b_i, a_i \in I, b_i \in I^{-1}$. Let $I' = (a_1, \dots, a_r) \subset I$. Then $I'I^{-1} = R = II^{-1}$, and so $I' = I$, and I is finitely generated.

R is integrally closed. Let $x \in K$, integral over R . Then $I := R[x] = \sum_{0 \leq i < d} Rx^i \subset K$ is a fractional ideal. Obviously $I^2 = I$, so $I = I^2 I^{-1} = II^{-1} = R$, i.e. $x \in R$.

Every non-zero prime is maximal. Take $\{0\} \neq Q \subset P \subsetneq R$ where P, Q are prime. Then $R \subsetneq P^{-1} \subset Q^{-1}$, and $Q \subsetneq P^{-1}Q \subset R$, and $P(P^{-1}Q) = Q$, so as Q is prime and $P^{-1}Q \not\subset R$, we must have $P \subset Q$, and so $P = Q$.

- Let R be a semi-local Dedekind domain with non-zero primes P_1, \dots, P_n . Choose $x \in R$ with $x \in P_1 \setminus P_1^2, x \in P_2, \dots, P_n$. Then $P_1 = (x)$ and every ideal is a product of powers of $\{P_i\}$ (see below), hence R is a PID.

□

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

- The group of fractional ideals is freely generated by the non-zero prime ideals, and

$$I = \prod_P P^{v_P(I)}$$

with $v_P(I) = \inf_{x \in I} (v_P(x))$.

- If $(R : I) < \infty$ for all $I \neq (0)$, then for all I, J , $(R : IJ) = (R : I)(R : J)$.

Proof.

- If $I \neq R$, then $I \subset P$ for some prime ideal P . Then $I = PI', I' = IP^{-1} \supsetneq I$. Then by Noetherian induction, I is a product of powers of prime ideals, say $I = \prod P^{a_P}$.

We get the same for fractional ideals $J = x^{-1}I$.

Consider the homomorphisms $\{\text{fractional ideals of } R\} \rightarrow \{\text{fractional ideals of } R_P\} \rightarrow \mathbb{Z}$ given by $I \mapsto IR_P, (\pi^n) \mapsto n$.

The composition is $I \mapsto v_P(I)$, and if $Q \neq P$ then $v_P(Q) = 0$.

So $\{\text{fractional ideals of } R\} \rightarrow \bigoplus_P \mathbb{Z}$ maps $\prod P^{a_P}$ to $(a_P)_P$. Hence the a_P are unique and this is an isomorphism.

- By unique factorisation of ideals (part 1.), $\prod P^{a_P} \cap \prod P^{b_P} = \prod P^{\max a_P, b_P}$. So if $I + J = R$, then $IJ = I \cap J$, and so by CRT, $R/IJ \cong R/I \cap J \cong R/I \times R/J$, and we are done in this case.

Hence this step reduces to showing that $(R : P^{n+1}) = (R : P)(R : P^n)$.

Now localising at P gives $P^n \cong R_P/P^n R_P$, so WLOG R is local, hence a DVR, and $P = (\pi)$.

Then $R/(\pi^n) \cong (\pi)/(\pi^{n+1})$ via multiplication by π , and hence $(R : P^{n+1}) = (R : P)(R : P^n)$.

□

The quotient group $Cl(R) := \{\text{fractional ideals of } R\} / \{\text{principal fractional ideals of } R\}$ is the *class group* (or *Picard group*) of R .

If K is a number field, then we write $Cl(K) = Cl(O_K)$, the *ideal class group* of K .

Theorem 2.3. *For K a number field, $Cl(K)$ is finite.*

The proof will come later.

2.1 Places of Number Fields

Recall Ostrowski's theorem, which says that $V_{\mathbb{Q}} = \{p : p \text{ prime}\} \cup \{\infty\}$.

Let $\mathfrak{p} \subset O_K$ be a nonzero prime ideal. Then \mathfrak{p} determines a discrete valuation $v_{\mathfrak{p}}$ of K , and so a non-archimedean absolute value $|x|_{\mathfrak{p}} = r^{-v_{\mathfrak{p}}(x)}$ where $r > 1$.

Theorem 2.4. *This gives a bijection $\{\text{primes of } O_K\} \rightarrow V_{K,f}$.*

Proof. Let $P \neq Q$. Then there exists $x \in P \setminus Q$, and then $|x|_P < 1 = |x|_Q$, so $|\cdot|_P, |\cdot|_Q$ are inequivalent, and the map is injective.

Let $|\cdot|$ be a non-archimedean absolute value on K , with valuation ring $R = \{x \in K : |x| \leq 1\}$. As $|\cdot|$ is non-archimedean, $\mathbb{Z} \subset R$ and hence $R \supset O_K$ as R is integrally closed. So $R \supset O_{K,P}$ for some prime $P = \mathfrak{m}_R \cap O_K$. Hence $R = O_{K,P}$ because by 1.1, $O_{K,P}$ is a maximal subring of K .

Hence $|\cdot|$ and $|\cdot|_P$ are equivalent. \square

For $v \in V_{K,f}$, write P_v for the corresponding prime ideal of O_K . Then K_v , the completion of K at v , is a complete discretely valued field, with valuation ring O_v or $O_{K_v} \subset K_v$, not to be confused with O_{K,P_v} .

The normalised discrete valuation will be the one for which $v : K^\times \rightarrow \mathbb{Z}$ is surjective. We will denote by $\pi_v \in O_v$ any generator of the maximal ideal. We often assume $\pi_v \in K$. Then $v(\pi_v) = 1$.

We write $k_v = O_K/P_v \cong O_v/(\pi_v)$, is finite, of order $q_v = p^{f_v}$ for a rational prime p divisible by v .

We then normalise the absolute value so that $|x|_v = q_v^{-v(x)}$, so that $|\pi_v|_v = \frac{1}{q_v}$.

For infinite places, we have the unique infinite place ∞ of \mathbb{Q} , with $\mathbb{Q}_\infty = \mathbb{R}$. So then $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{v \in V_{K,\infty}} K_v$. Each K_v is a finite extension of \mathbb{R} , so is one of \mathbb{R} and \mathbb{C} . These correspond to the cases where we say v is real or complex respectively.

In the complex case, since $K \subset K_v$ is dense, we cannot have $K \subset \mathbb{R}$. On the other hand, by Galois theory $\Sigma_K = \{\text{homomorphisms } K \hookrightarrow \mathbb{C}\}$ has order $n = [K : \mathbb{Q}]$, and $K \otimes_{\mathbb{Q}} \mathbb{C} \cong \prod_{\sigma \in \Sigma_K} \mathbb{C}$. Complex conjugation acts on both sides by $x \otimes z \mapsto x \otimes \bar{z}$ and $(z_{\bar{\sigma}})_{\sigma} \mapsto (\bar{z}_{\bar{\sigma}})_{\sigma}$.

Let $\sigma_1, \dots, \sigma_{r_1} : K \hookrightarrow \mathbb{R}$, $\sigma_{r_1+1} = \bar{\sigma}_{r_1+r_2+1}, \dots, \sigma_{r_1+r_2} = \bar{\sigma}_{r_1} : K \hookrightarrow \mathbb{C}$ where $r_1 + 2r_2 = n$. Then, taking fixed points under complex conjugation,

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

Therefore we have:

Theorem 2.5. *There is a bijection*

$$\Sigma_K / (\sigma \sim \bar{\sigma}) \xrightarrow{\sim} V_{K,\infty}$$

given by $\sigma \mapsto |\sigma(\cdot)|$, where $|\cdot|$ is the Euclidean absolute value in \mathbb{R} or \mathbb{C} .

We write $K_\infty := K \otimes_{\mathbb{Q}} \mathbb{R}$, which is canonically isomorphic to $\prod_{v \in V_{K,\infty}} K_v$ and noncanonically isomorphic to $\mathbb{R}^{\#\{\text{real } v\}} \times \mathbb{C}^{\#\{\text{complex } v\}}$.

We now choose the normalised absolute values such that, if v is real corresponding to $\sigma : K \hookrightarrow \mathbb{R}$, then $|x|_v = |\sigma(x)|_\infty$, and if v is complex, then $|x|_v = \sigma(x)\bar{\sigma}(x) = |\sigma(x)|^2$.

If v is finite and $w|v$, then L_w/K_v is a finite extension of non-archimedean local fields, and $[L_w : K_v] = e(w|v)f(w|v)$.

If v is infinite and $w|v$, then $L_w/K_v = \begin{cases} \mathbb{R}/\mathbb{R} & f = e = 1 \\ \mathbb{C}/\mathbb{C} & f = e = 1 \\ \mathbb{C}/\mathbb{R} & v \text{ ramified, } e = 2, f = 1 \end{cases}$

Proposition 2.6. *Let $x \in L, v \in V_K$. Then:*

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

Proof. $N_{L/K}(x) = \prod_{w|v} N_{L_w/K_v}(x)$, so it is enough to show that $|N_{L_w/K_v}(x)|_v = |x|_w$.

For v a finite place, it is enough to take $x = \pi_w \in L$. Then:

$$\begin{aligned} |N_{L_w/K_v}(\pi_w)|_v &= |u\pi_v^{f(w|v)}|_v \\ &= q_v^{-f(w|v)} = q_w^{-1} = |\pi_w|_w \end{aligned}$$

For v an infinite place, we need only consider $L_w/K_v \cong \mathbb{C}/\mathbb{R}$. But $N_{\mathbb{C}/\mathbb{R}}(z) = z\bar{z}$ by definition. \square

Theorem 2.7 (Product Formula). *Let $x \in K^\times$. Then:*

$$|x|_v = 1 \text{ for all but finitely many } v$$

and

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

Proof. Write $x = a/b$ where $a, b \in O_K^\times$. Then $\{v \in V_K : |x|_v \neq 1\} \subset V_{K,\infty} \cup \{v \in V_{K,f} : v(a) \text{ or } v(b) > 0\}$, a finite set.

Now $\prod_{v \in V_K} |x|_v = \prod_{p \leq \infty} \left(\prod_{v|p} |x|_v \right) = \prod_{p \leq \infty} |N_{K/\mathbb{Q}}(x)|_p$, so it is enough to prove this for $K = \mathbb{Q}$.

By multiplicativity, we reduce to $x = q$, a prime, or $x = -1$. In the former case, $|q|_p = \begin{cases} \frac{1}{q} & p = q \\ 1 & p \neq q, \infty, \text{ and in the latter, } |-1|_p = 1 \text{ for all } p \leq \infty. \end{cases}$ Hence the product over all of these is 1. \square

Remark. In \mathbb{R} , the standard measure dx transforms under \mathbb{R}^\times as $d(ax) = |a|dx$. In \mathbb{C} , the standard measure is $dx dy$. This transforms under \mathbb{C}^\times as $dx dy \mapsto |a|^2 dx dy$. In both these cases, we see the scaling is the normalised AV of a .

Fact: on K_v for any v there is a translation-invariant measure, the ‘‘Haar measure’’, $d_v(x)$. Then for all $a \in K_v^\times$, $d_v(ax) = |a|_v d_v(x)$, where $|\cdot|_v$ is a normalised AV.

3 Different and Discriminant

Suppose $R \subset S$ are commutative rings with 1, such that S is a free R -module of finite rank $n \geq 1$. Then we have a trace map $\text{Tr}_{S/R} : S \rightarrow R$, the trace of the R -linear map $y \mapsto xy$.

If x_1, \dots, x_n are elements of S , define the discriminant:

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

If $y_i = \sum_{j=1}^n r_{ji} x_j$, then $\text{Tr}_{S/R}(y_i y_j) = \sum_{k,\ell} r_{ki} r_{\ell j} \text{Tr}_{S/R}(x_k x_\ell)$.

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

Writing $S = \bigoplus_{i=1}^n R e_i$, we also define $\text{disc}(S/R) = (\text{disc}(e_i)) \subset R$, an ideal of R , independent of basis by the previous line.

This has the following basic properties:

- $S = S_1 \times S_2$ implies $\text{disc}(S/R) = \text{disc}(S_1/R) \text{disc}(S_2/R)$
- If $f : R \rightarrow R'$ is a ring homomorphism, then $\text{disc}(S \otimes_R R'/R') = f(\text{disc}(S/R)) \subset R'$.
- If R is a field, then $\text{disc}(S/R)$ is an ideal, so is R or $\{0\}$, and is R iff the R -bilinear form $(x, y) \mapsto \text{Tr}_{S/R}(xy)$ is non-degenerate.

If L/K is a finite field extension, then $\text{disc}(L/K) = K \iff$ the trace form is non-degenerate, which holds \iff there is some $x \in L$ with non-zero trace, i.e. iff L/K is separable. More generally:

Theorem 3.1. *Let k be a field and A a finite dimensional k -algebra. Then $\text{disc}(A/k) \neq 0$ (so $= k$) if and only if $A = \prod K_i$ where K_i/k are finite separable field extensions.*

Proof. We can write $A = \prod A_i$ where A_i are indecomposable, so local, k -algebras, and so we may assume A is local with maximal ideal \mathfrak{m} .

If $\mathfrak{m} = 0$, i.e. A is field, then this is reduced to the previous statement.

If not, then every element of \mathfrak{m} is nilpotent, so there is $x \in \mathfrak{m} \setminus 0$ nilpotent, and so the endomorphism $y \mapsto xy$ of A is nilpotent, and for all $r \in A$, so is $y \mapsto (rx)y$, and hence for all $r \in A$, $\text{Tr}_{A/k}(rx) = 0$, giving a degenerate trace form so a zero discriminant. \square

If R is a Dedekind domain, $K = \text{Frac}(R)$, and L/K is finite separable with S the integral closure of R in L , then we say S/R is an *extension of Dedekind domains*. Then S is a finitely generated R -module, but needn't be free.

Proposition 3.2. *S is a locally free R -module of rank $n = [L : K]$ (i.e. for all $P \subset R$, $S_P \cong R_P^n$).*

Proof. $S \subset L$ so S is torsion free, hence so is S_P , and R_P is a PID, so S_P is free. S spans L as a K -vector space, so S has rank $\dim_K L = n$. \square

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

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 $0 \neq P \subset R$, $y = \text{Tr}_{L/K}(x) \in R_P$, and $\bigcap_P R_P = \{x \in K : v_P(x) \geq 0 \forall P\} = R$. \square

Then there are 2 equivalent definitions of $\text{disc}(S/R)$:

Definition. $\text{disc}(S/R) :=$ the ideal of R generated by $\{\text{disc}_{L/K}(x_1, \dots, x_n) : x_1, \dots, x_n \in S\}$. If S is free, this gives the previous definition.

As $S \otimes_R K = L$ is separable over K , $\text{disc}(L/K) \neq 0$, and so $\text{disc}(S/R) \neq \{0\}$.

Proposition 3.4. $\text{disc}(S/R)R_P = \text{disc}(S_P/R_P)$ for all P .

Proof. We claim there exist $x_1, \dots, x_n \in S$ which are an R_P -basis for S_P . Certainly, there is such a basis in S_P , say e_1, \dots, e_n . Now let:

$$\mathcal{Q} := \{\text{primes } Q \subset S : v_Q(e_i) < 0 \text{ for some } i\}$$

\mathcal{Q} is finite. Then by the CRT, there are $a_i \in S$ such that $v_Q(a_i) + v_Q(e_i) \geq 0$ for all $Q \in \mathcal{Q}$, and $v_P(a_i) \geq 1$.

Then $x_i = a_i e_i \in S$, and $x_i \equiv e_i \pmod{PS}$. So (x_i) is an R/P -basis for $S/PS = S_P/PS_P$. So (x_i) is an R_P basis for S_P (this follows by Nakayama's lemma).

Hence the discriminant $\text{disc}(S_P/R_P) = \text{disc}(x_i)R_P$, and hence $\text{disc}(x_i) \in \text{disc}(S/R)$. So $\text{disc}(S_P/R_P) \subset \text{disc}(S/R)R_P$, and the other inclusion is obvious. \square

The alternate definition of $\text{disc}(S/R)$ is:

- if $x_1, \dots, x_n \in S$ is a K -basis for L , then $\text{disc}_{L/K}(x_i) \neq 0$.

Let $\mathcal{P} = \{P \subset R : v_P(\text{disc}_{L/K}(x_i)) > 0\}$, a finite set. So for all $P \notin \mathcal{P}$, $\text{disc}(S_P/R_P) = R_P$.

Then we can define $\text{disc}(S/R) = \prod_{P \in \mathcal{P}} P^{v_P(\text{disc}(S_P/R_P))}$.

This is equivalent to the previous definition by 3.4.

Theorem 3.5. $v_P(\text{disc}(S/R)) = 0$ if and only if P is unramified in S and for all $Q \subset S$ over P , the residue field extension $\frac{S}{Q}/\frac{R}{P}$ is separable.

Proof. We may assume R is local, so that S is a free R -module. We know $PS = \prod_Q Q^{e_Q}$. So:

$$S \otimes_R (R/P) \cong S/PS \cong \prod_Q S/Q^{e_Q}$$

So $v_P(\text{disc}(S/R)) = 0$ if and only if $\text{disc}(\frac{S}{PS}/\frac{R}{P}) = \frac{R}{P}$ if and only if each S/Q^{e_Q} is a finite separable field extension of R/P , if and only if, for all Q , $e_Q = 1$ and $\frac{S}{Q}/\frac{R}{P}$ is separable. \square

Corollary 3.6. In an extension S/R of Dedekind domains (i.e. S is the integral closure of R in a finite separable extension of $\text{Frac}(R)$), only finitely many primes are ramified - precisely the primes such that $v_P(\text{disc}(S/R)) > 0$.

Proposition 3.7. Let $P \subset R$. Then $v_P(\text{disc}(S/R)) = \sum_{Q \supset P} v_P(\text{disc}(\widehat{S}_Q/\widehat{R}_P))$.

Proof. By 3.4 we may assume R is local, so S is a free R -module, and then:

$$S \otimes_R \widehat{R} \cong \prod \widehat{S}_Q$$

So $v_P(\text{disc}(S/R)) = v_P(\text{disc}(S \otimes_R \widehat{R}/\widehat{R})) = \sum_Q v_P(\text{disc}(\widehat{S}_Q/\widehat{R}))$. \square

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

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

This is the dual of S with respect to the trace form $(x, y) \mapsto \text{Tr}_{L/K}(xy)$.

This is 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, i.e. $\text{Tr}_{L/K}(x_i y_j) = \delta_{ij}$. 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), and its inverse $\mathcal{D}_{S/R}$ is an ideal of S , called the *different*.

Proposition 3.8.

1. $P \subset R \implies \mathcal{D}_{S_P/R_P} = \mathcal{D}_{S/R} S_P$
2. $N_{L/K}(\mathcal{D}_{S/R}) = \text{disc}(S/R)$
3. $Q \subset S$ lying over $P \subset R$. Then $v_Q(\mathcal{D}_{S/R}) = v_Q(\mathcal{D}_{\widehat{S}_Q/\widehat{R}_P})$

Proof.

1. Exercise. Same idea as 3.4.
2. By (1) and 3.4, we can suppose R is local. Then S is a PID by 2.1.iii, so the inverse different $\mathcal{D}_{S/R}^{-1} = x^{-1}S$ for some $0 \neq x \in S$. Let (e_i) be a basis for S/R . Then there exists a basis (e'_i) for S/R such that

$$\text{Tr}_{L/K}(e_i x^{-1} e'_j) = \delta_{ij}$$

Let $x^{-1}e_j = \sum_k b_{kj}e_k$ where $b_{kj} \in K$. Then the ideal:

$$\begin{aligned} (1) &= (\det[\text{Tr}_{L/K}(e_i x^{-1} e'_j)]) \\ &= (\det(\text{Tr}_{L/K}(e_i e_j)) \det(b_{ij})) \\ &= \det(b_{ij}) \text{disc}(S/R) \end{aligned}$$

But $N_{L/K}(x^{-1}) = u \det(b_{ij})$ for some unit u in R . So $(1) = (N_{L/K}(x^{-1})) \text{disc}(S/R)$. Since we are in Dedekind domains we can cancel $\text{disc}(S/R)$, giving the result.

3. Assume R is local, $P = (\pi_P)$. Write $\widehat{K} = \text{Frac}(\widehat{R})$ for $Q = (\pi_Q) \subset S$, and $\widehat{L}_Q = \text{Frac}(\widehat{S}_Q)$. So $L \otimes_K \widehat{K} \cong \prod_Q \widehat{L}_Q$ via $x \mapsto (x_Q)_Q$, say, and $S \otimes_R \widehat{R} \cong \prod_Q \widehat{S}_Q$.

We also have $\text{Tr}_{L \otimes_K \widehat{K}/\widehat{K}}(x) = \sum_Q \text{Tr}_{\widehat{L}_Q/\widehat{K}}(x_Q)$.

Let $S = \bigoplus_{i=1}^n Rx_i$, and $\mathcal{D}_{S/R}^{-1} = \prod_Q \pi_Q^{-a_Q} S = \bigoplus_{i=1}^n Ry_i$ for some $a_Q \geq 0$, $y_i \in L$ a dual basis to x_i .

Then, as $S \otimes_R \widehat{R} = \bigoplus \widehat{R}x_i$ (really $x_i \otimes 1$), we have:

$$\begin{aligned} \mathcal{D}_{S \otimes_R \widehat{R}/\widehat{R}}^{-1} &:= \{x \in L \otimes_K \widehat{K} : \forall y \in S \otimes_R \widehat{R}, \text{Tr}_{L \otimes_K \widehat{K}/\widehat{K}}(xy) \in \widehat{R}\} \\ &= \bigoplus_{i=1}^n \widehat{R}y_i \\ &= \mathcal{D}_{S/R}^{-1} \cdot S \otimes_R \widehat{R} \subset L \otimes_K \widehat{K} \end{aligned}$$

On the other hand,

$$\mathcal{D}_{S \otimes_R \widehat{R}/\widehat{R}}^{-1} \cong \prod_Q \mathcal{D}_{\widehat{S}_Q/\widehat{R}}^{-1} \subset \prod_Q \widehat{L}_Q$$

So:

$$\begin{aligned} \mathcal{D}_{\widehat{S}_Q/\widehat{R}}^{-1} &= \left(\prod_{Q'} \pi_{Q'}^{-a_{Q'}} \right) \widehat{S}_Q \\ &= \pi_Q^{-a_Q} \widehat{S}_Q \end{aligned}$$

as $v_Q(\pi_{Q'}) = 0$ if $Q' \neq Q$.

□

Theorem 3.9. *Let $\mathfrak{p}S = \prod_{i=1}^g Q_i^{e_i} \subset S$. Then $Q_i | \mathcal{D}_{S/R} \iff e_i > 1$; and $Q_i^{e_i-1} | \mathcal{D}_{S/R}$.*

Proof. First assume R is complete and local, and $\mathfrak{p} = (\pi_R)$. Then S is also local and complete, and there is a unique prime $Q = (\pi_S)$. Then $\mathcal{D}_{S/R} = (\pi_S)^d$ for some $d \geq 0$. By 3.8.2, $\text{disc}(S/R) = (N_{L/K}(\pi_S)^d) = (\pi_R)^{df}$. So as $v_P(\text{disc}(S/R)) = 0 \iff \mathfrak{p}$ is unramified (3.5), the first statement holds.

For the second statement, we claim $\text{Tr}_{L/K}(Q) \subset \mathfrak{p}$. Let $x \in Q$. Then multiplication by x is a nilpotent endomorphism of $S \otimes (R/\mathfrak{p}) \cong S/Q^e$, and so $\text{Tr}_{S \otimes_R (R/\mathfrak{p})/(R/\mathfrak{p})}(x \otimes 1) = 0$, i.e. $\text{Tr}_{L/K}(x) = \text{Tr}_{S/R}(x) \in \mathfrak{p}$, and hence the claim.

Therefore $\text{Tr}_{L/K}(\pi_R^{-1}Q) = \text{Tr}_{L/K}(Q^{1-e}) \subset R$, and hence $Q^{1-e} \subset \mathcal{D}_{S/R}^{-1}$, or $Q^{e-1} | \mathcal{D}_{S/R}$.

For the general case, apply the above to $\widehat{S}_{Q_i}/\widehat{R}_P$ and use 3.8.3.

□

Some facts:

- If $p \nmid e_i$, then $v_{Q_i}(\mathcal{D}_{S/R}) = e_i - 1$
- If $p | e_i$ then $v_{Q_i}(\mathcal{D}_{S/R}) \geq e_i$.

More precisely, $v_{Q_i}(\mathcal{D}_{S/R})$ is determined by the orders of the higher ramification groups for a Galois closure of L/K . See e.g. Serre 'Local Fields', IV.2.4.

- If $S = R[x]$ and x has minimal polynomial $f \in R[T]$, then $\mathcal{D}_{S/R} = (f'(x))$ where f' is the derivative.

This means that $\mathcal{D}_{S/R}$ is the annihilator of the cyclic S -module $\Omega_{S/R}$ of Kahler differentials.

For an extension L/K of number fields, we write $\mathcal{D}_{L/K} = \mathcal{D}_{O_L/O_K}$, and $\delta_{L/K} = \text{disc}(O_L/O_K)$.

Remark. Take K/\mathbb{Q} , (e_i) a \mathbb{Z} -basis for O_K . Then $\delta_{K/\mathbb{Q}} \subset \mathbb{Z}$ is $(\text{disc}(e_i))$, and if (e'_i) is another basis, say $e'_i = \sum a_{ji} e_j$, then $\text{disc}(e'_i) = (\det a_{ij})^2 \text{disc}(e_i) = \text{disc}(e_i)$.

So the integer $\text{disc}(e_i)$ is independent of the basis (not just the ideal it generates). We call this the absolute discriminant $d_K \in \mathbb{Z} \setminus \{0\}$.

Theorem 3.10 (Kummer-Dedekind Criterion). *Let S/R be an extension of Dedekind domains, and $x \in S$ such that $L = K(x)$. Suppose there is $\mathfrak{p} \subset R$ such that $S_{\mathfrak{p}} = R_{\mathfrak{p}}[x]$.*

Let $g \in R[T]$ be the min. poly. of x , and $\bar{g} = \prod_i \bar{g}_i^{e_i} \in (R/\mathfrak{p})[T]$ be a factorisation of the reduction of g into powers of distinct irreducibles, where \bar{g}_i are monic. Let $g_i \in R[T]$ be any monic lift of \bar{g}_i , and $f_i = \deg(g_i) = \deg(\bar{g}_i)$.

Then $Q_i = \mathfrak{p}S + (g_i(x)) \subset S$ is prime, of residue degree $[S/Q_i : R/\mathfrak{p}] = f_i$, $Q_i \neq Q_j$ if $i \neq j$, and $\mathfrak{p}S = \prod_i Q_i^{e_i}$.

Proof. We can assume R is local, so $S = R[x]$. Set $\mathfrak{p} = (\pi)$, $R/\mathfrak{p} = k$. We claim Q_i is prime, $Q_i \neq Q_j$, with residue degree f_i .

Now $S/Q_i \cong k[T]/(\bar{g}_i)$, and \bar{g}_i is irreducible of degree f_i .

If $i \neq j$, then there exists $a, b \in R[T]$ such that $\bar{a}\bar{g}_i + \bar{b}\bar{g}_j = 1$, and so $1 = ag_i + bg_j + \pi c$ for some $c \in R[T]$, hence $1 \in Q_i + Q_j = (\pi, g_i(x), g_j(x))$.

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

$$\prod_i Q_i^{e_i} = \prod_i (\pi, g_i(x))^{e_i} \subset \prod_i (\pi, g_i(x)^{e_i}) \subset (\pi, \prod_i g_i(x)^{e_i}) = (\pi, \pi h(x)) \subset \mathfrak{p}S = (\pi)$$

Now $\dim_k(S/\mathfrak{p}S) = n = [L : K]$, and $\dim_k(S/Q_i^{e_i}) = \sum_{j=0}^{e_i-1} \dim_k(Q_i^j/Q_i^{j-1}) = e_i \dim_k(S/Q_i) = e_i f_i$.

Hence $\prod_i Q_i^{e_i} \subset \mathfrak{p}S$ gives $\sum e_i f_i \geq n$. As $\sum e_i f_i = \sum e_i \deg(\bar{g}_i) = \deg(\bar{g}) = n$, we have equality. \square

3.1 Examples

Quadratic Fields

Let $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Q}^\times$ not a square. Multiplying by a square, we may assume $d \in \mathbb{Z} \setminus \{0, 1\}$ squarefree.

Then $O_K \supset \mathbb{Z}[\sqrt{d}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$. Now the multiplication map by $a + b\sqrt{d}$ takes:

$$\begin{aligned} (a + b\sqrt{d}) \cdot 1 &= a \cdot 1 + b \cdot \sqrt{d} \\ (a + b\sqrt{d}) \cdot \sqrt{d} &= a\sqrt{d} + bd = bd \cdot 1 + a \cdot \sqrt{d} \end{aligned}$$

so we have:

$$\mathrm{Tr}_{K/\mathbb{Q}}(a + b\sqrt{d}) = \mathrm{Tr} \begin{pmatrix} a & bd \\ b & a \end{pmatrix} = 2a$$

And so $\mathrm{Tr}_{K/\mathbb{Q}}(1) = 2$, $\mathrm{Tr}_{K/\mathbb{Q}}(\sqrt{d}) = 0$, $\mathrm{Tr}_{K/\mathbb{Q}}(d) = 2d$. Then for the discriminant, we have:

$$\mathrm{disc}(1, \sqrt{d}) = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d$$

Hence we have one of 2 cases:

1. $d_K = 4d$, and so $O_K = \mathbb{Z}[\sqrt{d}]$, or:
2. $d_K = d$, and $(O_K : \mathbb{Z}[\sqrt{d}]) = 2$.

We are in the second case iff there are $m, n \in \mathbb{Z}$ not both even with $\frac{m+n\sqrt{d}}{2} \in O_K$ iff $\frac{1+\sqrt{d}}{2} \in O(K)$, since it is obvious that $\frac{1}{2}, \frac{\sqrt{d}}{2} \notin O_K$. The min poly of $\frac{1+\sqrt{d}}{2}$ is $T^2 - T - \frac{d-1}{4}$, so we have this precisely when $d \equiv 1 \pmod{4}$, in which case $O_K = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

In case 1, we can then compute $\text{Tr}_{K/\mathbb{Q}}(1 \cdot \frac{1}{2}) = 1$, $\text{Tr}_{K/\mathbb{Q}}(\sqrt{d} \cdot \frac{1}{2\sqrt{d}}) = 1$, so we have a dual basis for the trace form given by $\{\frac{1}{2}, \frac{1}{2\sqrt{d}}\}$, and hence $\mathcal{D}_{K/\mathbb{Q}}^{-1} = (\frac{1}{2}, \frac{1}{2\sqrt{d}}) = (\frac{1}{2\sqrt{d}}) = (2\sqrt{d})^{-1}$, and so $\mathcal{D}_{K/\mathbb{Q}} = (2\sqrt{d})$

In case 2, our basis is now $\{1, \frac{1+\sqrt{d}}{2}\}$. The dual basis is thus $\{\frac{1}{2}, \frac{1}{1+\sqrt{d}}\}$, so $\mathcal{D}_{K/\mathbb{Q}}^{-1} = (\frac{1}{2}, \frac{1}{1+\sqrt{d}}) = (2, 1 + \sqrt{d})^{-1} = (\sqrt{d})^{-1}$, so $\mathcal{D}_{K/\mathbb{Q}} = (\sqrt{d})$.

Alternatively, in case 1, $O_K = \mathbb{Z}[\sqrt{d}]$, and the min. poly. of \sqrt{d} is $f(T) = T^2 - d$. Hence $\mathcal{D}_{K/\mathbb{Q}} = (f'(\sqrt{d})) = (2\sqrt{d})$. In case 2, $O_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, so we have min. poly. $T^2 - T - \frac{d-1}{4}$, and so $\mathcal{D}_{K/\mathbb{Q}} = (2\frac{1+\sqrt{d}}{2} - 1) = (\sqrt{d})$.

We can now look at the decomposition of $(p) \subset O_K$. Using Kummer-Dedekind:

- If $p \neq 2$ or $d \not\equiv 1 \pmod{4}$, then $p \nmid (O_K : \mathbb{Z}[\sqrt{d}])$. So, applying the criterion to $T^2 - d$, we see:

$$(p) = \begin{cases} p^2 & \text{ramified, if } p|d, P = (p, \sqrt{d}) \\ p & \text{inert, if } p \nmid d, \left(\frac{d}{p}\right) = -1 \\ pP' & \text{split, if } p \nmid d, \left(\frac{d}{p}\right) = +1. P = (p, \sqrt{d} - a) \neq P' = (p, \sqrt{d} + a) \end{cases}$$

- If $p = 2$ and $d \equiv 1 \pmod{4}$, then we factor $T^2 - T - \frac{d-1}{4} \pmod{2}$ and get:

$$(2) = \begin{cases} (2) & \text{inert, if } d \equiv 5 \pmod{8} \\ pP' & \text{split, if } d \equiv 1 \pmod{8} P = (2, \frac{\sqrt{d}+1}{2}) \neq P' = (2, \frac{\sqrt{d}-1}{2}) \end{cases}$$

Cyclotomic Fields

Recall some Galois theory: if $n > 1$, and K is a field of characteristic prime to n . Suppose $L = K(\zeta_n)$, where ζ_n is a primitive n^{th} root of unity. Equivalently, ζ_n is a root of the n^{th} cyclotomic polynomial Φ_n of degree $\varphi(n)$, defined recursively by

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

Then L/K is Galois with abelian Galois group, and an injective homomorphism

$$\text{Gal}(L/K) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

given by

$$g \mapsto a \text{ s.t. } g(\zeta_n) = \zeta_n^a$$

Theorem 3.11. Let $L = \mathbb{Q}(\zeta_n)$. Then:

1. $\text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
2. p ramifies in L iff $p|n$.
3. $O_L = \mathbb{Z}[\zeta_n]$.

Remark. Condition 1 is equivalent to Φ_n being irreducible over \mathbb{Q} , iff $[L : \mathbb{Q}] = \varphi(n)$.

Proof. Let $n = p^r m$ for $r \geq 1$ where p is a prime not dividing m . Let $\zeta_m = \zeta_n^{p^r}$, $\zeta_{p^r} = \zeta_n^m$. Then there exist $a, b \in \mathbb{Z}$ such that $p^r a + mb = 1$, so $\zeta_n = \zeta_{p^r}^a \zeta_m^b$. Now let $K = \mathbb{Q}(\zeta_m)$. Then $L = K(\zeta_{p^r})$. We will prove:

- Φ_{p^r} is irreducible over K .
- If $v \in V_{K,f}$ and $v \nmid p$, then v is unramified in L/K .
- If $v|p$ then v is totally ramified in L/K .
- $O_L = O_K[\zeta_{p^r}]$.

This will prove the theorem by induction on n .

For a place w of L , write $x_w \in L_w$ for the image of ζ_{p^r} under $L \hookrightarrow L_w$. Now suppose $v|p$. By induction, v is unramified in K/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 $O_{K_v}[T]$, congruent to $T^{p^{r-1}(p-1)} \pmod{p}$, and the constant coefficient is p , so it has valuation 1.

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

Now let $v|q \neq p$. Then Φ_{p^r} is separable mod q . We have:

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

Let $f_w \in O_{K_v}[T]$ be the minimal polynomial of $x_w|K_v$. Then $\prod_{w|v} f_w = \Phi_{p^r}$, so the reduction of f_w at v is separable, and hence L_w/K_v is unramified. Then, by local fields again, $O_{L_w} = O_{K_v}[x_w]$, and $\prod_{w|v} O_{L_w} = \prod_{w|v} O_{K_v}[T]/(f_w) \cong O_{K_v}[T]/(\Phi_{p^r})$.

Hence, for all $v \in V_{K,f}$,

$$O_{K_v} \otimes_{O_K} O_K[\zeta_{p^r}] \cong O_{K_v}[T]/(\Phi_{p^r}) \cong \prod_{w|v} O_{L_w} \cong O_{K_v} \otimes_{O_K} O_L$$

So we must have $O_K[\zeta_{p^r}] = O_L$. □

Given L/K a Galois extension of number fields with $w|v$ finite places, with $G = \text{Gal}(L/K) \supset G_w \cong \text{Gal}(L_w/K_v)$, the decomposition group of w , we have a short exact sequence:

$$0 \rightarrow I_w \rightarrow G_w \rightarrow \text{Gal}(\ell_w/k_v) \rightarrow 1$$

Suppose w is unramified in L/K (iff v unramified in L/K). Then $I_w = \{1\}$. We define the **Frobenius at w** to be the element $\sigma_w \in G_w$ mapping to the generator $x \mapsto x^{q_v}$ of $\text{Gal}(\ell_w/k_v)$.

So the order of $\sigma_w = f(w|v) = [\ell_w : k_v] = [\ell_{w'} : k_v]$ for any other $w'|v$.

In particular, $\sigma_w = 1 \iff v$ splits completely in L/K , i.e., there are precisely $[L : K]$ places of L over v .

Now suppose G is abelian. Then G_w, σ_w are independent of w , so depend only on v , and so we write σ_v or $\sigma_{L/K,v}$ for σ_w , the **(arithmetic) Frobenius at v** .

Remark. If $L/F/K$ with L/K abelian, then $\sigma_{L/K}|_F = \sigma_{F/K}$, by definition.

Example. Take $L = \mathbb{Q}(\zeta_n), K = \mathbb{Q}, n > 2$. We have $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\lambda} \text{Gal}(L/\mathbb{Q})$, given by

$$\lambda(a \bmod n) : \zeta_n \mapsto \zeta_n^a$$

We now claim $\sigma_p = \sigma_{L/\mathbb{Q},p} = \lambda(p)$ if $p \nmid n$.

Indeed, σ_p is characterised by, the following property: for all $v|p$, σ_p induces $(x \mapsto x^p)$ on the residue field $\mathbb{Z}[\zeta_n]/\mathfrak{p}_v$, whereas $\lambda(p)$ induces $(x \mapsto x^p)$ on $\mathbb{Z}[\zeta_n]/(p)$.

Remarks.

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

We will now specialise to the case where $n = q$ is a prime > 2 . Then $\text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$, cyclic of order $q - 1$. So we have a unique index 2 subgroup H , the squares.

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 2 is unramified we must have $K = \mathbb{Q}(\sqrt{q^*})$, where $q^* = \begin{cases} q & q \equiv 1 \pmod{4} \\ -q & q \equiv 3 \pmod{4} \end{cases}$.

Note that $d_K = q^*$.

Now let $p \neq q$ be an odd prime. Then $\sigma_{K/\mathbb{Q},p} = 1 \iff \sigma_{L/\mathbb{Q},p} \in H \iff \left(\frac{p}{q}\right) = 1$.

But $\sigma_{K/\mathbb{Q},p} = 1 \iff p$ splits in K which is equivalent to saying that $\left(\frac{q^*}{p}\right) = 1$, and so:

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$$

Combining this with $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ gives quadratic reciprocity.

In algebraic number theory terms, quadratic reciprocity says that the splitting of p in K/\mathbb{Q} depends only on the congruence class of $p \bmod$ something. Class field theory tells us that a similar thing holds for any abelian extension of number fields. There is a law describing the decomposition of primes in an abelian extension which is just a congruence condition.

[[Apparently my numbering is off compared to the lecturer - I can't work out where this happened, so we're skipping section numbers 4 and 5]]

6 Ideles and Adeles

To study congruences mod p^n , Hensel introduced $\mathbb{Z}, \mathbb{Q}_p, \mathbb{Q} \hookrightarrow \mathbb{Q}_p$. 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 $p \leq \infty$. The first guess for how to do this would be to embed into $\prod_{p \leq \infty} \mathbb{Q}_p$, but this product is not nice.

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 we introduce a small product with better properties. We introduce two objects:

- \mathbb{A}_K , the ring of adeles of K (or valuation vectors).
- J_K , the group of ideles of K .

These are topological rings/groups respectively, and are highly disconnected.

Definition of \mathbb{A}_K . Let K be a number field, and $V_K = V_{K,\infty} \sqcup V_{K,f}$. It's completion is K_v and if $v \in V_{K,f}$ then $O_v \subset K_v$.

We then define:

$$\begin{aligned} \mathbb{A}_K &:= \{(x_v) \in \prod_{v \in V_K} K_v : \text{for all but finitely many } v, x_v \in O_v\} \\ &= \bigcup_{\text{finite } S \subset V_{K,f}} U_{K,S} \subseteq \prod_{v \in V_K} K_v \end{aligned}$$

where

$$U_{K,S} = \prod_{v \in V_{K,\infty}} K_v \times \prod_{v \in S} K_v \times \prod_{v \in V_{K,f} \setminus S} O_v$$

We will sometimes refer to $K_\infty = \prod_{v \in V_{K,\infty}} K_v = K \otimes_{\mathbb{Q}} \mathbb{R}$.

\mathbb{A}_K is a ring. We then put a topology on \mathbb{A}_K . It will be generated by all $V \subset U_{K,S}$ open as S varies, where $U_{K,S}$ has the product topology.

This means in particular, every $U_{K,S} \subset \mathbb{A}_K$ is open.

$$U_{K,\emptyset} = K_\infty \times \prod_{v \in V_{K,f}} O_v$$

is open and has the product topology.

For example, take $K = \mathbb{Q}$. Then $\mathbb{A}_{\mathbb{Q}} = \mathbb{R} \times \{(x_p) \in \prod_{p < \infty} \mathbb{Q}_p : \text{for all but finitely many } p, x_p \in \mathbb{Z}_p\}$.

So, letting $m = \prod_p (\text{denominator } p^i \text{ of } x_p) \in \mathbb{Z}_{>0}$, we see that $m \cdot (x_p)_p \in \prod_{p < \infty} \mathbb{Z}_p = \widehat{\mathbb{Z}}$.

I.e., $(x_p)_p \in \frac{1}{m} \widehat{\mathbb{Z}} \subset \prod_p \mathbb{Q}_p$.

Let $\widehat{\mathbb{Q}} = \bigcup_{m \geq 1} \frac{1}{m} \widehat{\mathbb{Z}} \cong \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$. Then $\mathbb{A}_{\mathbb{Q}} = \mathbb{R} \times \widehat{\mathbb{Q}}$.

Proposition 6.1. \mathbb{A}_K is Hausdorff and locally compact (i.e. every point has a compact neighbourhood).

Proof. $U_{K,\emptyset} = K_\infty \times \prod_{v \nmid \infty} O_v \cong K_\infty \times \widehat{O_K}$ is Hausdorff and locally compact (as K_∞ is locally compact and $\widehat{O_K}$ is compact), and is an open neighbourhood of 0. Then by translation, \mathbb{A}_K is Hausdorff and locally compact. \square

We have the diagonal embedding $K \hookrightarrow \mathbb{A}_K$.

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

Proof. We need to find a neighbourhood of 0 containing only $0 \in K$. Let

$$U = \{x = (x_v) \in \mathbb{A}_K : \forall v \in V_{K,f} |x_v|_v \leq 1, \forall v \in V_{K,\infty} |x_v|_v < 1\}$$

Then $U \subseteq \mathbb{A}_K$ is open. If $x \in K \cap U$, then the first condition implies $x \in O_K$, and the second implies $|N_{K/\mathbb{Q}}(x)| < 1$, so $x = 0$. Hence K is discrete. \square

Remark. Intuitively, this must be true - if not, we would have a place-independent topology on K .

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

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

$$\mathbb{A}_K^n \xrightarrow{f} \mathbb{A}_K \otimes_K L \xrightarrow{g} \mathbb{A}_L$$

given by $(x^{(i)}) \mapsto \sum x^{(i)} \otimes_K a_i \mapsto \sum a_i x^{(i)}$. 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 $L = \bigoplus K a_i \cong K^n$, f is an \mathbb{A}_K -module isomorphism. By definition, g is a ring homomorphism. So it is sufficient to prove that $g \circ f$ is bijective, and that it maps $X^n = (K_\infty \times \widehat{O_K})^n$ homeomorphically to an open subgroup of O_L .

Note that multiplication by any $x \in K^\times$ is a self-homeomorphism of \mathbb{A}_K with itself, and so is multiplication by x^{-1} . The same is true for \mathbb{A}_L . So we may replace a_i by non-zero K -multiples, and hence WLOG we may take $a_i \in O_L$.

Let $S = \{v \in V_{K,f} : v((O_L : \sum a_i O_K)) > 0\}$ - this is a finite subset of $V_{K,f}$. Then for all $v \in V_{K,f} \setminus S$,

$$O_{K_v}^n \cong \prod_{w|v} O_{L_w} \cong O_{K_v} \otimes_{O_K} O_L$$

and for all $v \in S$, $\sum a_i O_{K_v} = M_v$ is an open O_{K_v} -submodule of $\prod_{w|v} O_{L_w}$.

Hence $gf((K_\infty \times \widehat{O_K})^n) = L_\infty \times \prod_{v \notin S, v \nmid \infty} \prod_{w|v} O_{L_w} \times \prod_v M_v$ is a homeomorphism onto an open subgroup of \mathbb{A}_L .

Moreover, for any finite $S' \supset S \supset V_{K,\infty}$,

$$gf : \left(\prod_{v \in S'} K_v \times \prod_{v \notin S'} O_{K_v} \right)^n \rightarrow \prod_{w|v \in S'} L_w \times \prod_{w|v \notin S'} O_{L_w}$$

so gf is a bijection. \square

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

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

$$\begin{array}{ccccccc}
\prod_{w|v} L_w & \hookrightarrow & A_L & \xleftarrow{\sim} & A_K \otimes L & \xleftarrow{\sim} & L \\
\downarrow \sum_w \text{Tr}_{L_w/K_v} & & \downarrow \text{Tr}_{A_L/A_K} & & \downarrow \text{id} \otimes \text{Tr}_{L/K} & & \downarrow \text{Tr}_{L/K} \\
K_v & \hookrightarrow & A_K & = & A_K & \xleftarrow{\sim} & K
\end{array}$$

Proof. Exercise. □

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

Proof. K is closed in \mathbb{A}_K , and \mathbb{A}_K is Hausdorff, 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 we may assume $K = \mathbb{Q}$. Let $X = [0, 1] \times \widehat{\mathbb{Z}} \subset \mathbb{A}_{\mathbb{Q}}$. X is compact, so it's enough to show that $X + \mathbb{Q} = \mathbb{A}_{\mathbb{Q}}$, as then $X \rightarrow \mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$. Let $x = (x_p)_{p \leq \infty} \in \mathbb{A}_{\mathbb{Q}}$, and let $S = \{p < \infty : x_p \notin \mathbb{Z}_p\}$ - a finite set of finite places.

Then there is $r_p \in \mathbb{Z}[1/p]$ 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 primes $p < \infty$, $x_p - r \in \mathbb{Z}_p$, i.e. $x - r \in \mathbb{R} \times \widehat{\mathbb{Z}}$, and then for suitable $m \in \mathbb{Z}$, $x - (r + m) \in [0, 1] \times \widehat{\mathbb{Z}}$. □

From 6.3 we also get

$$\mathbb{A}_K = K_{\infty} \times \widehat{K}$$

where $\widehat{K} = \widehat{O_K \otimes_{\mathbb{Z}} \mathbb{Q}} = \widehat{O_K} \otimes_{O_K} K$, and $\widehat{O_K} = \prod_p \widehat{O_{K,p}} = \prod_{v \nmid \infty} O_{K_v}$.

6.1 Ideles

Definition 6.6. The **idele group of K** is $J_K = \mathbb{A}_K^{\times}$, the group of units of \mathbb{A}_K . In other words, this is

$$\{(x_v) \in \prod_{v \in V_K} K_v^{\times} : \text{for all but finitely many } v, x_v \in O_v^{\times}\}$$

We can write this in a similar way as we did adeles:

$$\bigcup_{S \subset K_{K,f}} \left(K_{\infty}^{\times} \times \prod_{v \in S} K_v^{\times} \times \prod_{v \in V_{K,f} \setminus S} O_v^{\times} \right)$$

We call this set in the union $J_{K,S}$, and the topology on J_K is generated by open subsets of $J_{K,S}$ where $J_{K,S}$ has the product topology.

In particular, $K_{\infty}^{\times} \times \prod_{v \nmid \infty} O_v^{\times}$ is an open subgroup and has the product topology. We have an embedding $J_K \hookrightarrow \mathbb{A}_K$ which is continuous, but is not a homomorphism onto its image, as $x \mapsto x^{-1}$ is not continuous for the \mathbb{A}_K -topology.

However, $x \mapsto (x, x^{-1})$ is a homeomorphism $J_K \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$ onto the closed subset $\{xy = 1\} \subset \mathbb{A}_K^2$.

$K^\times \hookrightarrow J_K$ since $x \in K^\times \implies |x|_v = 1$ for all but finitely many v , and has a discrete image. We define $C_K = J_K/K^\times$, the *idele class group* of K . This is a Hausdorff locally compact topological group.

We have 2 important homomorphisms:

- The *idele norm*. Let $x = (x_v) \in J_K$. Then for all v , $|x_v|_v \neq 0$, and for all but finitely many v , $|x_v|_v = 1$. So we can define a homomorphism:

$$|\cdot|_{\mathbb{A}} : J_K \rightarrow \mathbb{R}_{>0}; |(x_v)|_{\mathbb{A}} = \prod_{v \in V_K} |x_v|_v$$

This is continuous since the restriction to $J_{K,S}$ is.

If $x \in K^\times$, then $|x|_{\mathbb{A}} = 1$ by the product formula, so $|\cdot|_{\mathbb{A}} : J_K \rightarrow C_K \rightarrow \mathbb{R}_{>0}$. We define $J_K^1 = \{x \in J_K : |x|_{\mathbb{A}} = 1\}$, and $C_K^1 = J_K^1/K^\times$. Clearly $|\cdot|_{\mathbb{A}}$ is surjective, as $K_\infty^\times \subset J_K$.

Proposition 6.7. $J_K \cong J_K^1 \times \mathbb{R}_{>0}$, $C_K \cong C_K^1 \times \mathbb{R}_{>0}$

Proof. We have $|\cdot|_{\mathbb{A}} : J_K \twoheadrightarrow \mathbb{R}_{>0}$. Consider $i : \mathbb{R}_{>0} \rightarrow K_\infty^\times \subset J_K$ given by $x \mapsto (x^{1/n})_{v|\infty}$. Because $|x|_v$ is $|x|_\infty$ if v is real and $|v|^2$ if v is complex, this homomorphism is a right inverse to $|\cdot|_{\mathbb{A}}$, so defines a splitting $J_K \cong J_K^1 \times \mathbb{R}_{>0}$.

Since $i(\mathbb{R}_{>0}) \cap K^\times = \{1\}$, we also have $C_K \cong C_K^1 \times \mathbb{R}_{>0}$. \square

- The *content map*, $c : J_K \rightarrow I(K)$, the group of fractional ideals of K , which is a free abelian group generated by $V_{K,f}$, given by $(x_v) \mapsto \prod_{v \in V_{K,f}} P_v^{v(x_v)}$, where P_v is the prime ideal corresponding to the finite place v . We write v also for the corresponding normalised discrete valuation. This is a continuous homomorphism, since $\ker(c) = J_{K,\emptyset} = K_\infty^\times \times \prod_{v \nmid \infty} O_v^\times$ is open.

If $x \in K^\times$, then $c(x)$ is the principal fractional ideal (x) . So c descends to a homomorphism $c : C_K = J_K/K^\times \rightarrow Cl(K) = I(K)/P(K)$, where $P(K)$ is the group of principal fractional ideals. The image of this inclusion $K^\times \hookrightarrow J_K$ is called the subgroup of principal ideles.

c is clearly surjective, since $K_v^\times \twoheadrightarrow \mathbb{Z}$, so $C_K \twoheadrightarrow Cl(K)$. As $\mathbb{R}_{>0} \xrightarrow{c \circ i} Cl(K)$ is zero, we have a surjection $C_K^1 \twoheadrightarrow Cl(K)$. We will now prove that $C_K^1 = J_K^1/K^\times$ is compact, and the corollary of this will be that $Cl(K)$ is finite, since it's compact and discrete.

Variant: suppose $S \subset V_{K,f}$ is a finite subset, we can define a restricted map $c^S : J_K \rightarrow I^S(K)$, the fractional ideals prime to S , i.e. I such that, for all $v \in S$, $v(I) = 0$ by $c^S((x_v)) = \prod_{v \in V_{K,f} \setminus S} P_v^{v(x_v)}$. This will be useful later on.

7 Geometry of Numbers

Classically, we embed $K \hookrightarrow K_\infty \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$, and study the image $\sigma(I) \subset \mathbb{R}^n$. Let U be a finite dimensional vector space. A *lattice* $\Lambda \subset U$ is a discrete subgroup such that U/Λ is compact.

Proposition 7.1. A subgroup $\Lambda \subseteq U$ is a lattice iff $\Lambda = \bigoplus \mathbb{Z}e_i$ where (e_i) is an \mathbb{R} -basis for U .

Proof. Ex. Sheet. □

Theorem 7.2 (Minkowski). *Let $\Lambda \subset \mathbb{R}^n$ be a lattice, and let $\mu_\Lambda = \text{vol}(\mathbb{R}^n/\Lambda)$ be the covolume of Λ . Let $X \subset \mathbb{R}^n$ be a compact subset, which is convex (so that given $x, y \in X, t \in [0, 1]$, we have $tx + (1-t)y \in X$) and symmetric about 0 (so that $x \in X \implies -x \in X$).*

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

Proof. We have $\pi : \mathbb{R}^n \rightarrow \mathbb{R}^n/2\Lambda$. Then $\text{vol}(\pi(X)) \leq \text{vol}(\mathbb{R}^n/2\Lambda) = 2^n \text{vol}(\mathbb{R}^n/\Lambda) < \text{vol}(X)$. So π is not injective, so there are $x \neq y$ such that $x - y = 2\lambda \in 2\Lambda$. But then $\lambda \neq 0$, so $\lambda = \frac{1}{2}x + \frac{1}{2}(-y) \in X$ by symmetry and convexity. □

Theorem 7.3. *There is a constant $r_K > 0$ such that, if $(d_v)_{v \in K}$ is the positive reals with $d_v \in |K_v^\times|_v = \{|x|_v : x \in \mathbb{K}_v^\times\} \subset \mathbb{R}_{>0}$, $d_v = 1$ for all but finitely many v , and $\prod_{v \in V_K} d_v > r_K$. Then $\{x \in K : \forall v, |x|_v \leq d_v\} \neq \{0\}$.*

Proof. For all $v \nmid \infty$, we can write $d_v = q_v^{-n_v}$, where $n_v \in \mathbb{Z}$. $I = \{x \in K : \forall v \nmid \infty, |x|_v \leq d_v\} = \prod P_v^{n_v}$ is a fractional ideal of K .

Then $\mu_{\sigma(I)} = m^{-n} \mu_{\sigma(mI)} = m^{-n} \mu_{\sigma(O_K)}(\sigma(O_K) : \sigma(mI)) = m^{-n} \mu_{\sigma(O_K)} N(mI) = \mu_{\sigma(O_K)} \prod q_v^{n_v}$, and $\sigma(I)$ is a lattice in \mathbb{R}^n .

Let

$$X = \{x \in \prod_{v|\infty} K_v \cong \mathbb{R}^n : \forall v, |x_v|_v \leq d_v\} = \prod_{v \text{ real}} [-d_v, d_v] \times \prod_{v \text{ complex}} \{|z|^2 \leq d_v\}$$

which is convex, compact, symmetric, with volume $2^{r_1} \pi^{r_2} \prod_{v|\infty} d_v > 2^n \mu_{\sigma(I)} = 2^n \prod_{v \nmid \infty} d_v^{-1} \mu_{\sigma(O_K)}$, provided that $\prod_{\text{all } v} d_v > r_K = (4/\pi)^{r_2} \mu_{\sigma(O_K)}$. Then apply Minkowski. □