Algebraic Number Theory

Harry Armitage

February 10, 2021

Contents

1 Absolute Values and Places

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

i) $|x| = 0 \iff x = 0$

ii) $|xy| = |x||y|$

iii) $|x + y| \leq |x| + |y|$

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

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

An AV is ***non-archimedean*** if it satisfies

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):

iii') $\exists\, \alpha > 0$ 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. □

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:*

i) $|\cdot|, |\cdot|'$ *are equivalent.*

ii) $|x| \leq |y| \iff |x|' \leq |y|'$.

iii) $|x| < |y| \iff |x|' < |y|'$.

Proof. From local fields, or exercise. □

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 $a_1, \ldots, a_n \in K$, $\delta > 0$.*

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 $|\frac{z_j^N}{z_j^N+1}|_i \to 0$ as $N \to \infty$ 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 $|y|_2, \ldots, |y|_{n-1} < 1$. 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. □

Remark. If $K = \mathbb{Q}$, $|\cdot|_1, \ldots, |\cdot|_n$ 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 $x \equiv a_i \mod p_i^{n_i}$ 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 $v : K^\times \to \mathbb{R}$ 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 $v_1, \ldots, v_n$ 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 Cassesl 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 $i_w : L \hookrightarrow I_w$. 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_is, 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 $L \otimes_K K_v \cong \prod L_w$. □

Corollary 1.6.

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

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 $gw = v_{g(P)}$.a

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.

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

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 $G_w = \mathrm{Gal}(L_w/K_v)$.

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 $K = \mathrm{Frac}(R)$. 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 $I = (a_1, \ldots, a_n)$. 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 $I' = (a_1, \ldots, a_r) \subset I$. 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 $I \coloneqq R[x] = \sum_{0 \leq i < d} Rx^i \subset K$ 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 $P = Q$.

3. Let R be a semi-local Dedekind domain with non-zero primes $P_1, \ldots, P_n$. Choose $x \in R$ with $x \in P_1 \setminus P_1^2, x \in P_2, \ldots, P_n$. 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:*

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

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

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

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

Proof.

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

2. 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 $(R : P^{n+1}) = (R : P)(P : P^{n+1}) = (R : P)(R : P^n)$.

□

The quotient group $Cl(R) \coloneqq \{\text{fractional ideals of } R\}/\{\text{principal fractional ideals of } R\}$ 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 $\{\text{primes of } O_K\} \to V_{K,f}$.*

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. □

For $v \in V_{K,f}$, write P_v for the corresponding prime deal 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 $v : K^\times \twoheadrightarrow \mathbb{Z}$ 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 $(z_\sigma)_\sigma \mapsto (\overline{z_{\bar{\sigma}}})_\sigma$.

Let $\sigma_1, \ldots, \sigma_{r_1} : K \hookrightarrow \mathbb{R}$, $\sigma_{r_1+1} = \bar{\sigma}_{r_1+r_2+1}, \ldots, \sigma_{r_1+r_2} = \bar{\sigma_n} : K \hookrightarrow \mathbb{C}$ 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 $K_\infty \coloneqq K \otimes_{\mathbb{Q}} \mathbb{R}$, 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. □

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, $|q|_p = \begin{cases} \frac{1}{q} & p = q \\ 1 & p \neq q, \infty \\ q & p = \infty \end{cases}$, and in the latter, $|-1|_p = 1$ for all $p \leq \infty$. Hence the product over all of these is 1. □

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 $dxdy$. This transforms under $\mathbb{C}^\times$ as $dxdy \mapsto |a|^2 dxdy$. 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 $\mathrm{Tr}_{S/R} : S \to R$, the trace of the R-linear map $y \mapsto xy$.

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

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

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

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

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

This has the following basic properties:

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

If L/K is a finite field extension, then $\mathrm{disc}(L/K) = K \iff$ 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* $\mathrm{disc}(A/k) \neq 0$ *(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 $r \in A$, $\mathrm{Tr}_{A/k}(rx) = 0$, giving a degenerate trace form so a zero discriminant. □

If R is a Dedekind domain, $K = \mathrm{Frac}(R)$, 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 $\dim_K L = n$. □

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

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

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

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

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

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

Proof. We claim there exist $x_1, \ldots, x_n \in S$ which are an R_P-basis for S_P. Certainly, there is such a basis in S_P, say $e_1, \ldots, e_n$. 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 $x_i \equiv e_i \bmod PS$. 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 $\mathrm{disc}(S_P/R_P) = \mathrm{disc}(x_i)R_P$, and hence $\mathrm{disc}(x_i) \in \mathrm{disc}(S/R)$. So $\mathrm{disc}(S_P/R_P) \subset \mathrm{disc}(S/R)R_P$, and the other inclusion is obvious. □

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

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

  Let $\mathcal{P} = \{P \subset R : v_P(\mathrm{disc}_{L/K}(x_i)) > 0\}$, a finite set. So for all $P \notin \mathcal{P}$, $\mathrm{disc}(S_P/R_P) = R_P$. Then we can define $\mathrm{disc}(S/R) = \prod_{P \in \mathcal{P}} P^{v_P(\mathrm{disc}(S_P/R_P))}$.

This is equivalent to the previous definition by **3.4**.

Theorem 3.5. $v_P(\mathrm{disc}(S/R)) = 0$ *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 $v_P(\mathrm{disc}(S/R)) = 0$ if and only if $\mathrm{disc}(\frac{S}{PS}/\frac{R}{P}) = \frac{R}{P}$ 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. □

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* $\mathrm{Frac}(R)$*), only finitely many primes are ramified - precisely the primes such that* $v_P(\mathrm{disc}(S/R)) > 0$.

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

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 $v_P(\mathrm{disc}(S/R)) = v_P(\mathrm{disc}(S \otimes_R \widehat{R}/\widehat{R})) = \sum_Q v_P(\mathrm{disc}(\widehat{S}_Q/\widehat{R}))$. □

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

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

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

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. $\mathrm{Tr}_{L/K}(x_i y_j) = \delta_{ij}$. Then $S \subset \mathscr{D}_{S/R}^{-1} \subset \bigoplus_{i=1}^n Ry_i$, so $\mathscr{D}_{S/R}^{-1}$ is a fractional ideal (since it is finitely generated), and its inverse $\mathscr{D}_{S/R}$ is an ideal of S, called the ***different***.

Proposition 3.8.

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

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 $\mathscr{D}_{S/R}^{-1} = x^{-1}S$ 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
$$\mathrm{Tr}_{L/K}(e_i x^{-1} e_j') = \delta_{ij}$$
Let $x^{-1}e_j = \sum_k b_{kj} e_k$ where $b_{kj} \in K$. Then the ideal:
$$\begin{aligned}(1) &= (\det[\mathrm{Tr}_{L/K}(e_i x^{-1} e_j')]) \\ &= (\det(\mathrm{Tr}_{L/K}(e_i e_j)) \det(b_i j)) \\ &= \det(b_{ij}) \, \mathrm{disc}(S/R)\end{aligned}$$
But $N_{L/K}(x^{-1}) = u \det(b_{ij})$ for some unit in R. So $(1) = (N_{L/K}(x^{-1}))\,\mathrm{disc}(S/R)$. Since we are in Dedekind domains we can cancel $\mathrm{disc}(S/R)$, giving the result.
3. Assume R is local, $P = (\pi_P)$. Write $\widehat{K} = \mathrm{Frac}(\widehat{R})$ for $Q = (\pi_Q) \subset S$, and $\widehat{L_Q} = \mathrm{Frac}(\widehat{S_Q})$. So $L \otimes_K \widehat{K} \cong \prod_Q \widehat{L}_Q$ viea $x \mapsto (x_Q)_Q$, say, and $S \otimes_R \widehat{R} \cong \prod_Q \widehat{S}_Q$.
We also have $\mathrm{Tr}_{L \otimes_K \widehat{K}/\widehat{K}}(x) = \sum_Q \mathrm{Tr}_{\widehat{L}_Q/\widehat{K}}(x)$.
Let $S = \bigoplus_{i=1}^n Rx_i$, and $\mathscr{D}_{S/R}^{-1} = \prod_Q \pi_Q^{-a_Q} S = \bigoplus_{i=1}^n Ry_i$ 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:
$$\begin{aligned}\mathscr{D}_{S \otimes_R \widehat{R}/\widehat{R}}^{-1} &\coloneqq \{x \in L \otimes_K \widehat{K} : \ \forall y \in S \otimes_R \widehat{R}, \mathrm{Tr}_{L \otimes_K \widehat{K}/\widehat{K}}(xy) \in \widehat{R}\} \\ &= \bigoplus_{i=1}^n \widehat{R} y_i \\ &= \mathscr{D}_{S/R}^{-1} \cdot S \otimes_R \widehat{R} \subset L \otimes_K \widehat{K}\end{aligned}$$

On the other hand,

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

So:

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

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 $Q_i | \mathscr{D}_{S/R} \iff e_i > 1$; and $Q_i^{e_i-1} | \mathscr{D}_{S/R}$.*

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 $\mathscr{D}_{S/R} = (\pi_S)^d$ for some $d \geq 0$. By **3.8.2**, $\operatorname{disc}(S/R) = (N_{L/K}(\pi_s)^d) = (\pi_R)^{df}$. So as $v_P(\operatorname{disc}(S/R)) = 0 \iff \mathfrak{p}$ is unramified (**3.5**), the first statement holds.

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

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

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

More precisely, $v_{Q_i}(\mathscr{D}_{S/R})$ 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 $\mathscr{D}_{S/R} = (f'(x))$ where f' is the derivative.

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

For an extension L/K of number fields, we write $\mathscr{D}_{L/K} = \mathscr{D}_{O_L/O_K}$, and $\delta_{L/K} = \operatorname{disc}(O_L/O_K)$. **Remark.** Take $K/\mathbb{Q}$, (e_i) a $\mathbb{Z}$-basis for O_K. Then $\delta_{K/\mathbb{Q}} \subset \mathbb{Z}$ is $(\operatorname{disc}(e_i))$, and if (e_i') is another basis, say $e_i' = \sum a_{ji}e_j$, then $\operatorname{disc}(e_i') = (\det a_{ij})^2 \operatorname{disc}(e_i) = \operatorname{disc}(e_i)$.

So the integer $\operatorname{disc}(e_i)$ 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 $S/Q_i \equiv k[T]/(\bar{g}_i)$, 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:

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

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. □

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:

$$(a + b\sqrt{d}) \cdot 1 = a \cdot 1 + b \cdot \sqrt{d}$$
$$(a + b\sqrt{d}) \cdot \sqrt{d} = a\sqrt{d} + bd = bd \cdot 1 + a \cdot \sqrt{d}$$

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 $d \equiv 1 \mod 4$, 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 $\mathrm{Tr}_{K/\mathbb{Q}}(1 \cdot \frac{1}{2}) = 1, \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt{d} \cdot \frac{1}{2\sqrt{d}}) = 1$, so we have a dual basis for the trace form given by $\{\frac{1}{2}, \frac{1}{2\sqrt{d}}\}$, and hence $\mathscr{D}_{K/\mathbb{Q}}^{-1} = (\frac{1}{2}, \frac{1}{2\sqrt{d}}) = (\frac{1}{2\sqrt{d}}) = (2\sqrt{d})^{-1}$, and so $\mathscr{D}_{K/\mathbb{Q}} = (2\sqrt{d})$

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 $\mathscr{D}_{K/\mathbb{Q}}^{-1} = (\frac{1}{2}, \frac{1}{1+\sqrt{d}}) = (2, 1+\sqrt{d})^{-1} = (\sqrt{d})^{-1}$, so $\mathscr{D}_{K/\mathbb{Q}} = (\sqrt{d})$.

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

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

- If $p \neq 2$ or $d \not\equiv 1 \mod 4$, 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 $d \equiv 1 \mod 4$, then we factor $T^2 - T - \frac{d-1}{4} \bmod 2$ and get:
$$(2) = \begin{cases} (2) & \text{inert, if } d \equiv 5 \mod 8 \\ PP' & \text{split, if } d \equiv 1 \mod 8 P = (2, \frac{\sqrt{d}+1}{2}) \neq P' = (2, \frac{\sqrt{d}-1}{2}) \end{cases}$$

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

$$\mathrm{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

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. $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
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 $\zeta_n = \zeta_{pr}^a \zeta_m^b$. 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 $T^{p^{r-1}(p-1)}$ mod 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 $G = \mathrm{Gal}(L/K) \supset G_w \cong \mathrm{Gal}(L_w/K_v)$, the decomposition group of w, we have a short exact sequence:

$$0 \to I_w \to G_w \to \mathrm{Gal}(\ell_w/k_v) \to 1$$

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 $\mathrm{Gal}(\ell_w/k_v)$.

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 $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow[\lambda]{\sim} \mathrm{Gal}(L/\mathbb{Q})$, given by

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

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 $\mathrm{Gal}(L/\mathbb{Q})$, since every integer prime to n is a product of $p \nmid n$. This gives with some thought another proof that $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
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 $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$, 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 $q^* = \begin{cases} q & q \equiv 1 \mod 4 \\ -q & q \equiv 3 \mod 4 \end{cases}$.

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 mod 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:

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

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 $\mathbb{A}_K$. IOt will be generated by al $V \subset U_{K,S}$ 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 Haudorff 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. □

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. □

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