

Algebraic Number Theory

Harry Armitage

January 30, 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

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 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 $i_w : L \hookrightarrow L_w$. 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 $P = Q$.

3. 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:*

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 $\{\text{fractional ideals of } R\} \rightarrow \{\text{fractional ideals of } R_P\} \rightarrow \mathbb{Z}$ 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.

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

□

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 $x \in \mathfrak{m}$ 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 $\cap_P R_P = \{x \in K : v_P(x) \geq 0 \forall P\} = R$. \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 .

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

Proposition 3.6. 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 3.7.

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.

□