Math 430
Notes from Class 10/18

Definition 13.1. The discriminant $\Delta(B'/A)$ is defined to be ideal generated by the determinants of all matrices $M = [\mathrm{T}_{L/K}(w_i w_j)]$ as $w_1, \ldots, w_n$ range over all bases for L consisting of elements contained in B'.

Example 13.2. The reason that we need to talk about the discriminant relative to A is that B' could be defined over two different Dedekind domains. For example, we could take $B' = \mathbb{Z}[\sqrt{3}, \sqrt{7}]$ which is an extension of $\mathbb{Z}$ as well as of $\mathbb{Z}[\sqrt{3}]$ and $\mathbb{Z}[\sqrt{7}]$. The various discriminants $\Delta(B'/\mathbb{Z})$, $\Delta(B'/\mathbb{Z}[\sqrt{3}])$, and $\Delta(B'/\mathbb{Z}[\sqrt{7}])$ may all be different.

One nice fact about discriminants is that they can be computed locally. We have the following.

Proposition 13.3. *With notation as throughout lecture, let S be a multiplicative subset of A not containing 0. Then*

$$S^{-1}A\Delta(B'/A) = \Delta(S^{-1}B'/S^{-1}A).$$

Proof. Since any basis with elements in B' is also in $S^{-1}B'$, it is obvious that

$$S^{-1}A\Delta(B'/A) \subseteq \Delta(S^{-1}B'/S^{-1}A).$$

Similarly, given a basis $v_1, \ldots, v_n$ for L/K contained in $S^{-1}B'$, see that the basis $w_1, \ldots, w_n$ where $w_i = sv_i$ is contained in B' for some $s \in S$. Now

$$\det(T_{L/K}(w_i w_j)) = s^n \det(T_{L/K}(v_i v_j)),$$

so $S^{-1}A\Delta(B'/A) \supseteq \Delta(S^{-1}B'/S^{-1}A)$. $\square$

We know that $\Delta(B'/A)$ is an ideal I. If $I = \prod_{i=1}^{m} \mathfrak{p}_i^{e_i}$, then $A_{\mathfrak{p}_i} I = \mathfrak{p}_i^{e_i}$, so to figure out what $\Delta(B'/A)$ is, all we have to do is figure out what $\Delta(S^{-1}B'/S^{-1}A)$ is for $S = A \setminus \mathfrak{p}$.

The trace also behaves well with respect to reduction. Recall that whenever we have a finite integral extension of a field, we can define a trace. We'll apply that with the field $k = A/\mathfrak{p}$ for a maximal ideal $\mathfrak{p}$ of A. Since this computation is local, we will work over $A_{\mathfrak{p}}$ (which is a DVR). This is just for simplicity, since we have $B'/\mathfrak{p}B' \cong S^{-1}B'/S^{-1}B'\mathfrak{p}$, so it isn't hard to see that the local computation gives the computation over A.

Lemma 13.4. *Let A and B' be as usual. Let $\mathfrak{p}$ be a maximal prime of A, let $k = A/\mathfrak{p}$, let $S = A \setminus \mathfrak{p}$, and let $\phi : S^{-1}B' \longrightarrow S^{-1}B'/S^{-1}B'\mathfrak{p}$ be* *the usual quotient map. Let us denote $S^{-1}B'/S^{-1}B'\mathfrak{p}$ as C. Then for any $y \in S^{-1}B'$, we have $\phi(T_{L/K}(y)) = \mathrm{T}_{C/k}(\phi(y))$.*

Proof. Let $\bar{w}_1, \ldots, \bar{w}_n$ be a basis for C over k and pick $w_i \in B'$ such that $\phi(w_i) = \bar{w}_i$. Since the $\bar{w}_i$ are linearly independent, the w_i must be as well. To see this, suppose that $\sum_{i=1}^{n} a_i w_i = 0$ for $a_i \in S^{-1}B'$ (remember that everything in L is x/a for $x \in B'$ and $a \in A$). By dividing through by a power of a generator π for $A_{\mathfrak{p}}\mathfrak{p}$, we can assume that not all of the a_i are in $S^{-1}B'\mathfrak{p}$. This means then that $\sum_{i=1}^{n} \phi(a_i)\bar{w}_i = 0$, with some $\phi(a_i) \neq 0$, which is impossible. Now, we are essentially done, since we can define the trace of any $y \in B'$ with respect to this basis. We have

$$yw_i = \sum_{j=1}^{n} m_{ij} w_j$$

with $m_{ij} \in A$, and

$$\phi(y)\bar{w}_i = \sum_{j=1}^{n} \phi(m_{ij})\bar{w}_j.$$

Hence,

$$\phi(\mathrm{T}_{L/K}(y)) = \sum_{i=1}^{n} \phi(m_{ii}) = \mathrm{T}_{C/k}(\phi(y)).$$

□

When B is the integral closure of A in L, and $\mathfrak{p}$ is maximal in A, we can write

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_m^{e_m}.$$

If $e_i > 1$ for some i, then we say that $\mathfrak{p}$ *ramifies* in B. When $B = A[\alpha]$, we know that $\mathfrak{p}$ ramifies in B if and only if $\Delta(B/A) \subseteq \mathfrak{p}$. That is true more generally.

Theorem 13.5. *Let B be the integral closure of A in L and let $\mathfrak{p}$ be maximal in A. Then $\Delta(B/A) \subseteq \mathfrak{p}$ if and only if $\mathfrak{p}$ ramifies in B or $B/\mathfrak{q}$ is inseparable over $A/\mathfrak{p}$ for some prime $\mathfrak{q}$ such that $\mathfrak{q} \cap A = \mathfrak{p}$.*

Proof. It will suffice to prove this locally, that is to say, it will suffice to replace A with $A_{\mathfrak{p}}$ and B with B where $S = A \setminus \mathfrak{p}$. As in the previous Lemma, we write $k = A/\mathfrak{p}$ and $C = B/\mathfrak{p}B$ and let

$$\phi : B \longrightarrow B/\mathfrak{p}B$$

Also, as in that Lemma let $\bar{w}_1, \ldots, \bar{w}_n$ be a basis for C over k and pick $w_i \in B$ such that $\phi(w_i) = \bar{w}_i$. It is clear then that

$$A_{\mathfrak{p}} w_1 + \ldots A_{\mathfrak{p}} w_n + \mathfrak{p}B = B,$$

so by Nakayama's Lemma, the w_i generate B as an $A_{\mathfrak{p}}$ module. From the Lemma above we have $T_{L/K}(w_i w_j) = T_{C/k}(\bar{w}_i \bar{w}_j)$, so the matrix $M = [\mathrm{T}_{C/k}(\bar{w}_i \bar{w}_j)]$ represents the form $(x, y) = \mathrm{T}_{C/k}(xy)$ on C/k. Let us now decompose C/k as ring, we have

$$C \cong B/\mathfrak{p}B \cong \bigoplus_{i=1}^{m} B/\mathfrak{q}_i^{e_i}$$

where

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_m^{e_m}.$$

If $e_i > 1$, then any element $z \in C$ such that $z = 0$ in every coordinate but i and has i-th coordinate in $\mathfrak{q}_i$, has the property that $z^{e_i} = 0$. Furthermore the set of such z forms an ideal. This means $T_{C/k}(zx) = 0$ for all $x \in C$, by your homework. Thus, the pairing

$$(x, y) = T_{C/k}(xy)$$

is degenerate, which means that $\Delta(B/A)$ is 0 zero modulo $\mathfrak{p}$.

If $e_i = 1$ for every i, then

$$C \cong B/\mathfrak{q}_1 \oplus \cdots \oplus B/\mathfrak{q}_m.$$

The trace form $(x, y) = \mathrm{T}_{C/k}(xy)$ decomposes into a sum of forms

$$(a, b) = \mathrm{T}_{(B/\mathfrak{q}_i)/k}(ab).$$

Now, $(a, b) = \mathrm{T}_{(B/\mathfrak{q}_i)/k}(ab)$ is nondegenerate if and only if $B/\mathfrak{q}_i$ is separable over k. Since a direct sum of forms is nondegenerate if and only if each form is nondegenerate, our proof is complete. □

Here is a simple and easy to prove fact comparing the discriminants of different subrings B and B' of L

Proposition 13.6. *Let $B' \subset B$ where B and B' are as usual (we will usually take B to the be the integral closure of A in L). Suppose that B has a basis $v_1, \ldots, v_n$ as an A-module and that B' has a basis $w_1, \ldots, w_n$ as an A-module. Writing*

$$w_i = \sum_{\ell=1}^{n} n_{i\ell} a_\ell,$$

and letting N be the matrix $[n_{i\ell}]$, we have

$$\det[\mathrm{T}_{L/K}(w_i w_j)] = (\det N)^2 \det[\mathrm{T}_{L/K}(v_i v_j)]. \tag{1}$$

Proof. Now,

$$\mathrm{T}_{L/K}(w_i w_j) = \sum_{\ell=1}^{n} \sum_{k=1}^{n} n_{i\ell} n_{jk} \, \mathrm{T}_{L/K}(v_i v_j).$$

A bit of linear algebra shows that this is exactly the same as the ij-th coordinate of the matrix $N^t M N$ where $M = [\mathrm{T}_{L/K}(v_i v_j)]$. Equation 1 follows. I gave an easier explanation on the board. $\square$

Corollary 13.7. *Let $B' \subset B$ with B' and B as usual. Then*

$$\Delta(B/A)(\Delta(B'/A))^{-1} = I^2$$

for some ideal I in A.

Proof. Recall that we can compute discriminants locally, and that a nonzero ideal J if and only if for every maximal $\mathfrak{p}$ in A, we have$A_{\mathfrak{p}} J = A_{\mathfrak{p}} \mathfrak{p}^{2e_{\mathfrak{p}}}$ for some integer $e_{\mathfrak{p}}$. At each $\mathfrak{p}$, taking $S = A \setminus \mathfrak{p}$ the $A_{\mathfrak{p}}$-modules $S^{-1}B$ and $S^{-1}B'$ are free $A_{\mathfrak{p}}$-modules, so we can apply the previous Proposition to $\Delta(S^{-1}B/A_{\mathfrak{p}})$ and $\Delta(S^{-1}B'/A_{\mathfrak{p}})$. Since $\det N \in A_{\mathfrak{p}}$, $(\det N)^2$ is an even power of $\mathfrak{p}$ (possibly 0). $\square$