Math 568
Notes from Class 10/08

We were proving the following:

Theorem 9.1. *Let $L \supseteq K$ be a finite extension of fields. Then the bilinear form $(x, y) = \mathrm{T}_{L/K}(xy)$ is nondegenerate $\Leftrightarrow$ L is separable over K.*

Proof. ($\Rightarrow$) We did last time.

($\Leftarrow$) We will denote $\mathrm{T}_{L/K}(xy)$ as (x, y). Recall the following: Choosing a basis $m_1, \ldots, m_n$ and writing x and y as vectors in terms of the m_i we can write

$$\mathbf{x}A\mathbf{y}^T$$

for some matrix A. The matrix A is given by $[a_{ij}]$ where $a_{ij} = (m_i, m_j)$ since we want

$$(\sum_{i=1}^{n} r_i a_i, \sum_{j=1}^{n} s_j a_j) = \sum_{i=1}^{n}\sum_{j=1}^{n} r_i s_j (a_i, a_j).$$

It is easy to see that that the form will be nondegenerate if and only if A is invertible, since $A\mathbf{y} = 0$ if and only $(x, y) = 0$ for every $y \in L$.

Now, since L is separable over K, we can write $L = K(\theta)$ for $\theta \in L$ and use $1, \theta, \ldots, \theta^{n-1}$ as a basis for L over K. Then we can write the matrix $A = [a_{ij}]$ with above with

$$a_{ij} = (\theta^{i-1}, \theta^{j-1}) = \mathrm{T}_{L/K}(\theta^{i+j-2}).$$

It isn't too hard to calculate these coefficients explicitly. In fact, if $\theta_1, \ldots, \theta_n$ are the roots of the minimal polynomial of θ, then

$$\mathrm{T}_{L/K}(\theta) = \sum_{\ell=1}^{n} \theta_\ell,$$

from what we proved earlier. Similarly, we have

$$a_{ij} = \mathrm{T}_{L/K}(\theta^{i+j-2}) = \sum_{\ell=1}^{n} \theta_\ell^{i+j-2}.$$

There is a trick to finding the determinant of such a matrix. Recall the van der Monde matrix in $V := V(\theta_1, \ldots, \theta_n)$. It is the matrix

$$\begin{pmatrix} 1 & \cdots & 1 \\ \theta_1 & \cdots & \theta_n \\ \cdots & \cdots & \cdots \\ \theta_1^n & \cdots & \theta_n^n \end{pmatrix}$$

The determinant of this matrix is

$$\det(V) = \prod_{i<j}(\theta_i - \theta_j).$$

It is easy to check that $VV^T = A$ (a messy but easy calculation). Thus,

$$\det(A) = \det(V)\det(V^T) = \det(V)^2 = \left(\prod_{i<j}(\theta_i - \theta_j)\right)^2 \neq 0,$$

since $\theta_i \neq \theta_j$ for $i \neq j$ and we are done.

□

The following Corollary is now immediate.

Corollary 9.2. *Let A be a Dedekind domain and let B be the integral closure of A in a finite separable extension of the field of fractions of A. Then B is a finitely generate A-module. In particular, B is Noetherian.*

Proposition 9.3. *Let A be a domain, $A \neq 0$, and let B be integral over A. Then for any prime $\mathcal{P}$ of A, we have $B\mathcal{P} \neq 1$.*

Proof. Suppose that $B\mathcal{P} = 1$. Then there are $x_1, \ldots, x_m \in A$ such that

$$b_1x_1 + \cdots + b_mx_m = 1.$$

Let $C = A[b_1, \ldots, b_m]$. Then C is finitely generated as an A-module and $\mathbb{P}C = 1$. Let $N = A_{\mathcal{P}}C$; then N is finitely generated and $A_{\mathcal{P}}\mathcal{P}N = N$. Since $A_{\mathcal{P}}$ is local, we must have $N = 0$ by Nakayama's lemma, which gives a contradiction, since $A \neq 0$. □

Let's fix our notation for the rest of the day: A is Dedekind with field of fractions K, $L \supseteq K$ is a finite separable field extension of degree n, and B is the integral closure of A in L. Sometimes, we will impose additional restrictions on A.

Corollary 9.4. *If A is a principal ideal domain and $[L : K] = n$ for L a separable extension of K, the field of fractions of A, then the integral closure of A in L is isomorphic to A^n as an A-module.*

Proof. If A is a principal ideal domain, then any finitely generated torsion-free A-module is a free module. In the proof of the theorem above, we saw that there is a free module of rank n, call it M such that $M \subset B \subset M^\dagger$. Since $M^\dagger$ is also of rank n, we see that the rank of B must be n. □

One more thing I wanted to mention about factorizations of ideals in Dedekind domains. If $I \subseteq \mathcal{P}$, then $\mathcal{P}$ must appear in the factorization

of I. This follows from the fact that $R_{\mathcal{P}}I$ is positive power of $R_{\mathcal{P}}\mathcal{P}$, which would not happen if I didn't have $\mathcal{P}$ in its factorization.

Let us continue with the set-up: A a Dedekind ring, K field of fractions of A, L a finite separable extension of K, and B the integral closure of A in L. We'll have $n = [L : K]$. Say we have a prime $\mathcal{P} \subset A$. What can we say about how $B\mathcal{P}$ factors?

Let's start with some basics. We write

$$B\mathcal{P} = \mathcal{Q}_1^{e_1} \cdots \mathcal{Q}_m^{e_m}.$$

The number e_i is called the **ramification degree** of $\mathcal{Q}_i$ over $\mathcal{P}$. There's another number associated with $\mathcal{Q}_i$ over $\mathcal{P}$ as well. Recall that we have an injection of fields

$$A/\mathcal{P} \hookrightarrow B/\mathcal{Q}_i.$$

We call the index $[B/\mathcal{Q}_i : A/\mathcal{P}]$ the **relative degree** of $\mathcal{Q}_i$ over $\mathcal{P}$. It isn't hard to see that f_i is finite and in fact $f_i \leq [L : K]$. We'll prove something more general along these lines in a bit. First, let's look at some examples...

Example 9.5. Let $A = \mathbb{Z}$ and $B = \mathbb{Z}[\sqrt{2}]$. Let's look at some factorizations of Bp into primes in p for various p.

(1) $2B = (\sqrt{2})^2$.
(2) $3B$ is a prime.
(3) $7B = (\sqrt{2} - 3)(\sqrt{2} + 3)$.

Theorem 9.6. *With the set-up above, for $\mathcal{P}$ a maximal ideal of A we have*

$$B\mathcal{P} = \mathcal{Q}_1^{e_1} \cdots \mathcal{Q}_m^{e_m}$$

and $f_i = [B/\mathcal{Q}_i : A/\mathcal{P}]$ with

$$\sum_{i=1}^{m} e_i f_i = n.$$

Proof. We know that

$$B/B\mathcal{P} \cong \sum_{i=1}^{m} B/\mathcal{Q}_i^{e_i}$$

by the Chinese remainder theorem. Now, let $S = A \setminus \mathcal{P}$. Then from above, $S^{-1}B$ is the integral closure of $A_{\mathcal{P}}$ in L. Hence, it is isomorphic to $A_{\mathcal{P}}^n$ as an $A_{\mathcal{P}}$ module. It follows that $S^{-1}B/S^{-1}B\mathcal{P}$ is a $A_{\mathcal{P}}/\mathcal{P}$ vector space of dimension n. Moreover, since $S \cap \mathcal{Q}_i$ is empty for each $\mathcal{Q}_i$, we see that $S^{-1}B\mathcal{Q}_i$ is a prime in $S^{-1}B$ and we have

$$S^{-1}B\mathcal{P} = S^{-1}B\mathcal{Q}_1^{e_1} \cdots \mathcal{Q}_m^{e_m}.$$

Combining this with homework results plus further localization, we obtain

$$S^{-1}B/S^{-1}B\mathcal{P} \cong \sum_{i=1}^{m}(S^{-1}B)/(S^{-1}B\mathcal{Q}_i^{e_i}) \cong \sum_{i=1}^{m} B_{\mathcal{Q}_i}/(B_{\mathcal{Q}_i}\mathcal{Q}_i^{e_i}).$$

Thus, we see that

$$\dim_{A_{\mathcal{P}}/A_{\mathcal{P}}\mathcal{P}}(\sum_{i=1}^{m} B_{\mathcal{Q}_i}/(B_{\mathcal{Q}_i}\mathcal{Q}_i^{e_i})) = n.$$

It will suffice to show, then, that

$$\dim_{(}\, A_{\mathcal{P}}/A_{\mathcal{P}}\mathcal{P})(\sum_{i=1}^{m} B_{\mathcal{Q}_i}/(B_{\mathcal{Q}_i}\mathcal{Q}_i^{e_i})) = \sum_{i=1}^{m} e_i f_i,$$

which would follow from

$$\dim_{(A_{\mathcal{P}}/A_{\mathcal{P}}\mathcal{P})}(B_{\mathcal{Q}_i}/(B_{\mathcal{Q}_i}\mathcal{Q}_i^{e_i})) = e_i f_i.$$

Since we can write

$$0 = B_{\mathcal{Q}_i}\mathcal{Q}_i^{e_i}/(B_{\mathcal{Q}_i}\mathcal{Q}_i^{e_i}) \subset (B_{\mathcal{Q}_i}\mathcal{Q}_i^{e_i})/(B_{\mathcal{Q}_i})\mathcal{Q}_i^{e_i-1} \subset \cdots \subset B_{\mathcal{Q}_i}/(B_{\mathcal{Q}_i}\mathcal{Q}_i^{e_i}),$$

we need only show that

$$\dim_{A_{\mathcal{P}}/\mathcal{P}}((B_{\mathcal{Q}_i}\mathcal{Q}_i^{j})/(B_{\mathcal{Q}_i}\mathcal{Q}_i^{j+1})) = f_i,$$

for any $j \geq 0$. Note that since $B_{\mathcal{Q}_i}$ is a DVR, its its maximal ideal is generated by a single element π. It follows that each power $B_{\mathcal{Q}_i}\mathcal{Q}_i^{j}$ is generated by π^j and that $(B_{\mathcal{Q}_i}\mathcal{Q}_i^{j})/(B_{\mathcal{Q}_i}\mathcal{Q}_i^{j+1})$ is therefore a 1-dimensional $B_{\mathcal{Q}_i}/B_{\mathcal{Q}_i}\mathcal{Q}_i$ vector space. Since $B/\mathcal{Q}_i$ is an f_i dimensional $A/\mathcal{P}$-vector space, it follows that $(B_{\mathcal{Q}_i}\mathcal{Q}_i^{j})/(B_{\mathcal{Q}_i}\mathcal{Q}_i^{j+1})$ is an f_i-dimensional $A/\mathcal{P}$ vector space and we are done. □