Math 8430 Tom Tucker
NOTES FROM CLASS 10/4
INDICATE WHERE IN THE BOOK CERTAIN THINGS ARE

Corollary 20.1. *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 $\mathcal{P}$ in A, we have$A_{\mathcal{P}}J = A_{\mathcal{P}}\mathcal{P}^{2e_{\mathcal{P}}}$ for some integer $e_{\mathcal{P}}$. At each $\mathcal{P}$, taking $S = A \setminus \mathcal{P}$ the $A_{\mathcal{P}}$-modules $S^{-1}B$ and $S^{-1}B'$ are free $A_{\mathcal{P}}$-modules, so we can apply the previous Proposition to $\Delta(S^{-1}B/A_{\mathcal{P}})$ and $\Delta(S^{-1}B'/A_{\mathcal{P}})$. Since $\det N \in A_{\mathcal{P}}$, $(\det N)^2$ is an even power of $\mathcal{P}$ (possibly 0). □

Corollary 20.2. *Let B' be as usual. Let $\mathcal{Q}$ be maximal in B' and let $\mathcal{P} = \mathcal{Q} \cap A$. Then $A_{\mathcal{Q}}$ is invertible whenever $\mathcal{P}^2$ doesn't divide $\Delta(B'/A)$.*

Proof. We replace B' with $S^{-1}B'$ where $S = A \setminus \mathcal{P}$, which we'll just write as B'. It will suffice to show that B' is a Dedekind domain, which is equivalent to showing that it is equal to the integral closure B of $A_{\mathcal{P}}$ in L. As in the proof of Proposition from last time, we choose bases $v_1, \ldots, v_n$ and $w_1, \ldots, w_m$ for B and B' respectively, and let N be the matrix $[n_{ij}]$ where $w_i = \sum_{j=1}^{n} n_{ij}v_j$. We let $\phi : B \longrightarrow B/\mathcal{P}B$ and let $\overline{N}$ be the matrix $[\phi(n_{ij})]$. Then $\phi(w_1), \ldots, \phi(w_n)$ is a basis for $B/\mathcal{P}B$ over $A/\mathcal{P}$ unless $\det \overline{N} = 0$. Furthermore, if $\phi(w_1), \ldots, \phi(w_n)$ is a basis for $B/\mathcal{P}B$ over $A/\mathcal{P}$, then $w_1, \ldots, w_n$ is a basis for B over A, again by Nakayama's Lemma, and we must have $B' = B$.

Now, $\det \overline{N} = 0$ if and only if $(\det N) \subset \mathcal{P}$. But if $(\det N) \subset \mathcal{P}$, then $\Delta(B'/A) = (\det N)^2\Delta(B/A)$, which means that $\Delta(B'/A) \subset \mathcal{P}^2$. □

Corollary 20.3. *If $\Delta(B'/A) \notin \mathcal{P}^2$, then $S^{-1}B'$ is integrally closed for $S = A \setminus cP$.*

Proof. From the previous corollary, we know that all the primies $\mathcal{Q}$ in $S^{-1}B'$ are invertible. Thus, B' is Dedekind and therefore integrally closed. □

We are most interested in the case $A = \mathbb{Z}$, $K = \mathbb{Q}$, and L is a number field. Suppose we start with θ integral over $\mathbb{Z}$ and such that $L = \mathbb{Q}(\theta)$. We want to find the integral closure $\mathcal{O}_L$ (also called the ring of integers and the maximal order of L). The following proposition (like Prop. 9.1 from the book) gives some info on it.

(Prop. 9.1, p. 47)

Proposition 20.4. *let $L = \mathbb{Q}(\theta)$ for integral θ. Write $|\Delta(\mathbb{Z}[\theta]/\mathbb{Z})| = dm^2$. Then the every element in the ring of integers $\mathcal{O}_L$ has the form*

$$\frac{a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}}{t}$$

with

$$\gcd(a_0, \ldots, a_{n-1}, t) = 1, \text{ and } t \mid m$$

Proof. Denote $\mathbb{Z}[\theta]$ as B'. If $p \not| m$, then setting $S = \mathbb{Z} \setminus p\mathbb{Z}$, the ring $S^{-1}B'$ is integrally closed. For any t such that $p|t$, any element of the form

$$\frac{a_0 + a_1\theta + \cdots + a_n\theta^{n-1}}{t}$$

is not in $S^{-1}B'$ and therefore not integral over $\mathbb{Z}$. Thus,

$$\frac{a_0 + a_1\theta + \cdots + a_n\theta^{n-1}}{t} \in \mathcal{O}_L$$

with $\gcd(a_0, \ldots, a_{n-1}, t) = 1$ implies that $t \mid m$.

□

Remark 20.5. It may very well be that $\mathbb{Z}[\theta]$ is already closed, so we may not have to allow *any* denominators at all not even denominators that divide m where $\Delta(\mathbb{Z}[\theta]/\mathbb{Z}) = dm^2$ for. Look at $\mathbb{Z}[\sqrt[3]{5}]$, for example, which has discriminant $3^3 5^2$, but is integrally closed.

Now, to change gears slightly, let's prove a few facts about our usual set-up when we take Galois of field K. In what follows, A is Dedekind, K is its field of fractions, L is a finite Galois extension of K, and B is the integral closure of A in M.

We have the following Lemma.

Lemma 20.6. *Keep the notation above. Let $\mathcal{P}$ be a maximal ideal of A. Let $\mathcal{Q}_1, \ldots, \mathcal{Q}_m$ be the primes in B for which $\mathcal{Q}_i \cap A = \mathcal{P}$. Then for every $\sigma \in \mathrm{Gal}(L/K)$, the set $\sigma(\mathcal{Q}_i)$ is one of the primes $\mathcal{Q}_j$ of B lying over $\mathcal{P}$. Furthermore, σ acts on the set $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_m\}$*

Proof. If y is integral over A, then so is $\sigma(y)$ for any $\sigma \in \mathrm{Gal}(L/K)$ (we showed this earlier). Thus $\sigma : B \longrightarrow B$ isomorphically. In particular, it sends any prime $\mathcal{Q}_i$ to some prime $\mathcal{Q}$. Since σ acts identically on K, we see that $\sigma(\mathcal{Q}_i \cap A) = \mathcal{Q}_i \cap A = \mathcal{P}$, so $\sigma(\mathcal{Q}_i) \cap A = \mathcal{P}$ and $\sigma(\mathcal{Q}_i) = \mathcal{Q}_j$ for some j.

To see that $\mathrm{Gal}(L/K)$ acts transitively $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_m\}$, we suppose that it didn't. Then we could divide $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_m\}$ into 2 disjoint sets

T and U such that $\sigma(\mathcal{Q}_i) \in T$ for each $\mathcal{Q}_i \in T$ and $\sigma(\mathcal{Q}_i) \in U$ for each $\mathcal{Q}_i \in U$. We then let

$$I = \prod_{\mathcal{Q}_i \in T} \mathcal{Q}_i \quad \text{and} \quad I = \prod_{\mathcal{Q}_j \in U} \mathcal{Q}_j.$$

We have $\sigma(I) = I$ and $\sigma(J) = J$. Now, I and J must be coprime, so we can find $x + y = 1$ for some $x \in I$ and $y \in J$. Then $x = 1 - y$ and

$$\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in I \cap K \subseteq \mathcal{P} \subseteq J,$$

(the last inclusion is because $\mathcal{P} \subseteq \mathcal{Q}_1 \cdots \mathcal{Q}_m$), but on the other hand

$$\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(1-y) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (1 - \sigma(y)) \in 1 + J,$$

which gives a contradiction. □

(Stuff from p. 32-33)

Theorem 20.7. *With notation as above (including L Galois over K), any maximal prime $\mathcal{P}$ factors in B as*

$$\mathcal{P}B = (\mathcal{Q}_1 \cdots \mathcal{Q}_m)^e$$

where the $\mathcal{Q}_i$ are distinct primes B. We also have

$$[B/\mathcal{Q}_i : A/\mathcal{P}] = [B/\mathcal{Q}_j : A/\mathcal{P}]$$

for any i, j.

Proof. Let $\mathcal{Q}_1, \ldots, \mathcal{Q}_m$ be all the primes in B lying over $\mathcal{P}$. Since $\mathcal{P} \subset A$ and every element $\sigma \in \mathrm{Gal}(L/K)$ acts identially on A, we have $\sigma(\mathcal{P}B) = \mathcal{P}\sigma(B) = \mathcal{P}B$. Writing

$$\mathcal{Q}_1^{e_1} \cdots \mathcal{Q}_m^{e_m} = \mathcal{P}B = \sigma(\mathcal{P}B) = \sigma(\mathcal{Q}_1)^{e_1} \cdots \sigma(\mathcal{Q}_m)^{e_m},$$

we see that $e_i = e_j$ for every i, j since for any i, j there is some σ such that $\sigma(\mathcal{Q}_i) = \sigma(\mathcal{Q}_j)$. Letting $e = e_i$, we have

$$\mathcal{P}B = (\mathcal{Q}_1 \cdots \mathcal{Q}_m)^e.$$

Since $\sigma \in \mathrm{Gal}(L/K)$ is an automorphism that fixes A, it induces an automorphism of $A/\mathcal{P}$ vector spaces from $B/\mathcal{Q}_i$ to $B/\sigma(\mathcal{Q}_i)$. Since σ acts transitively, this means that

$$[B/\mathcal{Q}_i : A/\mathcal{P}] = [B/\mathcal{Q}_j : A/\mathcal{P}]$$

for every i, j. □

We will want to work with norms of ideals in a bit. There is one more thing to prove about norms first. First a Lemma.

(stuff from p. 24)

Lemma 20.8. *Let L be a separable (not necessarily Galois) field extension of K of degree n, let M be the Galois closure of L over K, and let $G = \mathrm{Gal}(M/L)$. Let H_L be the subgroup of G that acts trivially on L and let $H\backslash G$ be a complete set of coset representatives for G over H. Then, for any $y \in L$, we have*

$$T_{L/K}(y) = \sum_{\sigma \in H\backslash G} \sigma(y)$$

and

$$\mathrm{N}_{L/K}(y) = \prod_{\sigma \in H\backslash G} \sigma(y)$$