Math 430
Notes from Class 10/20

Recall the following from last time.

Proposition 14.1. *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 $v_1, \dots, v_n$ as an A-module and that B' has a basis $w_1, \dots, w_n$ 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

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

Note that it follows from the above that when B is free with basis $\{v_1, \dots, v_n\}$, then $\Delta(B/A)$ is simply $\det[\mathrm{T}_{L/K}(v_i v_j)]$. It also follows if B is free and B' is as usual (integral over A with field of fractions L), then $B = B'$ if and only if $\Delta(B'/A) = \Delta(B/A)$.

Corollary 14.2. *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.

Corollary 14.3. *Let B' be as usual. Let $\mathfrak{q}$ be maximal in B' and let $\mathfrak{p} = \mathfrak{q} \cap A$. Then $\mathfrak{q}$ is invertible whenever $\mathfrak{p}^2$ doesn't divide $\Delta(B'/A)$.*

Proof. We replace B' with $S^{-1}B'$, where $S = A \setminus \mathfrak{p}$, which we'll just write as B', and replace A with $A_{\mathfrak{p}}$. 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 in L. Then $B' = B$ if and only if $\Delta(B/A) = \Delta(B'/A)$ and $\Delta(B'/A) = I^2\Delta(B/A)$ for some ideal I. So if $B' \neq B$, then $\mathfrak{p}^2$ divides $\Delta(B'/A)$. Thus, if $\mathfrak{p}^2$ doesn't divide $\Delta(B'/A)$, then $B = B'$.

□

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 14.4. *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 $p \nmid m$, 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 $t \mid m$. □

Now, to change gears slightly, let's prove a few facts about our usual set-up when we take Galois extensions 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 14.5. *Keep the notation above. Let $\mathfrak{p}$ be a maximal ideal of A. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ be the primes in B for which $\mathfrak{q}_i \cap A = \mathfrak{p}$. Then for every $\sigma \in \mathrm{Gal}(L/K)$, the set $\sigma(\mathfrak{q}_i)$ is one of the primes $\mathfrak{q}_j$ of B lying over $\mathfrak{p}$. Furthermore, σ acts transitively on the set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$*

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 $\mathfrak{q}_i$ to some prime $\mathfrak{q}$. Since σ acts identically on K, we see that $\sigma(\mathfrak{q}_i \cap A) = \mathfrak{q}_i \cap A = \mathfrak{p}$, so $\sigma(\mathfrak{q}_i) \cap A = \mathfrak{p}$ and $\sigma(\mathfrak{q}_i) = \mathfrak{q}_j$ for some j.

To see that $\mathrm{Gal}(L/K)$ acts transitively $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$, we suppose that it didn't. Then we could divide $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$ into 2 disjoint sets T and U such that $\sigma(\mathfrak{q}_i) \in T$ for each $\mathfrak{q}_i \in T$ and $\sigma(\mathfrak{q}_i) \in U$ for each $\mathfrak{q}_i \in U$. We then let

$$I = \prod_{\mathfrak{q}_i \in T} \mathfrak{q}_i \quad \text{and} \quad J = \prod_{\mathfrak{q}_j \in U} \mathfrak{q}_j.$$

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

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

(the last inclusion is because $\mathfrak{p} \subseteq \mathfrak{q}_1 \cdots \mathfrak{q}_m$), 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 14.6. *With notation as above (including L Galois over K), any maximal prime $\mathfrak{p}$ factors in B as*

$$\mathfrak{p}B = (\mathfrak{q}_1 \cdots \mathfrak{q}_m)^e$$

where the $\mathfrak{q}_i$ are distinct primes B. We also have

$$[B/\mathfrak{q}_i : A/\mathfrak{p}] = [B/\mathfrak{q}_j : A/\mathfrak{p}]$$

for any i, j.

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

$$\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_m^{e_m} = \mathfrak{p}B = \sigma(\mathfrak{p}B) = \sigma(\mathfrak{q}_1)^{e_1} \cdots \sigma(\mathfrak{q}_m)^{e_m},$$

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

$$\mathfrak{p}B = (\mathfrak{q}_1 \cdots \mathfrak{q}_m)^e.$$

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

$$[B/\mathfrak{q}_i : A/\mathfrak{p}] = [B/\mathfrak{q}_j : A/\mathfrak{p}]$$

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 14.7. *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 $H = H_L$ 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

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

Proof. Let $y_1, \ldots, y_m$ be the conjugates of y. Then we know that

$$\mathrm{T}_{L/K}(y) = [L : K(y)] \left(\sum_{i=1}^{m} y_i \right)$$

and

$$\mathrm{N}_{L/K}(y) = \left(\prod_{i=1}^{m} y_i \right)^{[L:K(y)]}$$

(since the characteristic polynomial of y must be a power of the minimal polynomial of y and for the degrees to match up that power must be $[L : K(y)]$).

Now, let H_y be the subgroup of G that acts identically on $K(y)$. Then H is a subgroup of H_y and $H\backslash G$ will contain will contain $[H_y : H] = [L : K(y)]$ copies of $H_y\backslash G$.

Then

$$\begin{aligned} \sum_{\sigma \in H\backslash G} \sigma(y) &= [L : K(y)] \sum_{\sigma \in H_y\backslash G} \sigma(y) \\ &= [L : K(y)] \left(\sum_{i=1}^{m} y_i \right) = \mathrm{T}_{L/K}(y), \end{aligned}$$

and

$$\begin{aligned} \prod_{\sigma \in H\backslash G} \sigma(y) &= \prod_{\sigma \in H_y\backslash G} \sigma(y)^{[L:K(y)]} \\ &= \left(\prod_{i=1}^{m} y_i \right)^{[L:K(y)]} = \mathrm{N}_{L/K}(y)^{[L:K(y)]}, \end{aligned}$$

as desired. □