Math 568 Tom Tucker
NOTES FROM CLASS 10/29

Last time, we had finished proving the following.

Corollary 14.1. *Let $\mathcal{P}$ be a prime of A. If $\Delta(B'/A)$ is not contained in $\mathcal{P}^2$, then $S^{-1}B'$ is integrally closed where $S = A \setminus \mathcal{P}$.*

Let's develop a general technique for finding the integral closure of a Dedekind domain A.

I will start with two examples

Example 14.2. Let $A = \mathbb{Z}$ and let $B' = A[\xi_{p^n}]$ where ξ_{p^n} is a primitive p^n-th root of unity. The minimal monic for ξ_{p^n} is $F(x) = x^{p^n - p^{n-1}} + x^{p^n - 2p^{n-1}} + \cdots + 1$. We have seen that $F(x+1)$ is Eistenstein and thus irreducible. Now, $\Delta(F)$ must divide the discriminant of $x^{p^n} - 1$. Thus, p is the only prime that can divide $\Delta(F)$. Thus, we see that $B'_{\mathcal{Q}}$ is integrally closed for any $\mathcal{Q}$ such that $\mathcal{Q} \cap \mathbb{Z} \neq (p)$. Now, let's check the primes lying over p. We see that since $F(x) \equiv (x-1)^{p^n - p^{n-1}} \pmod{p}$ that there is exactly one such prime and it is $(p, \xi_{p^n} - 1)$. Since $\mathrm{N}(\xi_{p^n} - 1) = p$, we see that p is in the ideal generated by $(\xi_{p^n} - 1)$, so this ideal $\mathcal{Q}$ is principal. Thus $B'_{\mathcal{Q}}$ is integrally closed so B' is 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). Prop. 9.1 from the book gives some info on it.

First a lemma. Note that when working over $\mathbb{Z}$, we can (by abuse of notation) just take $\Delta(B'/\mathbb{Z})$ to be the positive number generating the ideal $\Delta(B'/\mathbb{Z})$.

Lemma 14.3. *Let L be a finite extension of $\mathbb{Q}$ and let B' be an integral extension of $\mathbb{Q}$ with field of fractions equal to L. Let $\mathcal{O}_L$ denote the integral closure of $\mathbb{Z}$ in L. Suppose that $\alpha \in \mathcal{O}_L$ has the property that $p^n\alpha \in B'$ but $p^j\alpha \notin B'$ for $j < n$. Then $p^{2n} | \Delta(B'/A)\Delta(\mathcal{O}_L/\mathbb{Z})^{-1}$.*

Proof. Let $B_i = B'[p^i\alpha]$, so that we have a chain

$$B_n \subset B_{n-1} \subset \cdots \subset B_0.$$

Then $B_n = B'$ and $S^{-1}B_i \neq S^{-1}B_{i-1}$ for $i = 1 \ldots n$ (where $S = A \setminus \mathcal{P}$). Thus, we have $p^2 | \Delta(B_i/B_{i-1})$ for $i = 1, \ldots n$. Thus, p^{2n} divides $\Delta(B'/B_0)$. Since $B_0 \subseteq \mathcal{O}_L$, the result follows. □

(Prop. 9.1, p. 47)

Proposition 14.4. *Let $L = \mathbb{Q}(\theta)$ for integral θ of degree n. Write $|\Delta(\mathbb{Z}[\theta]/\mathbb{Z})| = dm^2$, where d is square-free. 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. Let $B' = \mathbb{Z}[\theta]$. Suppose that $\alpha \in L$ is in $\mathcal{O}_L$. We write

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

where $\gcd(a_0, \ldots, a_{n-1}, t) = 1$. Write $t = p_1^{r_1} \ldots p_s r_s$. For each i, let $t_i = t/p^{r_i}$. Then $p^{r_i}(t_i\alpha) \in B'$ but $p^j(t_i\alpha) \notin B'$ for $j < r_i$. Thus, p^{2r_i} must divide dm^2, so p^{r_i} must divide m, so t must divide m, as desired. □

Remark 14.5. 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.

By the way, we can say a bit more. In fact, we have

$$|\mathcal{O}_L/B'|^2 = \frac{\Delta(B'/A)}{\Delta(\mathcal{O}_L/A)}$$

where $\mathcal{O}_L/B'$ is the additive group quotient of $\mathcal{O}_L$ by B'.

This requires a little more work to prove, but you can use this fact when you compute the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt[3]{19})$.

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.