Math 430

Notes from Class 09/30

Last time we proved the following.

Theorem 10.1. *Let A be a Dedekind domain with field of fractions K. Let L be a finite separable extension of K and let B be the integral closure of A in L. Then B is Dedekind.*

We will mostly work with separable extensions, but it is easy to prove the following as well. We will leave part of this proof as an exercise.

We will use the following lemma, to be proved on your homework.

Lemma 10.2. *Let A be an integral domain such that (1) $A_{\mathfrak{m}}$ is Noetherian for every maximal ideal A and (2) every proper nonzero ideal of A is contained in at most finitely many maximal ideals. Then A is Noetherian.*

Theorem 10.3. *Let A be a Dedekind domain with field of fractions K. Let L be a totally inseparable extension of K and let B be the integral closure of A in L. Then B is Dedekind.*

Proof. We begin with a general observation: an element α is integral over a ring R if and only if α^m is for any positive integer m since α^m is in $R[\alpha]$ and $g(\alpha^m) = 0$ means $h(\alpha) = 0$ for $h = g(x^m)$. Now, if L is totally inseparable over K, then there is a q such that z^q is in K for all $z \in L$. Thus, $z \in L$ is integral over A if and only if $z^q \in A$, so B is simply the set of all elements of L whose q-th power is in A.

Now, let $\mathfrak{q}$ be a maximal ideal in B (which we know is one-dimensional) and let $\mathfrak{p} = \mathfrak{q} \cap A$. Let $S = A \setminus \mathfrak{p}$. We can show that $B_{\mathfrak{q}} = S^{-1}B$ by observing that if $z/r \in B_{\mathfrak{q}}$, then, since $r^q \in A$ and $r^q \notin \mathfrak{p}$, we have $r^q \in S$, so $z/r = r^{q-1}z/r^q$, which is an element of $S^{-1}B$. Since there is a bijection between primes in B that don't meet S and primes in $S^{-1}B$, it follows that $\mathfrak{q}$ is the only prime in B such that $\mathfrak{q} \cap A = \mathfrak{p}$.

Let I be a proper ideal in B. Then $I \cap A$ is contained in finitely many maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. For each i, let $\mathfrak{q}_i$ be the unique prime in B such that $\mathfrak{q}_i \cap A = B$. Then $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ are the only primes in B that can contain I. Thus, I is contained in finitely many primes of B.

We will be done now by Lemma 10.2 if we an show that $B_{\mathfrak{q}}$ is a DVR for every maximal ideal $\mathfrak{q}$ of B (since DVRs are Noetherian). To see this note that as above $B_{\mathfrak{q}}$ is the set of all $z \in L$ such that $z^q \in A_{\mathfrak{p}}$ where $\mathfrak{p} = A \cap \mathfrak{q}$. For $x \in L$, we define $w(x) = v(x^q)$. Then w is clearly multiplicative and $w(x + y) = v(x^q + y^q) \geq \max(w(x), w(y))$. Furthermore, w maps L onto $m\mathbb{Z}$ for some m (dividing q), so a suitable multiple of w is a discrete valuation L and $B_{\mathfrak{q}}$ is a DVR.

□

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 $\mathfrak{p} \subset A$. What can we say about how $B\mathfrak{p}$ factors?

Let's start with some basics. We write

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

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

$$A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}_i.$$

We call the index $[B/\mathfrak{q}_i : A/\mathfrak{p}]$ the **relative degree** of $\mathfrak{q}_i$ over $\mathfrak{p}$. 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 10.4. 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 10.5. *With the set-up above, for $\mathfrak{p}$ a maximal ideal of A we have*

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

and $f_i = [B/\mathfrak{q}_i : A/\mathfrak{p}]$ with

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

Proof. We know that

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

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

$$S^{-1}B\mathfrak{p} = S^{-1}B\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_m^{e_m}.$$

Thus, we have

$$S^{-1}B/S^{-1}B\mathfrak{p} \cong \sum_{i=1}^{m}(S^{-1}B)/(S^{-1}B\mathfrak{q}_i^{e_i}) \cong \sum_{i=1}^{m} B_{\mathfrak{q}_i}/(B_{\mathfrak{q}_i}\mathfrak{q}_i^{e_i}).$$

Thus, we see that

$$\dim_{A_\mathfrak{p}/A_\mathfrak{p}\mathfrak{p}}(\sum_{i=1}^{m} B_{\mathfrak{q}_i}/(B_{\mathfrak{q}_i}\mathfrak{q}_i^{e_i})) = n.$$

It will suffice to show, then, that

$$\dim_(A_\mathfrak{p}/A_\mathfrak{p}\mathfrak{p})(\sum_{i=1}^{m} B_{\mathfrak{q}_i}/(B_{\mathfrak{q}_i}\mathfrak{q}_i^{e_i})) = \sum_{i=1}^{m} e_i f_i,$$

which would follow from

$$\dim_{(A_\mathfrak{p}/A_\mathfrak{p}\mathfrak{p})}(B_{\mathfrak{q}_i}/(B_{\mathfrak{q}_i}\mathfrak{q}_i^{e_i})) = e_i f_i.$$

Since we can write

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

we need only show that

$$\dim_{A_\mathfrak{p}/\mathfrak{p}}((B_{\mathfrak{q}_i}\mathfrak{q}_i^j)/(B_{\mathfrak{q}_i}\mathfrak{q}_i^{j+1})) = f_i,$$

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