Math 430

Notes from Class 09/29

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.*

On the next few homework sets, we will work through a proof that this is also true when L is purely inseparable over K. Putting these two together will prove it for all finite extensions.

Proposition 10.2. *Let A be a domain, $A \neq 0$, and let B be integral over A. Then for any prime $\mathfrak{p}$ of A, we have $B\mathfrak{p} \neq B$.*

Proof. Suppose that $B\mathfrak{p} = 1$. Then there are $b_1, \ldots, b_m \in B$ and $x_1, \ldots, x_m \in \mathfrak{p}$ such that 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 $\mathfrak{p}C = C$. Let $N = A_\mathfrak{p}C$; then N is finitely generated and $A_\mathfrak{p}\mathfrak{p}N = N$. Since $A_\mathfrak{p}$ is local, we must have $N = 0$ by Nakayama's lemma, which gives a contradiction, since $A \neq 0$. $\square$

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 10.3. *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. $\square$

One more thing I wanted to mention about factorizations of ideals in Dedekind domains. If $I \subseteq \mathfrak{p}$, then $\mathfrak{p}$ must appear in the factorization of I. This follows from the fact that $R_\mathfrak{p}I$ is positive power of $R_\mathfrak{p}\mathfrak{p}$, which would not happen if I didn't have $\mathfrak{p}$ 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 $\mathfrak{p} \subset A$. 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

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

Combining this with homework results plus further localization, we obtain

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

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. □

Next time we will prove the following.

Proposition 10.6. *Let A be Dedekind. Let $\mathcal{P}$ be a maximal ideal of A and let α be an integral element of a finite separable extension of the field of fractions of A. Suppose that G is the minimal monic for α over A and that the reduction mod $\mathcal{P}$ of G, which we call $\bar{G}$ factors as*

$$\bar{G} = \bar{g}_1^{r_1} \cdots \bar{g}_m^{r_m},$$

with the $\bar{g}_i$ distinct, irreducible, and monic. Then choosing monic $g_i \in A[x]$ such that $g_i \equiv \bar{g}_i \pmod{\mathcal{P}}$, we have

(1) *$\mathcal{Q}_i = A[\alpha](g_i(\alpha), \mathcal{P})$ is a prime for each i; and*
(2) *r_i is the smallest positive integer such that*

$$R_{\mathcal{Q}_i}(\mathcal{Q}_i)^{r_i} \subseteq R_{\mathcal{Q}_i}\mathcal{P}.$$