Math 568 Tom Tucker
NOTES FROM CLASS 10/15

We want to work towards calculating the integral closure of a Dedekind domain in a finite separable extension.

Let's begin with the following Lemma, the proof of which is obvious.

Lemma 10.1. *Let I be an ideal in Dedekind domain. Write*

$$I = \mathcal{Q}_1^{e_1} \cdots \mathcal{Q}_m^{e_m}$$

where the $\mathcal{Q}_i$ are distinct primes. Then

$$e_i = \min\{t \mid M_{\mathcal{Q}_i}(\mathcal{Q}_i)^t \subseteq M_{\mathcal{Q}_i} I\}.$$

Proposition 10.2. *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*

$$\bar{G} = \bar{g}_1^{t_1} \cdots \bar{g}_m^{t_m},$$

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. *t_i is the smallest positive integer such that*

$$A[\alpha]_{\mathcal{Q}_i}(\mathcal{Q}_i)^{t_i} \subseteq A[\alpha]_{\mathcal{Q}_i}\mathcal{P}.$$

Proof. The proof is quite simple. Note that $A[\alpha]$ is isomorphic to $A[x]/G(x)$. We work in the ring $A[\alpha]/\mathcal{P}A[\alpha] \cong A[x]/(G(x), \mathcal{P})$, which is isomorphic to

$$(A/\mathcal{P})/(\bar{G}(x)) \cong \sum_{i=1}^{m} (A/\mathcal{P})[x]/\bar{g}_i(x)^{t_i}.$$

Since $\bar{g}_i(x)$ is irreducible in $(A/\mathcal{P})[x])$, we see that

$$(A/\mathcal{P})[x]/\bar{g}_i(x)$$

is a field, so $\mathcal{Q}_i$ is prime ideal since

$$A[\alpha]/\mathcal{Q}_i \cong (A/\mathcal{P})[x]/\bar{g}_i(x).$$

Now, since each $g_j(\alpha)$ is a unit in $A[\alpha]_{\mathcal{Q}_i}$ for $j \neq i$, we have

$$A[\alpha]_{\mathcal{Q}_i}/A[\alpha]_{\mathcal{Q}_i}\mathcal{P} \cong (A/\mathcal{P})[x]/\bar{g}_i(x)^{t_i},$$

so t_i is the smallest integer such that

$$g_i(\alpha)^{t_i} \subseteq A[\alpha]_{\mathcal{Q}_i}\mathcal{P}.$$

□

Corollary 10.3. *(Kummer) With notation as above, if $A[\alpha]$ is Dedekind, then*

$$A[\alpha]\mathcal{P} = \mathcal{Q}_1^{e_1} \cdots \mathcal{Q}_m^{e_m}.$$

Proof. Immediate from the lemma and proposition above. □

We will also want to deal with rings that are not Dedekind domains. Frequently, we will want to take rings of the form $A[\alpha]$ and try to decide whether or not they are in fact Dedekind. Here's a useful fact.

Proposition 10.4. *With notation as above, if $t_i = 1$ then the prime $A[\alpha](\mathcal{P}, g_i(\alpha))$ is invertible. If $t_i > 1$, then $\mathcal{Q}_i$ is invertible if and only if all the coefficients of the remainder mod g_i of G are in $\mathcal{P}^2$, i.e. if writing*

$$G(x) = q(x)g_i(x) + r(x), \tag{1}$$

we have $r(x) \in \mathcal{P}^2[x]$

Proof. For each j, select a monic polynomial $g_j \in A[x]$ such that $g_j \equiv g_j \pmod{\mathcal{P}}$. Since

$$g_1(x)^{t_1} \cdots g_m(x)^{t_m} \equiv f(x) \pmod{\mathcal{P}}$$

it is clear that

$$g_1(\alpha)^{t_1} \cdots g_m(\alpha)^{t_m} \in \mathcal{P}, \tag{2}$$

since α is a root of f. Furthermore, we know that for $j \neq i$, we must have that $g_i(\alpha)$ and $g_j(\alpha)$ are coprime. Now, suppose that $t_i = 1$ for some i; let $\mathcal{Q}_i = A[\alpha](g_i(\alpha), \mathcal{P})$. When we localize at $\mathcal{Q}_i$, all of the $g_j(\alpha)$ for which $j \neq i$ become units. Thus, (2) has the form $g_i(\alpha)u \in \mathcal{P}$ for u a unit, so $g_i(\alpha) \subset A[\alpha]\mathcal{P}$. We know that there exists a $\pi \in A$ such that $A_{\mathcal{P}} = A_{\mathcal{P}}\pi$ since $\mathcal{P}$ is invertible in A. Then

$$A[\alpha]_{\mathcal{Q}_i}(g_i(\alpha), \mathcal{P}) = A[x]_{\mathcal{Q}_i}\pi$$

so $\mathcal{Q}_i$ is invertible.

Now suppose that $m_i > 1$. Let $\phi : A_{\mathcal{P}}[x] \longrightarrow A_{\mathcal{P}}[\alpha]$ be the natural quotient map obtained by sending x to α. The kernel of this map is $A_{\mathcal{P}}[x]G$. The prime $\mathcal{Q}_i$ in $A_{\mathcal{P}}[\alpha]$ is generated by $(\pi, g_i(\alpha))$, so $\phi^{-1}(\mathcal{Q})$ is generated by $(\pi, g_i(x))$ since $G(x)$ is in the ideal generated by $(\pi, g_i(x))$ (since $g_i(x)$ divides G modulo $\mathcal{P}$). Denote $\phi^{-1}(\mathcal{Q})$ as J. It is easy to see that

$$\dim_{A_{\mathcal{P}}/A_{\mathcal{P}}\mathcal{P}} J/J^2 = 2d$$

where d is the degree of g_i since

$$\{\pi, \pi x, \ldots, \pi x^{d-1}, g_i, g_i x, \ldots, g_i x^{d-1}\}$$

is a basis for J/J^2 as a $A_{\mathcal{P}}/A_{\mathcal{P}}\mathcal{P}$-module. We see that ϕ induces a map

$$\tilde{\phi} : J/J^2 \longrightarrow \mathcal{Q}_i/\mathcal{Q}_i^2$$

which has kernel $A_{\mathcal{P}}[x]G(x) \pmod{J^2}$. From (1), this is generated by the remainder $r(x)$. Here we use the fact $q(x) \in J$; this follows from the fact that $t_i > 1$ so $q(x)$ is divisible by $g_i(x)$ modulo $\mathcal{P}$, which means that $q(x) \in A_{\mathcal{P}}[x](\mathcal{P}, g_i(x))$.

Now, since $\deg r < \deg g$, we have $r \in J^2$ if and only if $r \in \pi^2 A_{\mathcal{P}}[x]$. Thus, we see that

$$\dim_{A_{\mathcal{P}}/A_{\mathcal{P}}\mathcal{P}}(\mathcal{Q}_i/\mathcal{Q}_i^2) < 2d$$

if and only if $r \notin \pi^2 A_{\mathcal{P}}[x]$. Since

$$\dim_{A_{\mathcal{P}}/A_{\mathcal{P}}\mathcal{P}}(\mathcal{Q}_i/\mathcal{Q}_i^2) = d \dim_{A[\alpha]_{\mathcal{Q}_i}/A_[\alpha]_{\mathcal{Q}_i}\mathcal{Q}_i}(\mathcal{Q}_i/\mathcal{Q}_i^2)$$

we thus have

$$\dim_{A_{\mathcal{P}}/A_{\mathcal{P}}\mathcal{P}}(\mathcal{Q}_i/\mathcal{Q}_i^2) = 1$$

if and only if $r \notin \pi^2 A_{\mathcal{P}}[x]$.

$\square$