Math 430

Notes from Class 10/02

More on factoring primes in extensions. Remember we can only do this well for separable extensions.

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

Lemma 11.1. *Let I be an ideal in Dedekind domain. Write*

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

where the $\mathfrak{q}_i$ are distinct primes. Then

$$e_i = \min\{m \mid R_{\mathfrak{q}_i}(\mathfrak{q}_i)^m \subseteq R_{\mathfrak{q}_i} I\}.$$

Proposition 11.2. *Let A be Dedekind. Let $\mathfrak{p}$ 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 $\mathfrak{p}$ 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 $g_i \equiv \bar{g}_i \pmod{\mathfrak{p}}$, we have

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

$$R_{\mathfrak{q}_i}(\mathfrak{q}_i)^{r_i} \subseteq R_{\mathfrak{q}_i}\mathfrak{p}.$$

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

$$(A/\mathfrak{p})/(\bar{G}(x)) \cong \sum_{i=1}^{m} (A/\mathfrak{p})[x]/\bar{g}_i(x)^{r_i}.$$

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

$$(A/\mathfrak{p})[x]/\bar{g}_i(x)$$

is a field, so $\mathfrak{q}_i$ is prime ideal since

$$A[\alpha]/\mathfrak{q}_i \cong (A/\mathfrak{p})[x]/\bar{g}_i(x).$$

Now,

$$A[\alpha]_{\mathfrak{q}_i}/A[\alpha]_{\mathfrak{q}_i}\mathfrak{p} \cong (A/\mathfrak{p})[x]/\bar{g}_i(x)^{r_i},$$

so r_i is the smallest integer such that

$$g_i(x)^{r_i} \subseteq R_{\mathfrak{q}_i}\mathfrak{p}.$$

□

Corollary 11.3. *(Kummer) With notation as above, if $A[\alpha]$ is Dedekind, then*

$$A[\alpha]\mathfrak{p} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_m^{e_m}.$$

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 11.4. *With notation as above, if $r_i = 1$ then the prime $A[\alpha](\mathfrak{p}, g_i(\alpha))$ is invertible.*

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

$$g_1(x)^{r_1} \cdots g_m(x)^{r_m} \equiv f(x) \pmod{\mathfrak{p}}$$

it is clear that

$$g_1(\alpha)^{r_1} \cdots g_m(\alpha)^{r_m} \in \mathfrak{p}, \tag{1}$$

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 $r_i = 1$ for some i; let $\mathfrak{q}_i = A[\alpha](g_i(\alpha), \mathfrak{p})$. When we localize at $\mathfrak{q}_i$, all of the $g_j(\alpha)$ for which $j \neq i$ become units. Thus, (1) has the form $g_i(\alpha)u \in \mathfrak{p}$ for u a unit, so $g_i(\alpha) \subset A[\alpha]\mathfrak{p}$. We know that there exists a $\pi \in A$ such that $A_{\mathfrak{p}} = A_{\mathfrak{p}}\pi$ since $\mathfrak{p}$ is invertible in A. Then

$$A[\alpha]_{\mathfrak{q}_i}(g_i(\alpha), \mathfrak{p}) = A[x]_{\mathfrak{q}_i}\pi$$

so $\mathfrak{q}_i$ is invertible. □

Note: In fact, it is possible to prove the following though the proof is more difficult.

Proposition 11.5. *With notation as above, if $r_i = 1$ then the prime $A[\alpha](\mathfrak{p}, g_i(\alpha))$ is invertible. If $r_i > 1$, then $\mathfrak{q}_i$ is invertible if and only if all the coefficients of the remainder mod g_i of G are not all in $\mathfrak{p}^2$, i.e. if writing*

$$G(x) = q(x)g_i(x) + r(x),$$

we have $r(x) \notin \mathfrak{p}^2[x]$.

Example 11.6. Let d be a square-free odd integer and let $K = \mathbb{Q}(\sqrt{d})$. We know that $\mathbb{Z}[sqrtd]$ is a Dedekind domain if and only if d is congruent to 1 mod 4. Then $x^2 - d$ factors as $(x-2)^2$ modulo 2. To see if the prime $(2, x-2)$ is invertible we divide $x-2$ into $(x-2)^2$. We get a remainder of $d^2 - d$, which is divisible by 2^2 exactly when d is congruent to 1 modulo 4. So the prime above 2 is not invertible in this case. It is not hard to see that all other primes in $\mathbb{Z}[sqrtd]$ are invertible

How can we tell which primes we have to worry about (by this, I mean those for which some r_i is greater than 1)? We can use something called the discriminant of a finitely generated integral extension of rings B over A. We will work with several formulations, all of which are equivalent. Here's the definition of the discriminant of a polynomial.

Definition 11.7. Let K be a field and let F be the monic polynomial

$$F(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Then, writing

$$F(x) = \prod_{i=1}^{n}(x - \alpha_i)$$

where α_i are the roots of F in some algebraic closure of K, the discriminant $\Delta(F)$ is defined to be

$$\Delta(F) = (-1)^{n(n-1)/2}\prod_{i \neq j}(\alpha_i - \alpha_j) = \prod_{i<j}(\alpha_i - \alpha_j)^2.$$

Why is this discriminant useful? Because of the following obvious fact:

$$\Delta(F) \neq 0 \Leftrightarrow F \text{ does not have multiple roots.}$$