5 Factoring primes in Dedekind extensions

5.1 Ramification and inertia

Let us recall the "$AKLB$ setup": we are given a Dedekind domain A (assumed not a field) with fraction field K and a finite separable extension L/K, and we define B to be the integral closure of A in L. In the previous lecture we proved that B is a Dedekind domain and L with fraction field.

To simplify the language, whenever we have a Dedekind domain A, by a *prime* of A (or of its fraction field K), we mean a **nonzero** prime ideal; the prime elements of A are precisely those that generate nonzero principal prime ideals, so this generalizes the usual terminology. Note that 0 is (by definition) not prime, even though (0) is a prime ideal; when we refer to a prime of A we are specifically excluding the zero ideal, equivalently (since $\dim A = 1$), we are restricting to maximal ideals.

If $\mathfrak{p}$ is a prime of A, the ideal $\mathfrak{p}B$ is not necessarily a prime of B, but it can be uniquely factored in the Dedekind domain B as

$$\mathfrak{p}B = \prod_{\mathfrak{q}} \mathfrak{q}^{e_{\mathfrak{q}}}.$$

Our main goal for this lecture and the next is to understand the relationship between the prime $\mathfrak{p}$ and the primes $\mathfrak{q}$ dividing $\mathfrak{p}B$. Such prime ideals $\mathfrak{q}$ are said to *lie over* or *above* the prime ideal $\mathfrak{p}$. As an abuse of notation, we will often write $\mathfrak{q}|\mathfrak{p}$ to indicate this relationship (there is little risk of confusion, the prime $\mathfrak{p}$ is not divisible by any primes of A other than itself). We now note that the primes $\mathfrak{q}$ lying above $\mathfrak{p}$ are precisely those whose contraction to A is equal to $\mathfrak{p}$. This applies not only in the $AKLB$ setup, but whenever A is an integral domain of dimension one contained in a Dedekind domain B.

Lemma 5.1. *Let A be a domain of dimension one contained in a Dedekind domain B. Let $\mathfrak{p}$ be a prime of A and let $\mathfrak{q}$ be a prime of B. Then $\mathfrak{q}|\mathfrak{p}$ if and only if $\mathfrak{q} \cap A = \mathfrak{p}$.*

Proof. If $\mathfrak{q}$ divides $\mathfrak{p}B$ then it contains $\mathfrak{p}B$, and then $\mathfrak{q}\cap A$ contains $\mathfrak{p}B\cap A$ which contains $\mathfrak{p}$; the ideal $\mathfrak{p}$ is maximal and $\mathfrak{q} \cap A \neq A$, so $\mathfrak{q} \cap A = \mathfrak{p}$. Conversely, if $\mathfrak{q} \cap A = \mathfrak{p}$ then $\mathfrak{q} = \mathfrak{q}B$ certainly contains $(\mathfrak{q} \cap A)B = \mathfrak{p}B$, and B is a Dedekind domain, so $\mathfrak{q}$ divides $\mathfrak{p}B$. $\square$

The primes $\mathfrak{p}$ of A are all maximal ideals, so each has an associated residue field $A/\mathfrak{p}$, and similarly for primes $\mathfrak{q}$ of B. If $\mathfrak{q}$ lies above $\mathfrak{p}$ then we may regard the residue field $B/\mathfrak{q}$ as a field extension of $\mathfrak{q}$; indeed, the kernel of the map $A \hookrightarrow B \to B/\mathfrak{q}$ is $\mathfrak{p} = A\cap\mathfrak{q}$, and the induced map $A/\mathfrak{p} \to B/\mathfrak{q}$ is a ring homomorphism of fields, hence injective.

Definition 5.2. Assume $AKLB$, and let $\mathfrak{p}$ be a prime of A. The exponent $e_{\mathfrak{q}}$ in the factorization $\mathfrak{p}B = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_{\mathfrak{q}}}$ is the *ramification index of* $\mathfrak{q}$ and the degree $f_{\mathfrak{q}} = [B/\mathfrak{q} : A/\mathfrak{p}]$ is the *residue degree*, or *local degree*, of $\mathfrak{q}$. In situations where more than one relative extension of Dedekind domains is under consideration, we may write $e_{\mathfrak{q}/\mathfrak{p}}$ for $e_{\mathfrak{q}}$ and $f_{\mathfrak{q}/\mathfrak{p}}$ for $f_{\mathfrak{q}}$.

The residue degree $f_{\mathfrak{q}}$ is also called its *inertia degree* of $\mathfrak{q}$ for reasons that will be explained in later lectures. The set of primes $\mathfrak{q}$ lying above $\mathfrak{p}$ is called the *fiber* above $\mathfrak{p}$ which we may denote $\{\mathfrak{q}|\mathfrak{p}\}$; it is the fiber of the surjective map $\operatorname{Spec} B \to \operatorname{Spec} A$ defined by $\mathfrak{q} \mapsto \mathfrak{q} \cap A$.

Lemma 5.3. *Let A be a Dedekind domain with fraction field K, let $M/L/K$ be a tower of finite separable extension, and let B and C be the integral closures of A in L and M*

respectively. Then C is the integral closure of B in M, and if $\mathfrak{r}$ is a prime of M lying above a prime $\mathfrak{q}$ of L lying above a prime $\mathfrak{p}$ of K then $e_{\mathfrak{r}/\mathfrak{p}} = e_{\mathfrak{r}/\mathfrak{q}}e_{\mathfrak{q}/\mathfrak{p}}$ and $f_{\mathfrak{r}/\mathfrak{p}} = f_{\mathfrak{r}/\mathfrak{q}}f_{\mathfrak{q}/\mathfrak{p}}$.

Proof. Easy exercise. $\square$

Example 5.4. Let $A = \mathbb{Z}$, with $K = \operatorname{Frac} A = \mathbb{Q}$, and let $L = \mathbb{Q}(i)$ with $[L : K] = 2$. The prime $\mathfrak{p} = (5)$ factors in $B = \mathbb{Z}[i]$ into two distinct prime ideals:

$$5\mathbb{Z}[i] = (2 + i)(2 - i)$$

The prime $(2 + i)$ has ramification index $e_{(2+i)} = 1$, and $e_{(2-i)} = 1$ as well. The residue field $\mathbb{Z}/(5)$ is isomorphic to the finite field $\mathbb{F}_5$, and we also have $\mathbb{Z}[i]/(2 + i) \simeq \mathbb{F}_5$ (as can be determined by counting the $\mathbb{Z}[i]$-lattice points in a fundamental parallelogram of the sublattice $(2 + i)$ in $\mathbb{Z}[i]$), so $f_{(2+i)} = 1$, and similarly, $f_{(2-i)} = 1$.

By contrast, the $\mathfrak{p} = (7)$ remains prime in $B = \mathbb{Z}[i]$; its prime factorization is simply

$$7\mathbb{Z}[i] = (7),$$

where now (7) denotes a principal ideal in B (this is clear from context). The ramification index of (7) is thus $e_{(7)} = 1$, but its residue field degree is $f_{(7)} = 2$, because $\mathbb{Z}/(7) \simeq \mathbb{F}_7$, but $\mathbb{Z}[i]/(7) \simeq \mathbb{F}_{49}$ has dimension 2 has an $\mathbb{F}_7$-vector space.

The prime $\mathfrak{p} = (2)$ factors as

$$(2) = (1 + i)^2,$$

since $(1+i)^2 = (1+2i-1) = (2i) = (2)$ (note that i is a unit). You might be thinking that $(2) = (1 + i)(1 - i)$ factors into distinct primes, but note that $(1 + i) = -i(1 + i) = (1 - i)$. Thus $e_{(1+i)} = 2$, and $f_{(1+i)} = 1$ because $\mathbb{Z}/(2) \simeq \mathbb{F}_2 \simeq \mathbb{Z}[i]/(1 + i)$.

Let us now compute the sum $\sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}}$ for each of the primes $\mathfrak{p}$ we factored above:

$$\sum_{q|(2)} e_{\mathfrak{q}} f_{\mathfrak{q}} = e_{(1+i)} f_{(1+i)} = 2 \cdot 1 = 2,$$
$$\sum_{q|(5)} e_{\mathfrak{q}} f_{\mathfrak{q}} = e_{(2+i)} f_{(2+i)} + e_{(2-i)} f_{(2-i)} = 1 \cdot 1 + 1 \cdot 1 = 2,$$
$$\sum_{q|(7)} e_{\mathfrak{q}} f_{\mathfrak{q}} = e_{(7)} f_{(7)} = 2 \cdot 1 = 2.$$

In all three cases we obtain $2 = [\mathbb{Q}(i) : \mathbb{Q}]$; as we shall shortly prove, this is not an accident.

Example 5.5. Let $A = \mathbb{C}[x]$, with $K = \operatorname{Frac} A = \mathbb{C}(x)$, and let $L = \mathbb{C}(\sqrt{x}) = \operatorname{Frac} B$, where $B = \mathbb{C}[x, y]/(y^2 - x)$. Then $[L : K] = 2$. The prime $\mathfrak{p} = (x - 4)$ factors in B into two distinct prime ideals:

$$(x - 4) = (y^2 - 4) = (y + 2)(y - 2).$$

We thus have $e_{(y+2)} = 1$, and $f_{(y+2)} = [B/(y + 2) : A/(x - 4)] = [\mathbb{C} : \mathbb{C}] = 1$. Similarly, $e_{(y-2)} = 1$ and $f_{(y-2)} = 1$.

The prime $\mathfrak{p} = x$ factors in B as

$$(x) = (y^2) = (y)^2,$$

and $e_{(y)} = 2$ and $f_{(y)} = 1$. As in the previous example, $\sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}} = [L : K]$ in both cases:

$$\sum_{\mathfrak{q}|(x-4)} e_{\mathfrak{q}} f_{\mathfrak{q}} = e_{(y+2)} f_{(y+2)} + e_{(y-2)} f_{(y-2)} = 1 \cdot 1 + 1 \cdot 1 = 2,$$

$$\sum_{\mathfrak{q}|(x)} e_{\mathfrak{q}} f_{\mathfrak{q}} = e_{(y)} f_{(y)} = 2 \cdot 1 = 2.$$

Before proving that $\sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}} = [L : K]$ always holds, we note the following. While the ring $B/\mathfrak{p}B$ is in general not a field extension of $A/\mathfrak{p}$ (because it is not necessarily a field), it is always an $(A/\mathfrak{p})$-algebra, and in particular, an $(A/\mathfrak{p})$-vector space.

Lemma 5.6. *Assume AKLB and let $\mathfrak{p}$ be a prime of A. The dimension of $B/\mathfrak{p}B$ as an $A/\mathfrak{p}$-vector space is equal to the dimension of L as a K-vector space, that is*

$$[B/\mathfrak{p}B : A/\mathfrak{p}] = [L : K].$$

Proof. Let $S = A - \mathfrak{p}$, let $A' = S^{-1}A = A_{\mathfrak{p}}$ and let $B' = S^{-1}B$ (note that S is closed under finite products, both as a subset of A and as a subset of B, so this makes sense). Then

$$A'/\mathfrak{p}A' = (S^{-1}A)/(\mathfrak{p}S^{-1}A) = A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}}) \simeq A/\mathfrak{p},$$

and

$$B'/\mathfrak{p}B' = S^{-1}B/\mathfrak{p}S^{-1}B \simeq B/\mathfrak{p}B,$$

Thus if the lemma holds when $A = A_{\mathfrak{p}}$ is a DVR then it also holds for A, so we may assume without loss of generality that A is a DVR, and in particular, a PID. We proved in the previous lecture that B is finitely generated as an A-module (see Proposition 4.60), and it is certainly torsion free as an A-module, since it is a domain and contains A. It follows from the structure theorem for modules over PIDs that B is free of finite rank over A, and B spans L as a K-vector space (see Proposition 4.55). It follows that the rank of B as an A-module (which is the same as the rank of $B/\mathfrak{p}B$ as an $A/\mathfrak{p}$-module), is the same as the dimension of L as a K-vector space: any basis for B as an A-module is also a basis for L as a K-vector space, and after clearing denominators if necessary, any basis for L as a K-vector space is also a basis for B as an A-module. Thus $[B/\mathfrak{p}B : A/\mathfrak{p}] = [L : K]$. □

Theorem 5.7. *Assume AKLB. For each prime $\mathfrak{p}$ of A we have*

$$\sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}} = [L : K].$$

Proof. We have

$$B/\mathfrak{p}B \simeq \prod_{\mathfrak{q}|\mathfrak{p}} B/\mathfrak{q}^{e_{\mathfrak{q}}}$$

Applying the previous proposition gives

$$\begin{aligned}
[L : K] &= [B/\mathfrak{p}B : A/\mathfrak{p}] \\
&= \sum_{\mathfrak{q}|\mathfrak{p}} [B/\mathfrak{q}^{e_q} : A/\mathfrak{p}] \\
&= \sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} [B/\mathfrak{q} : A/\mathfrak{p}] \\
&= \sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}}.
\end{aligned}$$

The third equality uses the fact that $B/\mathfrak{q}^{e_\mathfrak{q}}$ has dimension $e_\mathfrak{q}$ as a $B/\mathfrak{q}$-vector space; indeed, we can take the images in $B/\mathfrak{q}^{e_\mathfrak{q}}$ of any $b_i \in B$ with $v_\mathfrak{q}(b_i) = i$ for $i = 0, \ldots, e_\mathfrak{q} - 1$ as a basis (recall that $\mathfrak{q}^{e_\mathfrak{q}} = \{b \in B : v_\mathfrak{q}(b) \geq e_\mathfrak{q}\}$). Indeed, if we pick a uniformizer π for $B_\mathfrak{q}$ that lies in B then $B/\mathfrak{q}^{e_\mathfrak{q}} \simeq (B/\mathfrak{q})[\overline{\pi}] \simeq (B/\mathfrak{q})[x]/(x^{e_\mathfrak{q}})$, where $\overline{\pi}$ is the image of π in $B/\mathfrak{q}^{e_\mathfrak{q}}$. □

For each prime $\mathfrak{p}$ of A, let $g_\mathfrak{p} := \{\mathfrak{q}|\mathfrak{p}\}$ denote the cardinality of the fiber above $\mathfrak{p}$.

Corollary 5.8. *Assume $AKLB$ and let $\mathfrak{p}$ be a prime of A. The integer $g_\mathfrak{p}$ lies between* 1 *and $n = [L : K]$, as do the integers $e_\mathfrak{q}$ and $f_\mathfrak{q}$ for each $\mathfrak{q}|\mathfrak{p}$.*

We now define some standard terminology that is used in the $AKLB$ setting to describe how a prime $\mathfrak{p}$ of K splits in L (that is, for a nonzero prime ideal $\mathfrak{p}$ of A, how the ideal $\mathfrak{p}B$ factors into nonzero prime ideals $\mathfrak{q}$ of B).

Definition 5.9. Assume $AKLB$, let $\mathfrak{p}$ be a prime of A.

- L/K is *totally ramified at* $\mathfrak{q}$ if $e_\mathfrak{q} = [L : K]$ (equivalently, $f_\mathfrak{q} = 1 = g_\mathfrak{p} = 1$).
- L/K is *unramified at* $\mathfrak{q}$ if $e_\mathfrak{q} = 1$ **and** $B/\mathfrak{q}$ is a separable extension of $A/\mathfrak{p}$.
- L/K is *unramified above* $\mathfrak{p}$ if it is unramified at all $\mathfrak{q}|\mathfrak{p}$, equivalently, if $B/\mathfrak{p}B$ is a finite étale algebra over $A/\mathfrak{p}$.

When L/K is unramified above $\mathfrak{p}$ we say that

- $\mathfrak{p}$ *remains inert in* L if $\mathfrak{p}B$ is prime (equivalently, $e_\mathfrak{q} = g_\mathfrak{p} = 1$, and $f_\mathfrak{q} = [L : k]$).
- $\mathfrak{p}$ *splits completely in* L if $g_\mathfrak{p} = [L : K]$ (equivalently, $e_\mathfrak{q} = f_\mathfrak{q} = 1$ for all $\mathfrak{q}|\mathfrak{p}$).

5.2 Extending valuations

Recall that associated to each prime $\mathfrak{p}$ in a Dedekind domain A we have a discrete valuation $v_\mathfrak{p}$ on the fraction field K; it is the extension of the discrete valuation $v_\mathfrak{p}$ on the DVR $A_\mathfrak{p}$ (which also has fraction field K). In the $AKLB$ setup the primes $\mathfrak{q}$ of B similarly give rise to discrete valuations $v_\mathfrak{q}$ on L, and we would like to understand the relationship between the valuation $v_\mathfrak{p}$ and the valuations $v_\mathfrak{q}$.

Definition 5.10. Let L/K be a finite separable extension, and let v and w be discrete valuations on K and L respectively. If $w|_K = ev$ for some $e \in \mathbb{Z}_{>0}$ then we say that w *extends v with index e.*

We will show that the discrete valuations of L that extend discrete valuations $v_\mathfrak{p}$ of K are precisely the discrete valuations $v_\mathfrak{q}$ for $\mathfrak{q}|\mathfrak{p}$, and that each such $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with index $e_\mathfrak{q}$, where $e_\mathfrak{q}$ is the ramification index. This should strike you as remarkable. Valuations are in some sense a geometric notion, since they give rise to absolute values that can be used to define a distance metric, it is thus a bit surprising that they are also sensitive to the splitting of primes in extensions, which is very much an algebraic notion.

Theorem 5.11. *Assume $AKLB$ and let $\mathfrak{p}$ be a prime of A. For each prime $\mathfrak{q}|\mathfrak{p}$, the discrete valuation $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with index $e_\mathfrak{q}$. Moreover, the map $\mathfrak{q} \mapsto v_\mathfrak{q}$ is a bijection from the set of primes $\mathfrak{q}|\mathfrak{p}$ to the set of discrete valuations of L that extend $v_\mathfrak{p}$.*

Proof. Let $\mathfrak{q}|\mathfrak{p}$ and let $\mathfrak{p}B = \prod_{\mathfrak{r}|\mathfrak{p}} \mathfrak{r}^{e_\mathfrak{r}}$ be the prime factorization of $\mathfrak{p}B$. We have

$$(\mathfrak{p}B)_\mathfrak{q} = \left(\prod_{\mathfrak{r}|\mathfrak{p}} \mathfrak{r}^{e_\mathfrak{r}}\right)_\mathfrak{q} = \prod_{\mathfrak{r}|\mathfrak{p}} \mathfrak{r}_\mathfrak{q}^{e_\mathfrak{r}} = \prod_{\mathfrak{r}|\mathfrak{p}} (\mathfrak{r}B_q)^{e_\mathfrak{r}} = (\mathfrak{q}B_\mathfrak{q})^{e_\mathfrak{q}},$$

since $\mathfrak{r}B_\mathfrak{q} = B_\mathfrak{q}$ for all primes $\mathfrak{r} \neq \mathfrak{q}$ (because elements of $\mathfrak{r} - \mathfrak{q}$ are units in $B_\mathfrak{q}$). For any $m \in \mathbb{Z}$ we have $\mathfrak{p}^m B_\mathfrak{q} = (\mathfrak{q}B_\mathfrak{q})^{e_\mathfrak{q} m}$. Therefore $v_\mathfrak{q}(\mathfrak{p}^m B_\mathfrak{q}) = e_\mathfrak{q} m = e_\mathfrak{q} v_\mathfrak{p}(\mathfrak{p}^m A_\mathfrak{p})$, and it follows that for any $I \in \mathcal{I}_A$ we have $v_\mathfrak{q}(IB_\mathfrak{q}) = e_\mathfrak{q} v_\mathfrak{p}(IA_\mathfrak{p})$. In particular, for any $x \in K^\times$ we have

$$v_\mathfrak{q}(x) = v_\mathfrak{q}(xB_\mathfrak{q}) = e_\mathfrak{q} v_\mathfrak{p}(xA_\mathfrak{p}) = e_\mathfrak{q} v_\mathfrak{p}(x),$$

which shows that $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with index $e_\mathfrak{q}$ as claimed.

If $\mathfrak{q}$ and $\mathfrak{r}$ are two distinct primes above $\mathfrak{p}$ then neither contains the other and for any $x \in \mathfrak{q} - \mathfrak{r}$ we have $v_\mathfrak{q}(x) > 0 \geq v_\mathfrak{r}(x)$, thus $v_\mathfrak{q} \neq v_\mathfrak{r}$ and the map $\mathfrak{q} \mapsto v_\mathfrak{q}$ is injective..

Let w be a discrete valuation on L that extends $v_\mathfrak{p}$, let $W = \{x \in L : w(x) \geq 0\}$ be the associated DVR, and let $\mathfrak{m} = \{x \in L : w(x) > 0\}$ be its maximal ideal. Since $w|_K = ev_\mathfrak{p}$, the discrete valuation w is nonnegative on A, so $A \subseteq W$. And W is integrally closed in its fraction field L, since it is a DVR, so $B \subseteq W$. Let $\mathfrak{q} = \mathfrak{m} \cap B$. Then $\mathfrak{q}$ is prime (since $\mathfrak{m}$ is), and $\mathfrak{p} = \mathfrak{m} \cap A = \mathfrak{q} \cap A$, so $\mathfrak{q}$ lies over $\mathfrak{p}$. The ring W contains $B_\mathfrak{q}$ and is properly contained in L, which is the fraction field of $B_\mathfrak{q}$. But there are no intermediate rings between a DVR and its fraction field (such a ring R would contain an element $x \in L$ with $v_\mathfrak{q}(x) < 0$ and also every $x \in L$ with $v_\mathfrak{q}(x) \geq 0$, and this implies $R = L$), so $W = B_\mathfrak{q}$ and $w = v_\mathfrak{q}$. $\square$

MIT OpenCourseWare
http://ocw.mit.edu

18.785 Number Theory I
Fall 2015

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.