11 Totally ramified extensions and Krasner's lemma

In the previous lecture we showed that in the $AKLB$ setup, if A is a complete DVR with maximal ideal $\mathfrak{p}$ then B is a complete DVR with maximal ideal $\mathfrak{q}$ and $[L:K] = n = e_{\mathfrak{q}} f_{\mathfrak{q}}$. Assuming the residue field extension is separable (always true if K is a local field), by decomposing the extension if necessary we can always reduce to the case that L/K is either unramified or totally ramified, and we showed that in the unramified case ($e_q = 1$), if K is a local field then $L \simeq K(\zeta_{q^n-1})$. We now consider the totally ramified case ($f_{\mathfrak{q}} = 1$).

11.1 Totally ramified extensions of a complete DVR

Definition 11.1. Let A be a DVR with maximal ideal $\mathfrak{p}$. A monic polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in A[x]$$

is *Eisenstein* (or an *Eisenstein polynomial*) if $a_i \in \mathfrak{p}$ for $0 \le i < n$ and $a_0 \notin \mathfrak{p}^2$; equivalently, $v_{\mathfrak{p}}(a_i) \ge 1$ for $0 \le i < n$ and $v_{\mathfrak{p}}(a_0) = 1$.

Lemma 11.2 (Eisenstein irreducibility)**.** *Let A be a DVR with fraction field K and maximal ideal $\mathfrak{p}$, and let $f \in A[x]$ be Eisenstein. Then f is irreducible in both $A[x]$ and $K[x]$.*

Proof. Suppose $f = gh$ with $g, h \notin A$ and put $f = \sum_i f_i x^i$, $g = \sum_i g_i x^i$, $h = \sum_i h_i x^i$. We have $f_0 = g_0 h_0 \in \mathfrak{p} - \mathfrak{p}^2$, so exactly one of g_0, h_0 lies in $\mathfrak{p}$. Without loss of generality assume $g_0 \notin \mathfrak{p}$, and let $i \ge 0$ be the least i for which $h_i \notin \mathfrak{p}$; such an i exists because the reduction of $h(x)$ modulo $\mathfrak{p}$ is not zero, since $g(x)h(x) \equiv f(x) \equiv x^n \bmod \mathfrak{p}$. We then have

$$f_i = g_0 h_i + g_1 h_{i-1} + \cdots + g_{i-1} h_1 + g_i h_0,$$

with the LHS in $\mathfrak{p}$ and all but the first term on the RHS in $\mathfrak{p}$, which is a contradiction. Thus f is irreducible in $A[x]$. Noting that the DVR A is a PID (hence a UFD), f is also irreducible in $K[x]$, by Gauss's Lemma. ☐

Remark 11.3. We can apply Lemma 11.2 to a polynomial $f(x)$ over a Dedekind domain A that is Eisenstein over a localization $A_{\mathfrak{p}}$; the rings $A_{\mathfrak{p}}$ and A have the same fraction field K and f is then irreducible in $K[x]$, hence in $A[x]$.

Proposition 11.4. *Let A be a DVR and let $f \in A[x]$ be an Eisenstein polynomial. Then $B := A[x]/(f(x)) = A[\pi]$ is a DVR with uniformizer π, the image of x in $A[x]/(f(x))$.*

Proof. Let $\mathfrak{p}$ be the maximal ideal of A. We have $f \equiv x^n \bmod \mathfrak{p}$, so by Lemma 10.13 the ideal $\mathfrak{q} = (\mathfrak{p}, x) = (\mathfrak{p}, \pi)$ is the only maximal ideal of B. Let $f = \sum f_i x^i$; then $\mathfrak{p} = (f_0)$, since $v_{\mathfrak{p}}(f_0) = 1$. Therefore $\mathfrak{q} = (f_0, \pi)$, and $f_0 = -f_1\pi - f_2\pi^2 - \cdots - \pi^n \in (\pi)$, so $\mathfrak{q} = (\pi)$. The unique maximal ideal of B is thus principal, so B is a DVR and π is a uniformizer. ☐

Theorem 11.5. *Assume $AKLB$, let A be a complete DVR, and let π be any uniformizer for B. Then L/K is totally ramified if and only if $B = A[\pi]$ and the minimal polynomial of π is Eisenstein.*

Proof. Let $n = [L:K]$, let $\mathfrak{p}$ be the maximal ideal of A, let $\mathfrak{q}$ be the maximal ideal of B (which we recall is a complete DVR, by Theorem 10.7), and let π be a uniformizer for B

with minimal polynomial f. If $B = A[\pi]$ and f is Eisenstein, then as in Proposition 11.4 we have $\mathfrak{p} = \mathfrak{q}^n$, so $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with index $e_\mathfrak{q} = n$ and L/K is totally ramified.

We now suppose L/K is totally ramified. Then $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with index n, which implies $v_\mathfrak{q}(K) = n\mathbb{Z}$. The set $\{\pi^0, \pi^1, \pi^2, \ldots, \pi^{n-1}\}$ is linearly independent over K, since the valuations $0, \ldots, n-1$ are distinct modulo $v_\mathfrak{q}(K) = n\mathbb{Z}$: the valuations of the nonzero terms in any linear combination $z = \sum_{i=0}^{n-1} z_i\pi^i$ must be distinct and we cannot have $z = 0$ unless every term is zero. Thus $L = K(\pi)$.

Let $f = \sum_{i=0}^{n} f_i x^i \in A[x]$ be the minimal polynomial of π (note $\pi \in \mathfrak{q} \subseteq B$, so π is integral over A). We have $v_\mathfrak{q}(f(\pi)) = v_\mathfrak{q}(0) = \infty$, and this implies that the terms of $f(\pi) = \sum_{i=0}^{n} f_i\pi^i$ cannot all have distinct valuations; indeed the valuations of two terms of minimal valuation must coincide (by the contrapositive of the nonarchimedean triangle equality). So let $i < j$ be such that $v_\mathfrak{q}(a_i\pi^i) = v_\mathfrak{q}(a_j\pi^j)$. As noted above, the valuations of $a_i\pi^i$ for $0 \le i < n$ are all distinct modulo n, so $i = 0$ and $j = n$. We have

$$v_\mathfrak{q}(a_0\pi^0) = v_q(a_n\pi^n) = v_q(\pi^n) = n$$

thus $v_\mathfrak{q}(a_0\pi^0) = nv_\mathfrak{p}(a_0) = n$ and $v_\mathfrak{p}(a_0) = 1$. And $v_\mathfrak{q}(a_i\pi^i) \ge v_\mathfrak{q}(a_0\pi^0) = n$ for $0 < i < n$ (since $a_0\pi^0$ is a term of minimal valuation), and since $v_\mathfrak{q}(\pi^i) < n$ for $i < n$ we must have $v_\mathfrak{q}(a_i) > 0$ and therefore $v_\mathfrak{p}(a_i) > 0$. It follows that f is Eisenstein, and Proposition 11.4 then implies that $A[\pi]$ is a DVR, and in particular, integrally closed, so $B = A[\pi]$. $\square$

Example 11.6. Let $K = \mathbb{Q}_3$. As shown in an earlier problem set, there are just three distinct quadratic extensions of $\mathbb{Q}_3$: $\mathbb{Q}_3(\sqrt{2})$, $\mathbb{Q}_3(\sqrt{3})$, and $\mathbb{Q}_3(\sqrt{6})$. The extension $\mathbb{Q}_3(\sqrt{2})$ is the unique unramified quadratic extension of $\mathbb{Q}_3$, and we note that it can be written as a cyclotomic extension $\mathbb{Q}_3(\zeta_8)$. The other two are both ramified, and can be defined by the Eisenstein polynomials $x^2 - 3$ and $x^2 - 6$.

Definition 11.7. Assume $AKLB$ with A a complete DVR and separable residue field k of characteristic $p \ge 0$. We say that L/K is *tamely ramified* if $p \nmid e_{L/K}$ (always true if $p = 0$ or if $e_{L/K} = 1$); note that an unramified extension is also tamely ramified. We say that L/K is *wildly ramified* if $p|e_{L/K}$; this can occur only when $p > 0$. If L/K is totally ramified, then we say it is *totally tamely ramified* if $p \nmid e_{L/K}$ and *totally wildly ramified* otherwise.

Example 11.8. Let π be a uniformizer for A. The extension $L = K(\pi^{1/e})$ is a totally ramified extension of degree e, and it is totally wildly ramified if $p|e$.

Theorem 11.9. *Assume $AKLB$ with A a complete DVR and separable residue field k of characteristic $p \ge 0$. Then L/K is totally tamely ramified if and only if $L = K(\pi^{1/e})$ for some uniformizer π of A with $p \nmid e$.*

Proof. Let v be the unique valuation of L extending the valuation of K with index $e = e_{L/K}$, and let π_K and π_L be uniformizers for A and B, respectively. Then $v(\pi_K) = e$ and $v(\pi_L) = 1$. Thus $v(\pi_L^e) = e = v(\pi_K)$, so $u\pi_K = \pi_L^e$ for some unit $u \in B^\times$. We have $L = K(\pi_L)$, since L is totally ramified, by Theorem 11.5, and $f_{L/K} = 1$ so B and A have the same residue field k. Let us choose π_K so that $u \equiv 1 \bmod \mathfrak{q}$, and let $g(x) = x^e - u$. Then $\bar{g} = x^e - 1$, and $\bar{g}'(1) = e \ne 0$ (since $p \nmid e$), so we can use Hensel's Lemma 9.16 to lift the root 1 of $\bar{g}$ in $k = B/\mathfrak{q}$ to a root r of g in B. Now let $\pi = \pi_L/r$. Then $L = K(\pi)$, and $\pi^e = \pi_L^e/r^e = \pi_L^e/u = \pi_K$, so $L = K(\pi_K^{1/e})$ as desired. $\square$

11.2 Krasner's lemma

We continue to work with a complete DVR A with fraction field K. In the previous lecture we proved that the absolute value $|\ |$ on K can be uniquely extended to any finite extension L/K by defining $|x| := |N_{L/K}(x)|^{1/n}$, where $n = [L : K]$ (see Theorem 10.7). As noted in Remark 10.8, if $\overline{K}$ is an algebraic closure of K, we can compute the absolute value of any $\alpha \in \overline{K}$ by simply taking norms from $K(\alpha)$ down to K; this defines an absolute value on $\overline{K}$ and it is the unique absolute value on $\overline{K}$ that extends the absolute value on K.

Lemma 11.10. *Let K be the fraction field of a complete DVR with algebraic closure $\overline{K}$ and absolute value $|\ |$ extended to $\overline{K}$. For $\alpha \in \overline{K}$ and $\sigma \in \operatorname{Aut}_K(\overline{K})$ we have $|\sigma(\alpha)| = |\alpha|$.*

Proof. The elements α and $\sigma(\alpha)$ must have the same minimal polynomial $f \in K[x]$ (since $\sigma(f(\alpha)) = f(\sigma(\alpha))$), so $N_{K(\alpha)/K}(\alpha) = f(0) = N_{K(\sigma(\alpha))/K}(\sigma(\alpha))$, by Proposition 4.44. It follows that $|\sigma(\alpha)| = |N_{K(\sigma(\alpha))/K}(\alpha)|^{1/n} = |N_{K(\alpha)/K}(\alpha)|^{1/n} = |\alpha|$, where $n = \deg f$. $\square$

Definition 11.11. Let K be the fraction field of a complete DVR with absolute value $|\ |$ extended to an algebraic closure $\overline{K}$. For $\alpha, \beta \in \overline{K}$, we say that β *belongs to* α if $|\beta - \alpha| < |\beta - \sigma(\alpha)|$ for all $\sigma \in \operatorname{Aut}_K(\overline{K})$ with $\sigma(\alpha) \neq \alpha$, that is, β is strictly closer to α than it is to any of its conjugates. By the nonarchimedean triangle inequality, this is equivalent to requiring that $|\beta - \alpha| < |\alpha - \sigma(\alpha)|$ for all $\sigma(\alpha) \neq \alpha$.

Lemma 11.12 (Krasner's lemma)**.** *Let K be the fraction field of a complete DVR and let $\alpha, \beta \in \overline{K}$ with α separable. If β belongs to α then $K(\alpha) \subseteq K(\beta)$.*

Proof. Suppose not. Then $\alpha \notin K(\beta)$, so there is an automorphism $\sigma \in \operatorname{Aut}_{K(\beta)}(\overline{K}/K(\beta))$ for which $\sigma(\alpha) \neq \alpha$ (here we are using the separability of α: the extension $K(\alpha, \beta)/K(\beta)$ is separable and nontrivial, so there must by an element of $\operatorname{Hom}_{K(\beta)}(K(\alpha, \beta), \overline{K})$ that moves α). By Lemma 11.10, for any $\sigma \in \operatorname{Aut}_{K(\beta)}(\overline{K}/K(\beta))$ we have

$$|\beta - \alpha| = |\sigma(\beta - \alpha)| = |\sigma(\beta) - \sigma(\alpha)| = |\beta - \sigma(\alpha)|,$$

since σ fixes β. But this contradicts the hypothesis that β belongs to α, since $\sigma(\alpha) \neq \alpha$. $\square$

Remark 11.13. Krasner's lemma can also be viewed as another version of "Hensel's lemma" in the sense that it characterizes Henselian fields (fraction fields of Henselian rings); although named after Krasner [1] it was proved earlier by Ostrowksi [2].

Definition 11.14. For a field K with absolute value $|\ |$ we define the L^1-*norm* on $K[x]$ via

$$\|f\|_1 := \sum_i |f_i|,$$

where $f = \sum_i f_i x^i \in K[x]$.

Lemma 11.15. *Let K be a field with absolute value $|\ |$ and let $f = \prod_{i=1}^n (x - \alpha_i) \in K[x]$ have roots $\alpha_1, \ldots, \alpha_n \in L$, where L/K is a field with an absolute value that extends $|\ |$. Then $|\alpha| < \|f\|_1$ for every root α of f.*

Proof. Exercise. $\square$

Proposition 11.16. *Let K be the fraction field of a complete DVR and let $f \in K[x]$ be a monic irreducible separable polynomial. There is a positive real number $\delta = \delta(f)$ such that for every monic polynomial $g \in K[x]$ with $\|f - g\|_1 < \delta$ the following holds:*

Every root β of g belongs to a root α of f for which $K(\beta) = K(\alpha)$.

In particular, g is separable and irreducible.

Proof. We first note that we can always pick $\delta < 1$, in which case any monic $g \in K[x]$ with $\|f - g\|_1 < \delta$ must have the same degree as f, so we can assume $\deg g = \deg f$. Let us fix an algebraic closure $\overline{K}$ of K with absolute value $|\ |$ extending the absolute value on K. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in $\overline{K}$, and write

$$f(x) = \prod_i (x - \alpha_i) = \sum_{i=0}^n f_i x^i.$$

Let ϵ be the lesser of 1 and the minimum distance $|\alpha_i - \alpha_j|$ between any two distinct roots of f. We now define

$$\delta := \delta(f) := \left(\frac{\epsilon}{2(\|f\|_1 + 1)} \right)^n > 0,$$

and note that $\delta < 1$, since $\|f\|_1 \geq 1$ and $\epsilon \leq 1$. Let $g = \sum_i g_i x^i$ be a monic polynomial of degree n with $|f - g|_1 < \delta$; then

$$\|g\|_1 \leq \|f\|_1 + \|f - g\|_1 < \|f\|_1 + \delta.$$

For any root β be of g in $\overline{K}$ we have

$$|f(\beta)| = |f(\beta) - g(\beta)| = |(f - g)(\beta)| = \left| \sum_{i=0}^n (f_i - g_i)\beta^i \right| \leq \sum_i^n |f_i - g_i||\beta|^i.$$

By Lemma 11.15, we have $|\beta| < \|g\|_1$, and $\|g\|_1 \geq 1$, so $\|g\|_1^i \leq \|g\|_1^n$ for $0 \leq i \leq n$. Thus

$$|f(\beta)| < \|f - g\|_1 \cdot \|g\|_1^n < \delta(\|f\|_1 + \delta)^n < \delta(\|f\|_1 + 1)^n \leq (\epsilon/2)^n,$$

and

$$|f(\beta)| = \prod_{i=1}^n |\beta - \alpha_i| < (\epsilon/2)^n,$$

so $|\beta - \alpha_i| < \epsilon/2$ for some unique α_i to which β must belong (by our choice of ϵ).

By Krasner's lemma, $K(\alpha) \subseteq K(\beta)$, and we have $n = [K(\alpha) : K] \leq [K(\beta) : K] \leq n$, so $K(\alpha) = K(\beta)$. The minimal polynomial h of β is separable and irreducible, and it divides g and has the same degree. Both g and h are monic, so $g = h$ is separable and irreducible. □

11.3 Local extensions come from global extensions

Let $\hat{L}$ be a local field. From our classification of local fields (Theorem 9.10), we know $\hat{L}$ is a finite extension of $\hat{K} = \mathbb{Q}_p$ (some prime $p \leq \infty$) or $\hat{K} = \mathbb{F}_q((t))$ (some prime power q). We also know that the completion of a global field at any of its nontrivial absolute values is such a local field (Corollary 9.8). It thus reasonable to ask whether $\hat{L}$ is the completion of a corresponding global field L that is a finite extension of $K = \mathbb{Q}$ or $K = \mathbb{F}_q(t)$.

More generally, for any fixed global field K and local field $\hat{K}$ that is the completion of K with respect to one of its nontrivial absolute values $|\ |$, we may ask whether every finite extension of local fields $\hat{L}/\hat{K}$ necessarily corresponds to an extension of global fields L/K, where $\hat{L}$ is the completion of L with respect to one of its absolute values (whose restriction to K must be equivalent to $|\ |$). The answer is yes. In order to simplify matters we restrict our attention to the case where $\hat{L}/\hat{K}$ is separable, but this is true in general.

Theorem 11.17. *Let K be a global field with a nontrivial absolute value $|\ |$, and let $\hat{K}$ be the completion of K with respect to $|\ |$. Every finite separable extension $\hat{L}$ of $\hat{K}$ is the completion of a finite separable extension L of K with respect to an absolute value that restricts to $|\ |$. Moreover, one can choose L so that $\hat{L}$ is the compositum of L and $\hat{K}$ and $[\hat{L}:\hat{K}] = [L:K]$.*

Proof. Let $\hat{L}/\hat{K}$ be a separable extension of degree n. Let us first suppose that $|\ |$ is archimedean. Then K is a number field and $\hat{K}$ is either $\mathbb{R}$ or $\mathbb{C}$; the only nontrivial case is when $\hat{K} = \mathbb{R}$ and $n = 2$, and we may then assume that $\hat{L} \simeq \mathbb{C}$ is $\hat{K}(\sqrt{-d})$ where $-d \in \mathbb{Z}_{<0}$ is a nonsquare in K (such a $-d$ exists because $K/\mathbb{Q}$ is finite). We may assume without loss of generality that $|\ |$ is the Euclidean absolute value on $\hat{K} \simeq \mathbb{R}$ (it must be equivalent to it), and uniquely extend $|\ |$ to $L = K(\sqrt{-d})$ by requiring $|\sqrt{-d}| = \sqrt{d}$. Then $\hat{L}$ is the completion of L with respect to $|\ |$, and clearly $[\hat{L}:\hat{K}] = [L:K] = 2$, and $\hat{L}$ is the compositum of L and $\hat{K}$.

We now suppose that $|\ |$ is nonarchimedean, in which case the valuation ring of $\hat{K}$ is a complete DVR and $|\ |$ is induced by the corresponding discrete valuation. By the primitive element theorem (Theorem 4.12), we may assume $\hat{L} = \hat{K}[x]/(f)$ where $f \in \hat{K}[x]$ is monic, irreducible, and separable. The field K is dense in its completion $\hat{K}$, so we can find a monic $g \in K[x] \subseteq \hat{K}[x]$ that is arbitrarily close to f: such that $\|g - f\|_1 < \delta$ for any $\delta > 0$. It then follows from Proposition 11.16 that $\hat{L} = \hat{K}[x]/(g)$ (and that g is separable). The field $\hat{L}$ is a finite separable extension of the fraction field of a complete DVR, so by Theorem 10.7 it is itself the fraction field of a complete DVR and has a unique absolute value that extends the absolute value $|\ |$ on $\hat{K}$.

Now let $L = K[x]/(g)$. The polynomial g is irreducible in $\hat{K}[x]$, hence in $K[x]$, so $[L:K] = \deg g = [\hat{L}:\hat{K}]$. The field $\hat{L}$ contains both $\hat{K}$ and L, and it is clearly the smallest field that does (since g is irreducible in $\hat{K}[x]$), so $\hat{L}$ is the compositum of $\hat{K}$ and L. The absolute value on $\hat{L}$ restricts to an absolute value on L extending the absolute value $|\ |$ on K, and $\hat{L}$ is complete, so $\hat{L}$ contains the completion of L with respect to $|\ |$. On the other hand, the completion of L with respect $|\ |$ contains both L and $\hat{K}$, so it must be $\hat{L}$. $\square$

In the preceding theorem, when the local extension $\hat{L}/\hat{K}$ is Galois one might ask whether the corresponding global extension L/K is also Galois, and whether $\mathrm{Gal}(\hat{L}/\hat{K}) \simeq \mathrm{Gal}(L/K)$. As shown by the following example, this need not be the case.

Example 11.18. Let $K = \mathbb{Q}$, $\hat{K} = \mathbb{Q}_7$ and $\hat{L} = \hat{K}[x]/(x^3 - 2)$. The extension $\hat{L}/\hat{K}$ is Galois because $\hat{K} = \mathbb{Q}_7$ contains ζ_3 (we can lift the root 2 of $x^2 + x + 1 \in \mathbb{F}_7[x]$ to a root of $x^2 + x + 1 \in \mathbb{Q}_7[x]$ via Hensel's lemma), and this implies that $x^3 - 2$ splits completely in $L_w = \mathbb{Q}_7(\sqrt[3]{2})$. But $L = K[x]/(x^3 - 2)$ is not a Galois extension of K because it contains only one root of $x^3 - 2$. However, we can replace K with $\mathbb{Q}(\zeta_3)$ without changing $\hat{K}$ (take the completion of K with respect to the absolute value induced by a prime above 7) or $\hat{L}$, but now $L = K[x]/(x^3 - 2)$ is a Galois extension of K.

In the example we were able to adjust our choice of the global field K without changing the local fields extension $\hat{L}/\hat{K}$ in a way that ensures that $\hat{L}/\hat{K}$ and L/K have the same automorphism group. Indeed, this is always possible.

Corollary 11.19. *For every finite Galois extension $\hat{L}/\hat{K}$ of local fields there is a corresponding Galois extension of global fields L/K and an absolute value $|\;|$ on L such that $\hat{L}$ is the completion of L with respect to $|\;|$, $\hat{K}$ is the completion of K with respect to the restriction of $|\;|$ to K, and* $\mathrm{Gal}(\hat{L}/\hat{K}) \simeq \mathrm{Gal}(L/K)$.

Proof. The archimedean case is already covered by Theorem 11.17 (take $K = \mathbb{Q}$), so we assume $\hat{L}$ is nonarchimedean and note that we may take $|\;|$ to be the absolute value on both $\hat{K}$ and on $\hat{L}$ (by Theorem 10.7). The field $\hat{K}$ is an extension of either $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$, and by applying Theorem 11.17 to this extension we may assume $\hat{K}$ is the completion of a global field K with respect to the restriction of $|\;|$. As in the proof of the theorem, let $g \in K[x]$ be a monic separable polynomial irreducible in $\hat{K}[x]$ such that $\hat{L} = \hat{K}[x]/(g)$ and define $L := K[x]/(g)$ so that $\hat{L}$ is the compositum of $\hat{K}$ and L.

Now let M be the splitting field of g over K, the minimal extension of K that contains all the roots of g (which are distinct because g is separable). The field $\hat{L}$ also contains these roots (since $\hat{L}/\hat{K}$ is Galois) and $\hat{L}$ contains K, so $\hat{L}$ contains a subextension of K isomorphic to M (by the universal property of a splitting field), which we now identify with M; note that $\hat{L}$ is also the completion of M with respect to the restriction of $|\;|$ to M.

We have a group homomorphism $\varphi\colon \mathrm{Gal}(\hat{L}/\hat{K}) \to \mathrm{Gal}(M/K)$ induced by restriction, and φ is injective (each $\sigma \in \mathrm{Gal}(\hat{L}/\hat{K})$ is determined by its action on any root of g in M). If we now replace K by the fixed field of the image of φ and replace L with M, the completion of K with respect to the restriction of $|\;|$ is still equal to $\hat{K}$, and similarly for L and $\hat{L}$, and now $\mathrm{Gal}(L/K) = \mathrm{Gal}(\hat{L}/\hat{K})$ as desired. $\square$

11.4 Completing a separable extension of Dedekind domains

We now return to our general $AKLB$ setup: A is a Dedekind domain with fraction field K with a finite separable extension L/K, and B is the integral closure of A in L, which is also a Dedekind domain. Recall from Theorem 9.2 that if $\mathfrak{p}$ is a nonzero prime of A, each prime $\mathfrak{q}|\mathfrak{p}$ gives a valuation $v_\mathfrak{q}$ of L that extends the valuation $v_\mathfrak{p}$ of K with index $e_\mathfrak{q}$, meaning that $v_\mathfrak{q}|_K = e_\mathfrak{q} v_\mathfrak{p}$. Moreover, every valuation of L that extends $v_\mathfrak{p}$ arises in this way. We now want to look at what happens when we complete K with respect to the absolute value $|\;|_\mathfrak{p}$ induced by $v_\mathfrak{p}$, and similarly complete L with respect to $|\;|_\mathfrak{q}$ for some $\mathfrak{q}|\mathfrak{p}$. This includes the case where L/K is an extension of global fields, in which case we get a corresponding extension $L_\mathfrak{q}/K_\mathfrak{p}$ of local fields for each $\mathfrak{q}|\mathfrak{p}$, but note that $L_\mathfrak{q}/K_\mathfrak{p}$ may have strictly smaller degree than L/K because if we write $L \simeq K[x]/(f)$, the irreducible polynomial $f \in K[x]$ need not be irreducible over $K_\mathfrak{p}$. Indeed, this will necessarily be the case if there is more than one prime $\mathfrak{q}$ lying above $\mathfrak{p}$; there is a one-to-one correspondence between factors of f in $K_\mathfrak{p}[x]$ and primes $\mathfrak{q}|\mathfrak{p}$. If L/K is Galois, so is $L_\mathfrak{q}/K_\mathfrak{p}$ and each $\mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p})$ is isomorphic to the decomposition group $D_\mathfrak{q}$ (which perhaps helps to explain the terminology).

The following theorem gives a complete description of the situation.

Theorem 11.20. *Assume $AKLB$, let $\mathfrak{p}$ be a prime of A, and let $\mathfrak{p}B = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}$ be the factorization of $\mathfrak{p}B$ in B. Let $K_\mathfrak{p}$ denote the completion of K with respect to $|\;|_\mathfrak{p}$, and let $\hat{\mathfrak{p}}$ denote the maximal ideal of its valuation ring. For each $\mathfrak{q}|\mathfrak{p}$, let $L_\mathfrak{q}$ denote the completion of L with respect to $|\;|_\mathfrak{q}$, and let $\hat{\mathfrak{q}}$ denote the maximal ideal of its valuation ring. The following hold:*

1. *Each $L_\mathfrak{q}$ is a finite separable extension of $K_\mathfrak{p}$;*
2. *Each $\hat{\mathfrak{q}}$ is the unique prime of $L_\mathfrak{q}$ lying over $\hat{\mathfrak{p}}$.*

(3) *Each $\hat{\mathfrak{q}}$ has ramification index $e_{\hat{\mathfrak{q}}} = e_{\mathfrak{q}}$ and residue field degree $f_{\hat{q}} = f_{\mathfrak{q}}$.*

(4) $[L_{\mathfrak{q}} : K_{\mathfrak{p}}] = e_{\mathfrak{q}} f_{\mathfrak{q}}$;

(5) *The map $L \otimes_K K_{\mathfrak{p}} \to \prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}$ defined by $\ell \otimes x \mapsto (\ell x, \ldots, \ell x)$ is an isomorphism of finite étale $K_{\mathfrak{p}}$-algebras.*

(6) *If L/K is Galois then each $L_{\mathfrak{q}}/K_{\mathfrak{p}}$ is Galois and we have isomorphisms of decomposition groups $D_{\mathfrak{q}} \simeq D_{\hat{\mathfrak{q}}} = \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ and inertia groups $I_{\mathfrak{q}} \simeq I_{\hat{\mathfrak{q}}}$.*

Proof. We first note that the $K_{\mathfrak{p}}$ and the $L_{\mathfrak{q}}$ are all fraction fields of complete DVRs; this follows from Proposition 8.11 (note: we are not assuming they are local fields, in particular, their residue fields need not be finite).

(1) For each $\mathfrak{q}|\mathfrak{p}$ the embedding $K \hookrightarrow L$ induces an embedding $K_{\mathfrak{p}} \hookrightarrow L_{\mathfrak{q}}$ via the map $[(a_n)] \mapsto [(a_n)]$ on equivalence classes of Cauchy sequences; a sequence (a_n) that is Cauchy in K with respect to $|\ |_{\mathfrak{p}}$, is also Cauchy in L with respect to $|\ |_{\mathfrak{q}}$ because $v_{\mathfrak{q}}$ extends $v_{\mathfrak{p}}$. We thus view $K_{\mathfrak{p}}$ as a subfield of $L_{\mathfrak{q}}$, which also contains L. There is thus a K-algebra homomorphism $\phi_{\mathfrak{q}}\colon L \otimes_K K_{\mathfrak{p}} \to L_{\mathfrak{q}}$ defined by $\ell \otimes x \mapsto \ell x$, which we may view as a linear map of $K_{\mathfrak{p}}$ vector spaces. We claim that $\phi_{\mathfrak{q}}$ is surjective.

If $\alpha_1, \ldots, \alpha_m$ is any basis for $L_{\mathfrak{q}}$ then its determinant with respect to $\mathcal{B}$, i.e., the $m \times m$ matrix whose jth row contains the coefficients of α_j when written as a linear combination of elements of $\mathcal{B}$, must be nonzero. The determinant is a polynomial in the entries of this matrix, hence a continuous function with respect to the topology on $L_{\mathfrak{q}}$ induced by the absolute value $|\cdot|_{\mathfrak{q}}$. It follows that if we replace $\alpha_1, \ldots, \alpha_m$ with $\ell_1, \ldots, \ell_m$ chosen so that $|\alpha_j - \ell_j|_{\mathfrak{q}}$ is sufficiently small, the matrix of $\ell_1, \ldots, \ell_m$ with respect to $\mathcal{B}$ must also be nonzero, and therefore $\ell_1, \ldots, \ell_m$ is also a basis for $L_{\mathfrak{q}}$. We can thus choose a basis $\ell_1, \ldots, \ell_m \in L$, since L is dense in its completion $L_{\mathfrak{q}}$. But then $\{\ell_j\} = \{\phi_{\mathfrak{q}}(\ell_j \otimes 1)\} \subseteq \operatorname{im} \phi_{\mathfrak{q}}$ spans $L_{\mathfrak{q}}$, so $\phi_{\mathfrak{q}}$ is surjective as claimed.

The $K_{\mathfrak{p}}$-algebra $L \otimes_K K_{\mathfrak{p}}$ is the base change of a finite étale algebra, hence finite étale, by Proposition 4.33. It follows that $L_{\mathfrak{q}}$ is a finite separable extension of $K_{\mathfrak{p}}$: it certainly has finite dimension as a $K_{\mathfrak{p}}$-vector space, since $\phi_{\mathfrak{q}}$ is surjective, and it is separable because every $\alpha \in L_{\mathfrak{q}}$ is the image $\phi_{\mathfrak{q}}(\beta)$ of an element $\beta \in L \otimes_K K_{\mathfrak{p}}$ that is a root of a separable (but not necessarily irreducible) polynomial $f \in K_{\mathfrak{p}}[x]$, as explained after Definition 4.28; we then have $0 = \phi_{\mathfrak{q}}(0) = \phi_{\mathfrak{q}}(f(\beta)) = f(\alpha)$, so α is a root of f, hence separable.

(2) The valuation rings of $K_{\mathfrak{p}}$ and $L_{\mathfrak{q}}$ are complete DVRs, so this follows immediately from Theorem 10.1.

(3) The valuation $v_{\hat{\mathfrak{q}}}$ extends $v_{\mathfrak{q}}$ with index 1, which in turn extends $v_{\mathfrak{p}}$ with index $e_{\mathfrak{q}}$. The valuation $v_{\hat{\mathfrak{p}}}$ extends $v_{\mathfrak{p}}$ with index 1, and it follows that $v_{\hat{q}}$ extends $v_{\hat{p}}$ with index $e_{\mathfrak{q}}$ and therefore $e_{\hat{\mathfrak{q}}} = e_{\mathfrak{q}}$. The residue field of $\hat{\mathfrak{p}}$ is the same as that of $\mathfrak{p}$: for any Cauchy sequence (a_n) over K the a_n will eventually all have the same image in the residue field at $\mathfrak{p}$ (since $v_{\mathfrak{p}}(a_n - a_m) > 0$ for all sufficiently large m and n). Similar comments apply to each $\hat{\mathfrak{q}}$ and $\mathfrak{q}$, and it follows that $f_{\hat{\mathfrak{q}}} = f_{\mathfrak{q}}$.

(4) It follows from (2) that $[L_{\mathfrak{q}} : K_{\mathfrak{p}}] = e_{\hat{\mathfrak{q}}} f_{\hat{\mathfrak{q}}}$, since $\hat{\mathfrak{q}}$ is the only prime above $\hat{\mathfrak{p}}$, and (3) then implies $[L_{\mathfrak{q}} : K_{\mathfrak{p}}] = e_{\mathfrak{q}} f_{\mathfrak{q}}$.

(5) Let $\phi = \prod_{\mathfrak{q}|\mathfrak{p}} \phi_{\mathfrak{q}}$, where $\phi_{\mathfrak{q}}$ are the surjective $K_{\mathfrak{p}}$-algebra homomorphisms defined in the proof of (1). Then $\phi\colon L \otimes_K K_{\mathfrak{p}} \to \prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}$ is a $K_{\mathfrak{p}}$-algebra homomorphism. Applying (4) and the fact that base change preserves dimension (see Proposition 4.33):

$$\dim_{K_{\mathfrak{p}}} (L \otimes_K K_{\mathfrak{p}}) = \dim_K L = [L : K] = \sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}} = \sum_{\mathfrak{q}|\mathfrak{p}} [L_{\mathfrak{q}} : K_{\mathfrak{p}}] = \dim_{K_{\mathfrak{p}}} \left(\prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}} \right).$$

The domain and range of ϕ thus have the same dimension, and ϕ is surjective (since the $\phi_{\mathfrak{q}}$ are), so it is an isomorphism.

(6) We now assume L/K is Galois. Each $\sigma \in D_{\mathfrak{q}}$ acts on L and respects the valuation $v_{\mathfrak{q}}$, since it fixes $\mathfrak{q}$ (if $x \in \mathfrak{q}^n$ then $\sigma(x) \in \sigma(\mathfrak{q}^n) = \sigma(\mathfrak{q})^n = \mathfrak{q}^n$). It follows that if (x_n) is a Cauchy sequence in L, then so is $(\sigma(x_n))$, thus σ is an automorphism of $L_{\mathfrak{q}}$, and it fixes $K_{\mathfrak{p}}$. We thus have a group homomorphism $\varphi\colon D_{\mathfrak{q}} \to \operatorname{Aut}_{K_{\mathfrak{p}}}(L_{\mathfrak{q}})$.

If $\sigma \in D_{\mathfrak{q}}$ acts trivially on $L_{\mathfrak{q}}$ then it acts trivially on $L \subseteq L_{\mathfrak{q}}$, so $\ker \varphi$ is trivial. Also,

$$e_{\mathfrak{q}} f_{\mathfrak{q}} = |D_{\mathfrak{q}}| \le \#\operatorname{Aut}_{K_{\mathfrak{p}}}(L_{\mathfrak{q}}) \le [L_{\mathfrak{q}} : K_{\mathfrak{p}}] = e_{\mathfrak{q}} f_{\mathfrak{q}},$$

by Theorem 11.20, so $\#\operatorname{Aut}_{K_{\mathfrak{p}}}(L_{\mathfrak{q}}) = [L_{\mathfrak{q}} : K_{\mathfrak{p}}]$ and $L_{\mathfrak{q}}/K_{\mathfrak{p}}$ is Galois, and this also shows that φ is surjective and therefore an isomorphism. There is only one prime $\hat{q}$ of $L_{\mathfrak{q}}$, and it is necessarily fixed by every $\sigma \in \operatorname{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$, so $\operatorname{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}) \simeq D_{\hat{\mathfrak{q}}}$. The inertia groups $I_{\mathfrak{q}}$ and $I_{\hat{\mathfrak{q}}}$ both have order $e_{\mathfrak{q}} = e_{\hat{\mathfrak{q}}}$, and φ restricts to a homomorphism $I_{\mathfrak{q}} \to I_{\hat{\mathfrak{q}}}$, so the inertia groups are also isomorphic. □

Corollary 11.21. *Assume AKLB and let $\mathfrak{p}$ be a prime of A. For every $\alpha \in L$ we have*

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\mathfrak{q}|\mathfrak{p}} \mathrm{N}_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(\alpha) \qquad \text{and} \qquad \mathrm{T}_{L/K}(\alpha) = \sum_{\mathfrak{q}|\mathfrak{p}} \mathrm{T}_{L_{\mathfrak{q}}/K_{\mathfrak{q}}}(\alpha).$$

where we view α as an element of $L_{\mathfrak{q}}$ via the canonical embedding $L \hookrightarrow L_{\mathfrak{q}}$.

Proof. The norm and trace are defined as the determinant and trace of K-linear maps $L \xrightarrow{\times\alpha} L$ that are unchanged upon tensoring with $K_{\mathfrak{p}}$; the corollary then follows from the isomorphism in part (5) of Theorem 11.20, which commutes with the norm and trace. □

Remark 11.22. Theorem 11.20 can be stated more generally in terms of (equivalence classes of) absolute values (or *places*). Rather than working with a prime $\mathfrak{p}$ of K and primes $\mathfrak{q}$ of L above $\mathfrak{p}$, one works with an absolute value $|\ |_v$ of K (for example, $|\ |_{\mathfrak{p}}$) and inequivalent absolute values $|\ |_w$ of L that extend $|\ |_v$. Places will be discussed further in the next lecture.

Corollary 11.23. *Assume AKLB with A a DVR with maximal ideal $\mathfrak{p}$. Let $\mathfrak{p}B = \prod \mathfrak{q}^{e_{\mathfrak{q}}}$ be the factorization of $\mathfrak{p}B$ in B. Let $\hat{A}$ denote the completion of A, and for each $\mathfrak{q}|\mathfrak{p}$, let $\hat{B}_{\mathfrak{q}}$ denote the completion of $B_{\mathfrak{q}}$. Then $B \otimes_A \hat{A} \simeq \prod_{\mathfrak{q}|\mathfrak{p}} \hat{B}_{\mathfrak{q}}$.*

Proof. Since A is a DVR (and therefore a torsion-free PID), the ring extension B/A is a free A module of rank $n := [L : K]$, and therefore $B \otimes_A \hat{A}$ is a free $\hat{A}$-module of rank n. And $\prod \hat{B}_{\mathfrak{q}}$ is a free $\hat{A}$-module of rank $\sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}} = n$. These two $\hat{A}$-modules lie in isomorphic $K_{\mathfrak{p}}$-vector spaces, $L \otimes_K K_{\mathfrak{p}} \simeq \prod L_{\mathfrak{q}}$, by part (5) of Theorem 11.20. To show that they are isomorphic it suffices to check that they are isomorphic after reducing modulo $\hat{\mathfrak{p}}$, the maximal ideal of $\hat{A}$.

For the LHS, note that $\hat{A}/\hat{\mathfrak{p}} \simeq A/\mathfrak{p}$, so

$$B \otimes_A \hat{A}/\hat{\mathfrak{p}} \simeq B \otimes_A A/\mathfrak{p} \simeq B/\mathfrak{p}B.$$

On the RHS we have

$$\prod_{\mathfrak{q}|\mathfrak{p}} \hat{B}_{\mathfrak{q}}/\hat{\mathfrak{p}}\hat{B}_{\mathfrak{q}} \simeq \prod_{\mathfrak{q}|\mathfrak{p}} \hat{B}_{\mathfrak{q}}/\mathfrak{p}\hat{B}_{\mathfrak{q}} \simeq \prod_{\mathfrak{q}|\mathfrak{p}} B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}} = \prod_{\mathfrak{q}|\mathfrak{p}} B_{\mathfrak{q}}/\mathfrak{q}^{e_{\mathfrak{q}}} B_{\mathfrak{q}}$$

which is isomorphic to $B/\mathfrak{p}B$ on the LHS because $\mathfrak{p}B = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_{\mathfrak{q}}}$. □

References

[1] Marc Krasner, *Théorie non abélienne des corps de classes pour les extensions finies et séparables des corps valués complets: principes fondamentaux; espaces de polynomes et transformation T ; lois d'unicité, d'ordination et d'existence*, C. R. Acad. Sci. Paris **222** (1946), 626–628.

[2] Alexander Ostrowski, *Über sogenannte perfekte Körper*, J. Reine Angew. Math. **147** (1917), 191–204