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 $[L:K] = n = e_{\mathfrak{q}} f_{\mathfrak{q}}$; see Theorem 10.4 (note that the *AKLB* setup includes the assumption that L/K is separable). In this setting we may unambiguously write $e_{L/K}$ for $e_{\mathfrak{q}}$ and $f_{L/K}$ for $f_{\mathfrak{q}}$, since $\mathfrak{q}$ is the unique prime of L. Provided the residue field extension is separable (always the case if K is a local field), we can decompose the extension L/K as a tower of field extensions $L/E/K$ in which E/K is unramified (so $e_{E/K} = 1$ and $f_{E/K} = f_{L/K}$) and L/E is totally ramified (so $e_{L/E} = e_{L/K}$ and $f_{L/E} = 1$), by Theorem 10.23.

In the previous lecture we classified unramified extensions of (fraction fields of) complete DVRs, and showed that when the residue field is finite (always true for local fields), unramified extensions are all cyclotomic extensions of the form $K(\zeta_n)/K$ for some n coprime to the residue field characteristic; see Corollary 10.17. In this lecture we will classify totally ramified extensions of complete DVRs.

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 $v_{\mathfrak{p}}(a_0) = 1$. Note that this means a_0 is a uniformizer.

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

Proof. Suppose not. Then $f = gh$ has degree $n \ge 2$ for some non-constant monic $g, h \in A[x]$. Put $f = \sum_i f_i x^i$, $g = \sum_i g_i x^i$, $h = \sum_i h_i x^i$. Then $v_{\mathfrak{p}}(f_0) = v_{\mathfrak{p}}(g_0 h_0) = v_{\mathfrak{p}}(g_0) + v_{\mathfrak{p}}(h_0) = 1$, where $\mathfrak{p}$ is the maximal ideal of A, and without loss of generality we may assume $v_{\mathfrak{p}}(g_0) = 0$ and $v_{\mathfrak{p}}(h_0) = 1$. Let $i > 0$ be the least i for which $v_{\mathfrak{p}}(h_i) = 0$; such an $i < n$ exists since h is monic and $\deg h < n$. We have

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

with $v_{\mathfrak{p}}(f_i) \ge 1$ since f is Eisenstein and $i < n$, but the valuation of the RHS is zero, since $v_{\mathfrak{p}}(g_0 h_i) = 0$ and $v_{\mathfrak{p}}(g_j h_{i-j}) \ge 1$ for $0 \le j < i$, by the minimality of i, which is a contradiction. Thus f is irreducible in $A[x]$, and since A is a DVR, and therefore a PID and thus a UFD, f is irreducible in $K[x]$, by Gauss's Lemma [1]. □

Remark 11.3. We can apply Lemma 11.2 to any 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 $A[x]$; this gives the *Eisenstein criterion* for irreducibility.

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

Proof. Let $\mathfrak{p}$ be the maximal ideal of A. We have $f \equiv x^n \bmod \mathfrak{p}$, so by Corollary 10.11 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 $\mathfrak{p} = (f_0)$ and $\mathfrak{q} = (f_0, \pi)$, and $f_0 = -f_1\pi - f_2\pi^2 - \cdots - \pi^n \in (\pi)$, so $\mathfrak{q} = (\pi)$. The unique maximal ideal (π) of B is nonzero and principal, so B is a DVR with uniformizer π. □

Theorem 11.5. *Assume AKLB with A a complete DVR and π a uniformizer for B. The extension 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 10.4), and let π be a uniformizer for B with minimal polynomial f. If $B = A[\pi]$ and f is Eisenstein, then as in Lemma 11.4 we have $\mathfrak{p}B = \mathfrak{q}^n$, 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 $\{\pi^0, \pi^1, \pi^2, \dots, \pi^{n-1}\}$ is linearly independent over K, since the valuations of $\pi^0, \dots \pi^{n-1}$ are distinct modulo $v_\mathfrak{q}(K) = n\mathbb{Z}$ (if $\sum_{i=0}^{n-1} a_i\pi^i = 0$ we must have $v_\mathfrak{q}(a_i\pi^i) = v_\mathfrak{q}(a_j\pi^j)$ for some nonzero a_i and a_j with $i \neq j$, which is impossible). Thus $L = K(\pi)$.

Let $f = \sum_{i=0}^{n} a_i x^i \in A[x]$ be the minimal polynomial of π. We have $v_\mathfrak{q}(f(\pi)) = \infty$ and $v_\mathfrak{q}(a_i\pi^i) \equiv i \bmod n$ for $0 \leq i \leq n$. The former implies that the minimum value of the nonnegative integers $v_\mathfrak{q}(a_i\pi^i)$ cannot occur uniquely, and the latter implies that these integers are distinct for distinct values of i mod n. We therefore must have

$$v_\mathfrak{q}(a_0) = v_\mathfrak{q}(a_0\pi^0) = v_\mathfrak{q}(a_n\pi^n) = v_\mathfrak{q}(\pi^n) = n < v_\mathfrak{q}(a_i\pi^i) \text{ for } 0 < i < n,$$

This implies $v_\mathfrak{p}(a_0) = 1$, since $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with index n, and $v_\mathfrak{p}(a_i) \geq 1$ for $0 \leq i < n$. Thus f is Eisenstein $A[\pi] \subseteq B$ is a DVR, by Lemma 11.4, hence maximal, so $B = A[\pi]$. □

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 extension of characteristic $p \geq 0$. The extension L/K is *tamely ramified* if $p \nmid e_{L/K}$ (always true if $p = 0$); note that unramified extensions are tamely ramified. Otherwise L/K is *wildly ramified* if $p | e_{L/K}$. A totally ramified extension L/K is *totally tamely ramified* if $p \nmid e_{L/K}$, and it is *totally wildly ramified* if $e_{L/K}$ is a power of p (a totally ramified extension that is wildly ramified need not be totally wildly ramified).

Recall that ramification indices multiply in towers (Lemma 5.38), and separability is transitive in towers (Corollary 4.14). This yields the following proposition, which we note applies to all nonarchimedean local fields.

Proposition 11.8. *The properties of being unramified, tamely ramified, wildly ramified, totally ramified, totally tamely ramified, and totally wildly ramified are all transitive in towers of extensions of fraction fields of complete DVRs with separable residue field extensions.*

Proof. This follows immediately from the transitivity of separability and the multiplicativity of ramification indices and degrees in towers. □

Remark 11.9. A compositum of totally ramified extensions need not be totally ramified. From Example 11.6 we see that the compositum of the totally ramified quadratic extensions $\mathbb{Q}_3(\sqrt{3})$ and $\mathbb{Q}_3(\sqrt{6})$ of $\mathbb{Q}_3$ contains the unramified quadratic extension $\mathbb{Q}_3(\sqrt{2})$ of $\mathbb{Q}_3$.

Theorem 11.10. *Assume AKLB with A a complete DVR and separable residue field extension of characteristic $p \geq 0$ not dividing $n := [L : K]$. The extension L/K is totally tamely ramified if and only if $L = K(\pi_A^{1/n})$ for some uniformizer π_A of A.*

Proof. If $L = K(\pi_A^{1/n})$ then $\pi = \pi_A^{1/n}$ has minimal polynomial $x^n - \pi_A$, which is Eisenstein, so $A[\pi]$ is a DVR by Lemma 11.4. This implies $B = A[\pi]$, since DVRs are maximal, and Theorem 11.5 implies that L/K is totally tamely ramified, since $p \nmid n$.

Now assume L/K is totally tamely ramified and let $\mathfrak{p}$ and $\mathfrak{q}$ be the maximal ideals of A and B with uniformizers π_A and π_B respectively. Then $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with index $e_\mathfrak{q} = n$ and $v_\mathfrak{q}(\pi_B^n) = n = v_\mathfrak{q}(\pi_A)$. This implies that $\pi_B^n = u\pi_A$ for some unit $u \in B^\times$. We have $f_\mathfrak{q} = 1$, so B and A have the same residue field, and if we lift the image of u in $B/\mathfrak{q} \simeq A/\mathfrak{p}$ to a unit u_A in A and replace π_A with $u_A^{-1}\pi_A$, we can assume that $u \equiv 1 \bmod \mathfrak{q}$. Now define $g(x) := x^n - u \in B[x]$ with reduction $\bar{g} = x^n - 1$ in $(B/\mathfrak{q})[x]$. We have $\bar{g}'(1) = n \neq 0$ (since $p \nmid n$), so by Hensel's Lemma 9.15 we can lift the root 1 of $\bar{g}(x)$ in $B/\mathfrak{q}$ to a root r of $g(x)$ in B. Now let $\pi := \pi_B/r$. Then π is a uniformizer for B and $B = A[\pi]$ by Theorem 11.5, so $L = K(\pi)$, and $\pi^n = \pi_B^n/r^n = \pi_B^n/u = \pi_A$, so $L = K(\pi_A^{1/n})$ as desired. □

Proposition 11.11. *Let L be a totally ramified extension of the fraction field K of a complete DVR. There is a unique intermediate field E such that E/K is totally tamely ramified and L/E is totally wildly ramified.*

Proof. Let $e := e_{L/K}$ be the ramification index and let $p \geq 0$ be the characteristic of the residue field. If $p \nmid e$ then the proposition holds with $E = L$, so we assume $p|e$, and put $e = mp^a$ with $p \nmid m$ (possibly $m = 1$).

Let A be the valuation ring of K with maximal ideal $\mathfrak{p}$, and let B be the valuation ring of L (also a complete DVR) with maximal ideal $\mathfrak{q}$. As in the proof of Theorem 11.10, we can choose uniformizers π_A of A and π_B of B such that $\pi_B^n = u\pi_A$ with $u \in B^\times$ and $u \equiv 1 \bmod \mathfrak{q}$. Let $g(x) = x^m - u \in B[x]$; as in the proof of the theorem we can construct a root $r \in B$ of $g(x)$ by Hensel lifting the root 1 of $\bar{g} \in (B/\mathfrak{q})[x]$. Now consider the field extension $E := K(\pi)$, where $\pi := \pi_B^{p^a}/r$. We have $\pi^m = \pi_B^n/r^m = \pi_B^n/u = \pi_A$, so $E = K(\pi_A^{1/m})$ with $p \nmid m$. The polynomial $x^m - \pi_A$ of π is Eisenstein, hence irreducible, and has π as a root, so E/K has degree m. By Theorem 11.10, the extension E/K is totally tamely ramified (the residue field extension is trivial, so it is certainly separable), and the extension L/E has degree p^a and is thus totally wildly ramified.

To see that E is unique, suppose $E' \subseteq L$ is another totally tamely ramified extensions of K such that L/E' is totally wildly ramified. Then $E' = K(\pi_A'^{1/m})$ for some uniformizer π_A' of A, by Theorem 11.10. Now $\pi_A'/\pi_A = u$ is a unit with $u^{1/m} \in L$, and in fact $u^{1/m} \in K$, since L/K is totally ramified and $K(u^{1/m})$ is unramified (by Corollary 10.16, since $p \nmid m$). We can thus replace any mth root of π_A' with some mth root of π_A, and it follows that E and E' are both generated by a root of $x^m - \pi_A$. The ratio of these roots is a (not necessarily primitive) mth root of unity $\zeta \in L$ that must lie in K (as above, since L/K is totally ramified and $p \nmid m$), therefore $E' = E$. □

Corollary 11.12. *Let L be a finite separable extension of the fraction field K of a complete DVR with separable residue field extension. There is a unique intermediate field E such that E/K is tamely ramified and L/E is totally wildly ramified.*

Proof. Let F be the maximal unramified extension of K in L. By Corollary 10.15 we can assume $L = F(\alpha)$ where α is an integral element whose minimal polynomial g has separable

image in $k[x]$, where k is the residue field of K. Applying the previous proposition to the totally ramified extension L/F yields a tamely ramified extension E/F with L/E totally wildly ramified. Unramified extensions are tamely ramified, so $E/F/K$ is a tower of tamely ramified extensions, hence tamely ramified.

Any field E' with L/E' totally wildly ramified must contain α, otherwise $E'(\alpha)$ would be a non-trivial unramified subextension L/E' (here we are again applying Corollary 10.15 and the fact that the image of the minimal polynomial of α over E' must divide g and thus has separable image in $k[x]$ and in $k'[x]$, where k' is the residue field of E', since k' is an extension of k). Proposition 11.11 then implies $E' = E$. □

11.2 Krasner's lemma

Let K be the fraction field of a complete DVR with absolute value $|\ |$. By Theorem 10.4 we can uniquely extend $|\ |$ to any finite extension L/K by defining $|x| := |N_{L/K}(x)|^{1/n}$, where $n = [L : K]$; as noted in Remark 10.5, this induces a unique absolute value on $\overline{K}$ that restricts to the absolute value of K.

Lemma 11.13. *Let K be the fraction field of a complete DVR with algebraic closure $\overline{K}$ and absolute value $|\ |$ extended to $\overline{K}$. For all $\alpha \in \overline{K}$ and $\sigma \in \mathrm{Aut}_K(\overline{K})$ we have $|\sigma(\alpha)| = |\alpha|$.*

Proof. The elements α and $\sigma(\alpha)$ must have the same minimal polynomial $f \in K[x]$, since $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$, so $N_{K(\alpha)/K}(\alpha) = (-1)^n 1 f(0) = N_{K(\sigma(\alpha))/K}(\sigma(\alpha))$, by Proposition 5.6. It follows that $|\sigma(\alpha)| = |N_{K(\sigma(\alpha))/K}(\sigma(\alpha))|^{1/n} = |N_{K(\alpha)/K}(\alpha)|^{1/n} = |\alpha|$, where $n = \deg f$. □

Definition 11.14. 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 β *belongs to* α if $|\beta - \alpha| < |\beta - \sigma(\alpha)|$ for all $\sigma \in \mathrm{Aut}_K(\overline{K})$ with $\sigma(\alpha) \neq \alpha$, that is, β is strictly closer to α than it is to any of its conjugates. This is equivalent to requiring that $|\beta - \alpha| < |\alpha - \sigma(\alpha)|$ for all $\sigma(\alpha) \neq \alpha$, since every nonarchimedean triangle is isosceles (if one side is shorter than another, it is the shortest of all three sides).

Lemma 11.15 (Krasner's lemma)**.** *Let K be the fraction field of a complete DVR and let $\alpha, \beta \in \overline{K}$, with α separable over K. If β belongs to α then $K(\alpha) \subseteq K(\beta)$.*

Proof. Suppose not. Then β belongs to α but $\alpha \notin K(\beta)$. The extension $K(\alpha, \beta)/K(\beta)$ is separable and non-trivial, so there is an automorphism $\sigma \in \mathrm{Aut}_{K(\beta)}(\overline{K})$ for which $\sigma(\alpha) \neq \alpha$ (let σ send α to a different root of the minimal polynomial of α over $K(\beta)$). Applying Lemma 11.13 to $\beta - \alpha \in \overline{K}$, 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 $\sigma(\alpha) \neq \alpha$. □

Remark 11.16. Krasner's lemma is another "Hensel's lemma" in the sense that it characterizes Henselian fields (fraction fields of Henselian rings); although the lemma is named after Krasner [2], it was proved earlier by Ostrowski in [3].

Definition 11.17. For a field K with absolute value $|\ |$ the *L^1-norm* of $f = \sum f_i x^i \in K[x]$ is

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

It is easy to check that $\| \ \|_1$ satisfies all the properties of Definition 10.1 and is thus a norm on the K-vector space $K[x]$.

Lemma 11.18. *Let K be a field with absolute value $|\ |$ and let $f := \prod_{i=1}^n (x-\alpha_i) \in K[x]$ be a monic polynomial with roots $\alpha_1, \dots, \alpha_n \in L$, where L/K is a field with an absolute value that extends $|\ |$. Then $|\alpha| < \|f\|_1$ for every root α of f.*

Proof. The lemma is clear for $n \le 1$, so assume $n \ge 2$. If $\|f\|_1 = 1$ then we must have $f = x^n$ and $\alpha = 0$, in which case $|\alpha| = 0 < 1 = \|f\|_1$ and the lemma holds. Otherwise $\|f\|_1 > 1$, and if $|\alpha| \le 1$ the lemma holds, so let α is a root of f with $|\alpha| > 1$. We have

$$0 = |f(\alpha)| = \left|\alpha^n + \sum_{i=0}^{n-1} f_i \alpha^i\right| \ge |\alpha|^n - \sum_{i=0}^{n-1} |f_i||\alpha|^i \ge |\alpha|^n - |\alpha|^{n-1} \sum_{i=0}^{n-1} |f_i| \ge |\alpha| - (\|f\|_1 - 1),$$

where we have used $|a| = |a+b-b| \le |a+b| + |-b| = |a+b| + |b|$ to get the general inequality $|a+b| \ge |a| - |b|$ which we applied repeatedly to get the first inequality above, we used $|\alpha| > 1$ to get the second (replacing $|\alpha|^i$ with $|\alpha|^{n-1}$ in each term) and the third (dividing by $|\alpha|^{n-1} \ge 1$). Thus $\|f\|_1 - 1 \ge |\alpha|$, and therefore $\|f\|_1 \ge |\alpha| + 1 > |\alpha|$. □

Theorem 11.19 (Continuity of roots)**.** *Let K be the fraction field of a complete DVR and $f \in K[x]$ a monic irreducible separable polynomial. There exists $\delta = \delta(f) \in \mathbb{R}_{>0}$ 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, every such g is separable, irreducible, and has the same splitting field as f.

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 $\alpha_1, \dots, \alpha_n$ 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 $\|f\|_1 \ge 1$ and $\epsilon \le 1$. Let $g(x) = \sum_i g_i x^i$ be a monic polynomial of degree n with $\|f-g\|_1 < \delta$. We then have

$$\|g\|_1 \le \|f\|_1 + \|g-f\|_1 = \|f\|_1 + \|f-g\|_1 < \|f\|_1 + \delta,$$

and for any root $\beta \in \overline{K}$ of g we have

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

We have $|\beta| < \|g\|_1$ by Lemma 11.18, and $\|g\|_1 \ge 1$, so $|\beta|^i < \|g\|_1^i \le \|g\|_1^n$. Thus

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

and therefore

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

It follows that $|\beta - \alpha_i| < \epsilon/2$ for at least one α_i, and the triangle inequality implies that this α_i must be unique since $|\alpha_i - \alpha_j| \geq \epsilon$ for $i \neq j$. Therefore β belongs to $\alpha := \alpha_i$.

By Krasner's lemma, $K(\alpha) \subseteq K(\beta)$, and we have $n = [K(\alpha) : K] \leq [K(\beta) : K] \leq n$, so $K(\alpha) = K(\beta)$. It follows that g is the minimal polynomial of β, since $\deg(g) = [K(\beta) : K]$. Thus g is irreducible, and it is also separable, since $\beta \in K(\beta) = K(\alpha)$ lies in a separable extension of K. We now observe that if a root β of g belongs to a root α of f, then for any $\tau \in \mathrm{Aut}_K(\overline{K})$ and all $\sigma \in \mathrm{Aut}_K(\overline{K})$ such that $\sigma(\alpha) \neq \alpha$ we have

$$|\tau(\beta) - \tau(\alpha)| = |\tau(\beta - \alpha)| = |\beta - \alpha| < |\alpha - \sigma(\alpha)| = |\tau(\alpha - \sigma(\alpha))| = |\tau(\alpha) - \tau(\sigma(\alpha))|.$$

Noting that $\sigma(\alpha) \neq \alpha \iff \tau(\sigma(\alpha)) \neq \tau(\alpha)$, this implies that $\tau(\beta)$ belongs to $\tau(\alpha)$. Now $\mathrm{Aut}_K(\overline{K})$ acts transitively on the roots of f and g, so every root β of g belongs to a distinct root α of f for which $K(\beta) = K(\alpha)$. Therefore g has the same splitting field as f. □

11.3 Local extensions come from global extensions

Let $\hat{L}$ be a local field. From our classification of local fields (Theorem 9.9), we know that $\hat{L}$ is (isomorphic to) a finite extension of $\hat{K} = \mathbb{Q}_p$ (some $p \leq \infty$) or $\hat{K} = \mathbb{F}_q((t))$ (some q). We also know that the completion of a global field at any of its nontrivial absolute values is a local field (Corollary 9.7). It is 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 11.20. *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 $|\ |$. One can choose L so that $[L:K] = [\hat{L}:\hat{K}]$, in which case $\hat{L} = \hat{K} \cdot L$.*

Proof. Let $\hat{L}/\hat{K}$ be a separable extension of degree n. If $|\ |$ is archimedean then K is a number field and $\hat{K}$ is either $\mathbb{R}$ or $\mathbb{C}$; the only nontrivial case is $\hat{K} \simeq \mathbb{R}$ and $n = 2$, and we may then assume that $\hat{L} = \hat{K}(\sqrt{d}) \simeq \mathbb{C}$ where $d \in \mathbb{Z}_{<0}$ is any 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 $[L:K] = [\hat{L}:\hat{K}] = 2$, and $\hat{L}$ is the compositum of $\hat{K}$ and L.

We now suppose that $|\ |$ is nonarchimedean, in which case the valuation ring of $\hat{K}$ is a complete DVR and $|\ |$ is induced by its 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 $g \in K[x] \subseteq \hat{K}[x]$ such that $\|g - f\|_1 < \delta$ for any $\delta > 0$. It then follows from Theorem 11.19 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 10.4 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 L and $\hat{K}$, so it must be $\hat{L}$. □

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 11.21. 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 $\hat{L}$. 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 11.22. *For every finite Galois extension $\hat{L}/\hat{K}$ of local fields there is a finite 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 $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\hat{L}/\hat{K})$.*

Proof. The archimedean case is already covered by Theorem 11.20 (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 10.4. The field $\hat{K}$ is an extension of either $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$, and by applying Theorem 11.20 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 $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\hat{L}/\hat{K})$ as desired. □

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 8.20 that if $\mathfrak{p}$ is a prime of K (a nonzero prime ideal of A), each prime $\mathfrak{q}|\mathfrak{p}$ induces a valuation $v_\mathfrak{q}$ of L that extends the valuation $v_\mathfrak{p}$ of K with index $e_\mathfrak{q}$, meaning that $v_\mathfrak{q}|_K = e_\mathfrak{q} v_\mathfrak{p}$ (and 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 $v_\mathfrak{p}$ to obtain a complete field $K_\mathfrak{p}$, and similarly complete L with respect to $|\ |_\mathfrak{q}$ for some $\mathfrak{q}|\mathfrak{p}$ to obtain $L_\mathfrak{q}$. 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 $\mathfrak{q}|\mathfrak{p}$; as proved below, the embedding $K \hookrightarrow L$ induces an embedding $K_\mathfrak{p} \hookrightarrow L_\mathfrak{q}$ of topological fields in which the absolute value $|\ |_\mathfrak{p}$ on $K_\mathfrak{p}$ is equivalent to the restriction of $|\ |_\mathfrak{q}$ to $K_\mathfrak{p}$ (if we define $|\ |_\mathfrak{q}$ as in Theorem 10.4, $|\ |_\mathfrak{p}$ will be the restriction of $|\ |_\mathfrak{q}$).

In general the extension $L_\mathfrak{q}/K_\mathfrak{p}$ may have smaller degree than L/K. If $L \simeq K[x]/(f)$, 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 $\mathfrak{p}$; the Dedekind-Kummer theorem gives a one-to-one correspondence between irreducible factors of f in $K_\mathfrak{p}[x]$ and primes $\mathfrak{q}|\mathfrak{p}$ (via Hensel's Lemma). The following theorem gives a complete description of the situation.

Theorem 11.23. *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 $K_\mathfrak{p}$ be the completion of K with respect to $|\ |_\mathfrak{p}$, and let $\hat{\mathfrak{p}}$ be 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 $\hat{\mathfrak{q}}$ the maximal ideal of its valuation ring. The following hold:*

(1) *Each $L_\mathfrak{q}$ is a finite separable extension of $K_\mathfrak{p}$ with $[L_\mathfrak{q} : K_\mathfrak{p}] \le [L : K]$.*

(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 $f_{\hat{\mathfrak{q}}} = f_\mathfrak{q}$.*

(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 $\ell \otimes x \mapsto (\ell x, \dots, \ell x)$ 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 that we are not assuming they are local fields).

(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 $[(x_n)] \mapsto [(x_n)]$ on equivalence classes of Cauchy sequences; a sequence (x_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 may thus view $K_\mathfrak{p}$ as a topological subfield of $L_\mathfrak{q}$, and it is clear that $[L_\mathfrak{q} : K_\mathfrak{p}] \le [L : K]$, since any K-basis $b_1, \dots, b_m$ for $L \subseteq L_\mathfrak{q}$ spans $L_\mathfrak{q}$ as a $K_\mathfrak{p}$-vector space: given a Cauchy sequence $y := (y_n)$ of elements in L, if we write each y_n as $x_{1,n}b_1 + \cdots + x_{m,n}b_m$ with $x_{i,n} \in K$ we obtain Cauchy sequences $x_1 := (x_{1,n}), \cdots, x_m := (x_{m,n})$ of elements in K (linear maps of finite dimensional normed spaces are uniformly continuous and thus preserves Cauchy sequences), and we can write $[y] = [x_1]b_1 + \cdots [x_m]b_m$ as a $K_\mathfrak{p}$-linear combination of $b_1, \dots, b_m$.

The field L is a finite étale K-algebra, since L/K is a separable extension, so its base change $L \otimes_K K_\mathfrak{p}$ to $K_\mathfrak{p}$ is a finite étale $K_\mathfrak{p}$-algebra, by Proposition 4.36. Let us now consider the $K_\mathfrak{p}$-algebra homomorphism $\phi_\mathfrak{q} \colon L \otimes_K K_\mathfrak{p} \to L_\mathfrak{q}$ defined by $\ell \otimes x \mapsto \ell x$. We have

$\phi_{\mathfrak{q}}(b_i \otimes 1) = b_i$ for each of our K-basis elements $b_i \in L$, and as noted above, $b_1, \dots b_m$ span $L_{\mathfrak{q}}$ as $K_{\mathfrak{p}}$-vector space, thus $\phi_{\mathfrak{q}}$ is surjective. As a finite étale $K_{\mathfrak{p}}$-algebra, $L \otimes_K K_{\mathfrak{p}}$ is by definition isomorphic to a finite product of finite separable extensions of $K_{\mathfrak{p}}$; by Proposition 4.32, $L_{\mathfrak{q}}$ is isomorphic to a subproduct and thus also a finite étale $K_{\mathfrak{p}}$-algebra; in particular, $L_{\mathfrak{q}}/K_{\mathfrak{p}}$ is separable.

(2) As noted above, the valuation rings of $K_{\mathfrak{p}}$ and the $L_{\mathfrak{q}}$ are complete DVRs, so this follows immediately from Theorem 9.22.

(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 $v_{\hat{\mathfrak{q}}}$ extends $v_{\hat{\mathfrak{p}}}$ 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 $[L_{\mathfrak{q}} : K_{\mathfrak{p}}] = e_{\mathfrak{q}} f_{\mathfrak{q}}$, by Theorem 5.43.

(5) Let $\phi := \prod_{\mathfrak{q}|\mathfrak{p}} \phi_{\mathfrak{q}}$, where $\phi_{\mathfrak{q}} \colon L \otimes_K K_{\mathfrak{p}} \to L_{\mathfrak{q}}$ is the surjective $K_{\mathfrak{p}}$-algebra homomorphism 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 taking the base change of a finite étale algebra does not change its dimension (see Proposition 4.36), we have

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

Pick a $K_{\mathfrak{p}}$-basis $\{\beta_i\}$ for $\prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}$, fix $\epsilon > 0$, and for each basis element $\beta_i = (\beta_{i,\mathfrak{q}})_{\mathfrak{q}|\mathfrak{p}}$ use the weak approximation theorem proved in Problem Set 4 to construct $\alpha_i \in L$ such that $|\alpha_i - \beta_{i,\mathfrak{q}}|_{\mathfrak{q}} < \epsilon$ for all $\mathfrak{q}|\mathfrak{p}$. In the metric space $\prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}$ (with the sup norm), each $\phi(\alpha_i \otimes 1)$ is close to β_i. The $K_{\mathfrak{p}}$-matrix whose jth column expresses $\phi(\alpha_j \otimes 1)$ in terms of the basis $\{\beta_i\}$ is then close to the identity matrix (with respect to $|\ |_{\mathfrak{p}}$), and the determinant D of this matrix is close to 1 (the determinant is continuous). For sufficiently small ϵ we must have $D \neq 0$, and then $\{\phi(\alpha_i \otimes 1)\}$ is a basis for $\prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}$. It follows that ϕ is surjective and therefore an isomorphism, since its domain and codomain have the same dimension.

(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 $\varphi \colon D_{\mathfrak{q}} \to \mathrm{Aut}_{K_{\mathfrak{p}}}(L_{\mathfrak{q}})$.

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,

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

by Theorem 11.23, so $\#\mathrm{Aut}_{K_{\mathfrak{p}}}(L_{\mathfrak{q}}) = [L_{\mathfrak{q}} : K_{\mathfrak{p}}]$ 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 $\hat{\mathfrak{q}}$ of $L_{\mathfrak{q}}$, and it is necessarily fixed by every $\sigma \in \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$, so $\mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}) \simeq D_{\hat{\mathfrak{q}}}$. 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 11.24. *Assume AKLB and let $\mathfrak{p}$ be a prime of A. For every $\alpha \in L$ we have*

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

where we view α as an element of $L_{\mathfrak{q}}$ and $\mathrm{N}_{L/K}(\alpha)$ as an element of $K_{\mathfrak{p}}$ via the canonical embeddings $L \hookrightarrow L_{\mathfrak{q}}$ and $K \hookrightarrow K_{\mathfrak{p}}$.

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 11.23, which commutes with the norm and trace. □

Remark 11.25. Theorem 11.23 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 $\mathfrak{q}|\mathfrak{p}$ of L, 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 11.26. *Assume AKLB and let $\mathfrak{p}$ be a prime of A. Let $\mathfrak{p}B = \prod \mathfrak{q}^{e_{\mathfrak{q}}}$ be the factorization of $\mathfrak{p}B$ in B. Let $\hat{A}_{\mathfrak{p}}$ denote the completion of A with respect to $|\ |_{\mathfrak{p}}$, and for each $\mathfrak{q}|\mathfrak{p}$, let $\hat{B}_{\mathfrak{q}}$ denote the completion of B with respect to $|\ |_{\mathfrak{q}}$. Then $B \otimes_A \hat{A}_{\mathfrak{p}} \simeq \prod_{\mathfrak{q}|\mathfrak{p}} \hat{B}_{\mathfrak{q}}$, as $\hat{A}_{\mathfrak{p}}$-algebras.*

Proof. After replacing A with $A_{\mathfrak{p}}$ and B with $B_{\mathfrak{p}}$ (localizing B as an A-module), we may assume that A is a DVR and B/A is a free A module of rank $n := [L : K] = \sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}}$. Then $B \otimes_A \hat{A}_{\mathfrak{p}}$ is a free $\hat{A}_{\mathfrak{p}}$-module of rank n. Viewing $\hat{A}_{\mathfrak{p}}$ and the $\hat{B}_{\mathfrak{q}}$ as valuation rings of $K_{\mathfrak{p}}$ and $L_{\mathfrak{q}}$, it follows from part (4) of Theorem 11.23 that $\prod \hat{B}_{\mathfrak{q}}$ is a free $\hat{A}_{\mathfrak{p}}$-module of rank $\sum_{\mathfrak{q}|\mathfrak{p}} [L_{\mathfrak{q}} : K_{\mathfrak{p}}] = \sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}} = n$. These isomorphic $\hat{A}_{\mathfrak{p}}$-modules lie in isomorphic finite étale $K_{\mathfrak{p}}$-algebras $L \otimes_K K_{\mathfrak{p}} \simeq \prod L_{\mathfrak{q}}$, by part (5) of Theorem 11.23, and this $K_{\mathfrak{p}}$-algebra isomorphism restricts to an $\hat{A}_{\mathfrak{p}}$-algebra isomorphism. □

Remark 11.27. Let A be a Dedekind domain with fraction field K. If we localize A at a prime $\mathfrak{p}$ we obtain a DVR $A_{\mathfrak{p}}$ with the same fraction field K. We can then complete $A_{\mathfrak{p}}$ with respect to $|\ |_{\mathfrak{p}}$ to obtain a complete DVR $\hat{A}_{\mathfrak{p}}$ whose fraction field $K_{\mathfrak{p}}$ is the completion of K with respect to $|\ |_{\mathfrak{p}}$, and $\hat{A}_{\mathfrak{p}}$ is then the valuation ring of $K_{\mathfrak{p}}$. Alternatively, we could first complete A with respect to the absolute value $|\ |_{\mathfrak{p}}$ induced by $\mathfrak{p}$ and then localize. But as explained in Lecture 8, completing A with respect to $|\ |_{\mathfrak{p}}$ is the same thing as taking the valuation ring of $K_{\mathfrak{p}}$, so the completion of A is already the complete DVR $\hat{A}_{\mathfrak{p}}$ we obtained by localizing and completing; there is no need to localize and nothing would change if we did. Completion not only commutes with localization, it makes localization unnecessary.

References

[1] Michael Artin, *Algebra*, 2nd edition, Pearson, 2010.

[2] 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.

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