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 $p$ then $B$ is a complete DVR with maximal ideal $q$ and $[L : K] = n = e_qf_q$. Assuming the residue field extension is separable (true if $K$ is a local field), after replacing $K$ with its maximal unramified extension in $L$ we obtain a totally ramified extension, with ramification index $e_q = n$ and residue field degree $f_q = 1$. We now consider this case.

11.1 Totally ramified extensions of a complete DVR

Definition 11.1. Let $A$ be a DVR with maximal ideal $p$. A monic polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in A[x]$$

is Eisenstein (or an Eisenstein polynomial) if $a_i \in p$ for $0 \leq i < n$ and $a_0 \not\in p^2$; equivalently, if $v_p(a_i) \geq 1$ for $0 \leq i < n$ and $v_p(a_0) = 1$. Note that $a_0$ is then a uniformizer for $A$.

Lemma 11.2 (Eisenstein irreducibility). Let $A$ be a DVR with fraction field $K$ and maximal ideal $p$, 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 $n \geq 2$ for some non-constant monic $g, h \in A[x]$. Put $f = \sum_i f_ix^i, g = \sum_i g_ix^i, h = \sum_i h_ix^i$. We have $f_0 = g_0h_0 \in p - p^2$, so exactly one of $g_0,h_0$ lies in $p$; assume without loss of generality that $g_0 \not\in p$ and $h_0 \in p$. Let $i > 0$ be the least $i$ for which $h_i \not\in p$; such an $i < n$ exists because $h$ is monic and $deg h < n$. We have

$$f_i = g_0h_i + g_1h_{i-1} + \cdots + g_{i-1}h_1 + g_ih_0,$$

with $f_i \in p$, since $f$ is Eisenstein and $i < n$, and $h_jg_{i-j} \in p$ for $0 \leq j < i$, by the minimality of $i$, which implies $g_0h_i \in p$, contradicting $g_0,h_i \not\in p$. Thus $f$ is irreducible in $A[x]$, and since $A$ is a DVR, and therefore 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 $A_p$; the rings $A_p$ and $A$ have the same fraction field $K$ and $f$ is then irreducible in $K[x]$, hence in $A[x]$; this yields the well known Eisenstein criterion for irreducibility.

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

Proof. Let $p$ be the maximal ideal of $A$. We have $f \equiv x^n \mod p$, so by Corollary 10.13 the ideal $q = (p,x) = (p,\pi)$ is the only maximal ideal of $B$. Let $f = \sum_i f_ix^i$; then $p = (f_0)$ and $q = (f_0,\pi)$, and $f_0 = -f_1\pi - f_2\pi^2 - \cdots - \pi^n \in (\pi)$, so $q = (\pi)$. The unique maximal ideal $(\pi)$ of $B$ is nonzero and principal, so $B$ is a DVR with uniformizer $\pi$.

Theorem 11.5. Assume $AKLB$ with $A$ a complete DVR and $\pi$ a uniformizer for $B$. The extension $L/K$ is totally ramified if and only if $B = A[\pi]$ and the minimal polynomial of $\pi$ is Eisenstein.

Proof. Let $n = [L : K]$, let $p$ be the maximal ideal of $A$, let $q$ be the maximal ideal of $B$ (which we recall is a complete DVR, by Theorem 10.6), and let $\pi$ be a uniformizer for $B$.

Andrew V. Sutherland
with minimal polynomial $f$. If $B = A[\pi]$ and $f$ is Eisenstein, then as in Lemma 11.4 we have $p = q^n$, so $v_q$ extends $v_p$ with index $e_q = n$ and $L/K$ is totally ramified.

We now suppose $L/K$ is totally ramified. Then $v_q$ extends $v_p$ with index $n$, which implies $v_q(K) = n\mathbb{Z}$. The set $\{\pi^0, \pi^1, \pi^2, \ldots, \pi^{n-1}\}$ is linearly independent over $K$, since the valuations of $\pi^0, \ldots, \pi^{n-1}$ are distinct modulo $v_q(K) = n\mathbb{Z}$ (if $\sum_{i=0}^{n-1} x_i\pi^i = 0$ we must have $v_q(x_i\pi^i) = v_q(x_i\pi^j)$ for some nonzero $x_i \neq x_j$, which is impossible). Thus $L = K(\pi)$.

Let $f = \sum_{i=0}^{n} a_ix^i \in A[x]$ be the minimal polynomial of $\pi$. We have $v_q(f(\pi)) = \infty$ and $v_q(a_i\pi^i \equiv i \bmod n$ for $0 \leq i \leq n$. This is possible only if

$$v_q(a_0) = v_q(a_0\pi^0) = v_q(a_n\pi^n) = v_q(\pi^n) = n,$$

and $v_q(a_i) \geq n$ for $0 \leq i < n$. This implies that $v_q(a_0) = 1$, since $v_q$ extends $v_p$ with index $n$, and $v_q(a_i) \geq 1$ for $0 \leq i < n$. Thus $f$ is Eisenstein and Lemma 11.4 implies that $A[\pi] \subseteq B$ is a DVR, 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 $p = 0$ or if $e_{L/K} = 1$, so an unramified extension is also tamely ramified). Otherwise $L/K$ is wildly ramified if $p | e_{L/K}$; this can occur only when $p > 0$. If $L/K$ is totally ramified, then it is totally tamely ramified if $p \nmid e_{L/K}$ and totally wildly ramified otherwise.

**Theorem 11.8.** 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 $\pi_A$ 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, in which case $p \nmid n$, and let $p$ and $q$ be the maximal ideals of $A$ and $B$ with uniformizers $\pi_A$ and $\pi_B$ respectively. Then $v_q$ extends $v_p$ with index $e_q = n$ and $v_q(\pi_B^n) = n = v_q(\pi_A)$. This implies that $\pi_B^n = u\pi_A$ for some unit $u \in B^\times$. We have $f_q = 1$, so $B$ and $A$ have the same residue field, and if we lift the image of $u$ in $B/q \simeq A/p$ to a unit $u_A$ in $A$ and replace $\pi_A$ with $u_A^{-1}\pi_A$, we can assume that $u \equiv 1 \bmod q$. Now define $g(x) := x^n - u \in B[x]$ with reduction $\bar{g} = x^n - 1 \bmod (B/q)[x]$. 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 $B/q$ to a root $r$ of $g(x)$ in $B$. Now let $\pi := \pi_B/r$. Then $\pi$ 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.

### 11.2 Krasner’s lemma

Let $K$ be the fraction field of a complete DVR with absolute value $\| \|$. By Theorem 10.6 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 10.7, this induces a unique absolute value on $K$ that restricts to the absolute value of $K$. 

18.785 Fall 2017, Lecture #11, Page 2
Lemma 11.9. Let $K$ be the fraction field of a complete DVR with algebraic closure $\overline{K}$ and absolute value $|\cdot|$ extended to $\overline{K}$. For all $\alpha \in \overline{K}$ and $\sigma \in \text{Aut}_K(\overline{K})$ we have $|\sigma(\alpha)| = |\alpha|$.

Proof. The elements $\alpha$ and $\sigma(\alpha)$ must have the same minimal polynomial $f \in K[x]$, since $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$, so $N_{K(\alpha)/K}(\alpha) = N_{K(\sigma(\alpha))/K(\alpha)}(\sigma(\alpha))$, by Proposition 4.51. It follows that $|\sigma(\alpha)| = |N_{K(\sigma(\alpha))/K(\alpha)}(\sigma(\alpha))|^{1/n} = |N_{K(\alpha)/K(\alpha)}(\alpha)|^{1/n} = |\alpha|$, where $n = \deg f$. \hfill \Box

Definition 11.10. Let $K$ be the fraction field of a complete DVR with absolute value $|\cdot|$ extended to an algebraic closure $\overline{K}$. For $\alpha, \beta \in \overline{K}$, we say $\beta$ belongs to $\alpha$ if $|\beta - \alpha| = |\beta - \sigma(\alpha)|$ for all $\sigma \in \text{Aut}_K(\overline{K})$ with $\sigma(\alpha) \neq \alpha$, that is, $\beta$ is strictly closer to $\alpha$ 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 11.11 (Krasner’s lemma). Let $K$ be the fraction field of a complete DVR and let $\alpha, \beta \in \overline{K}$, with $\alpha$ separable over $K$. If $\beta$ belongs to $\alpha$ then $K(\alpha) \subseteq K(\beta)$.

Proof. Suppose not. Then $\beta$ belongs to $\alpha$ but $\alpha \notin K(\beta)$. The extension $K(\alpha, \beta)/K(\beta)$ is separable and non-trivial, so there is an automorphism $\sigma \in \text{Aut}_{K(\beta)}(\overline{K}/K(\beta))$ for which $\sigma(\alpha) \neq \alpha$ (let $\sigma$ send $\alpha$ to a different root of the minimal polynomial of $\alpha$ over $K(\beta)$). Applying Lemma 11.9 to $\beta - \alpha \in \overline{K}$, for any $\sigma \in \text{Aut}_{K(\beta)}(\overline{K}/K(\beta))$ we have

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

since $\sigma$ fixes $\beta$. But this contradicts the hypothesis that $\beta$ belongs to $\alpha$, since $\sigma(\alpha) \neq \alpha$. \hfill \Box

Remark 11.12. 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 11.13. For a field $K$ with absolute value $|\cdot|$ the $L^1$-norm of $f \in K[x]$ is defined by.

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

where $f = \sum_i f_i x^i \in K[x]$; it is easily verified that $\|\cdot\|_1$ satisfies all the properties of Definition 10.3 and is thus a norm on the $K$-vector space $K[x]$.

Lemma 11.14. Let $K$ be a field with absolute value $|\cdot|$ and let $f := \prod_{i=1}^n (x - \alpha_i) \in K[x]$ be a monic polynomial with roots $\alpha_1, \ldots, \alpha_n \in L$, where $L/K$ is a field with an absolute value that extends $|\cdot|$. Then $|\alpha_i| < \|f\|_1$ for every root $\alpha$ of $f$.

Proof. The lemma is clear for $n \leq 1$, so assume $n \geq 2$. 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 $|\alpha| \leq 1$ the lemma holds, so let $\alpha$ be a root of $f$ with $|\alpha| > 1$. We have

$$0 = |f(\alpha)| = \alpha^n + \sum_{i=0}^{n-1} f_i \alpha^i \geq |\alpha|^n - \sum_{i=0}^{n-1} |f_i| |\alpha|^i \geq |\alpha|^n - |\alpha|^{n-1} \sum_{j=0}^{n-1} |f_j| \geq |\alpha| - (\|f\|_1 - 1),$$

where we have used $|\alpha| = |a + b - b| \leq |a + b| + | - b| = |a + b| + |b|$ to get the general inequality $|a + b| \geq |a| - |b|$ which we applied repeatedly to get the first inequality above, we used $|\alpha| > 1$ to get the second (replacing $|\alpha|^i$ with $|\alpha|^{i-1}$ in each term) and the third (dividing by $|\alpha|^{n-1} \geq 1$). Thus $\|f\|_1 - 1 \geq |\alpha|$, and therefore $\|f\|_1 \geq |\alpha| + 1 > |\alpha|$. \hfill \Box
Theorem 11.15 (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 $\beta$ of $g$ belongs to a root $\alpha$ 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 $\alpha_1, \ldots, \alpha_n$ 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 $\epsilon$ 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 $g(x) = \sum_i g_i x^i$ be a monic polynomial of degree $n$ with $\|f - g\|_1 < \delta$. We then have

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

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

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

We have $\|\beta\| < \|g\|_1$ by Lemma 11.14, and $\|g\|_1 \geq 1$, so $|\beta|^i < \|g\|_1 \leq \|g\|_1^n \leq \|g\|_1^n$. Thus

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

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 $\alpha_i$, and the triangle inequality implies that this $\alpha_i$ must be unique since $|\alpha_i - \alpha_j| \geq \epsilon$ for $i \neq j$. Therefore $\beta$ 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 $\beta$, 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 $\beta$ of $g$ belongs to a root $\alpha$ of $f$, then for any $\tau \in \text{Aut}_K(\overline{K})$ and all $\sigma \in \text{Aut}_K(\overline{K})$ 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 $\text{Aut}_K(\overline{K})$ acts transitively on the roots of $f$ and $g$, so every root $\beta$ of $g$ belongs to a distinct root $\alpha$ of $f$ for which $K(\beta) = K(\alpha)$. Therefore $g$ has the same splitting field as $f$. \qed
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 \( K = \mathbb{Q}_p \) (some \( p \leq \infty \)) or \( \hat{F}_q((t)) \) (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 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 \( | \cdot | \), 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 \( \hat{K} \) 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 11.16.** Let \( K \) be a global field with a nontrivial absolute value \( | \cdot | \), and let \( \hat{K} \) be the completion of \( K \) with respect to \( | \cdot | \). 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 \( | \cdot | \). One can choose \( L \) so that \( [L:K] = [\hat{L}:\hat{K}] \), in which case \( L = \hat{K} \cdot L \).

**Proof.** Let \( \hat{L}/\hat{K} \) be a separable extension of degree \( n \). If \( | \cdot | \) is archimedean then \( K \) is a number field and \( \hat{K} \) is either \( \mathbb{R} \) or \( \mathbb{C} \); the only nontrivial case is \( \hat{K} \simeq \mathbb{C} \) 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 \( | \cdot | \) 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 \( L \) is the compositum of \( \hat{K} \) and \( \hat{L} \).

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 \( \hat{L} = K[x]/(f) \) where \( f \in K[x] \) 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 \(|g-f| < \delta \) for any \( \delta > 0 \). It then follows from Theorem 11.15 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 10.6 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 to \(| | \) 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 \( \text{Gal}(\hat{L}/\hat{K}) \simeq \text{Gal}(L/K) \). As shown by the following example, this need not be the case.

**Example 11.17.** 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 \( \zeta_3 \) (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 11.18.** 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 $\text{Gal}(L/K) \simeq \text{Gal}(\hat{L}/\hat{K})$.

*Proof.* The archimedean case is already covered by Theorem 11.16 (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 10.6. The field $\hat{K}$ is an extension of either $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$, and by applying Theorem 11.16 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 $\varphi : \text{Gal}(\hat{L}/\hat{K}) \to \text{Gal}(M/K)$ induced by restriction, and $\varphi$ is injective (each $\sigma \in \text{Gal}(L/\hat{K})$ 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 $\varphi$ 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 $\text{Gal}(L/K) \simeq \text{Gal}(\hat{L}/\hat{K})$ as desired. \hfill $\square$

### 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 8.20 that if $p$ is a prime of $K$ (a nonzero prime ideal of $A$), each prime $q|p$ induces a valuation $v_q$ of $L$ that extends the valuation $v_p$ of $K$ with index $e_q$, meaning that $v_q|K = e_qv_p$ (and every valuation of $L$ that extends $v_p$ arises in this way). We now want to look at what happens when we complete $K$ with respect to the absolute value $| |_p$ induced by $v_p$ to obtain a complete field $K_p$, and similarly complete $L$ with respect to $| |_q$ for some $q|p$ to obtain $L_q$. This includes the case where $L/K$ is an extension of global fields, in which case we get a corresponding extension $L_q/K_p$ of local fields for each $q|p$; as proved above, the embedding $K \hookrightarrow L$ induces an embedding $K_p \hookrightarrow L_q$ of topological fields in which the absolute value $| |_p$ on $K_p$ is equivalent to the restriction of $| |_q$ to $K_p$ (if we define $| |_q$ as in Theorem 10.6 then $| |_p$ will be the restriction of $| |_q$).

In general the extension $L_q/K_p$ 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 $K_p$. Indeed, this will necessarily be the case if there is more than one prime $q$ lying above $p$; the Dedekind-Kummer theorem gives a one-to-one correspondence between irreducible factors of $f$ in $K_p[x]$.
and primes $q | p$ (via Hensel's Lemma). The following theorem gives a complete description of the situation.

**Theorem 11.19.** Assume $AKLB$, let $p$ be a prime of $K$, and let $pB = \prod_{q | p} q^{n_q}$ be the factorization of $pB$ in $B$. Let $K_p$ be the completion of $K$ with respect to $| \cdot |_p$, and let $\hat{p}$ be the maximal ideal of its valuation ring. For each $q | p$, let $L_q$ denote the completion of $L$ with respect to $| \cdot |_q$, and $\hat{q}$ the maximal ideal of its valuation ring. The following hold:

1. Each $L_q$ is a finite separable extension of $K_p$ with $[L_q : K_p] \leq [L : K]$.
2. Each $\hat{q}$ is the unique prime of $L_q$ lying over $\hat{p}$.
3. Each $\hat{q}$ has ramification index $e_\hat{q} = e_q$ and residue field degree $f_\hat{q} = f_q$.
4. $[L_q : K_p] = e_q f_\hat{q}$.
5. The map $L \otimes_K K_p \rightarrow \prod_{q | p} L_q$ defined by $\ell \otimes x \mapsto (\ell x, \ldots, \ell x)$ is an isomorphism of finite étale $K_p$-algebras.
6. If $L/K$ is Galois then each $L_q/K_p$ is Galois and we have isomorphisms of decomposition groups $D_q \simeq D_\hat{q} = Gal(L_q/K_p)$ and inertia groups $I_q \simeq I_\hat{q}$.

**Proof.** We first note that the $K_p$ and the $L_q$ 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 $q | p$ the embedding $K \rightarrowtail L$ induces an embedding $K_p \rightarrowtail L_q$ 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 $| \cdot |_p$, is also Cauchy in $L$ with respect to $| \cdot |_q$ because $v_q$ extends $v_p$. We may thus view $K_p$ as a topological subfield of $L_q$, and it is clear that $[L_q : K_p] \leq [L : K]$, since any $K$-basis $b_1, \ldots, b_m$ for $L \subseteq L_q$ spans $L_q$ as a $K_p$-vector space: given a Cauchy sequence $y := (y_n)$ of elements in $L$, if we write each $y_n$ as $x_1, b_1 + \cdots + x_m, b_m$ with $x_i \in K$ we obtain Cauchy sequences $x_1 := (x_1, b_1) \cdots, x_m := (x_m, b_m)$ 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 $K_p$-linear combination of $b_1, \ldots, b_m$.

The field $L$ is a finite étale $K$-algebra, since $L/K$ is separable, so its base change $L \otimes_K K_p$ to $K_p$ is a finite étale $K_p$-algebra, by Proposition 4.36. Let us now consider the $K_p$-algebra homomorphism $\phi_q : L \otimes_K K_p \rightarrow L_q$ defined by $\ell \otimes x \mapsto \ell x$. We have $\phi_q(b_i \otimes 1) = b_i$ for each of our $K$-basis elements $b_i \in L$, and as noted above, $b_1, \ldots, b_m$ span $L_q$ as $K_p$-vector space, thus $\phi_q$ is surjective. As a finite étale $K_p$-algebra, $L \otimes_K K_p$ is by definition isomorphic to a finite product of finite separable extensions of $K_p$; by Proposition 4.32, $L_q$ is isomorphic to a subproduct and thus also a finite étale $K_p$-algebra; in particular, $L_q/K_p$ is separable.

(2) As noted above, the valuation rings of $K_p$ and the $L_q$ are complete DVRs, so this follows immediately from Theorem 10.1.

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

(4) It follows from (2) that $[L_q : K_p] = e_q f_\hat{q}$, since $\hat{q}$ is the only prime above $\hat{p}$, and (3) then implies $[L_q : K_p] = e_q f_\hat{q}$, by Theorem 5.32.

(5) Let $\phi := \prod_{q | p} \phi_q$, where $\phi_q : L \otimes_K K_p \rightarrow L_q$ is the surjective $K_p$-algebra homomorphisms defined in the proof of (1). Then $\phi : L \otimes_K K_p \rightarrow \prod_{q | p} L_q$ is a $K_p$-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
\[
\dim_{\mathbb{Q}_p}(L \otimes_K K_p) = \dim_K L = [L : K] = \sum_{q \mid p} e_q f_q = \sum_{q \mid p} [L_q : K_p] = \dim_{\mathbb{Q}_p} \prod_{q \mid p} L_q.
\]
Pick a $K_p$-basis $\{\beta_i\}$ for $\prod_{q \mid p} L_q$, fix $\epsilon > 0$, and for each basis element $\beta_i = (\beta_{i,q})_{q \mid p}$ use the weak approximation theorem proved in Problem Set 4 to construct $\alpha_i \in L$ such that $|\alpha_i - \beta_{i,q}|_q < \epsilon$ for all $q \mid p$. In the metric space $\prod_{q \mid p} L_q$ (with the sup norm), each $\phi(\alpha_i \otimes 1)$ is close to $\beta_i$. The $K_p$-matrix whose $j$th column expresses $\phi(\alpha_j \otimes 1)$ in terms of the basis $\{\beta_i\}$ is then close to the identity matrix (with respect to $| \cdot |_p$), and the determinant $D$ of this matrix is close to 1 (the determinant is continuous). For sufficiently small $\epsilon$ we must have $D \neq 0$, and then $\{\phi(\alpha_i \otimes 1)\}$ is a basis for $\prod_{q \mid p} L_q$. It follows that $\phi$ is surjective and therefore an isomorphism, since its domain and codomain have the same dimension.

(6) We now assume $L/K$ is Galois. Each $\sigma \in D_q$ acts on $L$ and respects the valuation $v_q$, since it fixes $q$ (if $x \in q^n$ then $\sigma(x) \in q^{n \sigma} = q^n$). It follows that if $(x_n)$ is a Cauchy sequence in $L$, then so is $(\sigma(x_n))$, thus $\sigma$ is an automorphism of $L_q$, and it fixes $K_p$. We thus have a group homomorphism $\varphi : D_q \to \text{Aut}_{K_p}(L_q)$.

If $\sigma \in D_q$ acts trivially on $L_q$ then it acts trivially on $L \subseteq L_q$, so $\ker \varphi$ is trivial. Also,
\[
eq_q f_q = |D_q| \leq \#\text{Aut}_{K_p}(L_q) \leq [L_q : K_p] = e_q f_q,
\]
by Theorem 11.19, so $\#\text{Aut}_{K_p}(L_q) = [L_q : K_p]$ and $L_q/K_p$ is Galois, and this also shows that $\varphi$ is surjective and therefore an isomorphism. There is only one prime $\hat{q}$ of $L_q$, and it is necessarily fixed by every $\sigma \in \text{Gal}(L_q/K_p)$, so $\text{Gal}(L_q/K_p) \simeq D_q$. The inertia groups $I_q$ and $I_{\hat{q}}$ both have order $e_q = e_{\hat{q}}$, and $\varphi$ restricts to a homomorphism $I_q \to I_{\hat{q}}$, so the inertia groups are also isomorphic.

**Corollary 11.20.** Assume $AKLB$ and let $p$ be a prime of $A$. For every $\alpha \in L$ we have
\[
N_{L/K}(\alpha) = \prod_{q \mid p} N_{L_q/K_p}(\alpha) \quad \text{and} \quad T_{L/K}(\alpha) = \sum_{q \mid p} T_{L_q/K_p}(\alpha),
\]
where we view $\alpha$ as an element of $L_q$ via the canonical embedding $L \hookrightarrow L_q$.

**Proof.** The norm and trace are defined as the determinant and trace of $K$-linear maps $L \xrightarrow{\alpha} L$ that are unchanged upon tensoring with $K_p$; the corollary then follows from the isomorphism in part (5) of Theorem 11.19, which commutes with the norm and trace.

**Remark 11.21.** Theorem 11.19 can be stated more generally in terms of equivalence classes of absolute values, or *places*. Rather than working with a prime $p$ of $K$ and primes $q|p$ of $L$, one works with an absolute value $| \cdot |_v$ of $K$ (for example, $| \cdot |_p$) and inequivalent absolute values $| \cdot |_w$ of $L$ that extend $| \cdot |_v$. Places will be discussed further in the next lecture.

**Corollary 11.22.** Assume $AKLB$ and let $p$ be a prime of $A$. Let $pB = \prod q^n$ be the factorization of $pB$ in $B$. Let $\hat{A}_q$ denote the completion of $A$ with respect to $| \cdot |_p$, and for each $q|p$, let $\hat{B}_q$ denote the completion of $B$ with respect to $| \cdot |_q$. Then $B \otimes_A \hat{A}_p \simeq \prod_{q|p} \hat{B}_q$, as $\hat{A}_p$-algebras.

**Proof.** After replacing $A$ with $A_p$ and $B$ with $B_p$ (localizing $B$ as an $A$-module), we may assume that $A$ is a DVR and $B/A$ is a free $A$ module of rank $n := [L : K] = \sum_{q|p} e_q f_q$. 

18.785 Fall 2017, Lecture #11, Page 8
Then $B \otimes_A \hat{A}_p$ is a free $\hat{A}_p$-module of rank $n$. Viewing $\hat{A}_p$ and the $\hat{B}_q$ as valuation rings of $K_p$ and $L_q$, it follows from part (4) of Theorem 11.19 that $\prod \hat{B}_q$ is a free $\hat{A}_p$-module of rank $\sum_{q \mid p} [L_q : K_p] = \sum_{q \mid p} \epsilon_q l_q = n$. These isomorphic $\hat{A}_p$-modules lie in isomorphic finite étale $K_p$-algebras $L \otimes_K \hat{K}_p \simeq \prod L_q$, by part (5) of Theorem 11.19, and this $K_p$-algebra isomorphism restricts to an $\hat{A}_p$-algebra isomorphism.

**Remark 11.23.** Let $A$ be a Dedekind domain with fraction field $K$. If we localize $A$ at a prime $p$ we obtain a DVR $A_p$ with the same fraction field $K$. We can then complete $A_p$ with respect to $\mid \mid_p$ to obtain a complete DVR $\hat{A}_p$ whose fraction field $K_p$ is the completion of $K$ with respect to $\mid \mid_p$, and $\hat{A}_p$ is then the valuation ring of $K_p$. Alternatively, we could first complete $A$ with respect to the absolute value $\mid \mid_p$ induced by $p$ and then localize. But as explained in Lecture 8, completing $A$ with respect to $\mid \mid_p$ is the same thing as taking the valuation ring of $K_p$, so the completion of $A$ is already the complete DVR $A_p$ 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.

Henceforth if $A$ is a Dedekind domain and $p$ is a prime of $A$ (a nonzero prime ideal), by the *completion of $A$ at $p$* we mean the ring $\hat{A}_p$.

**References**


18.785 Number Theory I
Fall 2017

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