10 Extensions of complete DVRs

Let A be a complete DVR with fraction field K and maximal ideal $\mathfrak{p}$. In the previous lecture we showed that every finite separable extension L/K is complete with respect to the unique absolute value on L extending the absolute value $|\ |_\mathfrak{p}$ on K, and the valuation ring B of L (equivalently, the integral closure of A in L) is a complete DVR whose valuation $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with index $e_\mathfrak{q}$. In this situation the formula $n := [L : K] = \sum_{\mathfrak{p}|\mathfrak{q}} e_\mathfrak{q} f_\mathfrak{q}$ simplifies to $n = e_\mathfrak{q} f_\mathfrak{q}$, which we may simply write as $n = ef = e_{L/K} f_{L/K}$ since the primes $\mathfrak{p}$ and $\mathfrak{q}$ are both determined once K and L are given. Here $f := [l : k]$ is the degree of the residue field extension $l := (B/\mathfrak{q})$ over $k := (A/\mathfrak{p})$. We now simplify matters even further by reducing to the cases $n = e$ (a totally ramified extension) and $n = f$ (an unramified extension, provided that l/k is separable). We first consider the unramified case.

10.1 Unramified extensions of a complete DVR

Let A be a complete DVR with fraction field K and residue field k. Associated to any finite unramified extension of L/K of degree n is a corresponding finite separable extension of residue fields l/k of the same degree n.[1] Recall from Definition 5.9 that the separability of l/k is part of what it means for L/K to be an unramified extension L/K. One can have ramified extensions L/K for which the corresponing residue field extension l/k is inseparable, but for the cases we are interested in, K is a local field and l/k is necessary inseparable because the residue field k is finite (by Proposition 9.4), hence perfect.

Given that the extensions L/K and l/k are both finite separable extensions of the same degree, we might then ask how they are related. More precisely, if we fix K with residue field k, what is the relationship between finite unramified extensions L/K of degree n and the finite separable extensions l/k of degree n? We know each L uniquely determines a corresponding residue field l, but what about the converse?

This question has a surprisingly nice answer. The finite unramified extensions L of K form a category $\mathcal{C}_K$ whose morphisms are K-algebra homomorphisms, and the finite separable extensions l of k form a category $\mathcal{C}_k$ whose morphisms are k-algebra homomorphisms. These two categories are equivalent.

Theorem 10.1. *Let A be a complete DVR with fraction field K and residue field $k := A/\mathfrak{p}$. The categories of finite unramified extensions L/K and finite separable extensions l/k are equivalent via the functor $\mathcal{F}$ that sends each L to its residue field l and each K-algebra homomorphism $\varphi\colon L_1 \to L_2$ to the induced k-algebra homomorphism $\bar\varphi\colon l_1 \to l_2$ of residue fields defined by $\bar\varphi(\bar\alpha) := \overline{\varphi(\alpha)}$, where α denotes any lift of $\bar\alpha \in l_1 = B_1/\mathfrak{q}_1$ to B_1 and $\overline{\varphi(\alpha)}$ is the reduction of $\varphi(\alpha) \in B_2$ to $B_2/\mathfrak{q}_2 = l_2$.*

In particular, $\mathcal{F}$ defines a bijection between the isomorphism classes of objects in each category, and if L_1 and L_2 and have residue fields l_1 and l_2 then $\mathcal{F}$ gives a bijection

$$\mathrm{Hom}_K(L_1, L_2) \xrightarrow{\sim} \mathrm{Hom}_k(l_1, l_2).$$

Proof. Let us first verify that $\mathcal{F}$ is well-defined. It is clear that it maps finite unramified extensions L/K to finite separable extension l/k, but we should check that the map on morphisms actually makes sense. In particular, we should verify that it does not depend

[1] Note that when we refer to an unramified or totally ramified extension L/K, we are always assuming L/K is separable, this assumption was made in Definition 5.9 when we defined the terminology.

on the lift α of $\bar{\alpha}$ we pick. So let $\varphi\colon L_1 \to L_2$ be a K-algebra homomorphism, and for $\bar{\alpha} \in l_1$, let α and β be two lifts of $\bar{\alpha}$ to B_1. Then $\alpha - \beta \in \mathfrak{q}_1$, and this implies that $\varphi(\alpha - \beta) \in \varphi(\mathfrak{q}_1) \subseteq \mathfrak{q}_2$, and therefore $\overline{\varphi(\alpha)} = \overline{\varphi(\beta)}$. The inclusion $\varphi(\mathfrak{q}_1) \subseteq \mathfrak{q}_2$ follows from the fact that the K-algebra homomorphism φ (which becomes an isomorphism if we restrict its codomain to its image, since every field homomorphism is injective) must preserve the unique absolute values on L_1 and $\varphi(L_1)$ extending the absolute value on K. The key point is that these absolute values are completely determined by the corresponding valuation rings (the elements of absolute value up to 1), and by Theorem 9.25, the valuation rings of L_1 and $\varphi(L_1)$ are precisely the sets of integral elements: integrality is necessarily preserved by the K-algebra homomorphism φ, since it fixes the coefficients of any polynomial in $A[x]$. It's easy to see that $\mathcal{F}$ sends identity morphisms to identity morphisms and that it is compatible with composition, so we do in fact have a well-defined functor.

To show that $\mathcal{F}$ is an equivalence of categories we need to prove two things:

- $\mathcal{F}$ is essentially surjective: every l is isomorphic to the residue field of some L.
- $\mathcal{F}$ is full and faithful: the induced map $\operatorname{Hom}_K(L_1, L_2) \to \operatorname{Hom}_k(l_1, l_2)$ is a bijection.

We first show that $\mathcal{F}$ is essentially surjective. Given a finite separable extension l/k, we may apply the primitive element theorem to write

$$l \simeq k(\bar{\alpha}) = \frac{k[x]}{(\bar{g}(x))},$$

for some $\bar{\alpha} \in l$ whose minimal polynomial $\bar{g} \in k[x]$ is necessarily monic, irreducible, separable, and of degree $n := [l : k]$. Let $g \in A[x]$ be any lift of $\bar{g}$. Then g is also monic, irreducible, separable, and of degree n. Define

$$L := \frac{K[x]}{(g(x))} = K(\alpha),$$

where α is the image of x in $K[x]/g(x)$ and has minimal polynomial g. Then L/K is a finite separable extension with valuation ring $B = A[\alpha] = A[x]/(g(x))$, and its maximal ideal is $\mathfrak{q} = (\mathfrak{p}, g(\alpha))$, by the Dedekind-Kummer Theorem 6.13; note that $B = A[\alpha]$ by construction, it is not something we need to prove. The corresponding residue field is

$$B/\mathfrak{q}B \simeq \frac{A[x]}{(\mathfrak{p}, g(x))} \simeq \frac{(A/\mathfrak{p})[x]}{(\bar{g}(x))} \simeq l.$$

We have $[L : K] = \deg g = [l : k] = n$, and it follows that L/K is an unramified extension of degree $n = f := [l : k]$; the ramification index of $\mathfrak{q}$ is necessarily $e = n/f = 1$, and the extension l/k is separable by assumption.

We now show that the functor $\mathcal{F}$ is full and faithful. Given finite unramified extensions L_1, L_2 with valuation rings B_1, B_2 and residue fields l_1, l_2, we have induced maps

$$\operatorname{Hom}_K(L_1, L_2) \xrightarrow{\sim} \operatorname{Hom}_A(B_1, B_2) \longrightarrow \operatorname{Hom}_k(l_1, l_2).$$

The first map is given by restriction from L_1 to B_1, and since tensoring with K gives an inverse map in the other direction, it is a bijection. We need to show that the same is true of the second map, which sends $\varphi\colon B_1 \to B_2$ to the k-homomorphism $\overline{\varphi}$ that sends $\overline{\alpha} \in l_1 = B_1/\mathfrak{q}_1$ to the reduction of $\varphi(\alpha)$ modulo $\mathfrak{q}_2$, where α is any lift of $\bar{\alpha}$.

As above, use the primitive element theorem to write $l_1 = k(\bar{\alpha}) = k[x]/(\bar{g}(x))$ for some $\bar{\alpha} \in l_1$. If we now lift $\bar{\alpha}$ to $\alpha \in B_1$, we must have $L_1 = K(\alpha)$, since $[L_1 : K] = [l_1 : k]$ is equal to the degree of the minimal polynomial $\bar{g}$ of $\bar{\alpha}$ which cannot be less than the degree of the minimal polynomial g of α (both are monic). Moreover, we also have $B_1 = A[\alpha]$, since this is true of the valuation ring of every finite unramified extension in our category, as shown above.

Each A-module homomorphism in

$$\mathrm{Hom}_A(B_1, B_2) = \mathrm{Hom}_A\left(\frac{A[x]}{(g(x))}, B_2\right)$$

is uniquely determined by the image of x in B_2. Thus gives us a bijection between $\mathrm{Hom}_A(B_1, B_2)$ and the roots of g in B_2. Similarly, each k-algebra homomorphism in

$$\mathrm{Hom}_k(l_1, l_2) = \mathrm{Hom}_k\left(\frac{k[x]}{(\bar{g}(x))}, l_2\right)$$

is uniquely determined by the image of x in l_2, and there is a bijection between $\mathrm{Hom}_k(l_1, l_2)$ and the roots of $\bar{g}$ in l_2. Now $\bar{g}$ is separable, so every root of $\bar{g}$ in $l_2 = B_2/\mathfrak{q}_2$ lifts to a unique root of g in B_2, by Hensel's Lemma 9.13. Thus the map $\mathrm{Hom}_A(B_1, B_2) \longrightarrow \mathrm{Hom}_k(l_1, l_2)$ induced by $\mathcal{F}$ is a bijection. $\square$

Remark 10.2. In the proof above we actually only used the fact that L_1/K is unramified. The map $\mathrm{Hom}_K(L_1, L_2) \to \mathrm{Hom}_k(l_1, l_2)$ is a bijection even if L_2/K is not unramified.

Let us note the following corollary, which follows from our proof of Theorem 10.1.

Corollary 10.3. *Assume AKLB with A a complete DVR with residue field k. Then L/K is unramified if and only if $B = A[\alpha]$ for some $\alpha \in L$ whose minimal polynomial $f \in A[x]$ has separable image $\bar{f}$ in $k[x]$.*

When the residue field k is finite (always the case if K is a local field), we can give an even more precise description of the finite unramified extensions L/K.

Corollary 10.4. *Let A be a complete DVR with fraction field K and finite residue field $k = \mathbb{F}_q$, and let ζ_n be a primitive nth root of unity in some algebraic closure of $\overline{K}$, with n prime to the characteristic of k. The extension $K(\zeta_n)/K$ is unramified.*

Proof. The field $K(\zeta_n)$ is the splitting field of $f(x) = x^n - 1$ over K. The image $\bar{f}$ of f in $k[x]$ is separable if and only if n is not divisible by p: we can have $\gcd(\bar{f}, \bar{f}')$ nontrivial only when $\bar{f}' = nx^{n-1}$ is zero, equivalently, only when $p|n$. If $p \nmid n$ then $\bar{f}(x)$ is separable and so are all of its divisors, including the minimal polynomial of ζ_n. $\square$

Corollary 10.5. *Let A be a complete DVR with fraction field K and finite residue field $k = \mathbb{F}_q$. Let L/K be an extension of degree n. Then L/K is unramified if and only if $L \simeq K(\zeta_{q^n-1})$, where ζ_{q^n-1} denotes a primitive $(q^n - 1)$-root of unity; if this is the case then $B \simeq A[\zeta_{q^n-1}]$ is the ring of integers of L.*

Proof. By the previous corollary, $K(\zeta_{q^n-1})$ is unramified. We now show that if L/K is unramified and has degree n, then $L = K(\zeta_{q^n-1})$.

The residue field extension l/k has degree n, so $l \simeq \mathbb{F}_{q^n}$ has cyclic multiplicative group generated by an element $\bar{\alpha}$ of order $q^n - 1$. The minimal polynomial $\bar{g} \in k[x]$ of $\bar{\alpha}$ therefore divides $x^{q^n-1}-1$, and since $\bar{g}$ is irreducible, it is coprime to the quotient $(x^{q^n-1}-1)/\bar{g}$. By Hensel's Lemma 9.17, we can lift $\bar{g}$ to a polynomial $g \in A[x]$ that divides $x^{q^n-1}-1 \in A[x]$, and by Hensel's Lemma 9.13 we can lift $\bar{\alpha}$ to a root α of g, in which case α is also a root of $x^{q^n-1}-1$; it must be a primitive (q^n-1)-root of unity because its reduction $\bar{\alpha}$ is. $\square$

Example 10.6. Consider $A = \mathbb{Z}_p$, $K = \mathbb{Q}_p$, $k = \mathbb{F}_p$, and fix $\overline{\mathbb{F}}_p$ and $\overline{\mathbb{Q}}_p$. For each positive integer n, the finite field $\mathbb{F}_p$ has a unique extension of degree n in $\overline{\mathbb{F}}_p$, namely, $\mathbb{F}_{p^n}$. Thus for each positive integer n, the local field $\mathbb{Q}_p$ has a unique unramified extension of degree n; it can be explicitly constructed by adjoining a primitive root of unity ζ_{p^n-1} to $\mathbb{Q}_p$. The element ζ_{p^n-1} will necessarily have minimal polynomial of degree n dividing $x^{p^n-1}-1$.

Definition 10.7. Let L/K be a separable extension. The *maximal unramified extension of K in L* is the subfield

$$\bigcup_{\substack{K\subseteq E\subseteq L\\ E/K \text{ fin. unram.}}} E \subseteq L$$

where the union is over finite unramified subextensions E/K. When $L = K^{\text{sep}}$ is the separable closure of K, this is the *maximal unramified extension of K*, denoted K^{unr}.

Example 10.8. The field $\mathbb{Q}_p^{\text{unr}}$ is an infinite extension of $\mathbb{Q}_p$ with Galois group

$$\operatorname{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \varprojlim_n \operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}},$$

where the inverse limit is taken over positive integers n ordered by divisibility. The ring $\hat{\mathbb{Z}}$ is the *profinite completion* of $\mathbb{Z}$. The field $\mathbb{Q}_p^{\text{unr}}$ has value group $\mathbb{Z}$ and residue field $\mathbb{F}_p$.

10.2 Totally ramified extensions of a complete DVR

We now consider the opposite extreme, where we have a totally ramified extension L/K of the fraction field of a complete DVR.

Definition 10.9. Let A be a DVR with maximal ideal $\mathfrak{p}$. A monic polynomial

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

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 10.10 (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 $f_0 = g_0h_0 \in \mathfrak{p} - \mathfrak{p}^2$, 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

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

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. $\square$

Remark 10.11. We can apply Lemma 10.10 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 $A[x]$.

We now prove a local version of the Dedekind-Kummer theorem (Theorem 6.13); we could adapt our proof of the Dedekind-Kummer theorem but it is actually easier to prove this directly. Working with a DVR rather than an arbitrary Dedekind domain simplifies matters considerably. We first recall Nakayama's lemma, a very useful result from commutative algebra that comes in a variety of forms. The one most directly applicable to our needs is the following.

Lemma 10.12 (Nakayama's lemma)**.** *Let A be a local ring with maximal ideal $\mathfrak{p}$ and residue field $k = A/\mathfrak{p}$, and let M be a finitely generated A-module. If the images of $x_1, \ldots, x_n \in M$ generate $M/\mathfrak{p}M$ as an k-vector space then $x_1, \ldots, x_n$ generate M as an A-module.*

Proof. See [1, Corollary 4.8b]. $\square$

Lemma 10.13. *Let A be a DVR with maximal ideal $\mathfrak{p}$ and let $B = A[x]/(g(x))$ for some polynomial $g \in A[x]$. Every maximal ideal $\mathfrak{m}$ of B contains $\mathfrak{p}$.*

Proof. Suppose not. Then $\mathfrak{m} + \mathfrak{p}B = B$ for some maximal ideal $\mathfrak{m}$ of B. Let $z_1, \ldots, z_n$ be generators for $\mathfrak{m}$ as an A-module ($\mathfrak{m}$ is clearly finite over A). Every coset of $\mathfrak{p}B$ in B can be written as $z + \mathfrak{p}B$ for some A-linear combination z of $z_1, \ldots, z_n$, so the images of $z_1, \ldots, z_n$ generate $B/\mathfrak{p}B$ as a k-vector space. By Nakayama's lemma, $z_1, \ldots, z_n$ generate B, but then $\mathfrak{m} = B$, a contradiction. $\square$

Corollary 10.14. *Let A be a DVR with maximal ideal $\mathfrak{p}$ and residue field $k = A/\mathfrak{p}$, let $g \in A[x]$ be a polynomial, and let α be the image of x in $B = A[x]/(g(x)) = A[\alpha]$. The maximal ideals of B are $(\mathfrak{p}, h_i(\alpha))$, where $h_1, \ldots, h_m \in k[x]$ are the irreducible polynomials appearing in the factorization of g modulo $\mathfrak{p}$.*

Proof. Lemma 10.13 gives us a one-to-one correspondence between the maximal ideals of B and the maximal ideals of

$$\frac{B}{\mathfrak{p}B} \simeq \frac{A[x]}{(\mathfrak{p}, g(x))} \simeq \frac{k[x]}{(\bar{g}(x))},$$

where $\bar{g}$ denotes the reduction of g modulo $\mathfrak{p}$. Each maximal ideal of $k[x]/(\bar{g}(x))$ is generated by the image of one of the $h_i(x)$ (the quotients of the ring $k[x]/(\bar{g}(x))$ that are fields are precisely those isomorphic to $k[x]/(h(x))$ for some irreducible $h \in k[x]$ dividing $\bar{g}$). It follows that the maximal ideals of $B = A[\alpha]$ are precisely the ideals $(\mathfrak{p}, h_i(\alpha))$. $\square$

We now show that when B is a DVR (implying that A is also a DVR) and the residue field extension is separable, we can always write $B = A[\alpha]$ as required in the corollary (so our local version of the Dedekind-Kummer theorem is always applicable when L and K are local fields, for example).

Lemma 10.15. *Assume AKLB, with A and B DVRs for which the corresponding extension of residue fields is separable. Then $B = A[\alpha]$ for some $\alpha \in B$.*

Proof. Let $\mathfrak{p}$ and $\mathfrak{q}$ be the unique maximal ideals of A and B, respectively, with $\mathfrak{p}B = \mathfrak{q}^e$ and $f = [B/\mathfrak{q} : A/\mathfrak{p}]$ so that $ef = n = [L : K]$. Let $\bar{\alpha}_0 \in B/\mathfrak{q}$ be a generator for the separable residue field extension $(B/\mathfrak{q})/(A/\mathfrak{p})$ (by the primitive element theorem) with separable minimal polynomial $\bar{g}$ (so $\bar{g}(\bar{\alpha}_0) = 0$ and $\bar{g}'(\bar{\alpha}_0) \neq 0$). Let α_0 be any lift of $\bar{\alpha}_0$ to B, and let $g \in A[x]$ be a lift of $\bar{g}$ chosen so that $v_{\mathfrak{q}}(g(\alpha_0)) > 1$ and $v_{\mathfrak{q}}(g'(\alpha_0)) = 0$. This is possible since $g(\alpha) \equiv \bar{g}(\bar{\alpha}_0) = 0 \bmod \mathfrak{q}$, so $v_{\mathfrak{q}}(g(\alpha_0)) \geq 1$ and if equality holds we can replace g by $g - g(\alpha_0)$ without changing the fact that $g'(\alpha_0) \equiv \bar{g}'(\bar{\alpha}_0) \not\equiv 0 \bmod \mathfrak{q}$. Now let π_0 be any uniformizer for B and let $\alpha := \alpha_0 + \pi_0 \in B$ (so $\alpha \equiv \bar{\alpha}_0 \bmod \mathfrak{q}$) Writing $g(x + \pi_0) = g(x) + \pi_0 g'(x) + \pi_0^2 h(x)$ for some $h \in A[x]$ via Lemma 9.9, we have

$$v_{\mathfrak{q}}(g(\alpha)) = v_{\mathfrak{q}}(g(\alpha_0 + \pi_0)) = v_{\mathfrak{q}}(g(\alpha_0) + \pi_0 g'(\alpha_0) + \pi_0^2 h(\alpha_0)) = 1,$$

so $\pi = g(\alpha)$ is also a uniformizer for B.

We now claim $B = A[\alpha]$, equivalently, that $1, \alpha, \ldots, \alpha^{n-1}$ generate B as an A-module. By Nakayama's lemma, it suffices to show that the reductions of $1, \alpha, \ldots, \alpha^{n-1}$ span $B/\mathfrak{p}B$ as an $(A/\mathfrak{p})$-vector space. We have $\mathfrak{p} = \mathfrak{q}^e$, so $\mathfrak{p}B = (\pi^e)$. We can represent each element of $B/\mathfrak{p}B$ as a coset

$$b + \mathfrak{p}B = b_0 + b_1\pi + b_2\pi \cdots + b_{e-1}\pi^{e-1} + \mathfrak{p}B,$$

where $b_0, \ldots, b_{e-1}$ are determined up to equivalence modulo πB. Now $1, \bar{\alpha}, \ldots, \bar{\alpha}^{f-1}$ are a basis for $B/\pi B = B/\mathfrak{q}$ as an $A/\mathfrak{p}$-vector space and $\pi = g(\alpha)$, so we can rewrite this as

$$\begin{aligned} b + \mathfrak{p}B =& (a_0 + a_1\alpha + \cdots a_{f-1}\alpha^{f-1}) + \\ & (a_f + a_{f+1}\alpha + \cdots a_{2f-1}\alpha^{f-1})g(\alpha) + \\ & \cdots + \\ & (a_{ef-f+1} + a_{ef-f+2}\alpha + \cdots a_{ef-1}\alpha^{f-1})g(\alpha)^{e-1} + \mathfrak{p}B. \end{aligned}$$

Since $\deg g = f$, and $n = ef$, this expresses $b + \mathfrak{p}B$ in the form $b' + \mathfrak{p}B$ with b' in the A-span of $1, \ldots, \alpha^{n-1}$. The lemma follows. $\square$

Example 10.16. If A is a DVR with maximal ideal $\mathfrak{p} = (\pi)$ and $g \in A[x]$ is irreducible modulo $\mathfrak{p}$, then $B = A[x]/(g(x)) = A[\alpha]$ has a unique a maximal ideal $\mathfrak{p}B = \pi B$ which is principal; therefore B is a DVR (by Theorem 1.14). In particular, B is integrally closed; indeed, it is the integral closure of A in $L = K(\alpha)$.

Proposition 10.17. *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. $\square$

Theorem 10.18. *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 9.25), and let π be a uniformizer for B with minimal polynomial f. If $B = A[\pi]$ and f is Eisenstein, then as in Proposition 10.17 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 10.17 then implies that $A[\pi]$ is a DVR, and in particular, integrally closed, so $B = A[\pi]$. $\square$

Example 10.19. 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 $x^2 - 6$.

10.3 Decomposing finite extensions of complete DVRs

Theorem 10.20. *Assume AKLB with A a complete DVR and separable residue field extension l/k. Let $e_{L/K}$ and $f_{L/K}$ be the ramification index and residue field degrees, respectively. The following hold:*

(i) There is a unique intermediate field extension E/K that contains every unramified extension of K in L and it has degree $[E : K] = f_{L/K}$.

(ii) The extension L/E is totally ramified and has degree $[L : E] = e_{L/K}$.

(iii) If L/K is Galois then $\mathrm{Gal}(L/E) = I_{L/K}$, where $I_{L/K} = I_{\mathfrak{q}}$ is the inertia subgroup of $\mathrm{Gal}(L/K)$ for the unique prime $\mathfrak{q}$ of B.

Proof. (i) Let E/K be the finite unramified extension of K in L corresponding to the finite separable extension l/k given by the functor $\mathcal{F}$ in Theorem 10.1; then $[E : K] = [l : k] = f_{L/K}$ as desired. The image of the inclusion $l \subseteq l$ of the residue fields of E and L induces a field embedding $E \hookrightarrow L$ in $\mathrm{Hom}_K(E, L)$, via the functor $\mathcal{F}$. Thus we may regard E as a subfield of L, and it is unique up to isomorphism. If E'/K is any other unramified extension of K in L with residue field k', then the inclusions $k' \subseteq l \subseteq l$ induce embeddings $E' \subseteq E \subseteq L$ that must be inclusions.

(ii) We have $f_{L/E} = [l : l] = 1$, so $e_{L/E} = [L : E] = [L : K]/[E : K] = e_{L/K}$.

(iii) By Proposition 7.23, we have $I_{L/E} = \mathrm{Gal}(L/E) \cap I_{L/K}$, and these three groups all have the same order $e_{L/K}$ so they must coincide. $\square$

Definition 10.21. 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 10.22. 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 wildly ramified if $p|e$.

Theorem 10.23. *Assume AKLB with A a complete DVR and separable residue field k of characteristic $p \geq 0$. Then L/K is totally tamely ramified if and only if $L = K(\pi_K^{1/e})$ for some uniformizer π_K 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 10.18, 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 $\bar{g}'(1) = e \neq 0$ (since $p \nmid e$), so we can use Hensel's Lemma 9.13 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. $\square$

10.4 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 9.25). As noted in Remark 9.26, 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 10.24. *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 $\sigma \in \operatorname{Gal}(\overline{K}/K)$ 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 4.45. It follows that $|\sigma(\alpha)| = |N_{K(\sigma(\alpha))/K}(\alpha)|^{1/n} = |N_{K(\alpha)/K}(\alpha)|^{1/n} = |\sigma(\alpha)|$, where $n = \deg f$. $\square$

Definition 10.25. 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 $\sigma \in \operatorname{Gal}(\overline{K}/K)$ 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 10.26 (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 $\sigma \in \operatorname{Gal}(\overline{K}/K(\beta))$ 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 10.24, for any $\sigma \in \operatorname{Gal}(\overline{K}/K(\beta))$ 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 10.27. 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 [2] it was proved earlier by Ostrowksi [3].

Definition 10.28. 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 10.29. *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. □

Proposition 10.30. *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

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

By Lemma 10.29, 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. □

References

[1] David Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer, 1995.

[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