10 Extensions of complete DVRs

Recall that in our $AKLB$ setup, A is a Dedekind domain with fraction field K, the field L is a finite separable extension of K, and B is the integral closure of A in L; as we proved in Theorem 5.25, this implies that B is also a Dedekind domain (with L as its fraction field). We now want to consider the special case where A is a complete DVR; in this case B is also a complete DVR, but this will take a little bit of work to prove. We first show that B is a DVR.

Theorem 10.1. *Assume $AKLB$ and that A is a complete DVR with maximal ideal $\mathfrak{p}$. Then B is a DVR whose maximal ideal $\mathfrak{q}$ is necessarily the unique prime above $\mathfrak{p}$.*

Proof. We first show that $\#\{\mathfrak{q}|\mathfrak{p}\} = 1$. At least one prime $\mathfrak{q}$ of B lies above $\mathfrak{p}$, since the factorization of $\mathfrak{p}B \subsetneq B$ is non-trivial. Now suppose for the sake of contradiction that $\mathfrak{q}_1, \mathfrak{q}_2 \in \{\mathfrak{q}|\mathfrak{p}\}$ with $\mathfrak{q}_1 \neq \mathfrak{q}_2$. Choose $b \in \mathfrak{q}_1 - \mathfrak{q}_2$ and consider the ring $A[b] \subseteq B$. The ideals $\mathfrak{q}_1 \cap A[b]$ and $\mathfrak{q}_2 \cap A[b]$ are distinct prime ideals of $A[b]$ containing $\mathfrak{p}A[b]$, and both are maximal, since they are nonzero and $\dim A[b] = \dim A = 1$ (note that $A[b]$ is integral over A and therefore has the same dimension). The quotient ring $A[b]/\mathfrak{p}A[b]$ thus has at least two maximal ideals. Let $f \in A[x]$ be the minimal polynomial of b over K, and let $\bar{f} \in (A/\mathfrak{p})[x]$ be its reduction to the residue field $A/\mathfrak{p}$.

$$\frac{(A/\mathfrak{p})[x]}{(\bar{f})} \simeq \frac{A[x]}{(\mathfrak{p}, f)} \simeq \frac{A[b]}{\mathfrak{p}A[b]},$$

thus the ring $(A/\mathfrak{p})[x]/(\bar{f})$ has at least two maximal ideals, which implies that $\bar{f}$ is divisible by two distinct irreducible polynomials (because $(A/\mathfrak{p})[x]$ is a PID). We can thus factor $\bar{f} = \bar{g}\bar{h}$ with $\bar{g}$ and $\bar{h}$ coprime. By Hensel's Lemma 9.19, we can lift this to a non-trivial factorization $f = gh$ of f in $A[x]$, contradicting the irreducibility of f.

Every maximal ideal of B lies above a maximal ideal of A, but A has only the maximal ideal $\mathfrak{p}$ and $\#\{\mathfrak{q}|\mathfrak{p}\} = 1$, so B has a unique (nonzero) maximal ideal $\mathfrak{q}$. Thus B is a local Dedekind domain, hence a local PID, and not a field, so B is a DVR, by Theorem 1.16. $\square$

Remark 10.2. The assumption that A is complete is necessary. For example, if A is the DVR $\mathbb{Z}_{(5)}$ with fraction field $K = \mathbb{Q}$ and we take $L = \mathbb{Q}(i)$, then the integral closure of A in L is $B = \mathbb{Z}_{(5)}[i]$, which is a PID but not a DVR: the ideals $(1+2i)$ and $(1-2i)$ are both maximal (and not equal). But if we take completions we get $A = \mathbb{Z}_5$ and $K = \mathbb{Q}_5$, and now $L = \mathbb{Q}_5(i) = \mathbb{Q}_5 = K$, since x^2+1 has a root in $\mathbb{F}_5 \simeq \mathbb{Z}_5/5\mathbb{Z}_5$ that we can lift to $\mathbb{Z}_5$ via Hensel's lemma; thus if we complete A then $B = A$ is a DVR as required.

Definition 10.3. Let K be a field with absolute value $|\ |$ and let V be a K-vector space. A *norm* on V is a function $\|\ \| : V \to \mathbb{R}_{\geq 0}$ such that

- $\|v\| = 0$ if and only if $v = 0$.
- $\|\lambda v\| = |\lambda|\,\|v\|$ for all $\lambda \in K$ and $v \in V$.
- $\|v + w\| \leq \|v\| + \|w\|$ for all $v, w \in V$.

Each norm $\|\ \|$ induces a topology on V via the distance metric $d(v,w) := \|v - w\|$.

Example 10.4. Let V be a K-vector space with basis (e_i), and for $v \in V$ let $v_i \in K$ denote the coefficient of e_i in $v = \sum_i v_i e_i$. The *sup-norm* $\|v\|_\infty := \sup\{|v_i|\}$ is a norm on V (thus every vector space has at least one norm). If V is also a K-algebra, an absolute value $\|\ \|$ on V (as a ring) is a norm on V (as a K-vector space) if and only if it extends the absolute value on K (fix $v \neq 0$ and note that $\|\lambda\|\,\|v\| = \|\lambda v\| = |\lambda|\,\|v\| \Leftrightarrow \|\lambda\| = |\lambda|$).

Proposition 10.5. *Let V be a vector space of finite dimension over a complete field K. Every norm on V induces the same topology, in which V is a complete metric space.*

Proof. See Problem Set 5. $\square$

Theorem 10.6. *Let A be a complete DVR with fraction field K, maximal ideal $\mathfrak{p}$, discrete valuation $v_\mathfrak{p}$, and absolute value $|x|_\mathfrak{p} := c^{v_\mathfrak{p}(x)}$, with $0 < c < 1$. Let L/K be a finite extension of degree n. The following hold.*

(i) *There is a unique absolute value $|x| := |\mathrm{N}_{L/K}(x)|_\mathfrak{p}^{1/n}$ on L that extends $|\ |_\mathfrak{p}$;*

(ii) *The field L is complete with respect to $|\ |$, and its valuation ring $\{x \in L : |x| \leq 1\}$ is equal to the integral closure B of A in L;*

(iii) *If L/K is separable then B is a complete DVR whose maximal ideal $\mathfrak{q}$ induces*

$$|x| = |x|_\mathfrak{q} := c^{\frac{1}{e_\mathfrak{q}} v_\mathfrak{q}(x)},$$

where $e_\mathfrak{q}$ is the ramification index of $\mathfrak{q}$, that is, $\mathfrak{p}B = \mathfrak{q}^{e_\mathfrak{q}}$.

Proof. Assuming for the moment that $|\ |$ is actually an absolute value (which is not obvious!), for any $x \in K$ we have

$$|x| = |\mathrm{N}_{L/K}(x)|_\mathfrak{p}^{1/n} = |x^n|_\mathfrak{p}^{1/n} = |x|_\mathfrak{p},$$

so $|\ |$ extends $|\ |_\mathfrak{p}$ and is therefore a norm on L. The fact that $|\ |_\mathfrak{p}$ is nontrivial means that $|x|_\mathfrak{p} \neq 1$ for some $x \in K^\times$, and $|x|^a = |x|_\mathfrak{p} = |x|$ only for $a = 1$, which implies that $|\ |$ is the unique absolute value in its equivalence class extending $|\ |_\mathfrak{p}$. Every norm on L induces the same topology (by Proposition 10.5), so $|\ |$ is the only absolute value on L that extends $|\ |_\mathfrak{p}$.

We now show $|\ |$ is an absolute value. Clearly $|x| = 0 \Leftrightarrow x = 0$ and $|\ |$ is multiplicative; we only need to check the triangle inequality. It suffices to show $|x| \leq 1 \Rightarrow |x+1| \leq |x|+1$, since we always have $|y+z| = |z||y/z+1|$ and $|y|+|z| = |z|(|y/z|+1)$, and without loss of generality we assume $|y| \leq |z|$. In fact the stronger implication $|x| \leq 1 \Rightarrow |x+1| \leq 1$ holds:

$$|x| \leq 1 \iff |\mathrm{N}_{L/K}(x)|_\mathfrak{p} \leq 1 \iff N_{L/K}(x) \in A \iff x \in B \iff x+1 \in B \iff |x+1| \leq 1.$$

The first biconditional follows from the definition of $|\ |$, the second follows from the definition of $|\ |_\mathfrak{p}$, the third is Corollary 9.21, the fourth is obvious, and the fifth follows from the first three after replacing x with $x+1$. This completes the proof of (i), and also proves (ii).

We now assume L/K is separable. Then B is a DVR, by Theorem 10.1, and it is complete because it is the valuation ring of L. Let $\mathfrak{q}$ be the unique maximal ideal of B. The valuation $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with index $e_\mathfrak{q}$, by Theorem 8.20, so $v_\mathfrak{q}(x) = e_\mathfrak{q} v_\mathfrak{p}(x)$ for $x \in K^\times$. We have $0 < c^{1/e_\mathfrak{q}} < 1$, so $|x|_\mathfrak{q} := (c^{1/e_\mathfrak{q}})^{v_\mathfrak{q}(x)}$ is an absolute value on L induced by $v_\mathfrak{q}$. To show it is equal to $|\ |$, it suffices to show that it extends $|\ |_\mathfrak{p}$, since we already know that $|\ |$ is the unique absolute value on L with this property. For $x \in K^\times$ we have

$$|x|_\mathfrak{q} = c^{\frac{1}{e_\mathfrak{q}} v_\mathfrak{q}(x)} = c^{\frac{1}{e_\mathfrak{q}} e_\mathfrak{q} v_\mathfrak{p}(x)} = c^{v_\mathfrak{p}(x)} = |x|_\mathfrak{p},$$

and the theorem follows. $\square$

Remark 10.7. The transitivity of $\mathrm{N}_{L/K}$ in towers (Corollary 4.52) implies that we can uniquely extend the absolute value on the fraction field K of a complete DVR to an algebraic closure $\overline{K}$. In fact, this is another form of Hensel's lemma in the following sense: one can show that a (not necessarily discrete) valuation ring A is Henselian if and only if the absolute value of its fraction field K can be uniquely extended to $\overline{K}$; see [4, Theorem 6.6].

Corollary 10.8. *Assume $AKLB$ and that A is a complete DVR with maximal ideal $\mathfrak{p}$ and let $\mathfrak{q}|\mathfrak{p}$. Then $v_{\mathfrak{q}}(x) = \frac{1}{f_{\mathfrak{q}}} v_{\mathfrak{p}}(\mathrm{N}_{L/K}(x))$ for all $x \in L$.*

Proof. $v_{\mathfrak{p}}(\mathrm{N}_{L/K}(x)) = v_{\mathfrak{p}}(\mathrm{N}_{L/K}((x))) = v_{\mathfrak{p}}(\mathrm{N}_{L/K}(\mathfrak{q}^{v_{\mathfrak{q}}(x)})) = v_{\mathfrak{p}}(\mathfrak{p}^{f_{\mathfrak{q}} v_{\mathfrak{q}}(x)}) = f_{\mathfrak{q}} v_{\mathfrak{q}}(x)$. $\square$

Remark 10.9. One can generalize the notion of a discrete valuation to a *valuation*, a surjective homomorphism $v\colon K^\times \to \Gamma$, in which Γ is a (totally) ordered abelian group and $v(x+y) \geq \min(v(x), v(y))$; we extend v to K by defining $v(0) = \infty$ to be strictly greater than any element of Γ. In the $AKLB$ setup with A a complete DVR, one can then define a valuation $v(x) = \frac{1}{e_{\mathfrak{q}}} v_{\mathfrak{q}}(x)$ with image $\frac{1}{e_{\mathfrak{q}}}\mathbb{Z}$ that restricts to the discrete valuation $v_{\mathfrak{p}}$ on K. The valuation v then extends to a valuation on $\overline{K}$ with $\Gamma = \mathbb{Q}$. Some texts take this approach, but we will generally stick with discrete valuations (so our absolute value on L restricts to K, but our discrete valuations on L do not restrict to discrete valuations on K, they extend them with index $e_{\mathfrak{q}}$).

Remark 10.10. Recall that a *valuation ring* is an integral domain A with fraction field K such that for every $x \in K^\times$ either $x \in A$ or $x^{-1} \in A$ (possibly both). As you will show on Problem Set 6, if A is a valuation ring, then there exists a valuation $v\colon K \to \Gamma \cup \{\infty\}$ for some totally ordered abelian group Γ such that $A = \{x \in K : v(x) \geq 0\}$ is the valuation ring of K with respect to this valuation.

10.1 The Dedekind-Kummer theorem in a local setting

Recall that the Dedekind-Kummer theorem (Theorem 6.14) allows us to factor primes in our $AKLB$ setting by factoring polynomials over the residue field, provided that B is monogenic (of the form $A[\alpha]$ for some $\alpha \in B$), or the prime of interest does not contain the conductor. We now show that in the special case where A and B are DVRs and the residue field extension is separable, B is always monogenic; this holds, for example, whenever K is a local field. To prove this, we first recall a form of Nakayama's lemma.

Lemma 10.11 (Nakayama's Lemma)**.** *Let A be a local ring with maximal ideal $\mathfrak{p}$, 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 $(A/\mathfrak{p})$-vector space then $x_1, \ldots, x_n$ generate M as an A-module.*

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

Before proving our theorem on local monogenicity, we record a few corollaries of Nakayama's Lemma that will be useful later.

Corollary 10.12. *Let A be a local noetherian ring with maximal ideal $\mathfrak{p}$, let $g \in A[x]$, and let $B := A[x]/(g(x))$. Every maximal ideal $\mathfrak{m}$ of B contains the ideal $\mathfrak{p}B$.*

Proof. Suppose not. Then $\mathfrak{m} + \mathfrak{p}B = B$ for some maximal ideal $\mathfrak{m}$ of B. The ring B is finitely generated over the noetherian ring A, hence a noetherian A-module, so its A-submodules are all finitely generated. Let $z_1, \ldots, z_n$ be A-module generators for $\mathfrak{m}$. 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 an $(A/\mathfrak{p})$-vector space. By Nakayama's lemma, $z_1, \ldots, z_n$ generate B, in which case $\mathfrak{m} = B$, a contradiction. $\square$

As a corollary, we immediately obtain a local version of the Dedekind-Kummer theorem that does not even require A and B to be Dedekind domains.

Corollary 10.13. *Let A be a local noetherian ring with maximal ideal $\mathfrak{p}$, let $g \in A[x]$ be a polynomial with reduction $\bar{g} \in (A/\mathfrak{p})[x]$, and let α be the image of x in the ring $B := A[x]/(g(x)) = A[\alpha]$. The maximal ideals of B are $(\mathfrak{p}, g_i(\alpha))$, where $g_1, \ldots, g_m \in A[x]$ are lifts of the distinct irreducible polynomials $\bar{g}_i \in (A/\mathfrak{p})[x]$ that divide $\bar{g}$.*

Proof. By Corollary 10.12, the quotient map $B \to B/\mathfrak{p}B$ gives a one-to-one correspondence between maximal ideals of B and maximal ideals of $B/\mathfrak{p}B$, and we have

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

Each maximal ideal of $(A/\mathfrak{p})[x]/(\bar{g}(x))$ is the reduction of an irreducible divisor of $\bar{g}$, hence one of the $\bar{g}_i$ (because $(A/\mathfrak{p})[x]$ is a PID). The corollary follows. $\square$

Theorem 10.14. *Assume AKLB, with A and B DVRs with residue fields $k := A/\mathfrak{p}$ and $l := B/\mathfrak{q}$. If l/k is separable then $B = A[\alpha]$ for some $\alpha \in B$; if L/K is unramified this holds for every lift α of any generator $\bar{\alpha}$ for $l = k(\bar{\alpha})$.*

Proof. Let $\mathfrak{p}B = \mathfrak{q}^e$ be the factorization of $\mathfrak{p}B$ and let $f = [l : k]$ be the residue field degree, so that $ef = n := [L : K]$. The extension l/k is separable, so we may apply the primitive element theorem to write $l = k(\alpha_0)$ for some $\alpha_0 \in l$ whose minimal polynomial $\bar{g}$ is separable of degree equal to f. Let $g \in A[x]$ be a monic lift of $\bar{g}$, and let α_0 be any lift of $\bar{\alpha}_0$ to B. If $v_{\mathfrak{q}}(g(\alpha_0)) = 1$ then let $\alpha := \alpha_0$. Otherwise, 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 9.11, 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 k-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 a k-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 $1, \ldots, \alpha^{n-1}$. Thus $B = A[\alpha]$.

We now note that if L/K is unramified then l/k is separable (this is part of the definition of unramified), and $e = 1$, $f = n$, in which case there is no need to require $g(\alpha)$ to be a uniformizer and we can just take $\alpha = \alpha_0$ to be any lift of any $\bar{\alpha}_0$ that generates l over k. $\square$

In our $AKLB$ setup, if A is a complete DVR with maximal ideal $\mathfrak{p}$ then B is a complete DVR with maximal ideal $\mathfrak{q}|\mathfrak{p}$ and the formula $[L : K] = \sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}}$ given by Theorem 5.35 has only one term $e_{\mathfrak{q}} f_{\mathfrak{q}}$. We now simplify matters even further by reducing to the two extreme cases $f_{\mathfrak{q}} = 1$ (a totally ramified extension) and $e_{\mathfrak{q}} = 1$ (an unramified extension, provided that the residue field extension is separable).[1]

10.2 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. Given that the extensions L/K and l/k are finite separable extensions of the same degree, we might wonder 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 finite separable extensions l/k of degree n? Each L/K uniquely determines a corresponding l/k, but what about the converse?

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

Theorem 10.15. *Let A be a complete DVR with fraction field K and residue field $k := A/\mathfrak{p}$. The categories $\mathcal{C}_K^{\mathrm{unr}}$ and $\mathcal{C}_k^{\mathrm{sep}}$ are equivalent via the functor $\mathcal{F}\colon \mathcal{C}_K^{\mathrm{unr}} \to \mathcal{C}_k^{\mathrm{sep}}$ that sends each unramified extension L of K to its residue field l, and each K-algebra homomorphism $\varphi\colon L_1 \to L_2$ to the k-algebra homomorphism $\bar{\varphi}\colon l_1 \to l_2$ defined by $\bar{\varphi}(\bar{\alpha}) := \overline{\varphi(\alpha)}$, where α is 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 $l_2 := B_2/\mathfrak{q}_2$; here $\mathfrak{q}_1, \mathfrak{q}_2$ are the maximal ideals of the valuation rings B_1, B_2 of L_1, L_2, respectively.*

In particular, $\mathcal{F}$ gives a bijection between the isomorphism classes in $\mathcal{C}_K^{\mathrm{unr}}$ and $\mathcal{C}_k^{\mathrm{sep}}$, and if L_1, L_2 and have residue fields l_1, l_2 then $\mathcal{F}$ induces a bijection of finite sets

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

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 extensions l/k, but we should check that the map on morphisms does not depend 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 α' be two lifts of $\bar{\alpha}$ to B_1. Then $\alpha - \alpha' \in \mathfrak{q}_1$, and this implies that $\varphi(\alpha - \alpha') \in \varphi(\mathfrak{q}_1) = \varphi(B_1) \cap \mathfrak{q}_2 \subseteq \mathfrak{q}_2$, and therefore $\overline{\varphi(\alpha)} = \overline{\varphi(\alpha')}$. The identity $\varphi(\mathfrak{q}_1) = \varphi(B_1) \cap \mathfrak{q}_2 \subseteq \mathfrak{q}_2$ follows from the fact that φ restricts to an injective ring homomorphism $B_1 \to B_2$ and $B_2/\varphi(B_1)$ is a finite extension of DVRs in which $\mathfrak{q}_2$ lies over the prime $\varphi(\mathfrak{q}_1)$ of $\varphi(B_1)$. It's easy to see that $\mathcal{F}$ sends identity morphisms to identity morphisms and that it is compatible with composition, so we have a well-defined functor.

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

[1] Recall from Definition 5.37 that separability of the residue field extension is part of the *definition* of an unramified extension. If the residue field is perfect (as when K is a local field, for example), the residue field extension is automatically separable, but in general it need not be, even when L/K is unramified.

- $\mathcal{F}$ is essentially surjective: each separable l/k is isomorphic to the residue field of some unramified L/K
- $\mathcal{F}$ 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 monic lift of $\bar{g}$; then g is also irreducible, separable, and of degree n. Now let

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

where α is the image of x in $K[x]/g(x)$. Then L/K is a finite separable extension, and by Corollary 10.13, $(\mathfrak{p}, g(\alpha))$ is the unique maximal ideal of $A[\alpha]$ (since $\bar{g}$ is irreducible) and

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

We thus 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 (so in fact $B = A[\alpha]$, by Theorem 10.14).

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.

Each A-module homomorphism in

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

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

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

is uniquely determined by the image of x in l_2, and there is a bijection between $\operatorname{Hom}_k(l_1, l_2)$ 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 9.15. Thus the map $\operatorname{Hom}_A(B_1, B_2) \longrightarrow \operatorname{Hom}_k(l_1, l_2)$ induced by $\mathcal{F}$ is a bijection. $\square$

Remark 10.16. 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 10.15.

Corollary 10.17. *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 $g \in A[x]$ has separable image $\bar{g}$ in $k[x]$.*

Proof. The forward direction was proved in the proof of the theorem, and for the reverse direction note that $\bar{g}$ must be irreducible, since otherwise we could use Hensel's lemma to lift a non-trivial factorization of $\bar{g}$ to a non-trivial factorization of g, so the residue field extension is separable and has the same degree as L/K, so L/K is unramified. $\square$

Corollary 10.18. *Let A be a complete DVR with fraction field K and residue field k, and let ζ_n be a primitive nth root of unity in some algebraic closure of 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 when $p \nmid n$, since $\gcd(\bar{f}, \bar{f}') \neq 1$ only when $\bar{f}' = nx^{n-1}$ is zero, equivalently, only when $p|n$. When $\bar{f}$ is separable, so are all of its divisors, including the reduction of the minimal polynomial of ζ_n, which must be irreducible since otherwise we could obtain a contradiction by lifting a non-trivial factorization via Hensel's lemma. It follows that the residue field of $K(\zeta_n)$ is a separable extension of k, thus $K(\zeta_n)/K$ is unramified. $\square$

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

Corollary 10.19. *Let A be a complete DVR with fraction field K and finite residue field $\mathbb{F}_q$, and let L be a degree n extension of K. Then L/K is unramified if and only if $L \simeq K(\zeta_{q^n-1})$. When this holds, $A[\zeta_{q^n-1}]$ is the integral closure of A in L and L/K is a Galois extension with* $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/n\mathbb{Z}$.

Proof. The reverse implication is implied by Corollary 10.18; note that $K(\zeta_{q^n-1})$ has degree n over K because its residue field is the splitting field of $x^{q^n-1} - 1$ over $\mathbb{F}_q$, which is an extension of degree n (indeed, one can take this as the definition of $\mathbb{F}_{q^n}$).

Now suppose L/K is unramified. The residue field has degree n and is thus isomorphic to $\mathbb{F}_{q^n}$, so its multiplicative group is a cyclic of order $q^n - 1$ generated by some $\bar{\alpha}$. The minimal polynomial $\bar{g} \in \mathbb{F}_q[x]$ of $\bar{\alpha}$ 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 9.19, 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 9.15 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.

Let B be the integral closure of A in L. We have $B \simeq A[\zeta_{q^n-1}]$ by Theorem 10.14, and L is the splitting field of $x^{q^n-1} - 1$, since its residue field $\mathbb{F}_{q^n}$ is (we can lift the factorization of $x^{q^n-1} - 1$ from $\mathbb{F}_{q^n}$ to L via Hensel's lemma). It follows that L/K is Galois, and the bijection between $(q^n - 1)$-roots of unity in L and $\mathbb{F}_{q^n}$ induces an isomorphism $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(l/k) = \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z}$. $\square$

Corollary 10.20. *Let A be a complete DVR with fraction field K and finite residue field of characteristic p, and suppose that K does not contain a primitive pth root of unity. The extension $K(\zeta_m)/K$ is ramified if and only if p divides m.*

Proof. If p does not divide m then Corollary 10.18 implies that $K(\zeta_m)/K$ is unramified. If p divides m then $K(\zeta_m)$ contains $K(\zeta_p)$, which by Corollary 10.19 is unramified if and only if $K(\zeta_p) \simeq K(\zeta_{p^n-1})$ with $n := [K(\zeta_p) : K]$, which occurs if and only if p divides $p^n - 1$ (since $\zeta_p \notin K$), which it does not; thus $K(\zeta_p)$ and therefore $K(\zeta_m)$ is ramified when $p|m$. $\square$

Example 10.21. 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 $x^{p^n-1} - 1$.

Another useful consequence of Theorem 10.15 that applies when the residue field is finite is that the norm map $\mathrm{N}_{L/K}$ restricts to a surjective map $B^\times \to A^\times$ on unit groups; in fact, this property characterizes unramified extensions.

Theorem 10.22. *Assume AKLB with A a complete DVR with finite residue field. Then L/K is unramified if and only if $\mathrm{N}_{L/K}(B^\times) = A^\times$.*

Proof. See Problem Set 6. $\square$

Definition 10.23. 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 $L = K^{\mathrm{sep}}$ is the separable closure of K, this is the *maximal unramified extension of K*, denoted K^{unr}.

Example 10.24. The field $\mathbb{Q}_p^{\mathrm{unr}}$ is an infinite extension of $\mathbb{Q}_p$ with Galois group

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

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 $\mathbb{Q}_p^{\mathrm{unr}}$ has value group $\mathbb{Z}$ and residue field $\overline{\mathbb{F}}_p$.

Theorem 10.25. *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 Theorem 10.15; then $[E : K] = [l : k] = f_{L/K}$ as desired. The maximal unramified extension E' of K in L has the same residue field l as L, which is also the residue field of E, and equivalence of categories given by Theorem 10.15 implies that the trivial isomorphism $\ell \simeq \ell$ corresponds to an isomorphism $E \simeq E'$ that allows us to view E as a subfield of L; the same applies to any unramified extension of K with residue field l, so E is unique up to isomorphism.

(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 7.13, we have $I_{L/E} = \operatorname{Gal}(L/E) \cap I_{L/K}$, and these three groups all have the same order $e_{L/K}$ so they must coincide. □

References

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

[2] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta functions*, Springer, 1984.

[3] S. Lang, *Algebraic number theory*, second edition, Springer, 1994.

[4] J. Neukirch, *Algebraic number theory*, Springer, 1999.

18.785 Number Theory I
Fall 2019