10 Extensions of complete DVRs

We now return to our $AKLB$ setup, where 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 (which makes B a Dedekind domain with fraction field L). Recall that be a *prime* of A, we mean a nonzero prime ideal, equivalently, a maximal ideal, and similarly for B.

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

Proof. Existence is clear (the factorization of $\mathfrak{p}B$ in the Dedekind domain B is not trivial because $\mathfrak{p}B \neq B$). To prove uniqueness we use the generalized form of Hensel's lemma. Suppose $\mathfrak{q}_1, \mathfrak{q}_2 | \mathfrak{p}$ with $\mathfrak{q}_1 \neq \mathfrak{q}_2$. Choose $b \in \mathfrak{q}_1 - \mathfrak{q}_2$ and consider the ring $A[b] \subseteq B$. Then $\mathfrak{q}_1 \cap A[b]$ and $\mathfrak{q}_2 \cap A[b]$ are distinct primes of $A[b]$ lying above $\mathfrak{p}$. So $A[b]/\mathfrak{p}A[b]$ has at least two nonzero prime ideals and is not a field.

Let $F \in A[x]$ be the minimal polynomial of b over K and, and let $f \in k[a]$ be its reduction to the residue field $k := A/\mathfrak{p}$. Then

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

so the ring $k[x]/(f)$ is not a field. Therefore f is not irreducible and we can write $f = gh$ for some nonconstant coprime $g, h \in k[x]$. By the generalization of Hensel's lemma, $F = GH$ has a nontrivial factorization in $A[x]$, which is a contradiction. ☐

Corollary 10.2. *Assume $AKLB$ and that A is a complete DVR. Then B is a DVR.*

Proof. Every maximal ideal of B must lie above the unique maximal ideal of A, so Theorem 10.1 implies that B has a unique maximal ideal and is therefore a local Dedekind domain, hence a DVR (a semi-local Dedekind domain is a PID and a local PID is a DVR). ☐

Remark 10.3. 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 notice that 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; in this case $B = A$ is a DVR as required.

Definition 10.4. 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 $d(v, w) := \|x - y\|$.

Example 10.5. 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 a norm). If V is also a K-algebra (e.g. a field extension), 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 10.6. *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 a complete metric space.*

Proof. See Problem Set 5. □

Theorem 10.7. *Let A be a complete DVR with 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. Then*

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

is the unique absolute value on L extending $|\ |_\mathfrak{p}$, L is complete with respect to $|\ |$, and its valuation ring $\{x \in L : |x| \le 1\}$ is equal to the integral closure B of A in L.

If L/K is separable then B is a complete DVR with unique maximal ideal $\mathfrak{q}|\mathfrak{p}$ whose valuation $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with index $e_\mathfrak{q}$, and $|\ |$ is equal to the absolute value

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

induced by $v_\mathfrak{q}$.

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 $|x|_\mathfrak{p} \ne 1$ 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 $|\ |_\mathfrak{p}$. Inequivalent absolute values on L induce distinct topologies while every norm on L induces the same topology (by Theorem 10.7), so $|\ |$ is the unique absolute value on L that extends $|\ |_\mathfrak{p}$.

We now show $|\ |$ is an absolute value. Clearly $|x| = 0$ if and only if $x = 0$, and $|\ |$ is multiplicative; we only need to check the triangle inequality. For this it is enough to show that $|x + 1| \le |x| + 1$ whenever $|x| \le 1$, since we always have $|y + z| = |z||y/z + 1|$ and $|y| + |z| = |z|(|y/z| + 1)$, and may assume without loss of generality that $|y| \le |z|$. We have

$$|x| \le 1 \quad \Longleftrightarrow \quad |\mathrm{N}_{L/K}(x)|_\mathfrak{p} \le 1 \quad \Longleftrightarrow \quad N_{L/K}(x) \in A \quad \Longleftrightarrow x \in B,$$

where the first biconditional follows from the definition of $|\ |$, the second follows from the definition of $|\ |_\mathfrak{p}$, and the third is Corollary 9.22. We now note that $x \in B$ if and only if $x+1 \in B$, so $|x| \le 1$ if and only if $|x+1| \le 1$, thus for $|x| \le 1$ we have $|x+1| \le 1 \le |x|+1$, as desired. This also shows that B is the valuation ring $\{x \in L : |x| \le 1\}$ of L as claimed.

We now assume L/K is separable. Then B is a DVR, by Corollary 10.2, 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 9.2 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. □

Remark 10.8. The transitivity of $\mathrm{N}_{L/K}$ in towers (Corollary 4.48) 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 on its fraction field K can be uniquely extended to $\overline{K}$; see [4, Theorem 6.6].

Corollary 10.9. *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. $v_{\mathfrak{p}}(\mathrm{N}_{L/K}(x)) = v_{\mathfrak{p}}(\mathrm{N}_{L/K}((x))) = v_{\mathfrak{p}}(\mathrm{N}_{L/K}(\mathfrak{q}^{v_{\mathfrak{q}}(x)})) = v_{\mathfrak{p}}(\mathfrak{p}^{f_{\mathfrak{q}} v_{\mathfrak{q}}(x)}) = f_{\mathfrak{q}} v_{\mathfrak{q}}(x)$. □

Remark 10.10. One can generalize the notion of a discrete valuation to a *valuation* which is surjective homomorphism $v\colon K^\times \to \Gamma$, where Γ is a (totally) ordered abelian group and $v(x+y) \le \min(v(x), v(y))$; 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 $e_{\mathfrak{q}}$). You will have an opportunity to explore more valuations in a more general context on Problem Set 6.

Remark 10.11. In general one defines a *valuation ring* to be 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). One can show that this implies the existence of a valuation $v\colon K \to \Gamma \cup \{\infty\}$ for some Γ.

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 $[L : K] = \sum_{p|q} e_{\mathfrak{q}} f_{\mathfrak{q}}$ given by Theorem 5.31 consists of the single 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]

10.1 A local version of the Dedekind-Kummer theorem

To facilitate our investigation of extensions of complete DVRs we first 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 just prove this directly. Working with a DVR rather than an arbitrary Dedekind domain simplifies matters considerably; in particular, in the $AKLB$ setup, when A is a complete DVR and the residue field extension is separable, the extension L/K is guaranteed to be monogenic (so $B = A[\alpha]$ for some $\alpha \in B$).

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.*

[1] Recall from Definition 5.33 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 need not be.

Proof. See [1, Corollary 4.8b]. □

Lemma 10.13. *Let A be a DVR with maximal ideal $\mathfrak{p}$ and residue field $k := A/\mathfrak{p}$, 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. 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 k-vector space. By Nakayama's lemma, $z_1, \ldots, z_n$ generate B, which implies $\mathfrak{m} = B$, a contradiction. □

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 $(\mathfrak{p}, h_i(\alpha))$. □

We now show that when B is a DVR (always true if A is a complete 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).

Theorem 10.15. *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 any $\alpha \in B$ whose image generates the residue field extension l/k.*

Proof. Let $\mathfrak{p}B = \mathfrak{q}^e$ be the factorization of $\mathfrak{p}B$, with ramification index e, 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 $\alpha_i \in l$ whose minimal polynomial $\bar{g}$ is separable of degree f (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 monic 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 $g(\alpha_0) \equiv \bar{g}(\bar{\alpha}_0) = 0 \bmod \mathfrak{q}$, so $v_\mathfrak{q}(g(\alpha_0)) \geq 1$ and if equality holds we can replace g by $g - g(\alpha_0)$ without changing $g'(\alpha_0) \equiv \bar{g}'(\bar{\alpha}_0) \not\equiv 0 \bmod \mathfrak{q}$. 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 9.12, 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 $e = 1$ and $f = n$, 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. □

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 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 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 $\mathcal{C}_K$ 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 10.16. *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 $l_2 := B_2/\mathfrak{q}_2$.*

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, i.e. that it 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 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 is necessarily injective (it is a homomorphism of fields) and preserves integrality over A, since it fixes every polynomial in $A[x]$. Thus φ injects B_1 to a subring of B_2, and since both are DVRs the maximal ideal $\varphi(\mathfrak{q}_1)$ of $\varphi(B_1)$ must be equal to $\mathfrak{q}_2\cap\varphi(\mathfrak{q}_1)$ and lie in $\mathfrak{q}_2$. 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:

- $\mathcal{F}$ 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 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 $K[x]/g(x)$ and has minimal polynomial g. Then L/K is a finite separable extension, and it follows from Corollary 10.14 that $(\mathfrak{p}, g(\alpha))$ 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 10.15).

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

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

is uniquely determined by the image of x in B_2. Thus gives us a bijection between $\mathrm{Hom}_A(B_1, B_2)$ 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 9.16. 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. □

Remark 10.17. 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 10.16.

Corollary 10.18. *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 factorization of $\bar{g}$ to a factorization of g, so the residue field extension is separable and has the same degree as L/K, hence is unramified. □

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 10.19. *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, since $\gcd(\bar{f}, \bar{f}')$ is 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. □

Corollary 10.20. *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 $L \simeq K(\zeta_{q^n-1})$, in which case $B \simeq A[\zeta_{q^n-1}]$ 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. By the previous corollary, $K(\zeta_{q^n-1})$ is unramified, and it has degree n because the 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 $\mathbb{F}_{q^n}$). 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 9.20, 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 9.16 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.

We have $B \simeq A[\zeta_{q^n-1}]$ by Theorem 10.15, and L is the splitting field of $x^{q^n-1}-1$, since l is (we can lift the factorization of $x^{q^n-1}-1$ from l 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 l induces an isomorphism of Galois groups $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(l/k) = \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{\mathfrak{q}}) \simeq \mathbb{Z}/n\mathbb{Z}$. □

Corollary 10.21. *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 10.19 implies that $K(\zeta_m)/K$ is unramified. If p divides m then $K(\zeta_m)$ contains $K(\zeta_p)$, which by Corollary 10.20 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 $K(\zeta_n)$ is ramified when $p|m$. □

Example 10.22. 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 10.16 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 10.23. *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. Let $\mathfrak{p}$ be the maximal ideal of A, let $\mathfrak{q}$ be the maximal ideal of B, and let $k := A/\mathfrak{p}$ and $l := B/\mathfrak{q}$ be the corresponding residue fields. Put $q := \#k$, and let $n := [l : k]$.

We first note that $\mathrm{N}_{l/k}(l^\times) = k^\times$ and $\mathrm{T}_{l/k}(l) = k$. The surjectivity of the norm map $l^\times \to k^\times$ follows from the fact for any $a \in l^\times$ we have

$$\mathrm{N}_{l/k}(a) = a \cdot a^q \cdots a^{q^{n-1}} = a^{(q^n-1)/(q-1)},$$

since $\mathrm{Gal}(l/k)$ is generated by the Frobenius automorphism $x \mapsto x^q$, so $\ker \mathrm{N}_{l/k}$ consists of the roots of the polynomial $x^{(q^n-1)/(q-1)}-1$. There are at most $(q^n-1)/(q-1) = \#l^\times/\#k^\times$ roots, so $\mathrm{im}\, \mathrm{N}_{l/k}$ has cardinality at least $\#k^\times$ and must equal $k^\times$. The surjectivity of the trace map $l \to k$ follows from the fact that l/k is separable and therefore $\mathrm{T}_{l/k}$ is not the zero map, and it is a k-linear transformation whose image has dimension 1, so it is surjective.

Since L/K is unramified, we have $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(l/k)$ and the norm maps $\mathrm{N}_{L/K}$ and $\mathrm{N}_{l/k}$ commute with the reduction maps. Let $u \in A^\times$ have image $\bar{u}$ in $k^\times$. Then $\bar{u} = \mathrm{N}_{l/k}(\bar{\alpha}_0)$ for some $\bar{\alpha}_0 \in l^\times$, and for any lift $\alpha_0 \in B^\times$ of $\bar{\alpha}_0$ we have

$$u \equiv \mathrm{N}_{L/K}(\alpha_0) \bmod \mathfrak{p},$$

where $\mathfrak{p} = (\pi)$ is the maximal ideal of A. We then have

$$u\mathrm{N}_{L/K}(\alpha_0)^{-1} \equiv 1 + a_1\pi \bmod \mathfrak{p}^2$$

for some $a_1 \in A$, and if put $\alpha_1 = 1 + \pi x_1$, where $\mathrm{T}_{L/K}(x_1) \equiv a_1 \bmod \mathfrak{p}$, so that

$$\mathrm{N}_{L/K}(\alpha_1) \equiv 1 + a_1\pi \equiv u\mathrm{N}_{L/K}(\alpha_0)^{-1} \bmod \mathfrak{p}^2,$$

we then have

$$u \equiv \mathrm{N}_{L/K}(\alpha_0\alpha_1) \bmod \mathfrak{p}^2.$$

Continuing in this fashion yields a Cauchy sequence $(\alpha_0, \alpha_0\alpha_1, \alpha_0\alpha_1\alpha_2, \ldots)$ that converges to an element $\alpha \in B^\times$ for which $\mathrm{N}_{L/K}(\alpha) = u$.

We now suppose L/K is ramified, with ramification index $e > 1$. Let K' be the maximal unramified extension of of K in L with valuation ring A', maximal ideal $\mathfrak{p}'$ and residue field $k' := A'/\mathfrak{p}'$. Let $A_1 = 1 + \mathfrak{p}$ and similarly define A_1' and B_1. We have $A^\times \simeq k^\times \times A_1$ (and similarly for $A'^\times$ and $B^\times$), and the norm maps induce a commutative diagram

$$\begin{array}{ccccc} B^\times/B_1 & \xrightarrow{\mathrm{N}_{L/K'}} & A'^\times/A_1' & \xrightarrow{\mathrm{N}_{K'/K}} & A^\times/A_1 \\ \downarrow\wr & & \downarrow\wr & & \downarrow\wr \\ l^\times & \xrightarrow{(\mathrm{N}_{l/k'})^e} & k'^\times & \xrightarrow{\mathrm{N}_{k'/k}} & k^\times \end{array}$$

in which the vertical arrows are all isomorphisms. The right square corresponds to the unramified extension K'/K; the commutativity of the norm and reduction maps in this case were already noted above. The left square corresponds to a totally ramified extension of degree e, thus the residue field extension is trivial ($f = 1$), and $l^\times \simeq k^\times$. Thus any element of $B^\times/B_1$ can actually be represented by an element $x \in A'^\times \subseteq B^\times$, and $\mathrm{N}_{L/K'}(x) = x^e$. $\square$

Definition 10.24. 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 10.25. The field $\mathbb{Q}_p^{\mathrm{unr}}$ is an infinite extension of $\mathbb{Q}_p$ with Galois group

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

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 $\mathbb{F}_p$.

Theorem 10.26. *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 10.16; 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. □

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 function*, 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 2016