9 Local fields and extensions of complete DVRs

9.1 Local fields

Definition 9.1. A *local field* is a field K with a nontrivial absolute value that is locally compact under the induced topology.

Recall that a topological space is *locally compact* if every point has a compact neighborhood.[1] By the induced topology we mean the topology given by the metric $d(x,y) := |x-y|$, where $|\ |$ is the absolute value on K. A metric space is locally compact if and only if every point lies in a compact closed ball. Our first goal for this lecture is to give a precise characterization of local fields which shows that they are precisely the fields we get by completing a global field.

As in the previous lecture we use the following notation. The open ball of radius $r \in \mathbb{R}_{>0}$ about a point x in a metric space is denoted $B_{<r}(x)$, and the closed ball is denoted $B_{\le r}(x)$. In any metric space, open balls are open sets and closed balls are closed sets, but remember that the closure of an open ball is not necessarily a closed ball (in a nonarchimedean metric space every open ball is already closed).

Lemma 9.2. *Let K be a field with a nontrivial absolute value $|\ |$. Then K is a local field if and only if every (equivalently, any) closed ball in K is compact.*

Proof. Suppose K is a local field. The point $0 \in K$ lies in a compact neighborhood that contains some compact closed ball $B_{\le s}(0)$. Pick $c \in K^\times$ with $|c| > 1$ (this is possible because $|\ |$ is nontrivial). The map $x \mapsto cx$ is continuous and $|\ |$ is multiplicative, so $B_{\le |c|^n s}(0)$ is compact for every $n \in \mathbb{Z}_{>0}$. We thus have compact balls about 0 of arbitrarily large radii, implying that every closed ball $B_{\le r}(0)$ is a closed subset of a compact set, hence compact. The translation map $x \mapsto x + z$ is continuous, so every closed ball $B_{\le r}(z)$ is compact. This proves the forward implication, and the reverse implication is immediate. For the parenthetical, note that the argument above applies to any compact closed ball. □

Corollary 9.3. *Let K be a local field with absolute value $|\ |$. Then K is complete.*

Proof. Suppose not. Then there is a Cauchy sequence (x_n) in K that converges to a limit $x \in \hat{K} - K$. Pick $N \in \mathbb{Z}_{>0}$ so that $|x_n - x| < 1/2$ for all $n \ge N$ (here we are using the extension of $|\ |$ to $\hat{K}$), and consider the set $S := B_{\le 1}(x_N) \subseteq k$, which is compact by Lemma 9.2. The Cauchy sequence $(x_n)_{n \ge N}$ in S must converge to a limit in $S \subseteq K$, since S is compact, and this limit must be $x \notin K$, a contradiction. □

Proposition 9.4. *Let K be a field with discrete valuation v, valuation ring A, and uniformizer π. Then K is a local field if and only if K is complete and the residue field $k := A/\pi A$ is finite.*

Proof. Let us fix an absolute value $|x|_v := c^{v(x)}$ induced by v (with $0 < c < 1$). Suppose K is a local field. Then K is complete, by Corollary 9.3. The valuation ring

$$A = \{x \in K : v(x) \ge 0\} = \{x \in K : |x|_v \le 1\} = B_{\le 1}(0)$$

[1] There are a variety of other definitions of locally compact that are used, but they all imply this one. When X is Hausdorff (as it always will be for us) these alternative definitions are all equivalent to ours.

is a closed ball, hence compact, by Lemma 9.2. Each coset $x + \pi A$ of πA is an open ball $B_{<1}(x)$, since $y \in x+\pi A$ if and only if $|x-y|_v \le |\pi|_v = c < 1$. Two cosets $x+\pi A$ and $y+\pi A$ are either equal or disjoint, so we can cover A with disjoint open balls $B_{<1}(x) = x + \pi A$. This disjoint open cover must be finite, since A is compact, so $A/\pi A = k$ is finite.

Now suppose that K is complete and that $k = A/\pi A$ is finite. Then $A = \hat{A}$ is complete. Proposition 8.18 gives an isomorphism of topological rings

$$A \simeq \varprojlim_n \frac{A}{\pi^n A},$$

Each quotient $A/\pi^n A$ is finite, since $A/\pi A$ is finite, and therefore compact; it follows that the inverse limit, and therefore A, is compact; see [1, §I.9.6, Prop. 8]. Thus K contains a compact closed ball $B_{\le 1}(0) = A$ and is therefore locally compact, by Lemma 9.2. □

Corollary 9.5. *Let L be a global field with a nontrivial absolute value $|\ |_v$. The completion L_v of L with respect to $|\ |_v$ is a local field.*

Proof. If $|\ |_v$ is archimedean then L is a finite extension of $\mathbb{Q}$, and the completion of L with respect to $|\ |_v$ is a finite extension of $\mathbb{R}$ (the completion of $\mathbb{Q}$ with respect to its archimedean absolute value), therefore L_v is isomorphic to $\mathbb{R}$ or $\mathbb{C}$, both of which are local fields.

We now assume that $|\ |_v$ is nonarchimedean and let $v\colon L \to \mathbb{Z} \cup \{\infty\}$ denote the corresponding discrete valuation. We have already seen that global fields have finite residue fields, but let us spell out the details. The global field L is an extension of $K = \mathbb{Q}$ or $K = \mathbb{F}_q(t)$. The restriction of v to K is a discrete valuation of K, and there is an associated prime $\mathfrak{p} = \{x \in K : v(x) \ge 1\}$ of $A = \mathcal{O}_K$; for both $K = \mathbb{Q}$ and $K = \mathbb{F}_q(t)$ the residue field $A/\mathfrak{p}$ is finite (for $K = \mathbb{Q}$ it is $\mathbb{Z}/p\mathbb{Z}$ for some prime p and for $K = \mathbb{F}_q(t)$ it is $\mathbb{F}_q[t]/(f)$ for some irreducible $f \in \mathbb{F}_q[t]$). By Theorem 5.11, the valuation v is of the form $v_\mathfrak{q}$ for some prime $\mathfrak{q}|\mathfrak{p}$ of $B = \mathcal{O}_L$, and $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with finite index $e_\mathfrak{q}$; in particular, the residue field $B/\mathfrak{q}$ is also finite.

If we now consider the completion L_v with valuation ring B_v, we can take any uniformizer π for $\mathfrak{q} \subseteq B \subseteq B_v$ as a uniformizer for B_v (the valuation on L_v extends the valuation on L with index 1). We have

$$\frac{B}{\mathfrak{q}} \simeq \frac{B_\mathfrak{q}}{\mathfrak{q}B_\mathfrak{q}} = \frac{B_\mathfrak{q}}{\pi B_\mathfrak{q}} \simeq \frac{B_v}{\pi B_v},$$

which shows that $B_v/\pi B_v$ is finite, since $B/\mathfrak{q}$ is finite. Thus L_v is a complete field with a nontrivial absolute value and finite residue field, and therefore a local field, by Proposition 9.4. □

In order to classify all local fields we require the following result from topology.

Proposition 9.6. *A locally compact topological vector space over a nondiscrete locally compact field has finite dimension.*

Proof. See [6, Prop. 4-13]. □

Theorem 9.7. *Let L be a local field. If L is archimedean then it is isomorphic to $\mathbb{R}$ or $\mathbb{C}$, and otherwise L is isomorphic to a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$ for some prime p.*

Proof. Let L be a local field with nontrivial absolute value $|\ |$; then L is complete, by Corollary 9.3. If $\mathrm{char}(L) = 0$, then the prime field of L is $\mathbb{Q}$, and L contains the completion

of $\mathbb{Q}$ with respect to $|\ |$, by the universal property of completions. By Ostrowski's theorem (see Problem Set 1), L contains a subfield K isomorphic to $\mathbb{Q}_p$ for some prime p, or to $\mathbb{R}$.

If $\mathrm{char}(k) = p > 0$ then the prime field of L is $\mathbb{F}_p$, and L must contain a transcendental element t, since no algebraic extension of $\mathbb{F}_p$ has a nontrivial absolute value: in an algebraic extension L of $\mathbb{F}_p$, every nonzero $\alpha \in L^\times$ has some finite order n, and this implies $|\alpha| = 1$ because $\alpha^n = 1$ implies $|\alpha^n| = |\alpha|^n = 1$ and therefore $|\alpha| = 1$, because the only nth root of 1 in $\mathbb{R}_{\geq 0}$ is 1. Thus L contains the completion of $F = \mathbb{F}_p(t)$ with respect to $|\ |$, and every completion of $\mathbb{F}_p(t)$ is isomorphic to $\mathbb{F}_q((t))$ for some q a power of p, each of which is a finite extension of $\mathbb{F}_p((t))$. So in this case L contains a subfield K isomorphic to $\mathbb{F}_p((t))$.

If K is archimedean then Lemma 9.2 implies that $K = \mathbb{R}$ is a local field because every closed ball in $\mathbb{R}$ is compact, and if K is nonarchimedean then Proposition 9.4 implies that K is a local field, since $\mathbb{Q}_p$ and $\mathbb{F}_\mathfrak{p}((t))$ are both complete and have finite residue fields. Thus K is a local field and therefore locally compact, and it is nondiscrete because its absolute value is nontrivial; Proposition 9.6 then implies that L has finite degree over K. If K is archimedean then $K = \mathbb{R}$, and the only finite extensions of $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{C}$ (every finite extension is algebraic and $\mathbb{C} = \overline{\mathbb{R}}$). Otherwise L is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$. □

9.2 Hensel's Lemma

Definition 9.8. Let R be a (commutative) ring, and let $f(x) = \sum_{i=0}^d f_i x^i \in R[x]$ be a polynomial. The (*formal*) *derivative* f' of f is the polynomial $f'(x) := \sum_{i=1}^d i f_i x^{i-1} \in R[x]$.

Note that the canonical ring homomorphism $\mathbb{Z} \to R$ defined by $1 \mapsto 1$ allows us to view the integers i as elements of R (the map $\mathbb{Z} \to R$ will be injective only when R has characteristic zero, but it is well defined in any case). It is easy to verify that the formal derivative satisfies the following identities:

$$\begin{aligned}(f+g)' &= f' + g',\\ (fg)' &= f'g + fg',\\ (f\circ g)' &= (f'\circ g)g'.\end{aligned}$$

When the characteristic of R is positive, we may have $\deg f' < \deg f - 1$. For example, if R has characteristic $p > 0$ and $g(x) = f(x^p)$ for some $f \in R[x]$, then $g' = f'(x^p)px^{p-1} = 0$ (conversely, one can show that $g' = 0$ implies $g(x) = f(x^p)$ for some $f \in R[x]$).

Lemma 9.9. *Let R be a ring, let $f = \sum_{i=0}^d f_i x^i \in R[x]$ be a polynomial, and let $a \in R$. Then $f(x) = f(a) + f'(a)(x-a) + g(x)(x-a)^2$ for a unique $g \in R[x]$.*

Proof. Without loss of generality, we assume $d \geq 2$ (let $f_i = 0$ for $i > \deg f$). We have

$$\begin{aligned}
f(x) &= f(a + (x-a)) \\
&= \sum_{i=0}^{d} f_i (a + (x-a))^i \\
&= \sum_{i=0}^{d} f_i \sum_{j=0}^{i} \binom{i}{j} a^j (x-a)^{i-j} \\
&= f(a) + \sum_{i=1}^{d} f_i \sum_{j=0}^{i-1} \binom{i}{j} a^j (x-a)^{i-j} \\
&= f(a) + f'(a)(x-a) + \sum_{i=2}^{d} f_i \sum_{j=0}^{i-2} \binom{i}{j} a^j (x-a)^{i-j} \\
&= f(a) + f'(a)(x-a) + \left(\sum_{i=2}^{d} f_i \sum_{j=0}^{i-2} \binom{i}{j} a^j (x-a)^{i-2-j} \right) (x-a)^2,
\end{aligned}$$

so we can take $g(x) = \sum_{i=2}^{d} f_i \sum_{j=0}^{i-2} \binom{i}{j} a^j (x-a)^{i-2-j} \in R[x]$. □

Remark 9.10. The lemma can be viewed as giving the first two terms of a formal Taylor expansion of $f(x)$ about a. Note that the binomial coefficients $\binom{i}{j}$ are integers, hence well defined elements of R under the canonical homomorphism $\mathbb{Z} \to R$, even if $j!$ is divisible by the characteristic of R. In the usual Taylor expansion

$$f(x) = \sum_{i=0}^{\infty} \frac{f^{(i)}(a)}{i!} (x-a)^i$$

used in characteristic zero, if f is a polynomial then $f^{(i)}(a)$ is necessarily a multiple of $i!$, so $f^{(i)}(a)/i!$ is actually a well defined element of R.

Corollary 9.11. *Let R be a ring, $f \in R[x]$, and $a \in R$. Then $f(a) = f'(a) = 0$ if and only if a is (at least) a double root of f, that is, $f(x) = (x-a)^2 g(x)$ for some $g \in R[x]$.*

Definition 9.12. Let $f \in R[x]$ be a polynomial over a ring R and let $a \in R$. If $f(a) = 0$ and $f'(a) \neq 0$ then a is a *simple root* of f.

If R is a ring and I is an ideal, by a *lift* of an element of R/I, we mean a preimage under the quotient map $R \to R/I$. We now state the (apparently) weakest form of what is known as *Hensel's Lemma*.

Lemma 9.13 (Hensel's Lemma I)**.** *Let A be a complete DVR with maximal ideal $\mathfrak{p}$ and residue field $k := A/\mathfrak{p}$. Suppose $f \in A[x]$ is a monic polynomial whose reduction to $k[x]$ has a simple root $r \in k$. Then r can be lifted to a root of f in A.*

Proof. We work in the quotient field K of A. Let a_0 be any lift of r to A; the element a_0 is not necessarily a root of f, but it is a root modulo $\mathfrak{p}$. We will show that a_0 is the first term of a Cauchy sequence (a_n), where each a_n is a root of f modulo $\mathfrak{p}^{2^n}$. In terms of the absolute value $|\cdot| := c^{v_{\mathfrak{p}}(\cdot)}$ (for some $0 < c < 1$) on K, we have $|f(a_n)| \leq c^{2^n}$ rapidly

converging to 0. The assumption that r is a simple root means that $|f'(a_0)| = 1$, and we have $\epsilon := |f(a_0)/f'(a_0)^2| \le c < 1$.

Our proof only requires $\epsilon < 1$, so it actually works in many cases where r is not a simple root (see Lemma 9.14 below); we also don't need f to be monic. For each $n \ge 0$ we define

$$a_{n+1} := a_n - f(a_n)/f'(a_n).$$

We will prove by induction on n that

- **(a)** $|a_n| \le 1$ (so $a_n \in A$);
- **(b)** $|a_n - a_0| \le \epsilon < 1$ (so $a_n \equiv a_1 \bmod \mathfrak{p}$, equivalently, a_n is a lift of r);
- **(c)** $|f'(a_n)| = |f'(a_0)| \ne 0$ (so a_{n+1} is well defined);
- **(d)** $|f(a_n)| \le \epsilon^{2^n} |f'(a_0)|^2$ (so $|f(a_n)|$ and therefore $f(a_n)$ converges rapidly to 0).

The base case $n = 0$ is clear. We now assume (a), (b), (c), (d) for n and prove them for $n + 1$:

(a) $|a_{n+1} - a_n| = |f(a_n)/f'(a_n)| \le \epsilon^{2^n} |f'(a_0)^2|/|f'(a_0)| = \epsilon^{2^n} |f'(a_0)| \le \epsilon^{2^n}$ (by (c),(d)), therefore $|a_{n+1}| = |a_{n+1} - a_n + a_n| \le \max(|a_{n+1} - a_n|, |a_n|) \le 1$ (by (a)).

(b) $|a_{n+1} - a_0| \le \max(|a_{n+1} - a_n|, |a_n - a_0|) \le \max(\epsilon^{2^n}, \epsilon) = \epsilon$ (as above and using (b)).

(c) Applying Lemma 9.9 to $f'(x)$ at a_n and substituting a_{n+1} for x yields

$$f'(a_{n+1}) = f'(a_n) - f''(a_n)\frac{f(a_n)}{f'(a_n)} + \alpha \left(\frac{f(a_n)}{f'(a_n)}\right)^2,$$

where $f''(a_n) \in A$ and $\alpha = g(a_{n+1}) \in A$ for some $g \in A[x]$ (so $|f''(a_n)|, |\alpha| \le 1$). We have $|f(a_n)/f'(a_n)| = |f(a_n)|/|f'(a_0)| \le \epsilon^{2^n} |f'(a_0)|$, by (d), so the absolute values of the last two terms on the RHS are strictly smaller than first $|f'(a_n)| = |f'(a_0)|$, thus $|f'(a_{n+1})| = |f'(a_n)| = |f'(a_0)| \ne 0$.

(d) Applying Lemma 9.9 to $f(x)$ and substituting a_{n+1} for x yields

$$f(a_{n+1}) = f(a_n) - f'(a_n)\frac{f(a_n)}{f'(a_n)} + \beta \left(\frac{f(a_n)}{f'(a_n)}\right)^2 = \beta \left(\frac{f(a_n)}{f'(a_n)}\right)^2,$$

where $\beta = h(a_{n+1})$ for some $h \in A[x]$. We have $|\beta| \le 1$, so (d) gives

$$|f(a_{n+1})| \le |f(a_n)/f'(a_n)|^2 = |f(a_n)|^2/|f'(a_0)|^2 \le \epsilon^{2^{n+1}} |f'(a_0)|^2.$$

We have $|a_{n+1} - a_n| \le \epsilon^{2^n} \to 0$ as $n \to \infty$, and for a nonarchimedean absolute value this implies (a_n) is Cauchy. Thus $a := \lim_{n\to\infty} a_n \in A$, since A is complete. We have $f(a) = \lim_{n\to\infty} f(a_n) = 0$, so a is a root of f, and $|a - a_0| = \lim_{n\to\infty} |a_n - a_0| < 1$, so a is a lift of $r \equiv a_0 \bmod \mathfrak{p}$. □

We now record the stronger form of Hensel's lemma that we actually proved above.

Lemma 9.14 (Hensel's Lemma II)**.** *Let A be a complete DVR. Let $f \in A[x]$, and suppose $a_0 \in A$ satisfies*

$$|f(a_0)| < |f'(a_0)|^2$$

(in particular, $f'(a_1) \neq 0$), and for $n \geq 0$ define

$$a_{n+1} := a_n - f(a_n)/f'(a_n).$$

The sequence (a_n) is well-defined and converges to the unique root $a \in A$ of f for which

$$|a - a_0| \leq \epsilon := |f(a_0)|/|f'(a_0)|^2.$$

Moreover, $|f(a_n)| \leq \epsilon^{2n}|f'(a_0)|^2$ for all $n \geq 0$.

We should note the similarity between Lemma 9.14 and Newton's method for finding (or more closely approximating) a root of a polynomial given an initial approximation. Like Newton's method, the recurrence in Lemma 9.14 converges quadratically, meaning that we double the number of p-adic digits in our approximation with each iteration. But Lemma 9.14 is even better than Newton's method, for two reasons: (1) if the residue field is finite, finding an initial approximation is very easy, and (2) once we have an initial approximation with $\epsilon < 1$, convergence is guaranteed.

Remark 9.15. The hypothesis in Lemmas 9.13 and 9.14 that A is a complete DVR is not necessary, the proof generalizes to any complete local ring. But even completeness is not strictly necessary. A local ring A in which Lemma 9.13 holds without the hypothesis that A is a complete DVR is called a *henselian ring*. One can show that Lemma 9.14 necessarily also holds in any henselian ring, as do many other forms of "Hensel's Lemma", including Lemma 9.17 below. In general, any lemma that holds for a local ring if and only if it is a henselian ring may be called "Hensel's Lemma", and there are at least a dozen candidates, see [7, Tag 04GE], for example. One can define the *henselization* of a noetherian local ring R as the minimal extension of a ring that is henselian (as usual, it is minimal (and unique) in the sense of satisfying a universal property); in many cases this turns out to be the subring of the completion $\hat{R}$ consisting of elements that are algebraic over R. The henselization of R is often much smaller than its completion (e.g. finite over R in cases where $\hat{R}$ is not), and can serve as a substitute for the completion in algebraic settings.

Example 9.16. Let $A = \mathbb{Z}_5$ and $f(x) = x^2 - 6 \in \mathbb{Z}_5[x]$. Then $\bar{f}(x) = x^2 - 1 \in \mathbb{F}_5[x]$ has $r = 1$ as a simple root. By Lemma 9.13 there is a unique $a \in \mathbb{Z}_5$ such that $a^2 - 6 = 0$ and $a \equiv 1 \bmod 5$. We could also have chosen $r = -1$, which would give another distinct root of $f(x)$, which must be $-a$. Thus $\mathbb{Z}_5$ contains two distinct square roots of 6.

Now let $A = \mathbb{Z}_2$ and $f(x) = x^2 - 17$. Then $\bar{f}(x) = x^2 - 1 = (x-1)^2$ has no simple roots (note $\bar{f}' = 0$). But if we let $a_0 = 1$, then $f(a_0) = -16$ and $|f(a_0)| = 1/16$, while $f'(a_0) = 2$ and $|f'(a_0)| = 1/2$. We thus have $|f(a_0| < |f'(a_0)|^2$ and can apply Lemma 9.14 to get a square root of 17 in $\mathbb{Z}_2$.

There is a another version of Hensel's Lemma we need (which is considered by some to be the "canonical" one). Recall that polynomial over a ring is *primitive* if its coefficients generate the unit ideal (over a DVR this just means that at least one coefficient is a unit).

Lemma 9.17 (Hensel's lemma III)**.** *Let A be a complete DVR with maximal ideal $\mathfrak{p}$ and residue field k, let $F \in A[x]$ be a primitive polynomial with image f in $k[x]$, and suppose $f = gh$ for some coprime $g, h \in k[x]$. Then there exist polynomials $G, H \in A[x]$ for which $F = GH$ with $G \equiv g \bmod \mathfrak{p}$ and $H \equiv h \bmod \mathfrak{p}$ such that $\deg G = \deg g$..*

Proof. See [5, Theorem II.4.6]. □

This form of Hensel's lemma has the following useful corollary.

Lemma 9.18 (Hensel-Kürschák lemma)**.** *Let A be a complete DVR with fraction field K, and let $f \in K[x]$ be an irreducible polynomial whose leading and constant coefficients lie in A. Then $f \in A[x]$.*

Proof. Let $\mathfrak{p} = (\pi)$ be the maximal ideal of A, let $k := A/\mathfrak{p}$, and write $f = \sum_{i=0}^{n} f_i x^i$ with $f_n \neq 0$. Let $m = \min\{v_{\mathfrak{p}}(f_i)\}$. Suppose for the sake of contradiction that $m < 0$, and let $G := \pi^{-m} f = \sum_{i=0}^{d} g_i x^i \in A[x]$ is a primitive irreducible polynomial with $g_0, g_n \in \mathfrak{p}$ and $g_n \neq 0$, since $m < 0$ and $f_0, f_n \in A$. The reduction g of G to $k[x]$ is divisible by some maximal $u := x^d$ with $0 < d < n$ to which the quotient $v := g/x^d \in k[x]$ is coprime. It follows from Lemma 9.17 that $G = UV$ with $U, V \in A[x]$ and $0 < \deg U = \deg u < n$, in which case G is not irreducible, a contradiction. So $m \geq 0$ and therefore $f \in A[x]$. □

Corollary 9.19. *Let A be a complete DVR with fraction field K, and let L be a finite extension of K. Then $\alpha \in L$ is integral over A if and only if $\mathrm{N}_{L/K}(\alpha) \in A$.*

Proof. Let $f = \sum_{i=0}^{d} f_i x^i \in K[x]$ be the minimal polynomial of α. If α is integral over A then $f \in A[x]$ (by Proposition 2.1) and $N_{L/K}(\alpha) = f(0)^e \in A$, where $e = [L : K(b)]$, by Proposition 4.45. Conversely, if $N_{L/K}(\alpha) = f(0)^e \in A$, then $f(0) \in A$, since $f(0) \in K$ is a root of $x^e - N_{L/K}(\alpha) \in A[x]$ and A is integrally closed. Thus the constant coefficient of f lies in A, as does its leading coefficient (it is monic), so $f \in A[x]$, by Lemma 9.18. □

9.3 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 9.20. *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. □

Definition 9.21. 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 $v = 0$.

- $\|\lambda v\| = |\lambda| \cdot \|v\|$ for all $\lambda \in K$ and $v \in V$.
- $\|v + w\| \le \|v\| + \|w\|$ for all $v, w \in V$.

Example 9.22. For any K-vector space V, the *sup norm* $\|v\|_\infty := \sup\{|v_i|\}$ is a norm on V.

As with absolute values, there is a notion of equivalence for norms on a vector space.

Definition 9.23. Let V be a vector space over a field K with an absolute value. Two norms $\| \ \|_1$ and $\| \ \|_2$ are *equivalent* if there exist $c_1, c_2 \in \mathbb{R}_{\ge 0}$ such that $\|v\|_1 \le c_2\|v\|_2$ and $\|v\|_2 \le c_1\|v\|_1$ for all $v \in V$.

A norm $\| \ \|$ on a vector space V induces a topology on V via the distance metric $d(v, w) := \|x - y\|$. It is easy to see that equivalent norms induce the same topology: every open ball about a point $v \in V$ defined with respect to one norm both contains and is contained in an open ball defined with respect to another norm, and this makes it easy to show that any set open in one of the induced topologies must also be open in the other. We also have the following result which you may be familiar with from analysis.[2]

Proposition 9.24. *Let V be a finite-dimensional vector space over a complete field K with an absolute value. All norms on V are equivalent (and therefore induce the same topology).*

Proof. See [2, Theorem 5.2.1]. □

Theorem 9.25. *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*

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

is the unique absolute value on L extending $|\ |_\mathfrak{p}$, and L is complete with respect to $|\ |$.

If L/K is separable, then the valuation ring $\{x \in L : |x| \le 1\}$ is the integral closure B of A in L and a complete DVR with unique maximal ideal $\mathfrak{q}|\mathfrak{p}$. The discrete valuation $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with index $e_\mathfrak{q}$, and the absolute value $|\ |$ on L coincides with 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 in fact an absolute value (which is not obvious!), it is clear that it extends $|\ |_\mathfrak{p}$, since for $x \in K$ we have

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

and that $|\ |$ is a norm on L as a K-vector space and thus unique up to equivalence by Proposition 9.24. The fact that $|\ |_\mathfrak{p}$ is nontrivial means that $|x|_\mathfrak{p} \ne 1$ for some $x \in K^\times$, and if $|x|^a = |x|_\mathfrak{p} = |x|$ then we must have $a = 1$, so $|\ |$ is the only absolute value in its equivalence class that extends $|\ |_\mathfrak{p}$.

[2] We should note that the standard proof for real and complex vector spaces does not generalize to arbitrary complete fields where closed and bounded does not necessarily imply compact (the standard proof does work over any locally compact field, see [3, Theorem III.10] for example).

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

$$|x| \le 1 \iff |N_{L/K}(x)|_{\mathfrak{p}} \le 1 \iff N_{L/K}(x) \in A \iff x \in B;$$

the first biconditional is immediate from the definition of $|\ |$, the second is immediate form the definition of $|\ |_{\mathfrak{p}}$, and the third is Corollary 9.19. We now note that $x \in B$ if and only if $x + 1 \in B$, so if $|x| \le 1$ then $|x + 1| \le 1 \le |x| + 1$, as desired. This argument also shows that B is indeed the valuation ring $\{x \in L : |x| \le 1\}$ of L as claimed.

We now assume L/K is separable and show that B, the integral closure of A in L, is the valuation ring of L and a DVR. Every maximal ideal of B must lie above the unique maximal ideal $\mathfrak{p}$ of the DVR A, and Theorem 9.20 implies that B has a unique maximal ideal $\mathfrak{q}$. Thus B is a local Dedekind domain, hence a DVR.

The valuation $v_{\mathfrak{q}}$ extends $v_{\mathfrak{p}}$ with index $e_{\mathfrak{q}}$, by Theorem 5.11, so $v_{\mathfrak{q}}(x) = e_{\mathfrak{q}} v_{\mathfrak{p}}(x)$ for all $x \in K^\times$. 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 that it is equal to $|\ |$, it suffices to show that it extends $|\ |_{\mathfrak{p}}$, since we have already noted that $|\ |$ is the unique absolute value on L with this property. But this is clear: for any $x \in K$ we have $|x|_{\mathfrak{q}} = c^{v_{\mathfrak{q}}(x)/e_{\mathfrak{q}}} = c^{v_{\mathfrak{p}}(x)} = |x|_{\mathfrak{p}}$. It follows that $B = \{x \in L : v_{\mathfrak{q}}(x) \ge 0\} = \{x \in L : |x|_{\mathfrak{q}} \le 1\} = \{x \in L : |x| \le 1\}$ is the valuation ring of L as claimed. □

Remark 9.26. The transitivity of $N_{L/K}$ in towers (Corollary 4.46) 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 [5, Theorem 6.6].

Corollary 9.27. *Assume AKLB and that A is a complete DVR with maximal ideal $\mathfrak{p}$ and let $\mathfrak{q}|\mathfrak{p}$. Then $v_{\mathfrak{q}}(x) = \frac{1}{f_{\mathfrak{q}}} v_{\mathfrak{p}}(N_{L/K}(x))$ for all $x \in L$.*

Remark 9.28. 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 $v(0) = \infty$, where ∞ is defined to be strictly greater than any element of Γ. In the case of a discrete valuation $\Gamma = \mathbb{Z}$, but more generally one might take $\Gamma = \mathbb{Q}$, or any additive subgroup of $\mathbb{R}$. 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 general valuations on the problem sets.

Remark 9.29. 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.

References

[1] N. Bourbaki, *General Topology: Chapters 1-4*, Springer, 1985.

[2] F.Q. Gouvea, *p-adic numbers*, Springer, 1993.

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

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

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

[6] D. Ramakrishnan and R.J. Valenza, *Fourier analysis on number fields*, Springer, 1999.

[7] Stacks Project Authors, *Stacks Project*, `http://stacks.math.columbia.edu`.

18.785 Number Theory I
Fall 2015