9 Local fields and Hensel's lemmas

In this lecture we introduce the notion of a *local field*; these are precisely the fields that arise as completions of a *global field* (finite extensions of $\mathbb{Q}$ or $\mathbb{F}_q(t)$), but they can be defined in a more intrinsic way. In later lectures we will see that global fields can also be defined in a more intrinsic way, as fields whose completions are local fields and which admit a suitable product formula.

9.1 Local fields

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

Recall that a topological space is *locally compact* if every point has a compact neighborhood.[1] The topology induced by $|\ |$ is given by the metric $d(x,y) := |x-y|$. A metric space is locally compact if and only if every point lies in a compact closed ball.

Example 9.2. Under the standard archimedean absolute value both $\mathbb{R}$ and $\mathbb{C}$ are local fields but $\mathbb{Q}$ is not. Indeed no closed ball in $\mathbb{Q}$ is compact, since it is missing limit points (all irrational real numbers), and in a metric space a compact set must contains all its limit points. Finite fields are not local fields because they have no nontrivial absolute values.

Our first goal is to classify local fields by showing that they are precisely the fields we get by completing a global field. As in the previous lecture, we use $B_{<r}(x) := \{y : |y-x| < r\}$ to denote the open ball of radius $r \in \mathbb{R}_{>0}$ about x, and $B_{\le r}(x) := \{y : |y-x| \le r\}$ to denote a closed ball. Open balls are always open sets and closed balls are always closed sets, but in a nonarchimedean metric space, open balls are both open and closed, as are closed balls.

Remark 9.3. For nonarchimedean metric spaces whose metric is induced by a discrete valuation, every open ball of radius r is also a closed ball of some radius $s \le r$, but we need not have $s = r$; in particular, the closure of $B_{<r}(x)$ (which is already closed) need not be equal to $B_{\le r}(x)$, it could be strictly contained in $B_{\le r}(x)$. The key point is that not every $r \in \mathbb{R}_{\ge 0}$ actually arises as a distance, only countably many do.

Lemma 9.4. *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. Then $0 \in K$ lies in a compact neighborhood that contains a closed ball $B_{\le s}(0)$ which is compact. Let us fix $\alpha \in K^\times$ with $|\alpha| > 1$ (such an α exists because $|\ |$ is nontrivial). The map $x \mapsto \alpha x$ is continuous and $|\ |$ is multiplicative, so $B_{\le |\alpha|^n s}(0)$ is compact for every $n \in \mathbb{Z}_{>0}$ (recall that the continuous image of a compact set is compact). 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. For every $z \in K$ 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 follows immediately from the definition of local compactness. For the parenthetical, replace $B_{\le s}(0)$ in the argument above by any closed ball. $\square$

Corollary 9.5. *Let K be a local field with nontrivial absolute value $|\ |$. Then K is complete.*

[1] Weaker definitions of locally compact are sometimes used, but they all imply this one, and for Hausdorff spaces these weaker definitions are all equivalent to the one given here.

Proof. Suppose not. Then there is a Cauchy sequence (x_n) in K that converges to a limit $x \in \widehat{K} - K$. Pick $N \in \mathbb{Z}_{>0}$ so that $|x_n - x| < 1/2$ for all $n \geq N$ (here we are using the extension of $|\ |$ to $\widehat{K}$), and consider the closed ball $S := B_{\leq 1}(x_N)$ in K, which is compact by Lemma 9.4. The Cauchy sequence $(x_n)_{n \geq N}$ in S has a convergent subsequence whose limit lies in $S \subseteq K$, since S is compact and therefore sequentially compact (because K is a metric space). But this limit must be equal to $x \notin K$, a contradiction. □

Proposition 9.6. *Let K be a field with absolute value $|\ |_v$ induced by a discrete valuation v with valuation ring A and uniformizer π. Then K is a local field if and only if K is complete and the residue field $A/\pi A$ is finite.*

Proof. If K is a local field then K is complete, by Corollary 9.5, and the valuation ring

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

is a closed ball, hence compact, by Lemma 9.4. The cosets $x + \pi A$ of the subgroup $\pi A \subseteq A$ are open balls $B_{<1}(x)$, since $y \in x + \pi A$ if and only if $|x - y|_v \leq |\pi|_v < 1$. The collection $\{x + \pi A : x \in A\}$ of cosets of πA is an open cover of A by disjoint sets which must be finite, since A is compact; thus $A/\pi A$ is finite.

Now suppose that K is complete and $A/\pi A$ is finite. The valuation ring $A \subseteq K$ is also complete, and Proposition 8.11 gives an isomorphism of topological rings

$$A = \hat{A} \simeq \varprojlim_n \frac{A}{\pi^n A}.$$

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, by Proposition 8.10. Lemma 9.4 implies that K is a local field, since it contains a compact closed ball $B_{\leq 1}(0) = A$ and $|\ |_v$ is nontrivial (recall that discrete valuations surject onto $\mathbb{Z}$ and are thus non-trivial by definition). □

Corollary 9.7. *Let L be a global field with a nontrivial absolute value $|\ |_v$. Then the completion L_v of L with respect to $|\ |_v$ is a local field.*

Proof. Let L/K be a finite extension with $K = \mathbb{Q}$ or $K = \mathbb{F}_q(t)$ and $A = \mathbb{Z}$ or $A = \mathbb{F}_q[t]$, so that $K = \operatorname{Frac} A$. Then A is a Dedekind domain, as is its integral closure B in L, by Theorem 5.25 (and Remark 5.26 in the case that L/K is inseparable).[2]

If $|\ |_v$ is archimedean, then $K = \mathbb{Q}$ and the completion of L with respect to $|\ |_v$ must contain the completion of $\mathbb{Q}$ with respect to the restriction of $|\ |_v$ to $\mathbb{Q}$, which must be isomorphic to $\mathbb{R}$ (as shown on Problem Set 1, every archimedean absolute value on $\mathbb{Q}$ is equivalent to the usual Euclidean absolute value). Thus L_v is a finite extension of $\mathbb{R}$ and must be isomorphic to either $\mathbb{R}$ or $\mathbb{C}$ (as a topological field), both of which are local fields.

We now assume that $|\ |_v$ is nonarchimedean. We claim that in this case $|\ |_v$ is induced by a discrete valuation. Let $C := \{x \in L : |x|_v \leq 1\}$ be the valuation ring of L with respect to $|\ |_v$, and let $\mathfrak{m} := \{x \in L : |x|_v < 1\}$ be its maximal ideal, which is nonzero because $|\ |_v$ is nontrivial. The restriction of $|\ |_v$ to K is a nonarchimedean absolute value, and from the classification of absolute values on $\mathbb{Q}$ and $\mathbb{F}_q(t)$ proved on Problem Set 1, we can assume it is induced by a discrete valuation on A; in particular, $|x|_v \leq 1$ for all $x \in A$, and therefore

[2] In fact, we can always choose K so that L/K is separable: if L has positive characteristic p, let $\mathbb{F}_q$ be the algebraic closure of $\mathbb{F}_p$ in L, choose a separating transcendental element t, and put $K := \mathbb{F}_q(t)$. Such a t exists because $\mathbb{F}_q$ is perfect and $L/\mathbb{F}_q$ is finitely generated, see [3, Thm. 7.20].

$A \subseteq C$. Like all valuation rings (discrete or not), C is integrally closed in its fraction field L, and C contains A, so C contains B, since B is the integral closure of A in L. The ideal $\mathfrak{q} = \mathfrak{m} \cap B$ is maximal, and the DVR $B_{\mathfrak{q}}$ lies in C and must equal C, since there are no intermediate rings between a DVR and its fraction field (we cannot have $C = L$ because C is not a field). It follows that the absolute value induced by $v_{\mathfrak{q}}$ is equivalent to $|\ |_v$, since they have the same valuation rings. By choosing $0 < c < 1$ appropriately, we can assume that $|\cdot|_v = c^{v_{\mathfrak{q}}(\cdot)}$ is induced by $v_{\mathfrak{q}}$, which proves the claim.

The residue field $B_{\mathfrak{q}}/\mathfrak{q}B_{\mathfrak{q}} \simeq B/\mathfrak{q}$ is finite, since $B/\mathfrak{q}$ is a finite extension of the finite field $A/\mathfrak{p}$, where $\mathfrak{p} = \mathfrak{q} \cap A$. 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, and we have

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

so $B_v/\pi B_v$ is finite. Thus L_v is a complete field with an absolute value induced by a discrete valuation and finite residue field, and therefore a local field, by Proposition 9.6. □

In order to classify all local fields we require the following result from topology (here nondiscrete simply means that not every set is open).

Proposition 9.8. *A locally compact topological vector space over a nondiscrete locally compact field has finite dimension.*

Proof. See [4, Prop. 4-13.iv]. □

Theorem 9.9. *Let L be a local field. If L is archimedean then it is isomorphic to $\mathbb{R}$ or $\mathbb{C}$; otherwise, L is isomorphic to a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$.*

Proof. Let L be a local field with nontrivial absolute value $|\ |$; then L is complete, by Corollary 9.5. If L has characteristic zero then the prime field of L is $\mathbb{Q}$, and L contains the completion of $\mathbb{Q}$ with respect to the restriction of $|\ |$ to $\mathbb{Q}$. By Ostrowski's theorem, the restriction of $|\ |$ to $\mathbb{Q}$ is equivalent to either the standard archimedean absolute value, in which case the completion is $\mathbb{R}$, or it is equivalent to a p-adic absolute value, in which case the completion is $\mathbb{Q}_p$ (which, by definition, is the completion of $\mathbb{Q}$ with respect to the p-adic absolute value). Thus L contains a subfield K isomorphic to $\mathbb{R}$ or to $\mathbb{Q}_p$ for some prime p.

If L has positive characteristic p then the prime field of L is $\mathbb{F}_p$, and L must contain a transcendental element s, since no algebraic extension of $\mathbb{F}_p$ has a nontrivial absolute value (if $|\alpha| > 1$ for some algebraic $\alpha \in L$, then the restriction of $|\ |$ to the finite field $\mathbb{F}_p(\alpha)$ is nontrivial, but this is impossible). It follows that L contains $\mathbb{F}_p(s)$ and therefore contains the completion of $\mathbb{F}_p(s)$ with respect to $|\ |$. Every completion of $\mathbb{F}_p(s)$ is isomorphic to $\mathbb{F}_q((t))$ for some q a power of p and t transcendental over $\mathbb{F}_q$ (see Problem Set 5). Thus L contains a subfield K isomorphic to $\mathbb{F}_q((t))$.

If K is archimedean then $K = \mathbb{R}$ is a local field, and if K is nonarchimedean then $K = \mathbb{Q}_p$ or $K = \mathbb{F}_q((t))$ is a complete field with a discrete valuation and finite residue field, hence a local field by Proposition 9.6. The field K is therefore locally compact, and it is nondiscrete because its absolute value is nontrivial. Proposition 9.8 implies that L has finite degree over K. If K is archimedean then $K = \mathbb{R}$, and L must be $\mathbb{R}$ or $\mathbb{C}$; otherwise, L is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$ as claimed. □

9.2 Hensel's lemmas

Definition 9.10. Let R be a (commutative) ring, and let $f(x) = \sum f_i x^i \in R[x]$ be a polynomial. The (*formal*) *derivative* f' of f is the polynomial $f'(x) := \sum i f_i x^{i-1} \in R[x]$.

Note that the canonical ring homomorphism $\mathbb{Z} \to R$ defined by $1 \mapsto 1$ allows us to view the integers $i = 1 + 1 + \cdots + 1$ 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 for all $a, b \in R$ and $f, g \in R[x]$ the formal derivative satisfies the usual identities:

$$\begin{aligned} (af + bg)' &= af' + bg', && \text{(linearity)} \\ (fg)' &= f'g + fg', && \text{(Leibniz rule)} \\ (f \circ g)' &= (f' \circ g)g', && \text{(chain rule)} \end{aligned}$$

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

Lemma 9.11. *Let R be a ring, let $f = \sum f_i x^i \in R[x]$ 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. We have

$$\begin{aligned} f(x) = f(a + (x - a)) = \sum_{i \ge 0} f_i (a + (x - a))^i &= \sum_{i \ge 0} f_i \sum_{0 \le j \le i} \binom{i}{j} a^j (x - a)^{i-j} \\ &= f(a) + \sum_{i \ge 1} f_i \sum_{0 \le j < i} \binom{i}{j} a^j (x - a)^{i-j} \\ &= f(a) + f'(a)(x - a) + \sum_{i \ge 2} f_i \sum_{0 \le j \le i-2} \binom{i}{j} a^j (x - a)^{i-j} \\ &= f(a) + f'(a)(x - a) + g(x)(x - a)^2, \end{aligned}$$

where $g(x) = \sum_{i \ge 2} f_i \sum_{0 \le j \le i-2} \binom{i}{j} a^j (x - a)^{i-2-j} \in R[x]$. □

Remark 9.12. 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 when $j!$ 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 always a well defined element of R, even in positive characteristic.

Corollary 9.13. *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 9.14. 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 R-ideal, by a *lift* of an element $\bar{r}$ of the quotient R/I, we mean a preimage of $\bar{r}$ under the quotient map $R \twoheadrightarrow R/I$.

Lemma 9.15 (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 $\bar{a} \in k$. Then $\bar{a}$ can be lifted to a root of f in A.*

Proof. We work in the fraction field K of A. Let a_0 be any lift of $\bar{a}$ 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) in which each a_n is a root of f modulo $\mathfrak{p}^{2^n}$. To simplify the notation we fix $0 < c < 1$ and define the absolute value $|\cdot| := c^{v_\mathfrak{p}(\cdot)}$. The fact that $\bar{a}$ is a simple root implies that $f(a_0) \in \mathfrak{p}$ but $f'(a_0) \notin \mathfrak{p}$, so $|f(a_0)| \le c < 1$ and $|f'(a_0)| = 1$. We now define

$$\epsilon := \frac{|f(a_0)|}{|f'(a_0)|^2} < 1.$$

In what follows we will only use $\epsilon < 1$, which will allow our proof to work in cases where $\bar{a}$ is not necessarily a simple root (in particular, we won't assume $|f'(a_0)| = 1$).

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

The 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) and (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 9.11 to $f'(x)$ at a_n and substituting a_{n+1} for x yields

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

  where we have used $a_{n+1} - a_n = -f(a_n)/f'(a_n)$. We have $f''(a_n), g(a_{n+1}) \in A$, so $|f''(a_n)|, |g(a_{n+1})| \le 1$, and $|f(a_n)/f'(a_n)| = |f(a_n)|/|f'(a_0)| \le \epsilon^{2^n}|f'(a_0)|$, by (d), so the absolute values of the last two terms on the RHS are strictly smaller than the first term $|f'(a_n)| = |f'(a_0)|$. Therefore $|f'(a_{n+1})| = |f'(a_n)| = |f'(a_0)|$.
- (d) Applying Lemma 9.11 to $f(x)$ at a_n and substituting a_{n+1} for x yields

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

  for some $h \in A[x]$. We have $|h(a_{n+1})| \le 1$, so (c) and (d) imply

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

  which completes our inductive proof.

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 that (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 $a \equiv a_0 \bmod \mathfrak{p}$ is a lift of $\bar{a}$. □

Our proof of Lemma 9.15 did not actually use the assumption that f is monic, nor did it actually require $\bar{a}$ to be a simple root. Let us record the (apparently stronger) form of Hensel's lemma that what we actually proved.

Lemma 9.16 (Hensel's Lemma II)**.** *Let A be a complete DVR. Let $f \in A[x]$, and suppose $a_0 \in A$ satisfies*

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

(so in particular, $f'(a_0)$ divides $f(a_0)$), and for $n \ge 0$ 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

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

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

Lemma 9.16 can be viewed as a nonarchimedean version of 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 9.16 converges quadratically, meaning that we double the precision of our approximation with each iteration. But Lemma 9.16 is better than Newton's method, for two reasons: (1) in the most common scenario the residue field is finite, which makes finding an initial approximation very easy, and (2) once we have an initial approximation with $\epsilon < 1$, convergence is guaranteed.

Remark 9.17. In Lemmas 9.15 and 9.16 it is not actually necessary for A to be complete (or an integral domain). A local ring A for which Lemma 9.15 holds is called a *henselian ring* (this is a definition). One can show that Lemma 9.16 necessarily also holds in any henselian ring, as do many other forms of "Hensel's Lemma", including Lemma 9.19 below. In general, any condition that holds for a local ring if and only if it is a henselian ring may be called "Hensel's Lemma"; see [5, Lemma 10.148.3] for more than a dozen candidates. One can define the *henselization* of a noetherian local ring R as the minimal extension of R that is henselian (as usual, it is minimal in the sense of satisfying a universal property, and this forces it to be unique up to isomorphism). When R is a DVR its henselization is simply $\widehat{R} \cap K^{\mathrm{sep}}$, where K is the fraction field of R. Loosely speaking, in henselian rings, Cauchy sequences that converge (in the completion) to the root of a polynomial are required to converge, but not every Cauchy sequence needs to converge.

Example 9.18. 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 $\bar{a} = 1$ as a simple root. By Lemma 9.15 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 $\bar{a} = -1$, 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 9.16 to get a square root of 17 in $\mathbb{Z}_2$.

There is a another version of Hensel's Lemma that we need, which is arguably the most powerful (of course they are all equivalent by definition, but this version is most easily seen to imply all the others).

Lemma 9.19 (Hensel's lemma III). *Let A be a complete DVR with maximal ideal $\mathfrak{p}$ and residue field k, let $f \in A[x]$ have image $\bar{f}$ in $k[x]$, and suppose $\bar{f} = \bar{g}\bar{h}$ for some coprime $\bar{g}, \bar{h} \in k[x]$. Then there exist polynomials $g, h \in A[x]$ for which $f = gh$ with $g \equiv \bar{g} \bmod \mathfrak{p}$ and $h \equiv \bar{h} \bmod \mathfrak{p}$ such that $\deg g = \deg \bar{g}$.*

Proof. See [2, Theorem II.4.6] or [5, Lemma 10.148.3]. □

This form of Hensel's lemma has the following useful corollary, which is itself another form Hensel's lemma in the sense that it characterizes henselian fields (see Remark 9.17).[3]

Lemma 9.20 (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 $f_n \neq 0$. We must have $n > 0$ and $f_0 \neq 0$, since f is irreducible. Let $m := \min\{v_\mathfrak{p}(f_i)\}$. Suppose for the sake of contradiction that $m < 0$, and let $g := \pi^{-m} f = \sum_{i=0}^n g_i x^i \in A[x]$. Then g is an irreducible polynomial in $A[x]$ with $g_0, g_n \in \mathfrak{p}$, since $m < 0$ and $f_0, f_n \in A$, and g_i is a unit for some $0 < i < n$, by the minimality of m. The reduction $\bar{g}$ of g to $k[x]$ has positive degree and constant term 0, and is therefore divisible by x. If we let $\bar{u} := x^d$ be the largest power of x dividing $\bar{g}$, then $0 < d \leq \deg \bar{g} < n$ and $\bar{v} := \bar{g}/x^d \in k[x]$ is coprime to $\bar{u}$ (possibly $\deg \bar{v} = 0$). Lemma 9.19 implies that $g = uv$ for some $u, v \in A[x]$ with $0 < \deg u = \deg \bar{u} < n$. But this means g is not irreducible, a contradiction. □

Corollary 9.21. *Let A be a complete DVR with fraction field K, and let L/K be a finite extension of degree n. 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 1.28, and $\mathrm{N}_{L/K}(\alpha) = (-1)^n f(0)^e \in A$, where $e = [L : K(\alpha)]$, by Proposition 4.51. Conversely, if $\mathrm{N}_{L/K}(\alpha) = (-1)^n f(0)^e \in A$, then $f(0) \in A$, since $f(0) \in K$ is a root of $x^e - (-1)^n \mathrm{N}_{L/K}(\alpha) \in A[x]$ and A is integrally closed. The constant coefficient of f thus lies in A, as does its leading coefficient (it is monic), so $f \in A[x]$, by Lemma 9.20, and α is therefore integral over A. □

Theorem 9.22. *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

[3] See [2, §II.6] for a proof of this.

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. □

Remark 9.23. 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 $L = \mathbb{Q}_5(i) = \mathbb{Q}_5 = K$ and $B = \mathbb{Z}_5[i] = \mathbb{Z}_5 = A$ is a DVR, since $x^2 + 1$ has roots in $\mathbb{F}_5 \simeq \mathbb{Z}_5/5\mathbb{Z}_5$ that we can lift to roots in $\mathbb{Z}_5$ via Hensel's lemma.

Remark 9.24. In the previous example you might wonder what happens to the factorization $(5) = (1 + 2i)(1 - 2i)$ in $B = \mathbb{Z}_{(5)}[i]$ if we replace A with its completion $\mathbb{Z}_5$ and consider $B = \mathbb{Z}_5[i] = \mathbb{Z}_5$. The two maximal ideals $\mathfrak{q}_1 = (1 + 2i)$ and $\mathfrak{q}_2 = (1 - 2i)$ in $\mathbb{Z}_{(5)}[i]$ are coprime, thus $v_{\mathfrak{q}_1}(\mathfrak{q}_2) = 0$ and $\mathfrak{q}_2 B_{\mathfrak{q}_1}$ is the unit ideal, and conversely. No matter which maximal ideal we localize at, the RHS of the factorization $(5) = (1 + 2i)(1 - 2i)$ is locally the product of the maximal ideal and the unit ideal. The same thing happens if we work in the completion of A. If we pick $i \equiv 7 \bmod 25$ as a root of x^2+1 in $\mathbb{Z}_5$ we have $(1+2i) = (5)$ and $(1 - 2i) = (1)$, and the situation is reversed if we pick $i \equiv 18 \bmod 25$.

References

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

[2] Jürgen Neukirch, *Algebraic number theory*, Springer, 1999.

[3] Anthony W. Knapp, *Advanced algebra*, Digital Second Edition, 2016.

[4] Dinikar Ramakrishnan and Robert J. Valenza, *Fourier analysis on number fields*, Springer, 1999.

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

18.785 Number Theory I
Fall 2021