8 Complete fields and valuation rings

In order to make further progress in our investigation of finite extensions L/K of the fraction field K of a Dedekind domain A, and in particular, to determine the primes $\mathfrak{p}$ of K that ramify in L, we introduce a new tool that allows us to "localize" fields. We have seen how useful it can be to localize the ring A at a prime ideal $\mathfrak{p}$: this yields a discrete valuation ring $A_{\mathfrak{p}}$, a principal ideal domain with exactly one nonzero prime ideal, which is much easier to study than A. By Proposition 2.6, the localizations of A at its prime ideals $\mathfrak{p}$ collectively determine the ring A.

Localizing A does not change its fraction field K. But there is an operation we can perform on K that is analogous to localizing A: we can construct the *completion* of K with respect to one of its absolute values. When K is a global field, this yields a *local field* (which we will define in the next lecture). At first glance taking completions might seem to make things more complicated, but as with localization, it actually simplifies matters by allowing us to focus on a single prime.

For those who have not seen this construction before, we briefly review some background material on completions, topological rings, and inverse limits.

8.1 Completions

Recall that an absolute value on a field K is a function $|\ |\colon K \to \mathbb{R}_{\ge 0}$ that satisfies

1. $|x| = 0$ if and only if $x = 0$;
2. $|xy| = |x||y|$;
3. $|x + y| \le |x| + |y|$.

If in addition the stronger condition

4. $|x + y| \le \max(|x|, |y|)$

holds, then we say that $|\ |$ is nonarchimedean. This definition does not depend on the fact that K is a field; it makes sense for any ring. But note that absolute values exist only on rings that are integral domains, since $a, b \ne 0 \Rightarrow |a|, |b| \ne 0 \Rightarrow |ab| = |a||b| \ne 0 \Rightarrow ab \ne 0$.

For a more general notion, we can instead consider a metric on a set X, which we recall is a function $d : X \times X \to \mathbb{R}_{\ge 0}$ that satisfies

1. $d(x, y) = 0$ if and only if $x = y$;
2. $d(x, y) = d(y, x)$;
3. $d(x, z) \le d(x, y) + d(y, z)$.

A metric that also satisfies

4. $d(x, z) \le \max(d(x, y), d(y, z))$

is an *ultrametric* and said to be *nonarchimedean*. Every absolute value induces a metric $d(x, y) := |x - y|$. The metric d defines a topology on X generated by *open balls*

$$B_{<r}(x) := \{y \in X : d(x, y) < r\}.$$

with $r \in \mathbb{R}_{>0}$ and $x \in X$, and we call X a *metric space*. It is a Hausdorff space, since distinct $x, y \in X$ have disjoint open neighborhoods $B_{<r}(x)$ and $B_{<r}(y)$ (take $r = d(x,y)/2$), and we note that each *closed ball*

$$B_{\leq r}(x) := \{y \in X : d(x,y) \leq r\}$$

is a closed set, since its complement is the union of $B_{<(d(x,y)-r)}(y)$ over $y \in X - B_{\leq r}(x)$.

Definition 8.1. Let X be a metric space. A sequence (x_n) of elements of X *converges* (*to* x) if there is an $x \in X$ such that for every $\epsilon > 0$ there is an $N \in \mathbb{Z}_{>0}$ such that $d(x_n, x) < \epsilon$ for all $n \geq N$; the limit x is necessarily unique. The sequence (x_n) is *Cauchy* if for every $\epsilon > 0$ there is an $N \in \mathbb{Z}_{>0}$ such that $d(x_m, x_n) < \epsilon$ for all $m, n \geq N$. Every convergent sequence is Cauchy, but the converse need not hold. A metric space in which every Cauchy sequence converges is said to be *complete*.

When X is a ring whose metric is induced by an absolute value $|\ |$, we say that X is complete with respect to $|\ |$. Which sequences converge and which are Cauchy depends very much on the absolute value $|\ |$ that we use. As we have seen in the case $X = \mathbb{Q}$, a field may have infinitely many inequivalent absolute values. Equivalent absolute values necessarily agree on which sequences are convergent and which are Cauchy, so if a field is complete with respect to an absolute value it is complete with respect to all equivalent absolute values.

Definition 8.2. Let X be a metric space. Two Cauchy sequences (x_n) and (y_n) are *equivalent* if $d(x_n, y_n) \to 0$ as $n \to \infty$; this defines an equivalence relation on the set of Cauchy sequences in X and we use $[(x_n)]$ to denote the equivalence class of (x_n). The *completion* of X is the metric space $\widehat{X}$ whose elements are equivalence classes of Cauchy sequences with the metric

$$d([(x_n)], [(y_n)]) = \lim_{n\to\infty} d(x_n, y_n).$$

The space X is canonically embedded in its completion via the map $x \mapsto \hat{x} = [(x, x, \ldots)]$, and we view X as a subspace of $\widehat{X}$.

When X is a ring we extend the ring operations to $\widehat{X}$ a ring by defining

$$[(x_n)] + [(y_n)] := [(x_n + y_n)] \qquad \text{and} \qquad [(x_n)][(y_n)] := [(x_n y_n)].$$

The additive and multiplicative identities are then $0 := [(0, 0, \cdots)]$ and $1 := [(1, 1, \ldots)]$. If the metric on X is induced by an absolute value $|\ |$, we extend $|\ |$ to an absolute value on $\widehat{X}$ via

$$\big|[(x_n)]\big| := \lim_{n\to\infty} |x_n|$$

(that this limit exists follows from the triangle inequality and the fact that $\mathbb{R}$ is complete). When X is a field with a metric induced by an absolute value, the completion $\widehat{X}$ is also a field (this is false in general, see Problem Set 4 for a counter example). Indeed, given $[(x_n)] \neq 0$, we can choose (x_n) with $x_n \neq 0$ for all n, and use the multiplicative property of the absolute value (combined with the triangle inequality), to show that $(1/x_n)$ is Cauchy. We then have $1/[(x_n)] = [(1/x_n)]$, since $[(x_n)][(1/x_n)] = [(1, 1, \ldots] = 1$.

If $|\ |$ arises from a discrete valuation v on K (meaning $|x| := c^{v(x)}$ for some $c \in (0,1)$), we extend v to a discrete valuation on $\widehat{X}$ via

$$v([(x_n)]) := \lim_{n\to\infty} v(x_n) \in \mathbb{Z}.$$

Note that the sequence $(v(x_n))$ is eventually constant, hence the limit is an integer, and we have $|[(x_n)]| = c^{v([(x_n)])}$.

Proposition 8.3. *Let $\widehat{K}$ be the completion of a field K with respect to an absolute value $|\ |$. The field $\widehat{K}$ is complete, and has the following universal property: every embedding of K into a complete field L can be uniquely extended to an embedding of $\widehat{K}$ into L. Up to a canonical isomorphism, $\widehat{K}$ is the unique field with this property.*

Proof. See Problem Set 4. □

The proposition implies that the completion of $\widehat{K}$ is (isomorphic to) itself (apply the universal property of the completion of $\widehat{K}$ to the trivial embedding $\widehat{K} \to \widehat{K}$). Completing a field that is already complete has no effect. In particular, the completion of K with respect to the trivial absolute value is just K: the only sequences that are Cauchy with respect to the trivial absolute value are those that are eventually constant, all of which clearly converge.

8.1.1 Topological fields with an absolute value

Let K be a field with an absolute value $|\ |$. Then K is also a topological space under the metric $d(x,y) = |x-y|$ induced by the absolute value, and moreover it is a *topological field*.

Definition 8.4. An abelian group G is a *topological group* if it is a topological space in which the map $G \times G \to G$ defined by $(g,h) \mapsto g+h$ and the map $G \to G$ defined by $g \mapsto -g$ are both continuous (here $G\times G$ has the product topology). A commutative ring R is a *topological ring* if it is a topological space in which the maps $R \times R \to R$ defined by $(r,s) \mapsto r+s$ and $(r,s) \mapsto rs$ are both continuous; the additive group of R is then a topological group, since $(-1,s) \mapsto -s$ is continuous, but the unit group $R^\times$ need not be a topological group. A field K is a *topological field* if it is a topological ring whose unit group is a topological group.

If R is a ring with an absolute value then it is a topological ring under the induced topology, and its unit group is also a topological group ; in particular, if R is a field with an absolute value, then it is a topological field under the induced topology. These facts follow from the the triangle inequality and the multiplicative property of an absolute value.

Two absolute values on the same field induce the same topology if and only if they are equivalent; this follows from the Weak Approximation Theorem.

Theorem 8.5 (Weak Approximation)**.** *Let K be a field and let $|\cdot|_1,\ldots,|\cdot|_n$ be pairwise inequivalent nontrivial absolute values on K. Let $a_1,\ldots,a_n \in K$ and let $\epsilon_1,\ldots,\epsilon_n$ be positive real numbers. Then there exists an $x \in K$ such that $|x-a_i|_i < \epsilon_i$ for $1 \le i \le n$.*

Proof. See Problem Set 4. □

Corollary 8.6. *Let K be a field with absolute values $|\ |_1$ and $|\ |_2$. The induced topologies on K coincide if and only if $|\ |_1$ and $|\ |_2$ are equivalent.*

Proof. See Problem Set 4. □

The topology induced by a nonarchimedean absolute value has some features that may be counterintuitive to the uninitiated. In particular, every open ball is also closed, so the closure of $B_{<r}(x)$ is not $B_{\le r}(x)$ unless these two sets are already equal. The latter can definitely happen: the map $|\ |\colon K \to \mathbb{R}_{\ge 0}$ need not be surjective, and will even have discrete image when $|\ |$ arises from a discrete valuation. This means that is entirely possible

to have $B_{<r}(x) = B_{<s}(x)$ for $r \neq s$; indeed this must occur uncountably often if $|\ |$ arises from a discrete valuation. The reader may wish to verify that the following hold in any nonarchimedean metric space X:

1. Every point in an open ball is a center: $B_{<r}(y) = B_{<r}(x)$ for all $y \in B_{<r}(x)$.
2. Any pair of open balls are either disjoint or concentric (have a common center).
3. Every open ball is closed and every closed ball is open.
4. X is *totally disconnected*: every pair of distinct points have disjoint open neighborhoods whose union is the whole space (every connected component is a point).

For any topological space X, the continuity of a map $f\colon X \times X \to X$ implies that for every fixed $x \in X$ the maps $X \to X$ defined by $y \mapsto f(x, y)$ and $y \mapsto f(y, x)$ are continuous, since each is the composition $f \circ \phi$ of f with the continuous map $\phi\colon X \to X \times X$ defined by $y \mapsto (x, y)$ and $y \mapsto (y, x)$, respectively. For an additive topological group G this means that every translation-by-h map $g \mapsto g + h$ is a homeomorphism, since it is continuous and has a continuous inverse (translate by $-h$); in particular, translates of open sets are open and translates of closed sets are closed. Thus in order to understand the topology of a topological group, we can focus on neighborhoods of the identity; a base of open neighborhoods about the identity determines the entire topology. It also means that any topological property of a subgroup (such as being open, closed, or compact) applies to all of its cosets.

If $\widehat{K}$ is the completion of a field K with respect to an absolute value $|\ |$, then $\widehat{K}$ is a topological field with the topology induced by $|\ |$, and the subspace topology on $K \subseteq \widehat{K}$ is the same as the topology on K induced by $|\ |$. By construction, K is *dense* in $\widehat{K}$; indeed, $\widehat{K}$ is precisely the set of limit points of K. More generally, every open ball $B_{<r}(x)$ in K is dense in the corresponding open ball $B_{<r}(x)$ in $\widehat{K}$.

8.1.2 Inverse limits

Inverse limits are a general construction that can be applied in any category with products, although we will only be concerned with inverse limits in familiar concrete categories such as groups, rings, and topological spaces. Recall that a *concrete category* is one whose objects can be defined as sets (more formally, it is a category that admits a faithful functor to the category of sets), which allows us to speak of the elements of an object in the category.

Definition 8.7. A *directed set* is a set I with a relation "$\leq$" that is reflexive ($i \leq i$), anti-symmetric ($i \leq j \leq i \Rightarrow i = j$), and transitive ($i \leq j \leq k \Rightarrow i \leq k$), in which every finite subset has an upper bound (in particular, I is non-empty).

Definition 8.8. An *inverse system* (*projective system*) in a category is a family of objects $\{X_i : i \in I\}$ indexed by a directed set I and a family of morphisms $\{f_{ij}\colon X_i \leftarrow X_j : i \leq j\}$ (note the direction) such that each f_{ii} is the identity and $f_{ik} = f_{ij} \circ f_{jk}$ for all $i \leq j \leq k$.[1]

Definition 8.9. Let (X_i, f_{ij}) be an inverse system in a concrete category with products. The *inverse limit* (or *projective limit*) of (X_i, f_{ij}) is the object

$$X := \varprojlim X_i := \left\{ x \in \prod_{i \in I} X_i : x_i = f_{ij}(x_j) \text{ for all } i \leq j \right\} \subseteq \prod_{i \in I} X_i$$

[1]Some (but not all) authors reserve the term *projective system* for cases where the f_{ij} are epimorphisms. This distinction is not relevant to us, as our inverse systems will all use epimorphisms (surjections, in fact).

(whenever such an object X exists in the category). The restrictions $\pi_i\colon X \to X_i$ of the projections $\prod X_i \to X_i$ satisfy $\pi_i = f_{ij} \circ \pi_j$ for $i \le j$.

The object $X = \varprojlim X_i$ has the universal property that if Y is another object with morphisms $\psi_i\colon Y \to X_i$ that satisfy $\psi_i = f_{ij} \circ \psi_j$ for $i \le j$, then there is a unique morphism $Y \to X$ for which all of the diagrams

$$\begin{tikzcd} & Y \arrow[d, dashed, "\exists!"] \arrow[ddl, bend right, "\psi_i"'] \arrow[ddr, bend left, "\psi_j"] & \\ & X \arrow[dl, "\pi_i"] \arrow[dr, "\pi_j"'] & \\ X_i & & X_j \arrow[ll, "f_{ij}"] \end{tikzcd}$$

commute (this universal property defines an inverse limit in any category with products).

As with other categorical constructions satisfying (or defined by) universal properties, uniqueness is guaranteed, but existence is not. However, in all the categories that we shall consider, inverse limits exist.

Proposition 8.10. *Let (X_i, f_{ij}) be an inverse system of Hausdorff topological spaces. Then $X := \varprojlim X_i$ is a closed subset of $\prod X_i$, and if the X_i are compact then X is compact.*

Proof. The set X is the intersection of the sets $Y_{ij} := \{x \in \prod X_i : x_i = f_{ij}(x_j)\}$ with $i \le j$, each of which can be written as $Y_{ij} = \prod_{k \ne i,j} X_k \times Z_{ij}$, where Z_{ij} is the preimage of the diagonal $\Delta_i := \{(x_i, x_i) : x_i \in X_i\} \subseteq X_i \times X_i$ under the continuous map $X_i \times X_j \to X_i \times X_i$ defined by $(x_i, x_j) \mapsto (x_i, f_{ij}(x_j))$. Each Δ_i is closed in $X_i \times X_i$ (because X_i is Hausdorff), so each Z_{ij} is closed in $X_i \times X_j$, and each Y_{ij} is closed in $\prod X_i$; it follows that X is a closed subset of $\prod X_i$. By Tychonoff's theorem [1, Thm. I.9.5.3], if the X_i are compact then so is their product $\prod X_i$, in which case the closed subset X is also compact. □

8.2 Valuation rings in complete fields

We now want to specialize to absolute values derived from a discrete valuation $v\colon K^\times \twoheadrightarrow \mathbb{Z}$. If we pick a positive real number $c < 1$ and define $|x|_v := c^{v(x)}$ for $x \in K^\times$ and $|0|_v = 0$ then we obtain a nontrivial nonarchimedean absolute value $|\ |_v$. Different choices of c yield equivalent absolute values and thus do not change the topology induced by $|\ |_v$ or the completion $\widehat{K}$ of K with respect to $|\ |_v$. We will see later that there is a canonical choice for c when the residue field k of the valuation ring of K is finite (one takes $c = 1/\#k$).

It follows from our discussion that the valuation ring

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

is a closed (and therefore open) ball in $\widehat{K}$, and it is equal to the closure in $\widehat{K}$ of the valuation ring A of K. Note that $\widehat{K}$ is the fraction field of $\hat{A}$, since we have $x \in \widehat{K} - \hat{A}$ if and only if $1/x \in \hat{A}$; so rather than defining $\hat{A}$ as the valuation ring of $\widehat{K}$ we could equivalently define $\hat{A}$ as the completion of A (with respect to $|\ |_v$) and then define $\widehat{K}$ as its fraction field.

We now give another characterization of $\hat{A}$ as an inverse limit.

Proposition 8.11. *Let K be a field with absolute value $|\ |_v$ induced by a discrete valuation v, let A be the valuation ring of K, and let π be a uniformizer. The valuation ring* *of the completion of K with respect to $|\ |_v$ is a complete discrete valuation ring $\hat{A}$ with uniformizer π, and we have an isomorphism of topological rings*

$$\hat{A} \simeq \varprojlim_{n\to\infty} \frac{A}{\pi^n A}.$$

It is clear that $\hat{A}$ is a complete DVR with uniformizer π: it is complete because it is closed and therefore contains all its limit points in the complete field $\widehat{K}$, it is a DVR with uniformizer π because v extends to a discrete valuation on $\hat{A}$ with $v(\pi) = 1$.

Before proving the main part of the proposition, let us check that we understand the topology of the inverse limit $X := \varprojlim_n A/\pi^n A$. The valuation ring A is a closed ball $B_{\le 1}(0)$ (hence an open set) in the nonarchimedean metric space K, and this also applies to each of the sets $\pi^n A$ (they are closed balls of radius c^n about 0). Each quotient $A/\pi^n A$ therefore has the discrete topology, since the inverse image of any point under the quotient map is a coset of the open subgroup $\pi^n A$. The inverse limit X is a subspace of the product space $\prod_n A/\pi^n A$, whose open sets project onto $A/\pi^n A$ for all but finitely many factors (by definition of the product topology). It follows that every proper open subset U of X is the full inverse image (under the canonical projection maps given by the inverse limit construction) of a subset of $A/\pi^m A$ for some $m \ge 1$. When this set is a point we can describe U as a coset $a + \pi^m A$, for some $a \in A$; as a subset $U = \prod_n U_n$ of $\prod_n A/\pi^n A$ each U_n is the image of $a + \pi^m A$ under the quotient map $A \to A/\pi^n A$. In general, U is a union of such sets (all with the same m).

We can alternatively describe the topology on X in terms of an absolute value: for nonzero $x = (x_n) \in X = \varprojlim A/\pi^n A$, let $v(x)$ be the least $n \ge 0$ for which $x_{n+1} \ne 0$, and define $|x|_v := c^{v(x)}$. If we embed A in X in the obvious way, $a \mapsto (\bar{a}, \bar{a}, \bar{a}, \ldots)$, the absolute value on X restricts to the absolute value $|\ |_v$ on A, and the subspace topology A inherits from X is the same as that induced by $|\ |_v$. The open sets of X are unions of open balls $B_{<r}(a)$, where we can always choose $a \in A$ (because A is dense in X). If we let $m \ge 0$ be the least integer for which $c^m < r$, where $c \in (0,1)$ is the constant for which $|x| = c^{v(x)}$ for all $x \in A$, then $B_{<r}(a)$ corresponds to a coset $a + \pi^m A$ as above

Let us now prove the proposition.

Proof. The ring $\hat{A}$ is complete and contains A. For each $n \ge 1$ we define a ring homomorphism $\phi_n \colon \hat{A} \to A/(\pi^n)$ as follows: for each $\hat{a} = [(a_i)]$ let $\phi_n(\hat{a})$ be the limit of the eventually constant sequence $(\overline{a}_i)$ of images of a_i in $A/(\pi^n)$. We thus obtain an infinite sequence of surjective maps $\phi_n \colon \hat{A} \to A/\pi^n A$ that are compatible in that for all $n \ge m > 0$ and all $a \in \hat{A}$ the image of $\phi_n(a)$ in $A/\pi^m A$ is $\phi_m(a)$. This defines a surjective ring homomorphism $\phi \colon \hat{A} \to \varprojlim A/\pi^n A$. Now note that

$$\ker \phi = \bigcap_{n\ge 1} \pi^n \hat{A} = \{0\}, \tag{1}$$

so ϕ is injective and therefore an isomorphism. To show that ϕ is also a homeomorphism, it suffices to note that if $a + \pi^m A$ is a coset of $\pi^m A$ in A and U is the corresponding open set in $\varprojlim A/\pi^n A$, then $\phi^{-1}(U)$ is the closure of $a + \pi^m A$ in $\hat{A}$, which is the coset $a + \pi^m \hat{A}$, an open subset in $\hat{A}$ (as explained in the discussion above, every open set in the inverse limit corresponds to a finite union of cosets $a + \pi^m A$ for some m). Conversely ϕ maps open sets $a + \pi^m \hat{A}$ to open sets in $\varprojlim A/\pi^n A$. $\square$

Remark 8.12. Given any ring R with an ideal I, one can define the *I-adic completion* of R as the inverse limit of topological rings $\hat{R} := \varprojlim_n R/I^n$, where each R/I^n is given the discrete topology. Proposition 8.11 shows that when R is a DVR with maximal ideal $\mathfrak{m}$, taking the completion of R with respect to the absolute value $|\ |_{\mathfrak{m}}$ is the same thing as taking the $\mathfrak{m}$-adic completion. This is not true in general. In particular, the $\mathfrak{m}$-adic completion of a (not necessarily discrete) valuation ring R with respect to its maximal ideal $\mathfrak{m}$ need not be complete (either in the sense of Definition 8.1 or in the sense of being isomorphic to its $\mathfrak{m}$-adic completion). The key issue that arises is that the kernel in (1) need not be trivial; indeed, if $\mathfrak{m}^2 = \mathfrak{m}$ (which can happen) it certainly won't be. This problem does not occur for valuation rings that are noetherian, but these are necessarily DVRs.

Example 8.13. Let $K = \mathbb{Q}$ and let v_p be the p-adic valuation for some prime p and let $|x|_p := p^{-v_p(x)}$ denote the corresponding absolute value. The completion of $\mathbb{Q}$ with respect to $|\ |_p$ is the field $\mathbb{Q}_p$ of p-adic numbers. The valuation ring of $\mathbb{Q}$ corresponding to v_p is the local ring $\mathbb{Z}_{(p)}$. Taking $\pi = p$ as our uniformizer, we get

$$\widehat{\mathbb{Z}_{(p)}} \simeq \varprojlim_{n\to\infty} \frac{\mathbb{Z}_{(p)}}{p^n\mathbb{Z}_{(p)}} \simeq \varprojlim_{n\to\infty} \frac{\mathbb{Z}}{p^n\mathbb{Z}} = \mathbb{Z}_p,$$

the ring of p-adic integers.

Example 8.14. Let $K = \mathbb{F}_q(t)$ be the rational function field over a finite field $\mathbb{F}_q$ and let v_t be the t-adic valuation and let $|x|_t := q^{-v_t(x)}$ be the corresponding absolute value. with uniformizer $\pi = t$. The completion of $\mathbb{F}_q(t)$ with respect to $|\ |_t$ is isomorphic to the field $\mathbb{F}_q((t))$ of Laurent series over $\mathbb{F}_q$. The valuation ring of $\mathbb{F}_q(t)$ with respect to v_t is the local ring $\mathbb{F}_q[t]_{(t)}$ consisting of rational functions whose denominators have nonzero constant term. Taking $\pi = t$ as our uniformizer, we get

$$\widehat{\mathbb{F}_q[t]_{(t)}} \simeq \varprojlim_{n\to\infty} \frac{\mathbb{F}_q[t]_{(t)}}{t^n\mathbb{F}_q[t]_{(t)}} \simeq \varprojlim_{n\to\infty} \frac{\mathbb{F}_q[t]}{t^n\mathbb{F}_q[t]} \simeq \mathbb{F}_q[[t]],$$

where $\mathbb{F}_q[[t]]$ denotes the power series ring over $\mathbb{F}_q$.

Example 8.15. The isomorphism $\mathbb{Z}_p \simeq \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ gives us a canonical way to represent elements of $\mathbb{Z}_p$: we can write $a \in \mathbb{Z}_p$ as a sequence (a_n) with $a_{n+1} \equiv a_n \bmod p^n$, where each $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ is uniquely represented by an integer in $[0, p^n - 1]$. In $\mathbb{Z}_7$, for example:

$$\begin{aligned}
2 &= (2, 2, 2, 2, 2, \ldots)\\
2002 &= (0, 42, 287, 2002, 2002, \ldots)\\
-2 &= (5, 47, 341, 2399, 16805, \ldots)\\
2^{-1} &= (4, 25, 172, 1201, 8404, \ldots)\\
\sqrt{2} &= \begin{cases}(3, 10, 108, 2166, 4567\ldots)\\ (4, 39, 235, 235, 12240\ldots)\end{cases}\\
\sqrt[5]{2} &= (4, 46, 95, 1124, 15530, \ldots)
\end{aligned}$$

While this representation is canonical, it is also redundant. The value of a_n constrains the value of a_{n+1} to just p possible values among the p^{n+1} elements of $\mathbb{Z}/p^{n+1}\mathbb{Z}$, namely, those that are congruent to a_n modulo p^n. We can always write $a_{n+1} = a_n + p^n b_n$ for some $b_n \in [0, p-1]$, namely, $b_n = (a_{n+1} - a_n)/p^n$.

Definition 8.16. Let $a = (a_n)$ be a p-adic integer with each a_n uniquely represented by an integer in $\in [0, p^n - 1]$. The sequence $(b_0, b_1, b_2, \ldots)$ with $b_0 = a_1$ and $b_n = (a_{n+1} - a_n)/p^n$ is called the *p-adic expansion of a*.

Proposition 8.17. *Every element of $\mathbb{Z}_p$ has a unique p-adic expansion and every sequence $(b_0, b_1, b_2, \ldots)$ of integers in $[0, p-1]$ is the p-adic expansion of an element of $\mathbb{Z}_p$.*

Proof. This follows immediately from the definition: we can recover (a_n) from its p-adic expansion $(b_0, b_1, b_2, \ldots)$ via $a_1 = b_0$ and $a_{n+1} = a_n + pb_n$ for all $n \geq 1$. □

Thus we have a bijection between $\mathbb{Z}_p$ and the set of all sequences of integers in $[0, p-1]$ indexed by the nonnegative integers.

Example 8.18. We have the following p-adic expansion in $\mathbb{Z}_7$:

$$\begin{aligned}
2 &= (2, 0, 0, 0, 0, 0, 0, 0, 0, 0, \ldots) \\
2002 &= (0, 6, 5, 5, 0, 0, 0, 0, 0, 0, \ldots) \\
-2 &= (5, 6, 6, 6, 6, 6, 6, 6, 6, 6, \ldots) \\
2^{-1} &= (4, 3, 3, 3, 3, 3, 3, 3, 3, 3, \ldots) \\
5^{-1} &= (3, 1, 4, 5, 2, 1, 4, 5, 2, 1, \ldots) \\
\sqrt{2} &= \begin{cases} (3, 1, 2, 6, 1, 2, 1, 2, 4, 6 \ldots) \\ (4, 5, 4, 0, 5, 4, 5, 4, 2, 0 \ldots) \end{cases} \\
\sqrt[5]{2} &= (4, 6, 1, 3, 6, 4, 3, 5, 4, 6 \ldots)
\end{aligned}$$

You can easily recreate these examples (and many more) in Sage. To create the ring of 7-adic integers, use `Zp(7)`. By default Sage uses 20 digits of p-adic precision, but you can change this to n digits using `Zp(p,n)`.

Performing arithmetic in $\mathbb{Z}_p$ using p-adic expansions is straight-forward. One computes a sum of p-adic expansions $(b_0, b_1, \ldots) + (c_0, c_1, \ldots)$ by adding digits mod p and carrying to the right (don't forget to carry!). Multiplication corresponds to computing products of formal power series in p, e.g. $\left(\sum b_n p^n\right)\left(\sum c_n p^n\right)$, and can be performed by hand (or in Sage) using the standard schoolbook algorithm for multiplying integers represented in base 10, except now one works in base p. For more background on p-adic numbers, see [2, 3, 4, 5].

8.3 Extending valuations

Recall from Lecture 3 that each prime $\mathfrak{p}$ of a Dedekind domain A determines a discrete valuation (a surjective homomorphism) $v_\mathfrak{p} \colon \mathcal{I}_A \to \mathbb{Z}$ that assigns to a nonzero fractional ideal I the exponent $n_\mathfrak{p}$ appearing in the unique factorization of $I = \prod \mathfrak{p}^{n_\mathfrak{p}}$ into prime ideals; equivalently, $v_\mathfrak{p}(I)$ is the unique integer n for which $IA_\mathfrak{p} = \mathfrak{p}^n A_\mathfrak{p}$. This induces a discrete valuation $v_\mathfrak{p}(x) := v_\mathfrak{p}(xA)$ on the fraction field K, and a corresponding absolute value $|x|_\mathfrak{p} := c^{v_\mathfrak{p}(x)}$ (with $0 < c < 1$). In the $AKLB$ setup, where L/K is a finite separable extension and B is the integral closure of A in L, the primes $\mathfrak{q}|\mathfrak{p}$ of B similarly give rise to discrete valuations $v_\mathfrak{q}$ on L, each of which restricts to a valuation on K. We want to understand how the discrete valuations $v_\mathfrak{q}$ relate to $v_\mathfrak{p}$.

Definition 8.19. Let L/K be a finite separable extension, and let v and w be discrete valuations on K and L respectively. If $w_{|K} = ev$ for some $e \in \mathbb{Z}_{>0}$, then we say that w *extends v with index e.*

Theorem 8.20. *Assume AKLB and let $\mathfrak{p}$ be a prime of A. For each prime $\mathfrak{q}|\mathfrak{p}$, the discrete valuation $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with index $e_\mathfrak{q}$, and every discrete valuation on L that extends $v_\mathfrak{p}$ arises in this way. In other words, the map $\mathfrak{q} \mapsto v_\mathfrak{q}$ gives a bijection from $\{\mathfrak{q}|\mathfrak{p}\}$ to the set of discrete valuations of L that extend $v_\mathfrak{p}$.*

Proof. For each prime $\mathfrak{q}|\mathfrak{p}$ we have $v_\mathfrak{q}(\mathfrak{p}B) = e_\mathfrak{q}$ (by definition of the ramification index $e_\mathfrak{q}$), while $v_\mathfrak{q}(\mathfrak{r}B) = 0$ for all primes $\mathfrak{r} \neq \mathfrak{p}$ of A (since $\mathfrak{q}$ lies above only the prime $\mathfrak{p} = \mathfrak{q} \cap A$). If $I = \prod_\mathfrak{r} \mathfrak{r}^{n_\mathfrak{r}}$ is any nonzero fractional ideal of A then

$$v_\mathfrak{q}(IB) = v_\mathfrak{q}\left(\prod_\mathfrak{r} \mathfrak{r}^{n_\mathfrak{r}} B\right) = v_\mathfrak{q}(\mathfrak{p}^{n_\mathfrak{p}} B) = v_\mathfrak{q}(\mathfrak{p}B) n_\mathfrak{p} = e_\mathfrak{q} n_\mathfrak{p} = e_\mathfrak{q} v_\mathfrak{p}(I),$$

so $v_\mathfrak{q}(x) = v_\mathfrak{q}(xB) = e_\mathfrak{q} v_\mathfrak{p}(xA) = e_\mathfrak{q} v_\mathfrak{p}(x)$ for all $x \in K^\times$; thus $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with index $e_\mathfrak{q}$.

If $\mathfrak{q}$ and $\mathfrak{q}'$ are two distinct primes above $\mathfrak{p}$, then neither contains the other and for any $x \in \mathfrak{q} - \mathfrak{q}'$ we have $v_\mathfrak{q}(x) > 0 \geq v_{\mathfrak{q}'}(x)$, thus $v_\mathfrak{q} \neq v_{\mathfrak{q}'}$ and the map $\mathfrak{q} \mapsto v_\mathfrak{q}$ is injective..

Let w be a discrete valuation on L that extends $v_\mathfrak{p}$, let $W = \{x \in L : w(x) \geq 0\}$ be the associated DVR, and let $\mathfrak{m} = \{x \in L : w(x) > 0\}$ be its maximal ideal. Since $w_{|K} = ev_\mathfrak{p}$, the discrete valuation w is nonnegative on $A = \{x \in K : w(x) > 0\}$ therefore $A \subseteq W$, and elements of A with nonzero valuation are precisely the elements of $\mathfrak{p}$, thus $\mathfrak{p} = \mathfrak{m} \cap A$. The discrete valuation ring W is integrally closed in its fraction field L, so $B \subseteq W$. Let $\mathfrak{q} = \mathfrak{m} \cap B$. Then $\mathfrak{q}$ is prime (since $\mathfrak{m}$ is), and $\mathfrak{p} = \mathfrak{m} \cap A = \mathfrak{q} \cap A$, so $\mathfrak{q}$ lies over $\mathfrak{p}$. The ring W contains $B_\mathfrak{q}$ and is contained in $\operatorname{Frac} B_\mathfrak{q} = L$. But there are no intermediate rings between a DVR and its fraction field, so $W = B_\mathfrak{q}$ and $w = v_\mathfrak{q}$ (and $e = e_\mathfrak{q}$). ∎

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 functions*, Springer, 1984.

[4] A.M. Robert, *A course in p-adic analysis*, Springer, 2000.

[5] J.-P. Serre, *A course in arithmetic*, Springer, 1973.