Model Theory of Valued Fields
University of Illinois at Chicago

David Marker

Fall 2018

Contents

1 Valued Fields–Definitions and Examples

References

Large parts of part I of my lectures closely follow the notes of Zoé Chatzidakis [3], Lou van den Dries [9] and the book *Valued Fields* by Engler and Prestel [13].

Conventions and Notation

- In these notes *ring* will always mean commutative ring with identity and *domain* means an integral domain, i.e., a commutative ring with identity and no zero divisors.
- $A \subseteq B$ means that A is a subset of B and allows the possibility $A = B$, while $A \subset B$ means $A \subseteq B$ but $A \neq B$.
- A^X is the set of all functions $f : X \to A$. In particular, $A^{\mathbb{N}}$ is the set of all infinite sequences $a_0, a_1, \ldots$. We sometimes write (a_n) for $a_0, a_1, \ldots$.
- $A^{<\mathbb{N}}$ is the set of all finite sequence $(a_1, \ldots, a_n)$ where $a_1, \ldots, a_n \in A$.
- When studying a structure $\mathcal{M} = (M, \ldots)$, we say X is *definable* if it is definable with parameters. If we wish to specify that it is definable without parameters we will say that it is $\emptyset$-definable. More generally, if we wish to specify it is definable with parameters from A we will say that it is A-definable.
- Because we use $\overline{x}$ (as well as res(x)) to denote the residue of an element, it would be confusing to also use $\overline{x}$ to denote a sequence of elements or variables. We will instead use $\mathbf{x}$ to denote an arbitrary sequence $\mathbf{x} = (x_1, \ldots, x_n)$. The length of $\mathbf{x}$ will usually be clear from context.

1.1 Valuations and Valuation Rings

Definition 1.1 Let A be an integral domain, $(\Gamma, +, 0, <)$ an ordered abelian group, a *valuation* is a map $v : A^\times \to \Gamma$ such that:
i) $v(ab) = v(a) + v(b)$;
ii) $v(a + b) \geq \min(v(a), v(b))$.
We refer to (A, v) as an *valued ring*.

A *valued field* (K, v) is a field K with a valuation v. The image of K under v is called the *value group* of (K, v)

We also sometimes think of the valuation as a map from $v : A \to \Gamma \cup \{\infty\}$ where $v(0) = \infty$ and if $a \neq 0$, then $v(a) \neq \infty$. In this case we think of $\gamma < \infty$ and $\gamma + \infty = \infty + \infty = \infty$ for any $\gamma \in \Gamma$.

Often we will assume that the valuation $v : K^\times \to \Gamma$ is surjective, so the value group is Γ.

Examples

1. Let K be a field and define $v(x) = 0$ for all $x \in K^\times$. We call v the *trivial valuation* on K.

2. Let p be a prime number and define v_p on $\mathbb{Z}$ by $v_p(a) = m$ where $a = p^m b$ where $p \not| b$. We call v_p the *p-adic valuation* on $\mathbb{Z}$.

3. Let F be a field and define v on $F[X]$ such that $v(f) = m$ where $f = X^m g$ where $g(0) \neq 0$. More generally, if $p(X)$ is any irreducible polynomial we could define $v_p(f) = m$ where $f = p^m g$ and $p \not| g$.

4. Let F be a field and let $F[[T]]$ be the ring of formal power series over F. We could define a valuation $v : F[[T]] \to F$ by $v(f) = m$ when $f = a_m T^m + a_{m+1} T^{m+1} + \dots$ where $a_m \neq 0$.

Exercise 1.2 a) If A is an domain, K is its field of fractions and v is a valuation on A, show that we can extend v to K by $v(a/b) = v(a) - v(b)$.

b) Show that this is the only way to extend v to a valuation on K.

Thus we can extend to the valuation v_p on $\mathbb{Z}$ to $v_p : \mathbb{Q}^\times \to \mathbb{Z}$ and we can extend the valuations on $K[X]$ and $K[[X]]$ to $K(X)$, the field of rational functions on K, and $K((T))$, the field of formal *Laurent series*, respectively.

Let F be a field and let

$$F\langle T \rangle = \bigcup_{n=1}^{\infty} F((T^{\frac{1}{n}}))$$

be the field of *Puiseux series*. If $f \in F\langle T \rangle$ is nonzero then for some $m \in \mathbb{Z}$ and $n \geq 1$, $f = \sum_{i=m}^{\infty} a_i T^{\frac{i}{n}}$ and $a_m \neq 0$. We let $v(f) = m/n$. We will show later that if we start with an algebraically closed F of characteristic 0, then $F\langle T \rangle$ is also algebraically closed. For a more elementary direct proof see [29].

In the trivial valuation has value group $\{0\}$. The rational functions and Laurent series have value group $(\mathbb{Z}, +, <)$ and the Puiseux series have value group $\mathbb{Q}$.

We next give some very easy properties of valuations.

Lemma 1.3 *i)* $v(1) = 0$.
ii) $v(-1) = 0$.
iii) $v(x) = v(-x)$;
iv) If K *is a valued field and* $x \neq 0$, *then* $v(1/x) = -v(x)$.
v) If $v(a) < v(b)$, *then* $v(a + b) = v(a)$.

Proof i) $v(1) = v(1 \cdot 1) = v(1) + v(1)$, so $v(1) = 0$.

ii) $0 = v(1) = v((-1) \cdot (-1)) = v(-1) + v(-1)$. Because ordered groups are torsion free, $v(-1) = 0$.

iii) $v(-x) = v(-1 \cdot x) = v(-1) + v(x) = v(x)$.

iv) $v(1/x) + v(x) = v(1) = 0$. Thus $v(1/x) = -v(x)$.

v) we have $v(a + b) \geq \min(v(a), v(b))$. Thus, $v(a + b) \geq v(a)$. On the other hand $v(a) = v(a + b - b) \geq \min(v(a + b), v(b))$. Since $v(a) < v(b)$, we must have $v(a + b) < v(b)$ and $v(a) \geq v(a + b)$. □

Suppose (K, v) is a valued field. Let $\mathcal{O} = \{x \in K : v(x) \geq 0\}$ we call $\mathcal{O}$ the *valuation ring* of K. Let $U = \{x : v(x) = 0\}$. If $x \in U$, then $1/x \in U$. Moreover, if $v(x) > 0$, then $v(1/x) < 0$. Thus U is the set of units, i.e., invertible elements of $\mathcal{O}$.

Let $\mathfrak{m} = \{x \in \mathcal{O} : v(x) > 0\}$. It is easy to see that $\mathfrak{m}$ is an ideal. If $x \notin \mathfrak{m}$, then $v(x) \leq 0$ and $1/x \in \mathcal{O}$. Thus there is no proper ideal of $\mathcal{O}$ containing x. Thus $\mathfrak{m}$ is a maximal ideal and every proper ideal is contained in $\mathfrak{m}$.

Recall that a ring is *local* if there is a unique maximal ideal. We have shown that $\mathcal{O}$ is local. One property that we will use about local rings is that if A is local with maximal ideal $\mathfrak{m}$ and $a \in A$ is not a unit, then (a) is a proper ideal and extends to a maximal ideal. Since $\mathfrak{m}$ is the unique maximal ideal $a \in \mathfrak{m}$. Thus the unique maximal ideal of A is exactly the nonunits of A.

Exercise 1.4 Suppose A is a domain with fraction field K and $P \subset A$ is a prime ideal. Recall that the *localization* of A at P is

$$A_P = \{a/b \in K : a \in A \text{ and } b \notin P\}.$$

Let

$$A_P P = \{a_1 p_1 + \dots a_m p_m : a_1, \dots, a_m \in A_P, p_1, \dots, p_m \in P, m = 1, 2, \dots\}.$$

Show that A_P is a local ring with maximal ideal $A_P P$.

Lemma 1.5 *The ideals of $\mathcal{O}$ are linearly ordered by $\subset$ with maximal element $\mathfrak{m}$.*

Proof Suppose P and Q are ideals of $\mathcal{O}$, $x \in P \setminus Q$ and $y \in Q \setminus P$. Without loss of generality assume $v(x) \leq v(y)$. Then $v(y/x) = v(y) - v(x) \geq 0$ and $y/x \in \mathcal{O}$. But then $y = (y/x)x \in P$, a contradiction. We have already shown that $\mathfrak{m}$ is the unique maximal ideal. □

Exercise 1.6 Consider $A = \mathbb{C}[X, Y]_{(X,Y)}$. Argue that A is a local domain that is not a valuation ring. [Hint: Consider the ideals (X) and (Y) in A.]

Define $\boldsymbol{k} = \mathcal{O}/\mathfrak{m}$. Since $\mathfrak{m}$ is maximal, this is a field which we call the *residue field* of (K, v) and let $\text{res} : \mathcal{O} \to \boldsymbol{k}$ be the residue map $\text{res}(x) = x/\mathfrak{m}$. Often we write $\overline{x}$ for $\text{res}(x)$.

Examples

1. In the trivial valuation on K, the valuation ring is K, the maximal ideal is $\{0\}$ and the residue field is K.

2. For the p-adic valuation on $\mathbb{Q}$ the valuation ring is $\mathbb{Z}_{(p)} = \{m/n : m, n \in \mathbb{Z}, p \not| n.\}$, the maximal ideal is $p\mathbb{Z}_{(p)}$ and the residue field is $\mathbb{F}_p$, the p-element field.

3. Consider the field of formal Laurent series $F(\!(T)\!)$ with valuation $v(f) = m$ where $f = \sum_{n=m}^{\infty} a_n T^n$ where $a_m \neq 0$, then the valuation ring is $F[[T]]$, the maximal ideal is all series $\sum_{n=m}^{\infty} a_n T^n$ where $m > 0$ and the residue field is F.

Exercise 1.7 a) Suppose (K, v) is an algebraically closed valued field. Show that the value group is divisible and the residue field is algebraically closed.

b) Suppose (K, v) is a real closed valued field. Show that the value group is divisible but the residue field need not even have characteristic zero.

Exercise 1.8 Suppose L is an algebraic extension of K and v is a valuation on L.

a) Show that the value group of L is contained in the divisible hull of the value group of K.

b) Show that the residue field of L is an algebraic extension of the residue field of K.

The valuation topology

Let $v : K^\times \to \Gamma$ be a valuation. Let $a \in K$ and $\gamma \in \Gamma$ let

$$B_\gamma(a) = \{x \in K : v(x - a) > \gamma\}$$

be the open ball centered at a of radius γ.[1] The valuation topology on K is the weakest topology in which all $B_\gamma(a)$ are open.

Let

$$\overline{B}_\gamma(a) = \{x \in K : v(x - a) \geq \gamma\}$$

be the closed ball of radius γ centered at a. If $b \neq \overline{B}_\gamma(a)$, then $v(b-a) = \delta < \gamma$. If $x \in B_\delta(b)$, then $v(x - a) = v((x - b) + (b - a))$. Since $v(x - b) > \delta$ and $v(b - a) = \delta$, $v(x - a) = \delta < \gamma$. Thus $\overline{B}_\gamma(a) \cap B_\delta(b) = \emptyset$ and closed balls are indeed closed in the valuation topology.

Lemma 1.9 *If $b \in B_\gamma(a)$, then $B_\gamma(a) = B_\gamma(b)$ and the same is true for closed balls. In other words, every point in a ball is the center of the ball.*

Proof Let $b \in B_\gamma(a)$. If $v(x - a) > \gamma$, then

$$v(x - b) \geq \min(v(x - a), v(a - b)) > \gamma.$$

[1] Note this definition of *radius* is somewhat misleading. In particular, the balls get smaller as the radius gets larger!

□

When we have a valuation $v : K^\times \to \mathbb{Z}$, $\overline{B}_n(a) = B_{n+1}(a)$. Thus the closed balls are also open. So there is a clopen basis for the topology.

In fact closed balls are always open.

Lemma 1.10 *Every closed ball is open.*

Proof Let $B = \overline{B}_\gamma(a)$ be a closed ball. Consider the boundary

$$\partial B = \{x : v(x-a) = \gamma\}.$$

Suppose $b \in \partial B_\gamma(a)$. If $x \in B_\gamma(b)$, then

$$v(x-a) = v((x-b) + v(b-a)).$$

But $v(b-a) = \gamma$ and $v(x-b) > \gamma$. Thus $v(x-a) = \gamma$ and $B_\gamma(a)$ is contained in δB. Thus

$$B = B_\gamma(a) \cup \bigcup_{b \in \delta(B)} B_\gamma(b).$$

□

Exercise 1.11 Show that every closed ball B is a union of disjoint open balls each of which is a maximal open subball of B.

Exercise 1.12 Suppose $B_1, \ldots, B_m$ are disjoint open or closed balls where $m \geq 2$. Let a_i be the center of B_i and let $\delta = \min\{v(a_1 - a_i) : i = 2, \ldots, m\}$. Show that $\overline{B}_\delta(a_i)$ is the smallest ball containing $B_1 \cup \cdots \cup B_m$.

Exercise 1.13 Prove that in the valuation topology all polynomial maps are continuous. [Hint: Consider the Taylor expansion of $f(a+\epsilon)$]

Valuation rings

Interestingly, the ring structure of the valuation ring $\mathcal{O}$ alone gives us enough information to recover the valuation.

Definition 1.14 We say that a domain A with fraction field K. is a *valuation ring* if $x \in A$ or $1/x \in A$ for all $x \in K$.

Let A be a valuation ring. Let U be the group of units of A and let $\mathfrak{m} = A \backslash U$. We claim that $\mathfrak{m}$ is the unique maximal ideal of A. If $a \in \mathfrak{m}$ and $b \in A$, then $ab \notin U$ since otherwise $1/a = b(1/ab) \in A$. If $a, b \in \mathfrak{m}$. At least one of a/b and $b/a \in A$. Suppose $a/b \in A$. Then $a + b = b(a/b + 1) \in \mathfrak{m}$. Thus $\mathfrak{m}$ is closed under addition so it is an ideal. If $x \in A \setminus \mathfrak{m}$, then $A \in U$, so no ideal of A contains x. Thus $\mathfrak{m}$ is the unique maximal ideal of A. For $x, y \in K^\times$ we say $x|y$ if $y/x \in A$.

Let $G = K^\times/U$. Define a relation on G by $x/U \leq y/U$ if and only if $x|y$. For $u, v \in U$ we have $x|y$ if and only if $ux|vy$. Thus $<$ is well defined. If $x|y$ and $y|x$, then $x/y \in U$ and $x/U = y/U$. If $x/U \leq y/U$ and $y/U \leq z/U$. Then there

are $a, b \in A$ such that $y = ax$ and $z = by$. But then $z = abx$ and $x/U \leq z/U$. Thus $\leq$ is a linear order of Γ. We write $x/U < y/U$ if $x|y$ and $y \not| x$.

Exercise 1.15 Suppose $x/U < y/U$ and $z \in K^\times$. Show that $x/U \cdot z/U < y/U \cdot z/U$.

Thus $(G, \cdot, <)$ is an ordered abelian group. It is also easy to set that $1/U \leq x/U$ if and only if $x \in A$. If we rename the operation $+$ and the identity 0 we have shown that $w(x) = x/U$ is a valuation on K with valuation ring A.

Exercise 1.16 Suppose (K, v) is a valued field with surjective valuation $v : K^\times \Gamma$ and valuation ring $\mathcal{O}$ and let $w : K^\times \to G$ be the valuation recovered from $\mathcal{O}$ as above. If $\gamma \in \Gamma$, choose $x \in K$ with $v(x) = \gamma$ and define $\phi(\gamma) = w(g)$. Show that $\phi : \Gamma \to G$ is a well defined order isomorphism and $\phi(v(x)) = w(x)$ for all $x \in K^\times$. Thus the valuation we have recovered is, up to isomorphism, the one we began with.

There are some interesting contexts where the valuation ring arises more naturally than the valuation. Suppose $(F, <)$ is an ordered field and $\mathcal{O} \subset F$ is a proper convex subring. If $x \in F \setminus \mathcal{O}$, then, in particular, $|x| > 1$. But then, $|1/x| < 1$ so $1/x \in \mathcal{O}$. Thus $\mathcal{O}$ is a valuation ring.

One important example of this occurs when $\mathcal{O}$ is the convex hull of $\mathbb{Z}$. We call this the *standard valuation*.

Exercise 1.17 Let F be an ordered field with infinite elements and let $\mathcal{O}$ be the convex hull of $\mathbb{Z}$.

a) Show that the maximal ideal of $\mathcal{O}$ is the set of infinitesimal elements.

b) Suppose $\mathbb{R} \subset F$. Show that the residue field is isomorphic to $\mathbb{R}$.

c) Suppose that F is real closed (but not necessarily that $\mathbb{R} \subset F$). Show that the residue field is real closed and isomorphic to a subfield of $\mathbb{R}$.

The structure of the value group will depend on field F. Suppose F is real closed. In this case we can say is that it will be divisible. Suppose g is in the value group and $x \in F$ with $x > 0$ and $v(x) = g$. Then there is $y \in F$ with $y^n = x$. Hence $g = v(y^n) = nv(y)$.

Definition 1.18 An ordered group Γ is *archimedian* if for all $0 < g < h$, there is $n \in \mathbb{N}$ with $ng > h$.

Exercise 1.19 Show that an ordered abelian group is archimedian if and only if it is isomorphic to a subgroup of $(\mathbb{R}, +)$.

Exercise 1.20 Order $\mathbb{R}(X, Y)$ such that $X > r$ for all $r \in \mathbb{R}$ and $Y > X^n$ for all $n \in \mathbb{N}$. Let F be the real closure of $(\mathbb{R}(X, Y), <)$ and consider the standard valuation. Show that the value group in nonarchimedean.

1.2 Absolute Values

Definition 1.21 An *absolute value* on a ring A is a function $|\cdot| : A \to \mathbb{R}^{\geq 0}$ such that

i) $|x| = 0$ if and only if $|x| = 0$;
ii) $|xy| = |x||y|$;
iii) (triangle inequality) $|x + y| \leq |x| + |y|$;

The usual absolute values on $\mathbb{R}$ and $\mathbb{C}$ (or the restrictions to any subring) are absolute values in this sense and if $i : K \to \mathbb{C}$ is a field embedding we obtain an absolute value $|\cdot|$ on K by taking $|a| = ||i(a)||$.

If $v : A^\times \to \Gamma$ is a valuation where $\Gamma \subseteq \mathbb{R}$ and $0 < \alpha < 1$. Then we can construct and absolute value $|x| = \alpha^{v(x)}$ for $x \neq 0$. In this case $|x+y| = \alpha^{v(x+y)}$. Since $v(x+y) \geq \min(v(x), v(y))$ and $0 < \alpha < 1$, $|x+y| \leq \max(|x|, |y|) \leq |x|+|y|$. An absolute value that satisfies this strong form of the triangle inequality is called a *nonarchimedean absolute value* or *ultrametric*.

We also have the trivial absolute value where $|x| = 1$ for all nonzero x–this is of course the absolute value corresponding to the trivial valuation.

Exercise 1.22 We can extend an absolute value on a domain A to the fraction field.

Exercise 1.23 Suppose K is a field with a nonarchimedean absolute value $|\cdot|$.

a) Show that $\mathcal{O} = \{x \in K : |x| \leq 1\}$ is a valuation ring with maximal ideal $\mathfrak{m} = \{x : v(x) < 1\}$.

b) Show that the valuation topology associated with $\mathcal{O}$ is exactly the topology induced by the absolute value.

Once we have an absolute value we define a topology as usual by taking basic open balls $B_\epsilon(a) = \{x : |x-a| < \epsilon\}$. If we start with a valuation $v : \mathcal{K}^\times \to \mathbb{R}$ and take the absolute value $|x| = \alpha^{v(x)}$, then this is exactly the valuation topology. Note that if we chose a different β with $0 < \beta < 1$ and defined $|x| = \beta^{v(x)}$ we would define the same topology.

Definition 1.24 We say that two absolute values $|\cdot|_1$ and $|\cdot|_2$ on A are *equivalent* if they give rise to the same topology.

Consider the field $\mathbb{Q}$. We have the usual absolute value on it which we will denote $|\cdot|_\infty$. For p a prime we have the absolute value $|x|_p = (1/p)^{v_p(a)}$. This choice of base is convenient as it gives the *product formula*

$$|x|_\infty \prod_{p \text{ prime}} |x|_p = 1$$

which is trivial in this case but has nontrivial generalizations to number fields (see, for example, [2] §10.2).

Exercise 1.25 Show that the absolute values $|\cdot|_\infty, |\cdot|_2, |\cdot|_3, \ldots$ are pairwise inequivalent. [Hint: Consider the sequence $p, p^2, \ldots$.]

Exercise 1.26 Consider the sequence $4, 34, 331, 3334, 33334, \ldots$. Show that with the absolute value $|\cdot|_5$ on $\mathbb{Q}$ this sequence converges to $2/3$.

The next theorem shows that we have found all the absolute values on $\mathbb{Q}$. For a proof see, for example, [2] §2.2.

Theorem 1.27 (Ostrowski's Theorem) *Any nontrivial absolute value on $\mathbb{Q}$ is equivalent to $|\cdot|_\infty$ or some $|\cdot|_p$.*

Complete rings

Suppose $(A, |\cdot|)$ is a domain with absolute value $|\cdot|$. We say that a sequence $(a_n : n = 1, 2, \dots)$ in A is *Cauchy* if for all $\epsilon > 0$, there is an n such that if $i, j > n$ then $|a_i - a_j| < \epsilon$.

We say that A is *complete* if every Cauchy sequence converges. Clearly $\mathbb{R}$ and $\mathbb{C}$ with the usual absolute values are complete.

Lemma 1.28 *Consider the ring of power series $K(\!(X)\!)$ with the valuation $v(f) = m$ where $f = \sum_{n \geq m} a_n X^n$ where $a_m \neq 0$ and the absolute value $|f| = \alpha^{v(f)}$, where $0 < \alpha < 1$. Then K is complete.*

Proof Suppose $f_0, f_1, \dots$ is a Cauchy sequence. Suppose $f_i = \sum_{n \in \mathbb{N}} a_{i,n} X^n$ (where $a_{i,n} = 0$ for $m > i$ Let $\epsilon \leq \alpha^{1/n}$. There is m_n such that if $i, j > m_n$ then $|f_i - f_j| < \epsilon$. But then $a_{i,k} = a_{j,k}$ for all $k < n$. Let b_k be this common value. Let $g = \sum_{k \in \mathbb{N}} b_k X^k$. Then $|f_i - g| < 1/n$ for all $i \geq n$. It follows that (f_i) converges to g. □

Exercise 1.29 If $(A, |\cdot|)$ is a complete domain, then the extension to the fraction field is also complete.

in nonarchimedean complete domains we have a simple test for convergence of series.

Exercise 1.30 If $(A, |\cdot|)$ is a nonarchimedean complete domain, then the series $\sum_{n=0}^{\infty} a_n$ converges if and only if $\lim a_n = 0$.

If a is a domain with absolute value $|\cdot|$. We can follow the usual constructions from analysis to build a *completion* $\widehat{A}$ of A. The elements of $\widehat{A}$ are equivalence classes of Cauchy sequences from K where (a_n) and (b_n) are equivalent if and only if for any $\epsilon > 0$ there is an n such that $|a_i - b_j| < \epsilon$ for $i, j > n$. We can define an absolute value on $\widehat{A}$ such that the equivalence class of (a_n) has absolute value $\lim_{n \to \infty} |a_n|$. We identify A with the equivalence classes of constant sequences.

Exercise 1.31 Complete the construction of $\widehat{R}$. Prove that it is a complete ring and that if $L \supset K$ is any complete field with an absolute value extending the absolute value of K, then there is an absolute value preserving embedding of $\widehat{K}$ into L fixing K.

Lemma 1.32 *Suppose A is a complete domain with nonarchimedean absolute value $|\cdot|$. If (a_n) is a Cauchy sequence that does not converge to 0, then $|a_i| = |a_j|$ for all sufficiently large i and j. Thus when we pass to the completion $\widehat{A}$ we add no new absolute values.*

Proof We can find an N and ϵ such that $|a_n| > \epsilon$ and $|a_n - a_m| < \epsilon$ for all $n, m > N$. But then, since we have a nonarchimedean absolute value $|a_n| = |a_m|$ for all $n > N$. □

Definition 1.33 The ring of *p-adic integers* $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with the p-adic absolute value $|\cdot|_p$. Its fraction field is $\mathbb{Q}_p$ the field of *p-adic numbers.*

Lemma 1.34 *i) Suppose* (a_n) *is a sequence of integers. The series* $\sum_{i=0}^{\infty} a_i p^i$ *converges in* $\mathbb{Z}_p$.

ii) The map $(a_n) \mapsto \mathbb{Z}_p$ *is a bijection between* $\{0, \ldots, p-1\}^{\mathbb{N}}$ *and* $\mathbb{Z}_p$.

Proof i) If $m < n$, then

$$\left| \sum_{i=0}^{n} a_i p^i - \sum_{i=0}^{m} a_i p^i \right|_p < \frac{1}{p^m}.$$

Thus the sequence of partial sums is Cauchy and hence convergent.

ii) Suppose $(a_n) \in \mathbb{Z}^{\mathbb{N}}$ and $p \not| a_0$. Because $p | \sum_{n>0} a_n p^n$

$$\left| \sum_{n=0}^{\infty} a_n p^n \right|_p = |a_0|_p \neq 0.$$

Let (a_n) and $(b_n) \in \{0, \ldots, p-1\}^{\mathbb{N}}$ be distinct. Suppose m is least such that $a_m \neq b_m$. Then

$$\sum a_n p^n = \sum_{n<m} a_n p^n + a_m p^m + \sum_{n>m} a_n p^n$$

while

$$\sum b_n p^n = \sum_{n<m} a_n p^n + b_m p^m + \sum_{n>m} b_n p^n$$

It follows that $|\sum a_n p^n - \sum b_n p^n|_p = \frac{1}{p^m}$. Thus the map is injective. Given $x \in \mathbb{Z}_p$ choose $(a_n) \in \{0, \ldots, p-1\}^{\mathbb{N}}$ such that $\sum_{n<m} a_n p^n = x (\text{mod } p^m)$ for all m. Then $\sum_{n=0}^{\infty} a_n p^n = x$. Thus the map is surjective. □

It follows that every element $x \in \mathbb{Q}_p^{\times}$ can be represented as a series $x = \sum_{n=m} a_n p^n$ where $m \in \mathbb{Z}$, $a_m \neq 0$. and each $a_n \in 0, \ldots, p-1$ and $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. We have the p-adic valuation $v_p(x) = m$. The value group is $\mathbb{Z}$ and the residue field is $\mathbb{F}_p$.

Exercise 1.35 Suppose U is an open cover of $\mathbb{Z}_p$ by open balls $\{x : |x-a|_p < \epsilon\}$. Define $T \subset \{0, \ldots, p-1\}^{<\mathbb{N}}$ such that $\emptyset \in T$ and $(a_0, \ldots, a_m) \in T$ if and only if there is no ball of radius at least $1/p^{m+1}$ in U containing $a_0 + a_1 p + \cdots + a_n p^m$.

a) Show that T is a tree (i.e. if $\sigma \subseteq \tau$ and $\tau \in T$, then $\sigma \in T$).

b) Show that T has no infinite branches.

c) Conclude that $\mathbb{Z}_p$ is compact.

Exercise 1.36 For $i > j$ let $\phi_{i,j} : \mathbb{Z}/(p^i) \to \mathbb{Z}/(p^j)$ be the map $\phi_{i,j}(x) = x \text{mod } (p^j)$. Then $\mathbb{Z}_p$ is the inverse limit of the this system of ring homomorphisms.

Why valued fields?

Most of the most important example of valued fields arising in number theory, complex analysis and algebraic geometry have value groups that are discrete or, at the very least, contained in $\mathbb{R}$. Why are we focusing on valuations rather than absolute values? Here are a couple of answers.

1. Valued fields with value groups not contained in $\mathbb{R}$ arise naturally when looking at standard valuations on nonstandard real closed fields.

2. Once we start doing model theory we will frequently need to pass to elementary extensions. Even though $\mathbb{Q}_p$ has value group $\mathbb{Z}$ when we pass to an elementary extension the value need not be a subgroup of $\mathbb{R}$.

3. One of our big goals is the theorem of Ax–Kochen and Ershov theorem that for any sentence ϕ in the language of valued fields, ϕ is true in $\mathbb{F}_p(\!(T)\!)$ for all but finitely many p if and only if ϕ is true in $\mathbb{Q}_p$ for all but finitely many p. This is proved by taking a nonprinciple ultrafilter U on the primes and showing that
$$\prod \mathbb{F}_p(\!(T)\!)/U \equiv \prod \mathbb{Z}_p/U.$$
These fields will have very large value groups.

2 Hensel's Lemma

2.1 Hensel's Lemma, Equivalents and Applications

Definition 2.1 We say that a local domain A with maximal ideal $\mathfrak{m}$ is *henselian* if whenever $f(x) \in A[X]$ and there is $a \in A$ such that $f(a) \in \mathfrak{m}$ and $f'(a) \notin \mathfrak{m}$, then there is $\alpha \in A$ such that $f(\alpha) = 0$ and $\alpha - a \in \mathfrak{m}$.

Theorem 2.2 (Hensel's Lemma) *Suppose K is a complete field with nonarchimedian absolute value $|\cdot|$ and valuation ring $\mathcal{O} = \{x \in K : |x| \leq 1\}$. Then $\mathcal{O}$ is henselian.*

Proof Suppose $a \in \mathcal{O}$, $|f(a)| = \epsilon < 1$ and $|f'(a)| = 1$. We think of a as our first approximation to a zero of f and use Newton's method to find a better approximation. Let $\delta = \frac{-f(a)}{f'(a)}$. Note that $|\delta| = |f(a)/f'(a)| = \epsilon$. Consider the Taylor expansion

$$f(a + x) = f(a) + f'(a)x + \text{ terms of degree at least 2 in } x.$$

Thus

$$f(a + \delta) = f(a) + f'(a)\frac{-f(a)}{f'(a)} + \text{ terms of degree at least 2 in } \delta.$$

Thus $|f(a + \delta)| \leq \epsilon^2$. Similarly

$$f'(a + \delta) = f'(a) + \text{ terms of degree at least 2 in } \delta$$

and $|f'(a + \delta)| = |f'(a)| = 1$.

Thus starting with an approximation where $|f(a)| = \epsilon < 1$ and $|f'(a)| = 1$. We get a better approximation b where $|f(b)| \leq \epsilon^2$ and $|f'(b)| = 1$. We now iterate this procedure to build $a = a_0, a_1, a_2, \ldots$ where

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}.$$

It follows, by induction, that for all n:
i) $|a_{n+1} - a_n| \leq \epsilon^{2^{n+1}}$;
ii) $|f(a_n)| \leq \epsilon^{2^n}$;
iii) $|f'(a_n)| = 1$.
Thus (a_n) is a Cauchy sequence and converges to α, $|\alpha - a| \leq \epsilon$, and $f(\alpha) = \lim_{n\to\infty} f(a_n) = 0$. □

Thus the ring of p-adic integers and rings of formal power series $F[[T]]$ are henselian.

Exercise 2.3 Let $\mathcal{O}$ be the valuation ring of the field of Puiseux series $F\langle T\rangle$.

a) Show that $\mathcal{O}$ is not complete. [Hint: Consider the sequence $T^{\frac{1}{2}}, T^{\frac{1}{2}} + T^{\frac{2}{3}}, T^{\frac{1}{2}} + T^{\frac{2}{3}} + T^{\frac{3}{4}} + \ldots.$]

b) Show that $\mathcal{O}$ is henselian.

Exercise 2.4 Suppose K is henselain and $F \subseteq K$ is algebraically closed in K, then F is henselian.

The next lemma shows that in a Hensel's Lemma problem, there is at most one solution.

Lemma 2.5 *Let $\mathcal{O}$ be a local domain with maximal ideal $\mathfrak{m}$. Suppose $f(X) \in \mathcal{O}[X]$, $a \in \mathcal{O}$, $f(a) \in \mathfrak{m}$ and $f'(a) \notin \mathfrak{m}$. There is at most one $\alpha \in \mathcal{O}$ such that $f(\alpha) = 0$ and $\alpha - a \in \mathfrak{m}$*

Proof Considering the Taylor expansions

$$f'(\alpha) = f'(a) + (a - \alpha)b$$

for some $b \in \mathcal{O}$. Thus $f'(\alpha) \notin \mathfrak{m}$.

If $\epsilon \in \mathfrak{m}$, then

$$f(\alpha + \epsilon) = f(\alpha) + f'(\alpha)\epsilon + b\epsilon^2 = f'(\alpha) + b\epsilon^2$$

for some $b \in \mathcal{O}$. Since $f'(\alpha) \notin \mathfrak{m}$, $f(\alpha + \epsilon) \in \mathfrak{m}$, but $f(\alpha + \epsilon) \notin \mathfrak{m}^2$ unless $\epsilon = 0$. Thus if $\beta - a \in \mathfrak{m}$ and $\alpha \neq \beta$, $f(\beta) \neq 0$. □

There are many natural and useful equivalents of henselianity.

Lemma 2.6 *Let A be a local domain with maximal ideal $\mathfrak{m}$. The following are equivalent.*

i) A is henselian.

ii) If $f(X) = 1 + X + ma_2X^2 + \ldots_m a_dX^d$ where $m \in \mathfrak{m}$ and $a_2, \ldots, a_d \in A$, then f has a unique zero α in A, with $\alpha = -1 \bmod \mathfrak{m}$.

iii) Suppose $f(X) \in A[X]$, $a \in A$, $m \in \mathcal{M}$ and $f(a) = mf'(a)^2$, there is a unique $\alpha \in A$ such that $f(\alpha) = 0$ and $a - \alpha \in (cf'(a))$.

Proof i) ⇒ ii) is clear since $f(-1) \in \mathfrak{m}$ and $f'(-1) \notin \mathfrak{m}$.

ii) ⇒ iii) Then

$$f(a + X) = f(a) + f'(a)X + \sum_{i=2}^{d} b_i X^i$$

for some $b_i \in A$. But then

$$\begin{aligned} f(a + mf'(a)Y) &= mf'(a)^2 + mf'(a)^2Y + \sum_{i=2}^{d} b_i(mf'(a)Y)^i \\ &= mf'(a)^2 \left(1 + Y + \sum_{i=2}^{d} mc_iY^i\right) \end{aligned}$$

for some $c_2, \ldots, c_d \in A$. By ii) we can find t $u \in A$ such that $1+u+\sum mc_iu^i = 0$. Let $\alpha = a + mf'(a)u$. Then $f(\alpha) = 0$ and $a - \alpha \in \mathfrak{m}$, as desired.

iii) $\Rightarrow$ i) is immediate. $\square$

In a valuation ring $\mathcal{O}$, condition iii) can be restated $v(f(a)) > 2v(f'(a))$.

Exercise 2.7 Suppose R is a real closed field and $\mathcal{O} \subset R$ is a proper convex subring. Show that $\mathcal{O}$ is henselian. [Hint: Consider $f(X)$ as in ii) and show that f must change sign on $\mathcal{O}$.]

Exercise 2.8 Suppose $(K, <)$ is an ordered field, $\mathcal{O}$ is a proper convex subring, and $(K, \mathcal{O})$ is henselian with divisible value group and real closed residue field. Prove that every positive element of K is a square. [We will see in Corollary 5.14 that, in fact, K is real closed.]

The following equivalent is also useful.

Corollary 2.9 *Let A and $\mathfrak{m}$ be as above, then A is henselian if and only for every polynomial $f(Y) = 1 + Y + \sum_{i=2}^{n} a_i Y^i i$ where $a_2, \ldots, a_n \in \mathfrak{m}$, there is $\alpha = -1 (\mathrm{mod}\ n)$ such that $f(\alpha) = 0$.*

Proof ($\Rightarrow$) Clear.

($\Leftarrow$) It suffices to show that for every polynomial of the form $X^n + X^{n-1} + \sum_{i=0}^{n-2} a_i X^i$ where $a_0, \ldots, a_{n-2} \in \mathfrak{m}$ has a zero congruent to -1, or equivalently that every polynomial of the form

$$1 + (1/X) + \sum_{i=0}^{n-2} a_i (1/X)^{n+i}$$

has a zero congruent to -1. Letting $Y = 1/X$ we find the desired solution. $\square$

Corollary 2.10 *If (K, v) is an algebraically closed valued field, then K is henselian.*

Proof Consider the polynomial $f(X) = X^n + X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_0$ where $a_0, \ldots, a_{n-2} \in \mathfrak{m}$. It suffices to show that f has a zero congruent to $-1 (\mathrm{mod}\ \mathfrak{m})$. Any zero that is a unit must be congruent to $-1 (\mathrm{mod}\ \mathfrak{m})$, so it suffices to show that f has a zero that is a unit. Since K is algebraically closed, we can factor $f(X) = (X - b_1) \cdots (X - b_n)$. Each b_i must have nonnegative value, as if $v(b_i) < 0$, then $v(b_i^n) < v(a_i b^i)$ for all $i < n$ and $v(f(b_i)) = nv(b_i)$, so $f(b_i) \neq 0$. But $-\sum b_i = 1$ so some b_i must have value 0. $\square$

p-adic squares and sums of squares

A typical application of Hensel's lemma is understanding the squares in $\mathbb{Q}_p^\times$. First suppose $p \neq 2$. Let $a \in \mathbb{Q}_p$. Let $a = p^m b$ where b is a unit in $\mathbb{Z}_p$. If $a = c^2$, then $v_p(a) = 2v_p(c)$. Thus m is even. We still need to understand when a unit $b \in \mathbb{Z}_p$ is a square. Let $f(X) = X^2 - b$. Let $\overline{b}$ be the residue of f. Then if b is a square $\overline{b}$ must be a square in the residue field $\mathbb{F}_p$. If $x \in \mathbb{Z}_p$ such that $\overline{x}^2 = \overline{b}$. Then $v_p(x) = v_p(c) = 0$ and $v_p(f'(x)) = v_p(2x) = 0$. Thus, by Hensel's Lemma, there is $y \in \mathbb{Z}_p$, such that $y^2 = b$ and $v_p(x - y) > 0$. Thus $a \in \mathbb{Q}_p^2$ is a square if

and only if $a = p^{2n}b$ where b is a unit and $\overline{b}$ is a square in $\mathbb{F}_p$. Recall that for $p \neq 2$ the squares are an index 2 subgroup of $\mathbb{F}_p^\times$. It follows that the squares are an index 4 subgroup of $\mathbb{Q}_p^\times$.

We need to be a bit more careful in $\mathbb{Z}_2$. If $f(X) = X^2 - c$ and $\overline{x}^2 = \overline{c}$, then $v_2(x) = v_2(2x) = 1$ so we can not apply Hensel's Lemma directly. We can use the characterization iii) of Lemma 2.6 but we need to look at squares mod 8. Consider $f(X) = X^2 - b$. Suppose b is a unit in $\mathbb{Z}_2$ and b is a square. Then $\overline{b}$ is a square mod 8. We argue that the converse is true. Consider $f(X) = X^2 - b$. Suppose $x \in \mathbb{Z}_p$ and $x^2 - b = 0 (\text{mod } 8)$. Then $v_2(x) = 0$ and $v_2(2x) = 1$. Thus $v_2(f(x)) \geq 3$ while $v_2(f'(x)) = 1$. Thus b is a square in $\mathbb{Z}_2$. The nonzero squares mod 8 are 1 and 4. Thus $a \in \mathbb{Z}_2^\times$ is a square if and only if $a = 2^{2n}b$ where $b = 1$ or $4 (\text{mod } 8)$. Thus the squares are an index 8 subgroup of $\mathbb{Q}_2^\times$.

Exercise 2.11 a) Show that if $p \neq 2$, then $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \exists y \ y^2 = px^2 + 1\}$
b) Show that $\mathbb{Z}_2 = \{x \in \mathbb{Q}_2 : \exists y \ y^2 = 8x^2 + 1\}$.

Exercise 2.11 shows that the p-adic integers $\mathbb{Z}_p$ are definable in $\mathbb{Q}_p$ in the pure field language. Thus, from the point of view of definability, it doesn't matter if we view $\mathbb{Q}_p$ as a field or as a valued field.

Exercise 2.12 a) Suppose $p \not| \, n$. Show x is an n^{th}-power in $\mathbb{Q}_p$ if and only if $n | v_p(n)$ and $\text{res}(n)$ is an n^{th}-power in $\mathbb{F}_p$.
b) Suppose $p | n$. Show that x is an n^{th}-power in $\mathbb{Q}_p$ if and only if $x = p^{nm}y$ where y is a unit and y is an n^{th}-power mod $p^{2v(n)+1}$.
c) Conclude that the nonzero n^{th}-powers are a finite index subgroup of $\mathbb{Q}_p^\times$.

Exercise 2.13 a) Let K be a field of characteristic other than 2. Show that $K[[T]] = \{f \in K(\!(T)\!) : \exists g \ g^2 = Tf^2 + 1\}$.
b) Suppose K has characteristic 2 and give a definition of $K[[T]]$ in $K(\!(T)\!)$.

Lemma 2.14 *If p is an odd prime and $u \in \mathbb{Z}_p$ is a unit, then u is a sum of two squares in $\mathbb{Z}_p$.*

Proof In $\mathbb{F}_p$ there are $(p+1)/2$ squares. Since the set $\mathbb{F}_p^2$ and $\overline{u} - \mathbb{F}_p^2$ each of size $(p+1)/2$, they must have non-empty intersection. Let $x, y \in \mathbb{Z}_p$ such that $\overline{x}^2 + \overline{y}^2 = \overline{u}$. At least one of x and y is a unit. Say x is a unit. Let $f(X) = X^2 - (y^2 - u)$. By Hensel's Lemma we can find a zero z and $z^2 + y^2 = u$. □

Lemma 2.15 *Suppose $p = 1 (\text{mod } 4)$. Every element of $\mathbb{Z}_p$ is a sum of two squares.*

Proof We know that -1 is a square in $\mathbb{F}_p$. By Hensel's Lemma there is $\xi \in \mathbb{Z}_p$ with $\xi^2 = -1$.

Let $a \in \mathbb{Z}_p$. Note that

$$(a+1)^2 - (a-1)^2 = 4a.$$

Thus

$$a = \left(\frac{a+1}{2}\right)^2 + \left(\frac{\xi(a-1)}{2}\right)^2.$$

Note that since $p \neq 2$, $1/2 \in \mathbb{Z}_p$. Thus we have written a as a sum of squares in $\mathbb{Z}_p$. □

Corollary 2.16 *If $p = 1(\text{mod } 4)$ then every element of $\mathbb{Q}_p$ is a sum of two squares.*

Proof We can write $a = p^{2m}b$ for some $b \in \mathbb{Z}_p$. If $b = c^2 + d^2$, then $a = (pc)^2 + (pd)^2$. □

Lemma 2.17 *If $p = 3(\text{mod } 4)$, then $a \in \mathbb{Q}_p$ is a sum of two squares if and only if $v_p(a)$ is even.*

Proof If $a = p^{2m}u$ where u is a unit. Then u is a sum of two squares so a is as well.

Suppose $v_p(a)$ is odd and $a = x^2 + y^2$. Then a is not a square, thus both x and y are nonzero. Also $v_p(x) = v_p(y)$ as otherwise $v_p(a)$ is even. Let $x = p^m u$ and $y = p^m v$ where u, v are units in $\mathbb{Z}_p$. Then $a = p^{2m}(u^2 + v^2)$. But $v_p(a)$ is odd, thus $v_p(u^2 + v^2) > 0$ and $(u/v)^2 = -1(\text{mod } p)$, a contradiction since $p = 3(\text{mod } 4)$. □

Lemma 2.18 *In $\mathbb{Q}_2$ if $a = 2^m u$ where u is a unit, then a is a sum of two squares if an only if $u = 1(\text{mod } 4)$.*

Proof First suppose $u = 1(\text{mod } 4)$. We first show that u is a sum of squares. Then $u = 1$ or 5 (mod 8). If $u = 1(\text{mod } 8)$, then u is already a square in $\mathbb{Z}_2$. If $u = 5(\text{mod } 8)$, then $u/5 = x^2$ for some $x \in \mathbb{Z}_2$ and $u = x^2 + (2x)^2$.

Recall that a product of two sums of squares is a sum of squares as

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

Since $2 = 1 + 1$ and $1/2 = (1/4) + (1/4)$ are sum of two squares $2^m u$ is a sum of two squares.

Next suppose $u = 3(\text{mod } 4)$. If a is a sum of two squares, then, as above, u is also a sum of two squares. Say $u = x^2 + y^2$. This is impossible if $x, y \in \mathbb{Z}_2$ since the only sums of two squares mod 4 are 0, 1 and 2. Without loss of generality suppose $v_p(x) < 0$. But then we must have $v_p(y) = v_p(x) = -n$ where $n > 0$. Then $x = z/2^n$ and $y = w/2^n$ where z and w are units in $\mathbb{Z}_p$ and $4^n u = (z^2 + w^2)$. Thus $z^2 + w^2 = 0(\text{mod } 4)$. But z and w are units and, thus, $z^2, w^2 = 1(\text{mod } 4)$ and $z^2 + w^2 = 2(\text{mod } 4)$, a contradiction. □

We can use these results, particularly the result about primes congruent to 3(mod 4) to rephrase a classic result of Euler's. Recall that an integer $m > 0$ is a sum of two squares if and only if $v_p(m)$ is even for any prime $p = 3(\text{mod } 4)$ that divides m. See, for example, [27] §27.

Corollary 2.19 *An integer m is a sum of two squares if and only if it is a sum of squares in $\mathbb{R}$ and in each $\mathbb{Z}_p$.*

Proof ($\Rightarrow$) is clear.

($\Leftarrow$) If m is a square in $\mathbb{R}$, then $m \geq 0$. By Lemma 2.17, if $p = 3 (\text{mod } 4)$, then $v_p(m)$ is even. Thus m is a square in $\mathbb{Z}$. $\square$

This corollary can be though of as a baby version of a local-global principle. Hensel's Lemma gives us a powerful tool for solving equations in the p-adics. We have no comparable tool in the rational numbers. Of course if a system of polynomials over $\mathbb{Q}$ has no solution in $\mathbb{Q}_p$ or $\mathbb{R}$, then it has no solution in $\mathbb{Q}$. Sometimes, we can prove existence results in $\mathbb{Q}$ by proving them in all completions. These are called *local-global* results as they reduce question in the global field $\mathbb{Q}$ to the local fields $\mathbb{Q}_p$ and $\mathbb{R}$. These principles are very useful it is often much easier to decide if there is a solution in the local fields. One of the most general is the Hasse Principle. See for example [25] §IV.3.

Theorem 2.20 (Hasse Principle) *Let $p(X_1, \ldots, X_n) = \sum_{i,j \leq n} a_{i,j} X_i X_j \in \mathbb{Q}[X_1, \ldots, X_n]$. Then $p = 0$ has a nontrivial solution in $\mathbb{Q}$ if and only if it has nontrivial solutions in $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p.*

Exercise 2.21 Suppose $p > 2$ is prime. Let

$$F(X_1, \ldots, X_m, Y_1, \ldots, Y_m) = \sum_{i=1}^{n} a_i X_i^2 + \sum_{j=1}^{m} p b_j X_j^2$$

where $a_i, b_j \in \mathbb{Z}$ are not divisible by p.

a) Suppose F has a nontrivial zero in $\mathbb{Q}_p$. Show that either $\sum \overline{a}_i X_i^2$ or $\sum \overline{b}_i Y_i^2$ has a nontrivial solution in $\mathbb{F}_p$. [Hint: First show that there is a solution $(x_1, \ldots, x_m, y_1, \ldots, y_n) \in \mathbb{Z}_p$ where some x_i or y_j is a unit. Show that if some x_i is a unit, then $(\overline{x}_1, \ldots, \overline{x}_m)$ is a zero of $\sum \overline{a}_i X_i^2$ and otherwise $(\overline{y}_1, \ldots, \overline{y}_n)$ is a zero of $\sum \overline{b}_j Y_j^2$.

b) Use Hensel's Lemma to prove that if either $\sum \overline{a}_i X_i^2$ or $\sum b_j Y_j^2$ has a nontrivial zero in $\mathbb{F}_p$, then F as a nontrivial zero in $\mathbb{Q}_p$.

c) Show that $3X^2 + 2Y^2 - Z^2 = 0$ has no nontrivial solution in $\mathbb{Q}_3$ and hence no nontrival solution in $\mathbb{Q}$.

p-adic roots of unity

In the next exercises and lemma we will look for roots of unity in $\mathbb{Q}_p$.

Exercise 2.22 Let p be an odd prime.

a) Show that there are exactly $p - 1$ distinct $(p-1)^{\text{th}}$ roots of unity in $\mathbb{Z}_p$ and no two distinct roots are equivalent mod p

b) Suppose that ξ_1 and ξ_2 are roots of unity of order m_1 and m_2 where $p \not| \, m_1, m_2$. Show that if $\xi_1 = \xi_2 (\text{mod } p)$, then $\xi_1 = \mathbf{x}_2$. [Hint: Consider $f(X) = X^{m_1 m_2} - 1$ and apply Lemma 2.5.]

Lemma 2.23 *Let p be an odd prime.*

i) The only p^{th}-root of unity in $\mathbb{Q}^p$ is 1.

ii) The only p^{th}-power root of unity in $\mathbb{Q}_p$ is 1.

Proof i) Clearly any p^{th}-root of unity ξ is in $\mathbb{Z}_p$. Suppose $\xi^p = 1$. In $\mathbb{F}_p$, $\overline{\xi}^p = \overline{\xi}$, thus $\xi = 1 (\text{mod } p)$. Let $f(X) = X^p - 1$. Then $v_p(f'(\xi)) = 1$ and, by the uniqueness part of Lemma 2.5 iii), ξ is the unique zero of f in $\{x \in \mathbb{Z}_p : v_p(x - \xi) \geq 2\} = \xi + p^2\mathbb{Z}_p$. We will show that $1 \in \xi + p^2\mathbb{Z}_p$ and conclude that $\xi = 1$.

Suppose $\xi = 1 + px$ where $x \in \mathbb{Z}_p$. Then

$$1 = \xi^p = (1 + px)^p = 1 + p(px) + \sum_{i=2}^{p} \binom{p}{i} (px)^i$$

Each term $\binom{p}{i}(px)^i$ is divisible by p^3 thus $1 = 1 + p^2x (\text{mod } p^3)$. Hence $p^2x = 0 (\text{mod } p^3)$ and $p|x$. But then $\xi = 1 (\text{mod } p^2)$ and, since ξ is the p^{th}-root of unity in $\xi + p^2\mathbb{Z}_p$, $\xi = 1$.

ii) We prove by induction that if $\xi^{p^m} = 1$, then $X = 1$. If $\xi^{p^{m+1}} = 1$, then $(\xi^{p^m})^p = 1$ and, by i), $\xi^{p^m} = 1$. By induction $\xi = 1$. □

Corollary 2.24 *If p is an odd prime, then the only roots of unity in $\mathbb{Q}_p$ are the $p - 1$ roots of $X^{p-1} - 1$.*

Proof Let $n = p^k m$ where $p \not| m$. If $\xi^n = 1$, then $\xi = xy$ where $x^{p^k} = 1$ and $y^m = 1$. By the previous exercise and lemma, $x = 1$ and $y^{p-1} = 1$. □

Exercise 2.25 Prove that the only roots of unity in $\mathbb{Q}_2$ are ± 1.

The Implicit Function Theorem

We give a very different application of Hensel's Lemma in power series rings to a prove an algebraic version of the Implicit Function Theorem. Let F be a field and let $p(X, Y) \in F[X, Y]$ such that $f(0, 0) = 0$ and $\frac{\partial f}{\partial Y}(0, 0) \neq 0$. Consider the polynomial $g(Y) \in F[[T]][Y]$, where $g(Y) = f(T, Y)$. Then $g(0) = f(T, 0) = f(0, 0) = 0 \text{ (mod } (T))$. But

$$g'(Y) = \frac{\partial f}{\partial Y}(0, 0) \neq 0 \text{ (mod } T).$$

Thus by Hensel's Lemma, we can find $\phi(T) \in F[[T]]$ such that $f(T, \phi(T)) = 0$. Thus we have found a power series point on the curve. We think of the power series as parameterizing a branch on the curve near (0,0).

If $\frac{\partial f}{\partial Y}(0, 0) = 0$, but $\frac{\partial f}{\partial X}(0, 0) \neq 0$, we could find a $\psi(T)$ such that $f(\psi(T), T) = 0$. By changing variables we could, more generally shows that if $(a, b) \in F^2$ is any smooth point of the curve we can find a power series branch. This type of result can be extended to singular points but requires more specialize properties of power series and Puiseux series rings such as Weierstrass factorization (see, for example, [24]).

2.2 Lifting the residue field

In some of our later work it will be useful to view the residue field $\boldsymbol{k}$ as a subfield of the valued field K. Of course this is sometimes impossible. The p-adics have characteristic 0, while the residue field has characteristic p. However, when K is henselian and $\boldsymbol{k}$ is characteristic 0, this will always be possible.

Theorem 2.26 *Suppose K is a henselian valued field and the residue field $\boldsymbol{k}$ has characteristic 0. Then there is a field embedding $j : \boldsymbol{k} \to K$ such that* $\mathrm{res}(j(x)) = x$ *for all $x \in \boldsymbol{k}$.*

We call such a j a *section* of the residue map.

Proof We will inductively build $j : \boldsymbol{k} \to K$. At any stage of our construction we will have $\boldsymbol{k}_0 \subset \boldsymbol{k}$ a subfield and $j : \boldsymbol{k}_0 \to K$ a field embedding with $\mathrm{res}(j(x)) = x$ for all $x \in \boldsymbol{k}_0$. To start, since $\boldsymbol{k}$ has characteristic 0, we can take $\boldsymbol{k}_0 = \mathbb{Q}$ and let $j : \mathbb{Q} \to \mathbb{Q}$ be the identity map. The theorem will follow by induction using the following two claims.

claim 1 Suppose we have such a $j : \boldsymbol{k}_0 \to K$ where $\boldsymbol{k}_0$ is a subfield of $\boldsymbol{k}$ and $x \in \boldsymbol{k} \setminus \boldsymbol{k}_0$ is transcendental over $\boldsymbol{k}_0$. Then we can extend j to a suitable $\widehat{j} : \boldsymbol{k}_0(x) \to \boldsymbol{k}$.

Choose $y \in K$ such that $\mathrm{res}(y) = x$. We claim that y is transcendental over $K_0 = j(K)$. Suppose not. Then there is $p(X) \in K_0[X]$ such that $p(y) = 0$. But then $\overline{p}(x) = 0$. Since $\mathrm{res} \circ j$ is the identity on $\boldsymbol{k}_0$, $\overline{p}(X)$ is not identically 0, thus x is algebraic over $\boldsymbol{k}_0$ a contradiction. We extend j to $\widehat{j}$ by sending y to x. Since the residue map is a ring homomorphism, $\mathrm{res} \circ \widehat{j}$ is the identity.

claim 2 Suppose we have such a $j : \boldsymbol{k}_0 \to K$ where $\boldsymbol{k}_0$ is a subfield of $\boldsymbol{k}$ and $x \in \boldsymbol{k} \setminus \boldsymbol{k}_0$ is algebraic over $\boldsymbol{k}_0$. Then we can extend j to a suitable $\widehat{j} : \boldsymbol{k}_0(x) \to K$.

There is $y_0 \in \boldsymbol{k}$ with $\mathrm{res}(y_0) = x$. Suppose $p(X)$ is the minimal polynomial of x over $\boldsymbol{k}_0$. Then $p(x) = 0$ and $p'(x) \neq 0$. Let $q(X)$ be the image of the $p(X)$ under j. Since $\mathrm{res} \circ j = id$, $\overline{q} = p$. But then $\overline{q}(x) = 0$ and $\overline{q}'(x) \neq 0$, and, by henselianity, there is $y \in K$ such that $q(y) = 0$ and $\mathrm{res}(y) = \mathrm{res}(y_0) = x$. We extend j to $\widehat{j}$ by sending y to x. Since the residue map is a ring homomorphism, $\mathrm{res} \circ \widehat{j}$ is the identity. □

We can use this theorem to prove an easy result very much in the spirit of the Ax–Kochen and Ershov results we will see in §5.

Theorem 2.27 (Greenleaf) *Let $f_1, \ldots, f_m \in \mathbb{Z}[X_1, \ldots, X_n]$ then for all but finitely many primes p, every solution to $f_1 = \cdots = f_m = 0$ in $\mathbb{F}_p^n$, lifts to a solution in $\mathbb{Z}_p^n$.*

Proof We consider vauled fields as fields with a predicate for the valuation ring. Consider the sentence Θ in the language of valued fields

$$\forall \mathbf{x}\Big(f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}) \in \mathfrak{m} \to \exists \mathbf{y}\ f_1(\mathbf{y}) = \cdots = f_m(\mathbf{y}) = 0 \wedge y_i - x_i \in \mathfrak{m} \quad \text{for } i = 1, \ldots, n \Big).$$

Θ asserts that any zero of $f_1 = \cdots = f_m$ in the residue field lifts to the field. By Theorem 2.26, if K is a henselian valued field with characteristic zero residue field we can embed k into K, thus Θ holds. In particular, $\prod \mathbb{Z}_p/\mathcal{U} \models \Theta$ for any nonprincple ultrafilter $\mathcal{U}$. Thus, by the Fundamental Theorem of Ultraproducts, $\mathbb{Z}_p \models \Theta$ for all but finitely many primes. □

2.3 Sections of the value group

Once could ask similar questions about the value group. *This doesn't have anything to do with henselianity and could be moved later.*

If (K, v) is a valued field with value group Γ we say that $s : \Gamma \to K$ is a *section* of the valuation if $v(s(\gamma)) = \gamma$ and $s(\gamma + \gamma') = s(\gamma)s(\gamma')$ for all $\gamma, \gamma' \in \Gamma$.

For example, in the p-adics $n \mapsto p^n$ is a section. The next two lemmas give useful examples where sections exist.

Lemma 2.28 *Let (K, v) be a real closed or algebraically closed field. Then there is a section $s : \Gamma \to K$.*

Proof In either case Γ is divisible. Let $(\gamma_i : i \in I)$ be a basis for Γ as a $\mathbb{Q}$-vector space.

If K is real closed then for each i we pick $x_i \in K$ with $x_i > 0$ and $v(x_i) = \gamma_i$. Let $s(m_1\gamma_{i_1} + \ldots m_k\gamma_{i_k}) = x_i^{m_1} \cdots x_k^{m_k}$. Then s is the desired section.

If K is algebraically closed then for each i we need to choose a coherent sequence of n-th roots $x_{i,n}$ for $n = 1, 2, \ldots$ such that $x_{i,nm}^m = x_{i,n}$ for all n and m and $v(x_{i,1}) = \gamma_i$. We can then let $s(m_1\gamma_{i_1} + \ldots m_k\gamma_{i_k}) = x_{i_1,n_i}^{l_i} \cdots x_{i_k,n_k}^{l_k}$ where $m_i = l_i/n_i$ and l_i and n_i are relatively prime. Then s is the desired section. □

Exercise 2.29 Suppose K is a henselian valued field with divisible value group Γ and the residue field $\boldsymbol{k}$ is of characteristic zero with $\boldsymbol{k}^*$ divisible. Prove that there is a section $s : \Gamma \to K^\times$ of the valuation.

We will show that sufficiently rich fields have sections.

Theorem 2.30 *If (K, v) is an $\aleph_1$-saturated valued field with value group Γ, then there is a section $s : \Gamma \to K$.*

Corollary 2.31 *Every valued field has an elementary extension where there is a section of the value group.*

The Theorem follows from the next lemma. Recall that if G is an abelian group a subgroup $H \subseteq G$ is *pure* if G/H is torsion free, i.e., if $nx \in H$, then $x \in H$ for all $n > 0$. If $\Gamma_0 \subset \Gamma$ we say that $s : \Gamma_0 \to K^\times$ is a *partial section* if it is a homomorphism with $v \circ s = id$.

Lemma 2.32 *Suppose K is an $\aleph_1$-saturated valued field with value group Γ, $\Gamma_0 \subset \Gamma$ is a pure subgroup, $s : \Gamma_0 \to K^\times$ is a partial section and $g \in \Gamma \setminus \Gamma_0$. Then there is a pure subgroup $\Gamma_0 \cup \{g\} \subset \Gamma_1 \subseteq \Gamma$ and $\widehat{s} \supset s$ a partial section of Γ_1.*

We know that $\Gamma_0 = \{0\}$ is a pure subgroup of Γ with partial section $s(0) = 1$. By Zorn's Lemma there is a maximal partial section and by the Lemma it must be defined on all of Γ.

Proof of Lemma Let H be the group generated by $\Gamma \cup \{g\}$. We first look for a smallest pure subgroup Γ_1 containing H. Let $S = \{n > 0 :$ there is $b \in \Gamma$ such that b/H has order exactly n in Γ/H. If $n \in S$ there is $b \in \Gamma$, $c \in \Gamma_0$ and $m \in \mathbb{Z}$ such that $nb = c + mg$. We make some observations.

- if $m, n \in S$, let b/H have order m and c/H have order n, then $(b + c)/H$ has order d, where d is the least common multiple of m and n. Thus $d \in S$.

- If $(nk)b = c + (mk)g$, then $c = k(nb - mg) \in \Gamma_0$ and, by purity of Γ_0, $nb - mg \in \Gamma_0$. Thus b/H has order n. It follows that if $n \in S$, there are $b \in \Gamma$, $c \in \Gamma_0$ and $m \in \mathbb{Z}$ such that $nb = c + mg$ where n and m are relatively prime.

- If $nb = c + mg$ where n and m are relatively prime, then there is $b' \in \Gamma$ and $c' \in \Gamma_0$ such that $nb' = c' + g$.

There are integers u and v such that $un + vm = 1$. Then $n(ub) = uc + umg$ and $n(ub - vg) = uc + g$.

- If $nb = c + g$ and $nb' = c' + mg$, then b' is in the group generated by $\Gamma_0 \cup \{b\}$.

Note that $nmb = cm + mg$. Thus $n(b' - mb) = c' - mc \in \Gamma_0$. Thus, by the purity of Γ_0, $b' - mb \in \Gamma_0$.

Suppose for $n \in S$ we choose $b_n \in \Gamma$ and $c_n \in \Gamma_0$ such that $nb_n = c_n + g$. Note that $1 \in S$ and $b_1 = g$. Let Γ_1 be the subgroup generated by $\Gamma_0 \cup \{b_n : n \in S\}$. Putting together the previous observations, we see that Γ_1 is the smallest pure subgroup of Γ containing $\Gamma_0 \cup \{g\}$.

We need to find $(x_n : n \in S) \in K$ such that $v(x_n) = b_n$ and $x_n^n = s(c_n)x_1$ for all n. Consider the set of formulas

$$\Sigma = \{v(x_n) = b_n \wedge x_n^n = s(c_n)x_1 : n \in S\}.$$

Since (K, v) is $\aleph_1$-saturated, it suffices to show that every subset of Σ is consistent.

Let S_0 be a finite subset of S. Without loss of generality we may assume that $1 \in S_0$ and there is $N \in S_0$ such that $n|N$ for all $n \in S_0$. Choose x_N with $v(x_N) = b_N$. We must have $x_1 = \frac{x^N}{s(c_N)}$.

Suppose $n \in S_0$ and $N = nd$. Then $Nb_N = c_N + nb_n - c_N$. Thus

$$n(db_N - b_n) = c_N - c_n \in \Gamma_0$$

and there is $c_{N,n} \in \Gamma_0$ such that $db_N - b_n = c_{N,n}$. Then $s(c_{N,n})^n = \frac{s(c_N)}{s(c_n)}$.

Let $x_n = \frac{x_N^d}{s(c_{N,n})}$. Then

$$x_n^N = \frac{x_N^N}{s(c_{N,n})^n} = \frac{x_N^N s(c_n)}{s(c_N)} = s(c_n)x_1$$

and

$$v(x_n) = db_N - c_{N,n} = b_n,$$

as desired. Thus every finite subset of Σ is consistent. If $(x_n : n \in S)$ satisfies Σ we can extend s by sending $b_n \mapsto x_n$ for $n \in S$. □

Exercise 2.33 a) Modify the proof above to prove the following. Consider the language of groups where we add a unary predicate for a distinguished subgroup. Suppose (G, H) is an $\aleph_1$-saturated abelian group with proper subgroup such that G/H is torsion free. Prove that there is a section $s : G/H \to G$, i.e., a homomorphism such that $s(x/H)/H = x/H$.

b) Use the above to show that in every $\aleph_1$-saturated valued field K there is a section $s : \Gamma \to K^\times$ with $v \circ s = id$.

Unfortunately, we can not always find sections.

Exercise 2.34 Consider the field $\mathbb{Q}(X_1, X_2, \dots)$ with the valuation where $v(X_n) = 1/n$. Prove that there is no section of the value group.

2.4 Hahn fields

Let k be a field and let $(\Gamma, +, <)$ be an ordered abelian group. We will consider the multiplicative group of formal monomials $(T^\gamma : \gamma \in \Gamma)$ where $T^0 = 1$ and $T^{\gamma_1} T^{\gamma_2} = T^{\gamma_1 + \gamma_2}$ and formal series $f = \sum_{\gamma \in \Gamma} a_\gamma T^\gamma$ where $a_\gamma \in k$. The *support* of f is $\text{supp}(f) = \{\gamma : a_\gamma \neq 0\}$. We will only consider series f where $\text{supp}(f)$ is well ordered (i.e. every nonempty subset has a least element). The *Hahn series*field is

$$k(\!(\Gamma)\!) = \{f : \text{supp}(f) \text{ is well ordered}\}.$$

Addition is easy to define if $f = \sum_{\gamma \in \Gamma} a_\gamma T^\gamma$ and $g = \sum_{\gamma \in G} b_\gamma T^\gamma$. Then

$$a + b = \sum_{\gamma \in \Gamma} (a_\gamma + b_\gamma) T^\gamma.$$

Lemma 2.35 *Let A and B be well ordered subsets of Γ. Then $A + B$ is well ordered and for any $c \in A + B$ the set $\{(a, b) \in A \times B : a + b = c\}$ is finite.*

In particular, if $A \subset \Gamma$ is well ordered then the set $\Sigma_n = \{a_1 + \cdots + a_n : a_1, \dots, a_n \in A\}$ is well ordered and for all $g \in \Sigma_n$, $\{(a_1, \dots, a_n) \in A^n : \sum a_i = g\}$ is finite.

Proof Suppose $(a_0, b_0), (a_1, b_1), \dots$ are distinct such that $a_i + b_i \geq a_j + b_j$ for $i > j$. We can find a strictly monotonic subsequence of the a_i. Since A is a well ordered, the sequence can not be decreasing. Thus we may assume $a_0 \leq a_1 \leq \dots$. But then $b_0 > b_1 > \dots$ is an infinite descending sequence, contradicting the fact that B is well ordered. □

This allows us to define multiplication by

$$\left(\sum_{\gamma \in \Gamma} a_\gamma T^\gamma \right) \left(\sum_{\gamma \in \Gamma} b_\gamma T^\gamma \right) = \sum_{\gamma \in \Gamma} \sum_{\gamma_1 + \gamma_2 = \gamma} a_{\gamma_1} b_{\gamma_2} T^\gamma.$$

The usual proofs of commutativity and associativity in power series show that $k(\!(\Gamma)\!)$ is a domain. There is a natural valuation $v(f) = \min \operatorname{supp}(f)$. A stronger form of the last lemma is needed to show $k(\!(\Gamma)\!)$ is a field. For a proof see [1] §7.21.

Lemma 2.36 (Neumann's Lemma) *Suppose $A \subset \Gamma$ is well ordered and every element of A is positive. Let $\Sigma = \{a_1 + \cdots + a_n : (a_1, \ldots, a_n) \in A^{<\mathbb{N}}\}$. Then Σ is well ordered and for all $g \in \Sigma$ the set $\{(a_1, \ldots, a_n) \in A^{<\mathbb{N}} : n \in \mathbb{N}$ and $\sum a_i = g\}$ is finite.*

Proof Suppose $g_0 > g_1 > \ldots$ is an infinite decreasing sequence in Σ. For each i let $\sigma_i = (\sigma_i(1), \ldots, \sigma_i(n_i)) \in S$ be of minimal length such that $g_i = \sigma_i(1) + \cdots + \sigma_i(n_i)$ and n_i is the minimal length such that there is $(a_1, \ldots, a_m) \in S$ with $a_1 + \cdots + a_m = g_i$. We also assume that $\sigma_i(1) \leq \sigma_i(2) \leq \ldots$. We can thin the sequence such that $n_0 \leq n_1 \leq n_2 \geq \ldots$. [In this proof we use several times that in an ordered set every sequence has a strictly monotonic subsequence.]

claim By altering the sequence we may assume that the sequence $n_0, n_1, n_2 \ldots$ is constant.

The lemma will lead to a contradiction as we have shown that the set of sums of n-elements of A is well ordered for each n.

Suppose we have arranged things such that $n_0 = n_1 = \cdots = n_k < n_{k+1}$. We can pass to a subsequence fixing $\sigma_0, \ldots, \sigma_k$ but, perhaps, thinning the rest such that $\sigma_{k+1}(1), \sigma_{k+2}(1), \sigma_{k+3}(1), \ldots$ is strictly monotonic. Since A is well ordered, we must have $\sigma_{k+1}(1) \leq \sigma_{k+2}(1) \leq \sigma_{k+3}(1), \ldots$. For all $j > k$ let $\sigma'_j = (\sigma_j(2), \ldots, \sigma_j(n_j))$ and let $h_j = \sigma_j(2) + \cdots + \sigma_j(n_j)$. Since all element of A are nonnegative $h_j < g_j$ and since $\sigma_j(1) \geq \sigma_{k+1}(1)$ for $j > k$, $h_{k+1} > h_{k+2} > \ldots$. Replace g_j by h_j and σ_j by σ'_j for $j > k$. We have shortened the sequence σ_{k+1} by one. Repeating this procedure finitely many times we may assume that $\sigma_1, \ldots \sigma_{k+1}$ have the same length.

Repeating this process for each k we get may assume that $n_0, n_1, \ldots$ is constant. [Note that after stage k we never change σ_k.]

Thus we conclude that Σ is well ordered. We need to show that for all $g \in \Sigma$ there are only finitely many sequence $(a_1, \ldots, a_n) \in A^{<\mathbb{N}}$

Suppose $g \in \Sigma$ and there are $\sigma_0, \ldots, \sigma_n, \ldots$ distinct in $A^{<\mathbb{N}}$ such that $\sigma_i = (\sigma_i(1), \ldots, \sigma_i(n_i))$ and $\sigma_i(1) + \cdots + \sigma_i(n_i) = g$. Since g is well ordered we may assume that g is the least element of Σ where this is possible. Passing to a subsequence we may assume that $\sigma_0(1), \ldots, \sigma_n(0), \ldots$ is strictly monotonic. Since A is well ordered, it can not be strictly decreasing. Let $h_i = \sigma_i(2) + \cdots + \sigma_i(n_i) \in \Sigma$. If $\sigma_0(1), \ldots, \sigma_n(1), \ldots$ is strictly increasing $h_0 > h_1 > \ldots$ contradicting that Σ is well ordered. If $\sigma_0(1), \ldots, \sigma_n(1)$, is constant then every $h_i = h_0 - \sigma_0(1) < g$ since every element of A is positive. But this contradicts the minimality of g. □

Corollary 2.37 *If $\sum_{n=0} a_n X_n \in k[[X]]$, $f \in k(\!(\Gamma)\!)$ and $v(f) > 0$, then $\sum_{n=0} a_n f^n$ is a well defined element of $k(\!(\Gamma)\!)$.*

We can now show that $k(((\Gamma)))$ is a field. Suppose $f \neq 0$. Then $f = aT^\gamma(1-\epsilon)$ where $\epsilon \in k(((\Gamma)))$ and $a \in k^\times$. and $v(\epsilon) > 0$. Then $g = \sum_{n=0}^{\infty} \epsilon^n \in T$ and the usual arguments show that $g(1-\epsilon) = 1$. Thus $1/f = (1/a)T^{-\gamma}g$ and $k(((\Gamma)))$ is a field.

Definition 2.38 If $f, g \in k(((\Gamma)))$, $f = \sum a_\gamma T^\gamma$ and $\sum b_\gamma T^\gamma$, we say that g is an *end extension* of f or, alternatively, that f is a *truncation* of g if $\text{supp}(f) \subset \text{supp}(g)$, every element of $\text{supp}(g) \setminus \text{supp}(f)$ is greater than every element of $\text{supp}(f)$ and if $\gamma \in \text{supp}(f)$ then $a_\gamma = b_\gamma$. We write $f \lhd g$.

Exercise 2.39 Suppose we have $(f_\beta : \beta < \alpha)$ for some ordinal α where $f_\delta \lhd f_\beta$ for all $\delta < \beta < \alpha$. Let $f_\beta = \sum a_{\beta,\gamma} T^\gamma$. Show that $\bigcup_{\beta<\alpha} \text{supp}(f_\beta)$ is well ordered and if $f = \sum a_\gamma T^\gamma$ where $a_\gamma = a_{\beta,\gamma}$ for all sufficiently large $\beta < \alpha$. Moreover $v(f_\alpha - f) > \text{supp}(f_\alpha)$.

Lemma 2.40 *The field of Hahn series $k(((\Gamma)))$ is henselian.*

Proof While $k(((\Gamma)))$ need not be complete, we can mimic the proof of Hensel's Lemma with a transfinite iteration. Let $\mathcal{O}$ be the valuation ring, let $p(X) \in \mathcal{O}[X]$ and $a \in \mathcal{O}$ such that $v(p(a)) > 0$ and $v(p'(a)) = 0$. As we saw in the proof of Hensel's Lemma if we take $b = a - \frac{p(a)}{p'(a)}$, then $v(p(b)) \geq 2vp(a)$ and $v(p'(b)) = 1$.

We build a sequence of better and better approximations. Let $a_0 = a$. Given a_α if $p(a_\alpha) = 0$ we are done, otherwise let $a_{\alpha+1} = a + \alpha - p(a_\alpha)/overp'(a_\alpha)$ and let $\gamma_\alpha = v(p(a)) = v(a_{\alpha+1} - a_\alpha)$.

Suppose α is a limit ordinal and we have constructed $(a_\beta : \beta < \alpha)$. Let $a_\beta = \sum_{g\in\Gamma} b_{\beta,\gamma} T^\gamma$. If $\beta > \alpha$, then $a_{\beta,\gamma} = a_{\beta+1,\gamma}$ for all $\gamma < \gamma_\beta$. Let $f_\beta = \sum \gamma < \gamma_\beta a_{\beta+1,\gamma}$. Then $v(a_\delta - f_\beta) \geq \gamma_\beta$ and f_β is an initial segment of the series f_β for all $\beta > \alpha$. We can naturally take the limit of the series $(f_\alpha : \beta < \alpha)$ as in Exercise 2.39 and let this be a_α. We have $v(a_\alpha - a_\beta) > \gamma_\beta$ for all $\beta < \alpha$. As in the proof of Hensel's Lemma, this implies $v(p(a_\alpha) > \gamma_\beta$ for all $\beta < \alpha$ and $v(p'(a_\alpha)) = 1$.

Since we are building (γ_α) an increasing sequence in Γ, this process must stop at some ordinal $\alpha < |\Gamma|^+$, but it only stops when we find the desired zero of p. □

Corollary 2.41 *For any field k and any ordered abelian group Γ there is a henselian valued field with value group Γ and residue field k.*

Exercise 2.42 Suppose k is an ordered field.

a) Show that we can order $k(((\Gamma)))$, by $x > 0$ if and only if $x = at^\gamma(1+\epsilon)$ where $a > 0$.

b) Suppose ever nonnegative $a \in k$ is a square and Γ is 2-divisible, i.e., if $g \in \Gamma$ there is $h \in \Gamma$ with $2h = g$. Let $a \in k(((\Gamma)))$ with $a > 0$. Show that a is a square. Thus the ordering in a) is the only possible ordering of $k(((\Gamma)))$.

We will show in Corollary 3.17 that if k is real closed and Γ is divisible then $k(((\Gamma)))$ is real closed.

Hahn series fields recapture some aspects of completeness.

Definition 2.43 Let K be a valued field. We say that K is *spherically complete* if whenever $(I, <)$ is a linear order and $(B_i : i \in I)$ is a family of open balls such that $B_i \supset B_j$ for all $i < j$, then $\bigcap_{i\in I} B_i \neq \emptyset$.

Lemma 2.44 *Any Hahn series of field $k(((\Gamma)))$ is spherically complete.*

Proof Without loss of generality we may assume that there is an ordinal α $(B_\beta : \beta < \alpha)$ and $B_\delta \supset B_\beta$ for $\delta < \beta < \alpha$. Let $B_\beta = \{x : v(x - a_\beta) > \gamma_\beta\}$. For each $\beta < \alpha$ choose f_β such that $\sup \operatorname{supp}(f_\beta) = \gamma_\beta$ and $v(f_\beta - a_\beta) > \gamma_\beta$. Then $f_\delta \lhd f_\beta$ for $\delta < \beta < \alpha$. Let f be as in Exercise 2.39, then $f \in \bigcup_{\beta<\alpha} B_\beta$. □

maximal valued fields

Hahn fields $k(((\Gamma)))$ are the maximal fields with residue field k and value group Γ.

Definition 2.45 If (K, v) is a valued field extending L is a subfield, then K is an *immediate extension* if $v(K) = v(L)$ and $\boldsymbol{k}_K = \boldsymbol{k}_L$.

For example $\mathbb{Q}_p$ is an immediate extension of $\mathbb{Q}$.

Lemma 2.46 *$k(((\Gamma)))$ has no proper immediate extensions.*

Proof Suppose K is an immediate extension of $k(((\Gamma)))$ and $x \in K \setminus k(((\Gamma)))$. We build a series as follows: Let $\gamma_0 = v(x)$. Choose $a_0 \in k$ such that $\operatorname{res}(x/T^{\gamma_0}) = a_\gamma$. Then $v(x - a_0 T_0^\gamma) > \gamma_0$.

Suppose we have constructed $(a_\beta : \beta < \alpha)$ a sequence in k and $(\gamma_\beta : \beta < \alpha)$ an increasing sequence in Γ such that if $f_\alpha = \sum_{\delta<\beta} a_\delta T^{\gamma_\delta}$ then $v(x - f_\alpha) > \gamma_\beta$ for all $\beta < \alpha$. Let $\gamma_\alpha = v(x - f_\alpha)$. As before we can find $a_\alpha \in k$ such that $\operatorname{res}((x - f_\alpha)/T^{\gamma_\alpha}) = a_\alpha$. Then $v(x - f_\alpha + a_\alpha T^{\gamma_\alpha}) > \gamma_\alpha$ and we can continue the induction.

In this way we will build an increasing map from the ordinals into Γ, but this must stop by some $\alpha < |\Gamma|^+$, a contradiction. □

Definition 2.47 We say that (K, v) is a *maximal valued field* if it has no proper immediate extensions.

We will show that every valued field has a maximal extension.

Lemma 2.48 (Krull's Bound) *If K is a valued field, then $|K| \leq |\boldsymbol{k}|^{|\Gamma|}$.*

Proof Let $\kappa = |\boldsymbol{k}|$. Suppose B is a closed ball of radius of radius γ, then, as we saw in Lemma 1.10, that B is the union of κ disjoint open balls of radius γ. Let $(C_\alpha^B : \alpha < \kappa)$ be the listing. For $x \in K$ define $f_x : \Gamma \to \kappa$, be defined so that if B is the closed ball of radius γ around x, then $x \in C^B_{f_x(\gamma)}$. Suppose $x \neq y$ and $v(x - y) = \gamma$. Then $f_x(\delta) = f_y(\delta)$ for all $\delta < \gamma$, but $f_x(\gamma) \neq f_y(\gamma)$. Thus $x \mapsto f_x$ in injective and $|K| \leq |\boldsymbol{k}|^\Gamma$. □

Corollary 2.49 (Kaplansky) *If K is a valued field, then there is $K \subseteq L$ an immediate extension that is maximally valued.*

Proof By Krull's bound, the collection of immediate extensions of K is a set so we can apply Zorn's Lemma to find a maximal immediate extension. □

In Exercise 5.30 we will show that any maximally valued field is spherically complete.