Model Theory of Valued Fields
University of Illinois at Chicago

David Marker

Fall 2018

Contents

1 Valued Fields–Definitions and Examples **3**
- 1.1 Valuations and Valuation Rings 3
- 1.2 Absolute Values 8

2 Hensel's Lemma **12**
- 2.1 Hensel's Lemma, Equivalents and Applications 12
- 2.2 Lifting the residue field 19
- 2.3 Sections of the value group 20
- 2.4 Hahn fields 22

3 Extensions of Rings and Valuations **27**
- 3.1 Integral extensions 27
- 3.2 Extensions of Valuations 29

4 Algebraically Closed Valued Fields **35**
- 4.1 Quantifier Elimination for ACVF 35
- 4.2 Consequences of Quantifier Elimination 40
- 4.3 Balls 43
- 4.4 Real Closed Valued Fields 45

5 Algebra of Henselian Fields **47**
- 5.1 Extensions of Henselian Valuations 47
- 5.2 Algebraically Maximal Fields 51
- 5.3 Henselizations 53
- 5.4 Pseudolimits 55

6 The Ax–Kochen Eršov Theorem **60**
- 6.1 Quantifier Elimination in the Pas Language 60
- 6.2 Consequence of Quantifier Elimination 64
- 6.3 Artin's Conjecture 68

7 The Theory of $\mathbb{Q}_p$ **71**
7.1 p-adically Closed Fields 71
7.2 Consequences of Quantifier Elimination 75
7.3 Rationality of Poincaré Series 83

These lecture notes are based on a course given at the University of Illinois at Chicago in Fall 2018. The goal was to cover some of the classic material on the model theory of valued fields: the Ax–Kochen/Eršov Theorem, the model theory of $\mathbb{Q}_p$ and Denef's work on rationality of Poincaré series. The lectures assumed a basic knowledge of model theory (quantifier elimination tests, saturated models...) and graduate level algebra, but most results on the algebra of valuations were presented from scratch.

Parts of my lectures closely follow the notes of Zoé Chatzidakis [4], Lou van den Dries [12] and the book *Valued Fields* by Engler and Prestel [17].

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 $\mathrm{res}(x)$) 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 Valued Fields–Definitions and Examples

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 a *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 $p \nmid b$. 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 $p \nmid g$.

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 [40].

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

$$A_PP=\{a_1p_1+\ldots a_mp_m: a_1,\ldots,a_m\in A_P, p_1,\ldots,p_m\in P, m=1,2,\ldots\}.$$

Show that A_P is a local ring with maximal ideal A_PP.

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. $\square$

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 $\mathrm{res} : \mathcal{O} \to \boldsymbol{k}$ be the residue map $\mathrm{res}(x) = x/\mathfrak{m}$. Often we write $\overline{x}$ for $\mathrm{res}(x)$.

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.

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

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

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

$\square$

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

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

$\square$

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 $\mathfrak{m} = A \setminus U$. 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, [3] §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, [3] §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 $(a_n : n = 1, 2, \ldots)$ 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 $f_0, f_1, \ldots$ 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 $n > N$. $\square$

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 $\sum_{n<m} a_n p^n = x (\bmod\ p^m)$ for all m. Then $\sum_{n=0}^{\infty} a_n p^n = x$. Thus the map is surjective. $\square$

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 Eršov 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 $f(\alpha) = \lim_{n\to\infty} f(a_n) = 0$. $\square$

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 $\alpha \neq \beta$, $f(\beta) \neq 0$. $\square$

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

ii) $\Rightarrow$ iii) Then

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

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 5.17 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 $\alpha = -1 (\text{mod } n)$ 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 $-1(\text{mod } \mathfrak{m})$. Any zero that is a unit must be congruent to $-1(\text{mod } \mathfrak{m})$, 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 $\bar{b}$ be the residue of f. Then if b is a square $\bar{b}$ must be a square in the residue field $\mathbb{F}_p$. If $x \in \mathbb{Z}_p$ such that $\overline{x}^2 = \bar{b}$. 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 $x^2 - b = 0 (\mathrm{mod}\ 8)$. 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 $4 (\mathrm{mod}\ 8)$. 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 $\mathrm{res}(n)$ 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 $z^2 + y^2 = u$. $\square$

Lemma 2.15 *Suppose $p = 1 (\mathrm{mod}\ 4)$. 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 $\mathbb{Z}_p$. $\square$

Corollary 2.16 *If $p = 1(\mathrm{mod}\ 4)$ 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 $a = (pc)^2 + (pd)^2$. $\square$

Lemma 2.17 *If $p = 3(\mathrm{mod}\ 4)$, 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 $(u/v)^2 = -1(\mathrm{mod}\ p)$, a contradiction since $p = 3(\mathrm{mod}\ 4)$. $\square$

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 $u = 1(\mathrm{mod}\ 4)$.*

Proof First suppose $u = 1(\mathrm{mod}\ 4)$. We first show that u is a sum of squares. Then $u = 1$ or 5 (mod 8). If $u = 1(\mathrm{mod}\ 8)$, then u is already a square in $\mathbb{Z}_2$. If $u = 5(\mathrm{mod}\ 8)$, 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 $u = 3(\mathrm{mod}\ 4)$. 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 $z^2 + w^2 = 0(\mathrm{mod}\ 4)$. But z and w are units and, thus, $z^2, w^2 = 1(\mathrm{mod}\ 4)$ and $z^2 + w^2 = 2(\mathrm{mod}\ 4)$, a contradiction. $\square$

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 $p = 3(\mathrm{mod}\ 4)$ that divides m. See, for example, [38] §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 [36] §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 $\xi = 1$. $\square$

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 $y^{p-1} = 1$. $\square$

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 $g(0) = f(T, 0) = f(0, 0) = 0$ (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, [35]).

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 $x \in \boldsymbol{k} \backslash \boldsymbol{k}_0$ 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

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

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. $\square$

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. $\square$

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 $n \in S$. $\square$

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 $\mathrm{supp}(f) = \{\gamma : a_\gamma \neq 0\}$. We will only consider series f where $\mathrm{supp}(f)$ is well ordered (i.e. every nonempty subset has a least element). The *Hahn series*field is

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

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. $\square$

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. $\square$

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 $\sup \mathrm{supp}(f_\beta) = \gamma_\beta$ 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 $f \in \bigcup_{\beta < \alpha} B_\beta$. $\square$

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 $\mathrm{res}(x/T^{\gamma_0}) = a_\gamma$. 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 $\mathrm{res}((x - f_\alpha)/T^{\gamma_\alpha}) = a_\alpha$. 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. $\square$

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 $|K| \leq |\boldsymbol{k}|^\Gamma$. $\square$

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. $\square$

In Exercise 5.41 we will show that any maximally valued field is spherically complete.

3 Extensions of Rings and Valuations

When studying the model theory of certain theories of valued fields our first step will usually be to prove quantifier elimination in an appropriate language. Proofs of quantifier elimination in algebraic theories usually require some algebraic extension results. That is particular true in valued fields. In this section we will prove some basic results and then will use them in §4 to begin the study of the model theory of algebraically closed valued fields. In §5 we will focus on extension results for henselian valued fields.

For more details on some of the background results from commutative algebra see, for example [16] or [26]. All of the results we will be proving on extensions of valuations can be found in [17]. To be careful we will tend to state most results for domains even though many are true in more generality.

3.1 Integral extensions

We begin by reviewing some facts about the integral extensions.

Recall that a domain A is local if and only if A has a unique maximum ideal $\mathfrak{m}$ which is exactly the nonunits of A.

Definition 3.1 If $A \subset B$ are domains, we say that $b \in B$ is *integral* over A, if there are $a_0, \ldots, a_{n-1} \in A$ such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

for some n. We say that B *is integral over* A if every element of B is integral over A.

Lemma 3.2 *Let $A \subset B$ be domains and $b \in B$. The following are equivalent.*
i) b is integral over A.
ii) $A[b]$ is a subring of B that is a finitely generated A-module.
iii) $A[b]$ is contained in a finitely generated A-module.

Proof i) $\Rightarrow$ ii) If $b^m = \sum_{n=0}^{m-1} a_n b^n$ where $a_0, \ldots, a_{m-1} \in A$. Then $A[b]$ is generated over A by $1, b, \ldots b^{m-1}$.

ii) $\Rightarrow$ iii) is clear.

iii) $\Rightarrow$ i) Let $x_1, \ldots, x_m$ generate a submodule containing $A[b]$ over A. For $i = 1, \ldots m$ we can find $a_{i,1}, \ldots, a_{i,m} \in A$ such that

$$bx_i = \sum_{j=1}^{m} a_{i,j} x_j.$$

Let M be the matrix

$$\begin{pmatrix} a_{1,1} - b & a_{1,2} & \ldots & a_{1,m} \\ a_{2,1} & a_{2,2} - b & \ldots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \ldots & a_{m,m} - b \end{pmatrix}$$

i.e, the matrix with $a_{i,i} - b$ along the diagonal and $a_{i,j}$ everywhere else. Then $M(x_1, \ldots, x_m)^T = 0$. Let $\mathrm{Adj}(M)$ be the adjoint of M. Then

$$\mathrm{Adj}(M)M(x_1, \ldots, x_m)^T = (\det M x_1, \ldots, \det M x_m)^T = (0, \ldots, 0)^T.^2$$

Thus we must have $\det M = 0$. But $\det M$ is a monic polynomial in $A[b]$. $\square$

Corollary 3.3 *If $A \subset B \subset C$ are domains, B is an integral extension of A and C is an integral extension of B, then C is an integral extension of C.*

Proof Let $c \in C$. There are $b_0, \ldots, b_{n-1} \in B$ such that $c^n + \sum b_i c^i = 0$. Then $A[b_0, \ldots, b_{n-1}, c]$ is a finitely generated A-module and c is integral over A. $\square$

The next lemma is a simple but useful tool.

Lemma 3.4 *If A is a local subring of a field K, $x \in K^\times$ and $1 = a_0 + \frac{a_1}{x} + \ldots \frac{a_n}{x^n}$ where $a_0 \in \mathfrak{m}$ and $a_1, \ldots, a_n \in A$, then x is integral over A.*

Proof Then $(1 - a_0)x^n - a_1 x^{n-1} - \cdots - a_n = 0$. Since $a_0 \in \mathfrak{m}$, $1 - a_0 \notin \mathfrak{m}$. Since A is local, $1 - a_0$ is a unit and x is integral over A. $\square$

Lemma 3.5 *If $A \subset B$ are domains and B is integral over A, then A is a field if and only if B is a field.*

Proof ($\Leftarrow$) Suppose B is a field and $a \in A$ is nonzero. Then there are $c_0, \ldots, c_{m-1} \in A$ such that

$$(a^{-1})^m + \sum_{n=0}^{m-1} c_n (a^{-1})^n = 0.$$

Multiplying by a^{m-1} we see that

$$a^{-1} = -\sum_{n=0}^{m-1} c_n a^{m-n-1} \in A.$$

Thus A is a field.

($\Rightarrow$) Suppose A is a field and $b \in B$ is nonzero. Then, by Lemma 3.2 $A[b]$ is a finitely generated vector space over A. The map $z \mapsto bz$ is an injective linear transformation of $A[b]$ and, since $A[b]$ is a finite dimensional vector space must be surjective. Thus there is $z \in A[b]$ with $zb = 1$. $\square$

Definition 3.6 Let $A \subset B$ be domains and let $P \subset A$, $Q \subset B$ be prime ideals. We say that Q *lies over* P if $A \cap Q = P$.

Corollary 3.7 *Let $A \subset B$ be domains with B integral over A and let $P \subset A$ and $Q \subset B$ be prime ideals such that Q lies over P. Then P is maximal if and only if Q is maximal.*

[2] Remember Cramer's Rule!

Proof Since $P = A \cap Q$ we can view B/Q as an integral extension of A/P. By the last lemma, A/P is a field if and only if B/Q is a field. $\square$

Lemma 3.8 *Suppose $A \subset B$ are domains, B is integral over A, Q is a prime ideal in B and $P = Q \cap A$. Then then BA_P is integral over A_P.*

Proof Consider b/t where $b \in B$ and $t \in A \setminus Q$. There are $a_0, \ldots, a_{m-1} \in A$ with $b^m + \sum a_i b^i = 0$. But then

$$(b/t)^m + \sum (a_i/t^{m-i})(b/t^i) = 0.$$

$\square$

Lemma 3.9 *Suppose $A \subset B$ are domains, B is integral over A, $P \subset A$ is a prime ideal and $Q_1 \subseteq Q_2$ are prime ideals in B lying over P. Then $Q_1 = Q_2$.*

Proof Consider the localization A_P and the integral extension BA_P. Then Q_1A_P and Q_2A_P are prime ideals of BA_P lying over PA_P. But PA_P is maximal. Thus each Q_iA_P is maximal and we must have $Q_1A_P = Q_2A_P$. But if $x \in Q_2 \setminus Q_1$, then $x \notin Q_1A_P$. If we did have $x = q/t$ for some $q \in Q_1$ and $t \in A \setminus P$. Then $xt \in Q_1$ and since $x \notin Q_1$ and Q_1 is prime, we would have $t \in Q_1 \cap A = P$, a contradiction. $\square$

Theorem 3.10 (Lying Over Theorem) *Suppose $A \subset B$ are domains, B is integral over A and P is a prime ideal of A. There is a prime ideal Q of B such that $A \cap Q = P$.*

Proof First, suppose A was a local ring then P is the unique maximal of A. If $Q \subset B$ is any maximal idea extending P, then, by Corollary 3.7, $Q \cap A$ is maximal. But then $Q = P$.

In general, we pass to the localization A_P. As above, if Q_0 is any maximal ideal in BA_P, then $Q_0 \cap A_P = PA_P$. So $Q_0 \cap A = P$. Let $Q = Q_0 \cap B$. Then $Q \cap A = P$ and, since Q_0 is prime, Q is prime. $\square$

3.2 Extensions of Valuations

Theorem 3.11 (Chevalley's Theorem) *Suppose A is a subring of a field K and $P \subset A$ is a prime ideal. Then there is a valuation ring $\mathcal{O}$ of K with $A \cap \mathcal{M}_{\mathcal{O}} = P$*

Proof Replacing A by A_P we may assume that A is a local ring with maximal ideal P. Let $\mathcal{P}$ be the set of all local subrings B of K with $\mathfrak{m}_B \cap A = P$. Clearly $\mathcal{P}$ is partially ordered by $\subset$ and if $(B_i : i \in I)$ increasing chain in $\mathcal{P}$ then $\bigcup_{i \in I} B_i$ is an upper bound. Thus by Zorn's Lemma, $\mathcal{P}$ has maximal elements. Let $\mathcal{O} \in \mathcal{P}$ be maximal. Let $\mathfrak{m}$ be the maximal ideal of $\mathcal{O}$. We will argue that $\mathcal{O}$ is a valuation ring.

Suppose $x, 1/x \in K \setminus \mathcal{O}$. If x is integral over $\mathcal{O}$, then we can find a maximal ideal of $\mathcal{O}[x]$ lying over $\mathfrak{m}$ contradicting the maximality of $\mathcal{O} \in \mathcal{P}$. Thus x is not integral over $\mathcal{O}$.

By Lemma 3.4, $1 \notin \mathfrak{m}\mathcal{O}[1/x]$. Thus there is a maximal ideal Q of $\mathcal{O}[1/x]$ that lies over $\mathfrak{m}$, contradicting the maximality of $\mathcal{O}$. Thus for all $x \in K$ at least one of x and $1/x$ is in $\mathcal{O}$. □

Exercise 3.12 Show that if $v : K^\times \to \Gamma$ is a valuation and $L \supset K$ is an extension field, there is $\Gamma' \supseteq \Gamma$ and $w : L\times \to \Gamma'$ extending v.

integral closures and valuations

Definition 3.13 We say that A is *integrally closed in B* if no element of $B \setminus A$ is integral over A. We say that A is *integrally closed* if it is integrally closed in its fraction field.

The integral closure of A is the smallest integrally closed ring containing A.

Lemma 3.14 *If (K, v) is a valued field, then the valuation ring $\mathcal{O}$ is integrally closed.*

Proof Suppose $b \in K$ and $b^n+a_{n-1}b^{n-1}+\cdots+a_1b+a_0 = 0$ where $a_0, \ldots, a_{n-1} \in \mathcal{O}$. If $b \notin \mathcal{O}$, then $v(b) < 0$ and

$$v(a_ib^i) = v(a) + iv(b) < nv(b)$$

since $v(a_i) \geq 0$ for all i. Thus $v(b^n + a_{n-1}b^{n-1} + \cdots + a_1b + a_0) = nv(b) < 0$, a contradiction. □

We can use valuation rings to find the integral closure of a local subring.

Lemma 3.15 *Let A be a local subring of a field K with maximal ideal $\mathfrak{m}$. The integral closure of $A \in K$ is the intersection of all valuation rings $\mathcal{O} \subset K$ with $\mathfrak{m}_\mathcal{O}$ lying over $\mathfrak{m}$.*

Proof Suppose $x \in K$ be nonintegral over A. Then by Lemma 3.4, $1 \notin \mathfrak{m}A[1/x] + \frac{1}{x}A[1/x]$. Thus we can find a maximal ideal Q of $A[1/x]$ lying over $\mathfrak{m}$ with $1/x \in Q$. Let $\mathcal{O} \supseteq A[1/x]$ be a maximal local subring of K. Then, as in the proof of Theorem 3.11, $\mathcal{O}$ is a valuation ring, $\mathfrak{m}_\mathcal{O}$ lies over $\mathfrak{m}$ and $1/x \in \mathfrak{m}_\mathcal{O}$. Thus $x \notin \mathcal{O}$. □

Algebraic Extensions

Suppose $K \subset L$ are fields and v is a valuation on K. Then v restricts to a valuation on K. Let $\mathcal{O}_L, \Gamma_L, \boldsymbol{k}_L$ and $\mathcal{O}_K, \Gamma_K, \boldsymbol{k}_K$ denote the respective valuation rings, value groups and residue fields.

Lemma 3.16 *Then Γ_L is contained in the divisible hull of Γ_K and $\boldsymbol{k}_L$ is an algebraic extension of $\boldsymbol{k}_K$.*

Proof Let $x \in L \setminus K$. There are $a_0, \ldots, a_n \in K$ such that $\sum a_i x^i = 0$. There must be $i \neq j$ such that $v(a_i x^i) = v(a_j x^j)$. But then $v(x) = \frac{v(a_i) - v(a_j)}{j-i}$.

Suppose $x \in L$ and the residue $\overline{x} \in \boldsymbol{k}_L \setminus \boldsymbol{k}_K$. There is a polynomial $f[X] \in \mathcal{O}_K(X)$ such that $\overline{f(x)} = 0$. Let $f(X) = \sum a_i X^i$. Suppose a_j has minimal value and let $g(X) = \sum \frac{a_i}{a_j} X^i$. Then $\overline{g(x)} = 0$ and $\overline{g}(X)$ is not identically zero as some coefficient is 1. Thus $\overline{x}$ is algebraic over K. □

Corollary 3.17 *i) If k is an algebraically closed field, Γ is a divisible ordered abelian group and $K = k(((\Gamma)))$, then K is algebraically closed.*

ii) If k is a real closed, Γ is a divisible ordered abelian group and $K = k(((\Gamma)))$, then K is real closed.

Proof If K is not algebraically closed field let L/K be an algebraic extension, then we can extend the valuation to L and since $\boldsymbol{k}_L/k$ is algebraic and $\Gamma(L)$ is contained in the divisible hull of $\Gamma(K)$ by Exercise 1.8 (see also Lemma 3.16). But k is algebraically closed and Γ is divisible, thus L/K is immediate. But we saw in Lemma 2.46 that Hahn fields have no proper immediate extensions. Thus K is algebraically closed.

ii) If k is real closed, then $k^{\mathrm{alg}}(((\Gamma)))$ is a degree 2 algebraic extension of $k(((\Gamma)))$. Thus by the work of Artin and Schreier (see for example [26] XI §2 Proposition 3), $k(((\Gamma)))$ is real closed. □

We will prove much more general of these results later.

If L/K is a finite algebraic extension and $[L : K] = d$, then the argument above shows that $[\Gamma_L : \Gamma_K] \leq d$ and $[\boldsymbol{k}_L : \boldsymbol{k}_K] \leq d$. We will prove a much sharper bound. We let $e = [\Gamma_L : \Gamma_K]$ be the *ramification index* and $f = [\boldsymbol{k}_L : \boldsymbol{k}_K]$ be the *residue degree* . Note that if $e = f = 1$, then L is an immediate extension of K.

Theorem 3.18 (Fundamental Inequality) *If L/K is a finite algebraic extension of degree d then $ef \leq d$.*

Proof Choose $x_1, \ldots, x_e \in L$ such that $v(x_1), \ldots, v(x_n)$ represent distinct cosets of Γ_L/Γ_K. Choose $y_1, \ldots, y_f \in L$ such that $\overline{y}_1, \ldots, \overline{y}_f$ is a basis for $\boldsymbol{k}_L/\boldsymbol{k}_K$. It suffices to show that $(x_i y_j : i \leq e, j \leq f)$ are linearly independent over K.

Suppose

$$\sum_{i \leq e, j \leq f} a_{i,j} x_i y_j = 0$$

where not all $a_{i,j} = 0$. Pick $\widehat{i}$ and $\widehat{j}$ such that

$$v(a_{\widehat{i},\widehat{j}} x_{\widehat{i}}) = \min\{v(a_{i,j} x_i) : i \leq e, j \leq f\}.$$

Suppose $i \neq \widehat{i}$ and $j \leq f$. We claim that $v(a_{\widehat{i},\widehat{j}} x_{\widehat{i}}) < v(a_{i,j} x_i)$. If they were equal then

$$v(x_{\widehat{i}}) - v(x_i) = v(a_{i,j}) - v(a_{\widehat{i},\widehat{j}}) \in \Gamma_K,$$

contradicting that $v(x_{\widehat{i}})$ and $v(x_i)$ represent different cosets. Thus $v(a_{\widehat{i},\widehat{j}}x_{\widehat{i}}) < v(a_{i,j}x_i)$ for $i \neq \widehat{i}$.

Let $b_{i,j} = \frac{a_{i,j}}{a_{\widehat{i},\widehat{j}}}x_{\widehat{i}}$. Then

$$0 = \sum_{j=1}^{f}\sum_{i=1}^{e} b_{i,j}\frac{x_i}{x_{\widehat{i}}}y_j$$

and $b_{i,j}\frac{x_i}{x_{\widehat{i}}} \in \mathfrak{m}_L$ for $i \neq \widehat{j}$. Thus

$$\sum_{j=1}^{f}\frac{a_{\widehat{i},j}}{a_{\widehat{i},\widehat{j}}}y_j = -\sum_{j=1}^{f}\sum_{i\neq\widehat{i}} b_{i,j}x_iy_j \in \mathfrak{m}_L.$$

Let $c_{\widehat{i},j} = \mathrm{res}(a_{\widehat{i},j}/a_{\widehat{i},\widehat{j}})$. Then $c_{\widehat{i},\widehat{j}} = 1$ and

$$\sum_{j=1}^{f} c_{i,j}\overline{y}_j = 0,$$

contradicting that $\overline{y}_1, \ldots, \overline{y}_f$ are linearly independent over $\boldsymbol{k}_K$. $\square$

Exercise 3.19 Show that even if L/K is an infinite algebraic extension the argument above shows that if $(x_i : i \in I)$ represent distinct cosets of Γ_L/Γ_K and $(y_j : j \in J)$ are such that $(\overline{y}_j : j \in J)$ are linearly independent over $\boldsymbol{k}_K$, then $(x_iy_j : i \in I, j \in J)$ are linearly independent and $v(\sum a_{i,j}x_iy_j) = \min v(a_{i,j}x_iy_j)$.

Definition 3.20 If $K \subset L$ are fields and L/K is algebraic, we say that L/K is *normal* if L is a splitting field for every irreducible $f \in K[X]$ with a zero in L.

A separable normal extension is a *Galois extension.* Thus in characteristic 0 normal and Galois are the same. But in characteristic p we can build nonseparable normal extensions by taking p^{th}-roots.

Our goal for the rest of this section is to show that if L/K is a normal extension and $\mathcal{O}$ is a valuation ring of K, then the valuation rings of L extending $\mathcal{O}$ are all conjugate under the action of the Galois group.

We need a form of the Chinese Remainder Theorem.

Lemma 3.21 *Let A be a domain and let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be distinct maximal ideals of A. Then for any $a_1, \ldots, a_n$ we can find $a \in A$ such that $a = a_i (\mathrm{mod}\ \mathfrak{m}_i)$ for all i.*

Proof

claim For each i we can find b_i such $b_i = 1(\mathrm{mod}\ \mathfrak{m}_i)$ but $b_i \in \mathfrak{m}_j$ for $j \neq i$.

For notational simplicity assume $i = 1$. If $j \neq 1$ then $\mathfrak{m}_1 + \mathfrak{m}_j = A$, as otherwise $\mathfrak{m}_1 + \mathfrak{m}_j$ is an ideal, contradicting maximality. Thus there is $c_j \in \mathfrak{m}_1$ and $d_j \in \mathfrak{m}_j$ such that $c_j + d_j = 1$. Then

$$1 = \prod_{j\neq1}(c_j + d_j) = \prod_{j\neq1} d_j (\mathrm{mod}\ \mathfrak{m}_1).$$

Let $b_1 = \prod_{j \neq 1} d_j$. Then $b_1 = 1 (\mathrm{mod}\ \mathfrak{m}_1)$ but $b_1 \in \mathfrak{m}_i$ for $i \neq \jmath$.

Let $a = \sum a_i b_i$. Then $a = a_i (\mathrm{mod}\ \mathfrak{m}_i)$ for all i. □

Lemma 3.22 *Let A be a local domain integrally closed in its fraction field K and let L/K be normal. Let B be the integral closure of A in L. Then any two maximal ideals of B are conjugate under* $\mathrm{Gal}(L/K)$.[3]

Proof It suffices to prove this when L/K is finite. Let $\mathfrak{m}_0$ and $\mathfrak{m}_1$ be maximal ideal of B and suppose there is no $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma(\mathfrak{m}_1) = \mathfrak{m}_2$. Let $X_i = \{\sigma(\mathfrak{m}_i) : \sigma \in \mathrm{Gal}(L/K)\}$ then $X_0 \cap X_1 = \emptyset$. By the Chinese Remainder Theorem, we can find $b \in B$ such that $b \in \mathfrak{m}$ for $\mathfrak{m} \in X_0$ and $b = 1(\mathrm{mod}\ \mathfrak{m})$ for $\mathfrak{m} \in X_1$. Thus $\sigma(b) \in \mathfrak{m}_0 \setminus \mathfrak{m}_1$ for all $\sigma \in \mathrm{Gal}(L/K)$.

For the remainder of the proof we will assume that our fields have characteristic zero. One needs to be slightly more careful in characteristic p when we have an inseparable extension. Suppose $f(X) = X^d + \sum_{n=0}^{d-1} a_i X^i$, $a_0, \dots, a_{d-1} \in A$ be the minimal polynomial of b over K.. Since L/K is normal, $f(X) = \prod_{i=1}^{d} (X - \beta_i)$ where $\beta_1, \dots, \beta_d \in L$ are the distinct roots or f, i.e., the set of conjugates of b under $\mathrm{Gal}(L/K)$. Without loss of generality, we assume $L = K(\beta_1, \dots, \beta_d)$. Then

$$\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(b) = \prod_{i=1}^{d} \beta_i = a_0 \in A.$$

Each $\sigma(b) \in \mathfrak{m}_0$. Thus $a_0 \in \mathfrak{m}_0 \cap A = \mathfrak{m}_A \subseteq \mathfrak{m}_1$. But no $\sigma(b) \in \mathfrak{m}_1$, thus, since $\mathfrak{m}_1$ is prime $a_0 \notin \mathfrak{m}_1$, a contradiction. □

Lemma 3.23 *Let A be a valuation ring with fraction field K, let $L \supseteq K$ be an algebraic extension and let B be the integral closure of A in L. For every valuation ring $\mathcal{O} \subset K$ with $\mathfrak{m}_A \subseteq \mathfrak{m}_{\mathcal{O}}$ there is $\mathfrak{n}$ a maximal ideal of B with $\mathcal{O} = B_{\mathfrak{n}}$.*

Moreover, for every maximal ideal $\mathfrak{n} \subset B$, $B_{\mathfrak{n}}$ is a valuation ring.

Proof Let $\mathcal{O}$ be a valuation ring of L with $\mathfrak{m}_A \subseteq \mathfrak{m}_{\mathcal{O}}$. Since $\mathcal{O}$ is integrally closed in L, $B \subseteq \mathcal{O}$. Let $\mathfrak{n} = \mathfrak{m}_{\mathcal{O}} \cap B$.

If $x \in B \setminus \mathfrak{n}$, then $1/x \in \mathcal{O}$. Thus $B_{\mathfrak{n}} \subseteq \mathcal{O}$. Let $x \in \mathcal{O}$. Since L/K is algebraic, there are $a_0, \dots, a_d \in A$ not all zero such that $\sum a_i x^i = 0$. Let $m \leq d$ be maximal such that $v(a_m) = \min(v(a_i) : i = 0, \dots, d)$ and divide $\sum a_i x^i$ by $a_m x^m$. Thus, letting $b_i = a_i / a_m$ we have

$$\sum_{i=m+1}^{d} b_i x^{i-m} + 1 + \sum_{i=0}^{m-1} b_i x^{i-m} = 0.$$

Note that $b_0, \dots, b_{m-1} \in A$ and $b_{m+1}, \dots, b_d \in \mathfrak{m}_A$. Let $y = \sum_{i=m+1}^{d} b_i x^{i-m} + 1$ and $z = \sum_{i=0}^{m-1} b_i x^{i-m+1}$. Then $xy = -z$ and y is a unit in $\mathcal{O}$.

[3]We use $\mathrm{Gal}(L/K)$ to denote the group of automorphism of L/K even when L/K is not necessarily a Galois extension.

We claim that $y, z \in B$. Since B is the integral closure of A in L, by Lemma 3.15, it suffices to show that $x, y \in V$ for any valuation ring $V \subset \mathcal{L}$ with $\mathfrak{m}_V \cap A = \mathfrak{m}_A$. If $x \in V$, then $y \in V$ and $z = -xy \in V$. If $x \notin V$, then $1/x \in V$, $z = \sum_{i=0}^{m-1} b_i x^{i-m+1} \in V$ and $y = -z/x \in V$.

Since y is a unit in $\mathcal{O}$, $y \notin \mathfrak{n}$. Thus $x = -z/y \in B_{\mathfrak{n}}$. Thus $B_{\mathfrak{n}} = \mathcal{O}$.

To prove the last claim of the lemma we need to show that if $\mathfrak{n}$ is a maximal ideal of B, then $B_{\mathfrak{n}}$ is a valuation ring extending A. Clearly $\mathfrak{n} \cap A = \mathfrak{m}_A$. By Chevalley's Theorem, there is a valuation ring $\mathcal{O}$ such that $B \cap \mathfrak{m}_{\mathcal{O}} = \mathfrak{n}$. Then by the first part of the lemma $\mathcal{O} = B_{\mathfrak{n}}$. □

We summarize the last few lemmas.

Theorem 3.24 *Let A be a valuation ring with fraction field K, let $L \supseteq K$ be an algebraic extension and let B be the integral closure of A in L. There is a bijective correspondence $\mathfrak{m} \mapsto B_{\mathfrak{m}}$ between maximal ideals of B and valuation rings $\mathcal{O} \subset L$ with $\mathfrak{m}_O \cap A = \mathfrak{m}_A$. Moreover, if L/K is normal, then any two such valuation rings are conjugate under* $\mathrm{Gal}(L/K)$.

Corollary 3.25 *Let $(K, \mathcal{O})$ be a valued field and let L/K be a purely inseparable algebraic extension of K. Then there is a unique valuation ring $\mathcal{O}^*$ on L with $(K, \mathcal{O}) \subseteq (L, \mathcal{O}^*)$.*

Proof L is obtained from K by adjoining p^{th}-roots where K has characteristic p. Then L/K is normal but there are no nontrivial automorphisms of L fixing K. □

4 Algebraically Closed Valued Fields

4.1 Quantifier Elimination for ACVF

We now have developed enough machinery to begin the study of the model theory of algebraically closed valued fields.

Valued fields as structures

The first issue is deciding what kind of structure we are looking at, i.e., what language or signature do we use to study valued fields? There are several natural candidates.

One-sorted structures
We can think of valued fields as pairs $(K, \mathcal{O})$ where K is the field and $\mathcal{O}$ is the valuation ring. In this case the natural language would be the usual language of rings $\{+, -, \cdot, 0, 1\}$ together with a unary predicate $\mathcal{O}$ which picks out the valuation.

Three-sorted structures
We can think of valued fields as three-sorted structures $(K, \Gamma, \boldsymbol{k})$ where we have separate sorts for the field (which we refer to as the *home sort*, the value group and the residue field. On the home sort and on the residue field we will have the $+, -, \cdot, 0$, and 1. On the group we will have $+, -, <, 0$. We also have the valuation map v and the residue map res. [4]

It would also be natural to think of valued fields as two sorted structure (K, Γ) and later we will consider adding more imaginary sorts.
How does this effect definability? It's easy to see that it doesn't.

Lemma 4.1 *In the one-sorted structure $(K, \mathcal{O})$ we can interpret the value group Γ, the residue field $\boldsymbol{k}$ and the maps $v : K^\times \to \Gamma$ and $\mathrm{res} : \mathcal{O} \to \boldsymbol{k}$. Thus any subset of K^n definable in the three-sorted structure is definable in the one-sorted structure. Moreover if $X \subseteq K^l \times \Gamma^m \times \boldsymbol{k}^n$ is definable in the three-sorted structure, then there is $A \subseteq K^{l+m+n}$ definable in $(K, \mathcal{O})$ such that*

$$X = \{(a_1, \ldots, a_l), v(a_{l+1}, \ldots, v(a_{l+m}), \mathrm{res}(a_{l+m+1}), \ldots, \mathrm{res}(a_{l+m+n}) : (a_1, \ldots, a_{l+m+n}) \in A.$$

In the three-sorted structure (K, Γ, v) we can define the value ring $\mathcal{O} = \{x \in K : v(x) \geq 0\}$. Thus any subset of K^n definable in the one-sorted structure is definable in the three-sorted structure.

We will also look at further variants of these languages.

- When studying the p-adic field $\mathbb{Q}_p$, we have already shown in Exercise 2.11 that $\mathbb{Z}_p$ is definable in the field language. Thus any subset of $\mathbb{Q}_p^n$ definable in $(\mathbb{Q}_p, \mathbb{Z}_p)$ is already definable in $\mathbb{Q}_p$ in the field language. The exercises below show that this is not always possible.

[4] Note we should think of they symbols on each sort as being distinct, so while we routinely use $+$ on $K, \boldsymbol{k}$ and Γ, if we were more careful we would think of them as three distinct symbols.

- To prove quantifier elimination for algebraically closed valued fields we will work in the language of divisibility

$$\mathcal{L}_{\text{div}} = \{+, -, \cdot, \mathcal{O}, |, 0, 1\}$$

where $|$ is a binary function symbol which we interpret

$$(K, \mathcal{O}) \models x|y \text{ if and only if } \exists z \in \mathcal{O}\ xz = y.$$

The relation $x|y$ is definable in $(K, \mathcal{O})$ thus any subset of K^n definable in the language $\mathcal{L}_{\text{div}}$ is already definable in $(K, \mathcal{O})$.

Note that once we have added $|$ to the language we could get rid of $\mathcal{O}$ since $x \in \mathcal{O}$ if and only if $1|x$.

- To prove quantifier elimination for $\mathbb{Q}_p$ we will work in the *Macintyre Language* $\mathcal{L}_{\text{Mac}} = \{+, -, \cdot, \mathcal{O}, 0, 1, P_2, P_3, P_4, \dots\}$ where P_n is a unary predicate predicate which we interpret in $(\mathcal{K}, \mathcal{O})$ as the n^{th} powers of K. Since $x \in P_n$ if and only if $K \models \exists y\ y^n = x$, any subset of K^n definable in $\mathcal{L}_{\text{Mac}}$ is already definable using $\mathcal{L}$. Indeed in $\mathbb{Q}_p$ we can define $\mathbb{Z}_p$ in a quantifier free way using P_2 as in Exercise 2.11. Thus we don't really need the predicate for $\mathcal{O}$.

- In the original work of Ax and Kochen it was useful to work in the three-sorted language and add a symbol for $\pi : \Gamma \to K$ a section of the valuation. This is more problematic. We saw in Exercise 2.34 that not every valued field has a section. Moreover we will show that the section map is not definable in the three-sorted language. Thus, while adding the section can be useful, we will end up with new definable sets.

- An *angular component* map is a multiplicative homomorphism $\mathrm{ac} : K^\times \to \boldsymbol{k}^\times$ such that ac agrees with the residue map on the units. For example on $\mathbb{Q}_p$ if $v_p(x) = m$ then $x = a_m p^m + a_{m+1} p^{m+1} + \dots$ and we can let $\mathrm{ac}(x) = a_m$. Similarly, there is an angular component map on $K((T))$.

  If we have a section $\pi : \Gamma \to K$, then we can define an angular component map by $\mathrm{ac}(x) = \mathrm{res}(x/\pi(x))$. But, like sections, angular component maps need not exist and, even when they do exist, may change definability.

  Nevertheless, we will find it useful to work in the three-sorted language $\mathcal{L}_{\text{Pas}}$ where we add a symbol for an angular component map. This is called the *Pas language*

Exercise 4.2 Let $(K, \mathcal{O})$ be a valued field where K is algebraically closed or real closed. Show that $\mathcal{O}$ is not definable in K in the pure field language.

Exercise 4.3 Suppose $\pi : \Gamma \to K$ is a section of the valuation. Show that $\mathrm{ac}(x) = \mathrm{res}(x/\pi(x))$ is an angular component map.

Quantifier Elimination

We will prove quantifier elimination for algebraically closed valued fields in the language $\mathcal{L}_{\mathrm{div}}$. Let ACVF be the $\mathcal{L}_{\mathrm{div}}$-theory such that $(K, \mathcal{O}, |) \models$ ACVF if and only if K is an algebraically closed field with valuation ring $\mathcal{O}$ and $x|y$ if and only if there is $z \in \mathcal{O}$ such that $zx = y$. We will also assume that the valuation is nontrivial so there is $x \in K^{\times} \setminus \mathcal{O}$.

Theorem 4.4 (Robinson) *The theory of algebraically closed fields with a non-trivial valuation admits quantifier elimination in the language $\mathcal{L}_{\mathrm{div}}$.*[5]

Quantifier elimination will follow from the following proposition.

Proposition 4.5 *Suppose (K, v) and (L, w) are algebraically closed fields with non-trivial valuation and L is $|K|^+$-saturated. Suppose $R \subseteq K$ is a subring, and $f : R \to L$ is an $\mathcal{L}_{\mathrm{div}}$-embedding. Then f extends to a valued field embedding $g : K \to L$.*

Exercise 4.6 Show that the proposition implies quantifier elimination. [Hint: See [30] 4.3.28.]

We will prove the Proposition via a series of lemmas.

Definition 4.7 Suppose R is a subring of K. We say that a ring embedding $f : R \to L$ is an $\mathcal{L}_{\mathrm{div}}$-embedding if for $a, b \in R$,

$$R \models a|b \Leftrightarrow w(f(a)) \leq w(f(b)).$$

First, we show that without loss of generality we can assume R is a field.

Lemma 4.8 *Suppose (K, v) and (L, w) are valued fields, $R \subseteq K$ is a subring and $f : R \to L$ is and $\mathcal{L}_{\mathrm{div}}$-embedding. Then f extends to a valuation preserving embedding of K_0, the fraction field of R into L.*

Proof Extend f to K_0, by $f(a/b) = f(a)/f(b)$. If $x \in K_0$, then x is a unit in (K, v) if and only if $x|1$ and $1|x$ if and only in $f(x)$ is a unit in (L, w). Since the value group is given by $K^{\times}/U$, addition in the value group is preserved. So we need only show that the order is preserved.

Suppose $x, y \in K_0$. There are $a, b, c \in R$ such that $x = \frac{a}{c}$ and $y = \frac{b}{c}$. Then

$$v(x) \leq v(y) \Leftrightarrow v(a) \leq v(b) \leq R \models a|b \Leftrightarrow L \models f(a)|f(b) \Leftrightarrow w(f(x)) \leq w(f(y)).$$

$\square$

We next show that we can extend embedding from fields to their algebraic closures.

[5] Actually, Robinson only proved model completeness, but his methods extend to prove quantifier elimination.

Lemma 4.9 *Suppose (K, v) and (L, w) are algebraically closed valued fields, $K_0 \subseteq K$ is a field and $f : K_0 \to L$ is a valuation preserving embedding. Then f extends to a valuation preserving embedding of K_0^{alg}, the algebraic closure of K_0 into L.*

Proof It suffices to show that if $x \in K \setminus K_0$ is algebraic over K_0, then we can extend f to $K_0(x)$. Let $K_0(x) \subseteq F \subseteq K$ with F/K_0 normal. There is a field embedding $g : F \to L$ with $g \supset f$ and $g(v)$ gives rise to a valuation on $g(F)$ extending $f(v|K_0)$. Then $g(v|F)$ and $w|g(F)$ are valuations on $g(F)$ extending $f(v|K_0)$ on $f(K_0)$. By Theorem 3.24, there is $\sigma \in \mathrm{Gal}(g(F)/f(K_0))$ mapping $g(v|F)$ to $w|g(F)$. Thus $\sigma \circ g$ is the desired valued field embedding of F into L extending f. $\square$

Thus in proving Proposition 4.5 it suffices to show that if we have (K, v) and (L, w) non-trivially valued algebraically closed fields, L is $|K|^+$-saturated, $K_0 \subset K$ algebraically closed and $f : K_0 \to L$ a valuation preserving embedding, then we can extend f to K. There are three cases to consider.

case 1 Suppose $x \in K$, $v(x) = 0$ and $\overline{x}$ is transcendental over $\boldsymbol{k}_{K_0}$.

We will show that we can extend f to $K_0[x]$, then use Lemmas 4.8 and 4.9 to extend to $K_0(x)^{\mathrm{acl}}$. Since L is $|K|^+$-saturated, there is $y \in L$ such that $\overline{y}$ is transcendental over $\boldsymbol{k}_{f(K_0)}$. We will send x to y.

Suppose $a = m_0 + a_1x + \cdots + m_nx^n$, where $m_i \in K_0$. Suppose m_l has minimal valuation. Then $a = m_l(\sum b_ix^i)$ where $v(b_i) \geq 0$ and $b_l = 1$. Then $v(\sum b_ix^i) \geq 0$. If $v(\sum b_ix^i) > 0$, then taking residues we see that

$$\sum \overline{b}_i\overline{x}^i = 0,$$

but $\overline{b}_l = 1$, so this is a nontrivial polynomial and $\overline{x}$ is algebraic over $\boldsymbol{k}_{K_0}$. Thus $v(\sum b_ix^i) = 0$ and $v(a) = m_l$.

Thus $v(a) = \min\{v(m_i) : i = 0, \ldots, n\}$. Similarly, in L, $w(\sum f(m_i)y^i) = \min\{w(f(m_i)) : i = 0, \ldots, n\}$. Thus the extension of f to $K_0[x]$ is and $\mathcal{L}_d$-embedding.

case 2 Suppose $x \in K$ and $v(x) \notin v(K_0)$.

Let $\gamma = v(x)$. Suppose $a, b \in K_0$, $i < j$ are in $\mathbb{N}$, and $v(a) + i\gamma = v(b) + j\gamma$. Since K_0 is algebraically closed there is $c \in K_0$ such that $c^{j-i} = \frac{a}{b}$, but then $\gamma = v(c) \in v(K_0)$.

Suppose $a \in K_0[x]$ and $a = m_0 + m_1x + \ldots m_nx^n$. Since the $v(m_i) + i\gamma$ are distinct, $v(a) = \min(v(m_i) + i\gamma)$.

Since L is $|K|^+$-saturated, there is $y \in L$ realizing the type

$$\{w(f(a)) < w(y) : a \in K_0, v(a) < v(x)\} \cup \{w(y) < w(f(b)) : v(x) < v(a)\}.$$

Then $v(a)+iv(x) < v(b)+jv(x)$ if and only if $w(f(a))+iw(y) < w(f(b))+jw(y)$ for all $a, b \in K_0$ and the extension of f to $K_0[x]$ sending x to y is and $\mathcal{L}_{\mathrm{div}}$-embedding.

case 3 Suppose $x \in K \setminus K_0$, $v(K_0(x)) = v(K_0)$ and $\boldsymbol{k}_{K_0(x)} = \boldsymbol{k}_{K_0}$, i.e., $K_0(x)$ is an *immediate* extension of K_0.

Let $C = \{v(x-a) : a \in K_0\}$. Since $v(K_0(x)) = v(K_0)$, $C \subseteq v(K_0)$. We claim that C has no maximal element. Suppose $v(b) \in C$ is maximal. Then $v(\frac{x-a}{b}) = 0$ and, since $\boldsymbol{k}_{K_0} = \boldsymbol{k}_{K_0(x)}$, there is $c \in K_0$ such that $\frac{x-a}{b} - c = \epsilon$ where $v(\epsilon) > 0$. But then,

$$v(x - a - bc) = v(b\epsilon) > v(b),$$

a contradiction.

Consider the type

$$\Sigma(y) = \{w(y - f(a)) = w(b) : a, b \in K_0, v(x-a) = v(b).\}$$

We claim that Σ is finitely satisfiable. Suppose $a_1, \ldots, a_n, b_1, \ldots, b_n \in K_0$ and $v(x - a_i) = v(b_i)$. Because f is valuation preserving it suffices to find $c \in K_0$ with $v(c - a_i) = v(b_i)$ for $i = 1, \ldots, n$. Since C has no maximal element, there is $c \in K_0$ such that $v(x-c) > v(b_i)$ for $i = 1, \ldots, n$. Then $v(c - a_i) = v(x - a_i) = v(b_i)$.

By sending x to y we can extend f to a ring isomorphism between $K_0[x]$ and $f(K_0)[y]$. For $a \in K_0(x)$, there is $p(X) \in K_0[X]$ such that $d = p(x)$. Factoring p into linear factors over the algebraically closed field K_0, there is $a_0, \ldots, a_n$ such that

$$d = p(x) = a_0 \prod_{i=1}^{n} (x - a_i).$$

For each i we can find $b_i \in K_0$ such that $v(x - a_i) = v(b_i)$. Thus

$$v(d) = v(a_0) + \sum_{i=1}^{n} v(b_i)$$

By choice of y, we also have

$$w(f(d)) = w(f(a_0)) + \sum_{i=1}^{n} w(f(b_i)),$$

thus f preserves the valuation.

This concludes the proof of Proposition 4.5 and hence the proof that ACVF has quantifier elimination in the language $\mathcal{L}_{\text{div}}$.

The proofs we have given can readily be adapted to prove quantifier elimination in the three-sorted language.

Exercise 4.10 Modify the proofs above to verify that algebraically closed fields have quantifier elimination when viewed as three-sorted structures in the usual language.

4.2 Consequences of Quantifier Elimination

Completions of ACVF

ACVF is not a complete theory. We need to specify the characteristic of the field K and the residue field $\boldsymbol{k}$. If K has characteristic p, then $\boldsymbol{k}$ has characteristic p. If K has characteristic 0, the $\boldsymbol{k}$ may have any characteristic. Let a be either 0 or a prime. If $a = p$ a prime, then $b = p$. If a is zero, then b is either zero or a prime. Let $\mathrm{ACVF}_{a,b}$ be ACVF with additional axioms asserting the field has characteristic a and the residue field has characteristic b.

Corollary 4.11 *Each theory* $\mathrm{ACVF}_{a,b}$ *is complete and these are exactly the completions of* ACVF.

Proof If $(a, b) = (0, 0)$ let $R = (\mathbb{Q}, \mathbb{Q}, |)$. If $(a, b) = (0, p)$ let $R = (\mathbb{Q}, \mathbb{Z}_{(p)}, |)$ and if $(a, b) = (p, p)$, let $R = (\mathbb{F}_p, \mathbb{F}_p, |)$. Suppose $(K, \mathcal{O}_K, |)$ and $(L, \mathcal{O}_L, |)$ are models of $\mathrm{ACVF}_{a,b}$. Then R is a common substructure of both fields. Let ϕ be an $\mathcal{L}_{\mathrm{div}}$-sentence. Then there is a quantifier free $\mathcal{L}_{\mathrm{div}}$-sentence such that

$$\mathrm{ACVF} \models \phi \leftrightarrow \psi.$$

But then, since ψ is quantifier free,

$$K \models \phi \Leftrightarrow K \models \psi \Leftrightarrow R \models \psi \Leftrightarrow L \models \psi \Leftrightarrow K \models \phi.$$

Thus $\mathrm{ACVF}_{a,b}$ is complete.

We have listed the only possibilities for the characteristics of the field and residue field. Thus these are the only possible completions of ACVF.[6] □

Definable subsets of K

In any valued field we can always define open and closed balls and any finite boolean combination of balls.[7] We will show that in an algebraically closed valued field these are the only definable subsets of K.

Lemma 4.12 *Let (K, v) be an algebraically closed valued field. Suppose $f \in K[X]$. Then we can partition K into finitely many sets each of which is a finite boolean combination of balls such that that for each Y in the partition there are $n \geq 1$, $a \in K$ and $\gamma \in \Gamma$ in the value group such that $v(f(x)) = nv(x - a) + \gamma$ for all $x \in Y$.*

Proof Let $f(X) = c(X - a_1) \cdots (X - a_n)$ for $c \in K^\times$ and $a_1, \ldots, a_n \in K$. Then $v(f(x)) = v(c) + \cdots + v(x - a_1) + \cdots + v(x - a_n)$. We will show that we can partition K such that on each set in the partition there is i such that either

[6] Here we are using the assumption that our fields have nontrivial valuations. If we were to also consider the trivial valuation we would have completions saying that I have a trivial valued field of characteristic 0 or p. But these are just the completions of ACF.

[7] Here we allow trivial balls $K = \{x : v(x) < \infty\}$ and $\{a\} = \{x : v(x) = \infty\}$. If we don't want to do this, we should look at boolean combinations of points and balls instead.

$v(x - a_j) = v(x - a_i)$ for each set in the partition or $v(x - a_j)$ is constant on the partition.

For each partition I, J of $\{1, \ldots, n\}$ where I is nonempty, let $\widehat{i}$ be the least element of I. Let

$$Y_{I,J} = \{x \in K : v(x - a_i) = v(x - a_{\widehat{i}}) > v(x - a_j) \text{ for } i \in I, j \in J\}.$$

Then the sets $Y_{I,J}$ are boolean combinations of balls and they partition K (of course some $Y_{I,J}$ might be empty.

For $j \neq \widehat{i}$ let $\gamma_j = v(a_{\widehat{i}} - a_j)$. Then

- if $v(x - a_{\widehat{i}}) < \gamma_j$, then $v(x - a_j) = v(x - a_{\widehat{i}})$
- If $v(x - a_{\widehat{i}}) > \gamma_j$, then $v(x - a_j) = \gamma_j$
- We can not have $v(x - a_{\widehat{i}}) = \gamma_j$, as then $v(x - a_j) \geq \gamma_j$, contradicting $x \in Y_{I,J}$.

This allows to partition $Y_{I,J}$ into finitely many pieces each of which is a boolean combination of balls, such $v(x - a_j)$ is either $v(x - a_{\widehat{i}})$ or constant on each set in the partition. $\square$

Exercise 4.13 Show that if (K, v) is algebraically closed and $f, g \in K[X]$, then $\{x \in K : v(f(x)) \leq v(g(x))\}$ is a finite Boolean combination of balls.

Corollary 4.14 *If $(K, \mathcal{O}) \models$ ACVF and $X \subseteq K$ is definable, then X is a finite boolean combination of balls.*

Proof By quantifier elimination any definable subset of X is a finite boolean combination of sets of the form $\{x : f(x) = g(x)\}$ and $\{x : f(x)|g(x)\} = \{x : v(f(x)) \leq v(g(x))\}$ for $f, g \in K[X]$. $\square$

Definition 4.15 A *swiss cheese* is a definable set of the form $B \setminus (C_1 \cup \cdots \cup C_n)$ where $B, C_1, \ldots, C_n$ are balls and $C_i \subset B$ (and we allow the possibilities where $B = K$ or $\emptyset$, $n = 0$ and some B or C_i is a point.)

Exercise 4.16 a) Show the intersection of two swiss cheese is a finite disjoint union of swiss cheese.

b) Show that the complement of a swiss cheese is a finite disjoint union of swiss cheese.

c) Prove that every definable subset of K can be written in a unique way as a finite union of disjoint swiss cheese.

Corollary 4.17 *i) Any infinite definable subset of K has interior.*

ii) There is no definable section of the value group.

Proof i) Any infinite definable set will contain a swiss cheese $S = B \setminus (C_1 \cup \cdots \cup C_m)$, where $B \neq \emptyset$. If $a \in S$, then S contains a ball U with $a \in U$.

ii) The image of the section would be infinite with no interior. $\square$

Exercise 4.18 Suppose K is an algebraically closed valued field and $A \subseteq K^{m+n}$ is definable. For $x \in K^m$ let $A_x = \{y \in K^n : (x, y) \in A\}$. Show that $\{x : A_x$

is finite$\}$ is definable and that there is an N such that if A_x is finite, then $|A_x| \leq N$.

Exercise 4.19 Let $A \subset K$. Show that the model theoretic algebraic closure of A is the field theoretic algebraic closure of A.

In Exercise 5.25 we will characterize definable closure in ACVF.

Exercise 4.20 Let (K, v) be an algebraically closed valued field. Prove that there is no definable angular component map.

NIP

Let $\mathcal{M}$ be a structure. Recall that $\phi(x_1, \ldots, x_m, y_1, \ldots, y_n)$ has the *independence property* if for all k there are $\bar{b}_1, \ldots, \bar{b}_k \in \mathcal{M}^m$ and $(\bar{c}_J : J \subset \{1, \ldots, k\})$ in $\mathcal{M}^n$ such that

$$\mathcal{M} \models \phi(\bar{b}_i, \bar{c}_J) \Leftrightarrow i \in J).$$

In which case we say that ϕ *shatters* $\bar{b}_1 \ldots, \bar{b}_k$. Otherwise we say ϕ has NIP.

We say that a theory has NIP if no formula has the independence property. We need two basic facts about NIP. See [39] 2.9 and 2.11.

Lemma 4.21 *i) T has* NIP *if and only if every formula $\phi(x_1, y_1, \ldots, y_n)$ has NIP.*

ii) A boolean combination of NIP formulas has NIP.

Corollary 4.22 ACVF *has NIP.*

Proof By the lemma above and Corollary 4.14, it suffices to show that no definable family of balls has the independence property. We claim that the family of all balls can not shatter a set of size 3. Suppose a, b and $c \in K$ are distinct and, without loss of generality, $v(a-b) \leq v(a-c), v(b-c)$. Then any ball that contains a and b contains c. Thus the family of all balls does not shatter any three element set. □

Definable subsets of the value group and residue field

To study definable subsets of $\boldsymbol{k}^m$, Γ^n and, more generally $\boldsymbol{k}^m \times \Gamma^n$ we need to apply quantifier elimination in the three-sorted language. We will let variables $x_0, x_1, \ldots$ range over the home sort, while $y_0, y_1, \ldots$ ranges over the residue field and $z_0, z_1, \ldots$ range over the value group. Any atomic formula is equivalent to one in one of the following forms

- $t(x_0, \ldots, x_m) = 0$, where t is a polynomial over $\mathbb{Z}$;
- $t(y_0, \ldots, y_n, \mathrm{res}(x_0), \ldots, \mathrm{res}(x_m)) = 0$, where t is a polynomial over $\mathbb{Z}$;
- $s(z_0, \ldots, z_l, v(x_0), \ldots, v(x_m)) = 0$, where $s(u_0, \ldots, u_{l+m+1}) = \sum r_i u_i$, $r_i \in \mathbb{Z}$;
- $s(z_0, \ldots, z_l, v(x_0), \ldots, v(x_m)) > 0$, where $s(u_0, \ldots, u_{l+m+1}) = \sum r_i u_i$, $r_i \in \mathbb{Z}$;

We say that $A \subseteq \boldsymbol{k}^n \times \Gamma^m$ is a *rectangle* if there is $B \subseteq \boldsymbol{k}^n$ definable in the field structure on $\boldsymbol{k}$ and $C \subseteq \Gamma^m$ definable in the ordered abelian group Γ such that $A = B \times C$.

Corollary 4.23 (Orthogonality) *Every definable subset of $\boldsymbol{k}^n \times \Gamma^m$ is a finite union of rectangles.*

Proof By quantifier elimination, every definable set is a finite union of sets defined by conjunctions of atomic and negated atomic formulas. But atomic formulas defining subsets of $\boldsymbol{k}^n \times \Gamma^m$ only have variables over just the residue field sort or just the value group sort and the definable set is either of the form $\boldsymbol{k}^n \times A$ or $B \times \Gamma^n$ where $A \subseteq \boldsymbol{k}^n$ is already definable in $\boldsymbol{k}$ or $B \subseteq \Gamma^m$ is already definable in Γ. Thus any set defined by a conjunction of atomic and negated atomic formulas is a rectangle and every definable set is a finite union of rectangles. $\square$

Corollary 4.24 *i) Any definable function $f : \boldsymbol{k} \to \Gamma$ has finite image.*
ii) Any definable function $g : \Gamma \to \boldsymbol{k}$ has finite image.

This shows that the residue field and value group are as unrelated as possible. It also shows that the valuation structure induces no additional definability on the residue field and value group.

Corollary 4.25 *i) Any subset of $\boldsymbol{k}^n$ definable in $(K, \Gamma, \boldsymbol{k})$ is definable in the field $\boldsymbol{k}$.*
ii) Any subset of Γ^m definable in $(K, \Gamma, \boldsymbol{k})$ is definable in the ordered abelian group Γ.

In this case $\boldsymbol{k}$ with all induced structure, is just a pure algebraically closed field and hence ω-stable, while Γ with all induced structure, is a divisible ordered abelian group and hence *o*-minimal.

Definition 4.26 We say that a sort S is *stably embedded* if any subset of S^n that is definable in the full structure is definable using parameters from S.

Corollary 4.27 *The residue field and value group of an algebraically closed field are stably embedded.*

In the next section we give an example of an imaginary sort that is not stably embedded.

Exercise 4.28 Let $A \subset \boldsymbol{k}$. Prove that if $b \in \boldsymbol{k}$ is algebraic over A in the three-sorted valued field structure, then b is algebraic over A in the field $\boldsymbol{k}$.

4.3 Balls

For this section we start by thinking of valued fields as three-sorted structures $(K, \Gamma, \boldsymbol{k})$, but this also makes sense if we think of them as one-sorted structures $(K, \mathcal{O})$.

For any valued field we can introduce two new sorts $\mathcal{B}_o$ and $\mathcal{B}_c$ for open and closed balls. For $\mathcal{B}_o$ define an equivalence relation $\sim$ on $K \times \Gamma$ such that $(a, \gamma) \sim (b, \delta)$ if and only if $\gamma = \delta$ and $\gamma = \delta$ and $v(a - b) > \gamma$. Then

$$(a, \gamma) \sim (b, \gamma) \Leftrightarrow b \in B_\gamma(a) \Leftrightarrow a \in B_\gamma(b).$$

Thus we can identify $(a, \gamma)/\sim$ with $B_\gamma(a)$. Let $\mathcal{B}_o = K \times \Gamma/\sim$. We can indentify $\mathcal{B}_o$ with the open balls of K. There is a definable map $r : \mathcal{B}_o \to \Gamma$ given by $r((a, \gamma)/\sim) = \gamma$, i.e., r assigns each ball it's radius. There is a definable relation R_o on $K \times \mathcal{B}_o$ such that aR_ob if and only if $a \in b$. Replacing $\sim$ by $(a, \gamma) \sim^* (b, \delta)$ on $K \times \Gamma \cup \{\infty\}$ if and only if $\gamma = \delta$ and $v(a - b) \geq \gamma$, we can similarly define the sort of closed balls $\mathcal{B}_c$.

Exercise 4.29 Let $a \in K$ and let $X \subset S$ be the set of all open balls containing a. Prove that X is not definable with parameters from $\mathcal{B}_o$. [Hint: Show that for any finite subset A of $\mathcal{B}_o$ there is an automorphism (possibly of a larger field) fixing A pointwise but moving X.]

While up to this point the construction makes sense in any valued field, henceforth we will assume K is algebraically closed.

Lemma 4.30 *If $X \subseteq \mathcal{B}_c$ is an infinite definable set then either $r|X$ is finite-to-one, or there is an infinite definable $Z \subseteq X$ and a definable surjection $f : Z \to \boldsymbol{k}$.*

Proof If $r|X$ is not finite-to-one, there is $\gamma \in \Gamma$ such that $Y = \{B \in X : r(B) = \gamma\}$ is infinite. Let $A = \bigcup_{B \in Y} B$. Then A is an infinite definable subset of K and if $a \in A$, then $\overline{B}_\gamma(a) \in Y$.

claim There is a closed ball $\overline{B}_\epsilon(a)$ with $\epsilon < \gamma$ such that every closed ball of radius γ in $\overline{B}_\epsilon(a)$ is in Y.

By quantifier elimination A is a finite disjoint union of sets of $W = B \setminus (C_1 \cup \cdots \cup C_m)$, where $B, C_1, \ldots, C_m$ are balls. Since Y is infinite, some B must have radius $\delta < \gamma$. If $a \in W$, then $B_\gamma(a) \subset W$. Let a_i be the center of C_i, then $\delta \leq v(a - a_i) < \gamma$ for all i. Choose ϵ such that $\delta \leq v(a - a_i) < \epsilon < \gamma$. Then $\overline{B}_\epsilon(a) \subset W \subseteq A$. Thus if $b \in \overline{B}_\epsilon(a)$, then $\overline{B}_\gamma(b) \in Y$.

Let Z be the set of closed balls of radius γ contained in $B_\epsilon(a)$. Then Z is an infinite set of closed balls and $Z \subseteq Y$.

If we choose $c \in K$ with $v(c) = -\epsilon$, then $g(x) = c(x-a)$ is a bijection between $\overline{B}_\epsilon(a)$ and $\mathcal{O}$. If $b_1, b_2 \in \overline{B}_\epsilon(a)$ such that $v(b_1 - b_2) \geq \gamma$, then $v(g(b_1) - g(b_2)) = v(b_1 - b_2) - \epsilon > 0$. Thus $\mathrm{res}(g(b_1)) = \mathrm{res}(g(b_2))$. Thus the map $B_\gamma(b) \mapsto \mathrm{res}(g(b))$ is a well defined map from Z onto $\boldsymbol{k}$. $\square$

Corollary 4.31 *Suppose $f : \Gamma \to \mathcal{B}_c$. Let X be the image of f. Then $r|X$ is finite-to-one.*

Proof If not there is an infinite $Z \subseteq X$ and a definable surjection $g : Z \to \boldsymbol{k}$. Let $A = f^{-1}(Z)$. Then $g \circ f|A$ is a definable map from an infinite definable subset of Γ onto k, a contradiction. $\square$

Lemma 4.32 *If $X \subseteq \mathcal{B}_c$ is infinite, there is a definable $f : X \to \Gamma$ with infinite image. In particular, the image of f contains a non-trivial interval.*

Proof First consider the image of X under the radius map. If this is infinite, then we are done. If not, then, without loss of generality we may assume that all balls in X have radius γ. Let $A = \bigcup_{B \in Y} B$. As the proof of Lemma 4.30, there is a closed ball $\overline{B}_\epsilon(a) \subset A$ with $\epsilon < \gamma$. If $x, y \in \overline{B}_\epsilon(a) \setminus \overline{B}_\gamma(a)$ such that $v(x - y) \geq \gamma$, then $v(x - a) = v(y - a)$. Thus we have a well defined function $f : X \to \Gamma$ such that

$$f(B) = \begin{cases} v(x-a) & \text{if } B \subset \overline{B}_\epsilon(a) \setminus \overline{B}_\gamma(a) \text{ and } a \in B \\ 0 & \text{otherwise} \end{cases}.$$

Then the image of f is an infinite subset of Γ. $\square$

We can extend this result to balls in n-spaces. Let $\gamma \in \Gamma$ and let $\mathbf{a} = (a_1, \ldots, a_n) \in \Gamma^n$. Then

$$\overline{B}_\gamma(\mathbf{a}) = \{\mathbf{b} \in K^n : \bigwedge v(a_i - b_i) \geq \gamma\}$$

is the closed ball around $\mathbf{a}$ of radius γ. Let $\mathcal{B}_c^n$ be the collection of all closed balls in K^n. Let $\pi : K^n \to K^{n-1}$ be the projection onto the first $n-1$ coordinates. If $B \in \mathcal{B}_c^n$ is a closed ball of radius δ, then $\pi(B) \in \mathcal{B}_c^{n-1}$ and if $\overline{B}_\delta(a_1, \ldots, a_{n-1}) \in \mathcal{B}_c^{n-1}$ then B is in the fiber $\pi^{-1}(B_1)$ if and only if

$$B = \overline{B}_\delta(a_1, \ldots, a_n) = \overline{B}_\delta(a_1, \ldots, a_{n-1}) \times \overline{B}_\delta(a_n)$$

for some $a_n \in K$. Thus the fiber is in definable bijection with an infinite subset of $\mathcal{B}_c$.

Corollary 4.33 *If $X \subseteq \mathcal{B}_c^n$ is infinite and definable, there is a definable function $f : X \to \Gamma$ with infinite image.*

Proof We proceed by induction on n, knowing the result is true for $n = 1$. Let $X \subset \mathcal{B}_c^{n-1}$. Consider the projection of X to $\mathcal{B}_c^n$. If this is infinite we are done. If not, some fiber is infinite. But this gives rise to an infinite subset of $\mathcal{B}_c$ and we are done. $\square$

Corollary 4.34 *If $X \subseteq K^n$ is infinite and definable, then there is a definable $f : X \to \Gamma$ with infinite image.*

Proof We have a definable injection $\mathbf{a} \mapsto \{\mathbf{a}\} = \overline{B}_\infty(\mathbf{a})$ of K^n into $\mathcal{B}_c^n$. Thus this follows from the previous corollary. $\square$

4.4 Real Closed Valued Fields

We next consider valued fields $(K, \mathcal{O})$ where K is a real closed field and $\mathcal{O}$ is a proper convex subring. We call $\mathcal{O}$ a *real closed ring* and we refer to $(K, \mathcal{O})$ as a real closed valued field. In a series of exercises we will prove the following theorem of Cherlin and Dickmann.

Theorem 4.35 *The theory of theory of real closed valued fields admits quantifier elimination in the language* $\mathcal{L}_{\mathrm{div},<} = \{+, -, \cdot, <, |, 0, 1\}$.

As usual, the theorem will follow from an embedding lemma.

Lemma 4.36 *Let* $(K, \mathcal{O})$ *and* $(L, \mathcal{O}_L)$ *be real closed valued fields such that* L *is* $|K|^+$*-saturated. Let* R *be a subring of* K *and* $f : R \to L$ *is an embedding that preserves both the order and the divisibility relation. Then* f *extends to an order and valuation preserving embedding of* K *into* L.

Let K, L, R and $f : R \to K$ be as in the lemma. We let v denote the valuation on K and v_L denote the valuation on L.

Exercise 4.37 Let K_0 be the fraction field of R. Show that f extends to an order and and valuation preserving embedding of K_0 into L.

Exercise 4.38 Let K_0 be as above and let K_0^{rcl} be the real closure of K_0 inside K. Show that we can extend f to an order and valuation preserving of K_0^{rcl} into K.

Henceforth, we assume that we have K_0 a real closed subfield of K and $f : K_0 \to L$ an order and valuation preserving embedding.

Exercise 4.39 Suppose $x \in K \setminus K_0$, $v(x) = 0$ and $\overline{x}$ is transcendental over k_{K_0}. Show that we can extend f to $K_0(x)$ preserving the ordering and the valuation.

Exercise 4.40 Suppose $x \in K \setminus K_0$, $v(x) \notin v(K_0)$. Show that we can extend f to $K_0(x)$ preserving the ordering and the valuation.

Exercise 4.41 Suppose $x \in K \setminus K_0$ and K/K_0 is immediate. Show that we can extend f to $K_0[x]$ preserving the ordering and the valuation.

Exercise 4.42 Conclude that the theory of real closed rings has quantifier elimination. Show that the theory of real closed valued fields is complete.

Recall that an ordered structure $(M, <, \dots)$ is *weakly o-minimal* if every definable $X \subset M$ is a finite union of points and convex sets.

Exercise 4.43 Show that a real closed ring is weakly o-minimal and NIP.

A partial converse holds ([28]). It T is a theory all of whose models are weakly o-minimal rings, then they are real closed rings or real closed fields.

5 Algebra of Henselian Fields

5.1 Extensions of Henselian Valuations

Our first goal is to give two alternative characterizations of being henselian. The first is that for any algebraic extension there is a unique extension of the valuation. The second, under some additional assumptions, is that there are no proper immediate algebraic extensions.

We begin with a useful lemma.

Lemma 5.1 *Suppose $\mathcal{O}_1, \ldots, \mathcal{O}_m$ are valuation rings of K with maximal ideals $\mathfrak{m}_i$, $A = \mathcal{O}_1 \cap \cdots \cap \mathcal{O}_m$ and $\mathfrak{n}_i = A \cap \mathfrak{m}_i$. Then $\mathcal{O}_i = A_{\mathfrak{n}_i}$ for each i.*

Proof Let $\boldsymbol{k}_i$ denote the residue field of $\mathcal{O}_i$. Let $x \in \mathcal{O}_1$. We may assume $x \neq 1$. Let $I = \{i : x \in \mathcal{O}_i\}$.

Choose M so that:

- $M \neq 0(\mathrm{mod}\ \mathfrak{m}_i)$ for all i;
- for $i \in I$ either $x = 1(\mathrm{mod}\ \mathfrak{m}_i)$ or x is not a M^{th} root of unity in $\boldsymbol{k}_i$;
- for $i \notin I$ either $x = 1(\mathrm{mod}\ \mathfrak{m}_i)$ or $1/x$ is not a M^{th} root of unity in $\boldsymbol{k}_i$.

The next exercise is to show this is always possible. Let $y = 1 + x + \cdots + x^{M-1}$. Then y is a unit in $\mathcal{O}_i$ [if $x = 1(\mathrm{mod}\ \mathfrak{m}_j)$, then $y = M \neq 0(\mathrm{mod}\ \mathfrak{m}_j)$, while if $x \neq 1(\mathrm{mod}\ \mathfrak{m}_j)$, then $y = \frac{1-x^M}{1-x} \neq 0(\mathrm{mod}\ \mathfrak{m}_i)$]. In particular $xy^{-1} \in \mathcal{O}_i$ for $i \in I$.

Similarly, we can also assume that $z = 1 + x^{-1} + \cdots + x^{1-M}$ is a unit in $\mathcal{O}_j$ for $j \notin I$. But then $y^{-1} = x^{1-M} z^{-1} \in \mathcal{O}_j$ and $xy^{-1} = x^{2-M} z^{-1} \in \mathcal{O}_j$ for $j \notin I$. Thus $xy^{-1}, y^{-1} \in A$ and $y^{-1} \notin \mathfrak{n}_1$. Thus $x = (xy^{-1}/y^{-1}) \in A_{\mathfrak{n}_1}$. $\square$

Exercise 5.2 Show that it is always possible to choose M as in the above proof.

Lemma 5.3 *Let K be a field and let $\mathcal{O}_1, \ldots, \mathcal{O}_m$ be valuation rings of K such that $\mathcal{O}_i \not\subseteq \mathcal{O}_j$ for $i \neq j$, let $A = \mathcal{O}_1 \cap \cdots \cap \mathcal{O}_m$ and let $\mathfrak{n}_i = \mathfrak{m}_i \cap A$. Then*

i) $\mathfrak{n}_i \not\subseteq \mathfrak{n}_j$ for $i \neq j$;

ii) $\mathfrak{n}_1, \ldots, \mathfrak{n}_m$ are maximal ideals of A and every maximal ideal of A is one of the $\mathfrak{n}_i$;

iii) for $(a_1, \ldots, a_m) \in \mathcal{O}_1 \times \cdots \times \mathcal{O}_m$, there is $a \in A$ with $\overline{a} = \overline{a}_i$ in $\boldsymbol{k}_i$.

Proof i) If $\mathfrak{n}_i \subseteq \mathfrak{n}_j$, then $\mathcal{O}_j = A_{\mathfrak{n}_j} \subseteq A_{\mathfrak{n}_i} = \mathcal{O}_i$.

ii) Suppose $I \subset A$ is a proper ideal. We will show that $I \subset \mathfrak{n}_i$ for some i. Suppose not. For each i choose $a_i \in I \setminus \mathfrak{n}_i$. Also for $i \neq j$ choose $b_{i,j} \in \mathfrak{n}_i \setminus \mathfrak{n}_j$. Then

$$c_j = \prod_{i \neq j} b_{i,j} \in \mathfrak{n}_i \setminus \mathfrak{n}_j \text{ for all } i \neq j.$$

Thus $a_j c_j \in_i \setminus \mathfrak{n}_j$ for all $i \neq j$ and

$$d = \sum a_j c_j \in I \setminus \mathfrak{n}_i \text{ for all } i.$$

Thus $1/d \in \mathcal{O}_i$ for all i, so $1/d \in A$. But then $1 \in I$, a contradiction.

iii) We know that $\mathcal{O}_i = A_{\mathfrak{n}_i}$ and $\mathfrak{m}_i = \mathfrak{n}_i A_{\mathfrak{n}_i}$. Thus $\boldsymbol{k}_i = A_{\mathfrak{n}_i}/\mathfrak{n}_i A_{\mathfrak{n}_i} = A/\mathfrak{n}_i$. Now we can apply the Chinese Remainder Theorem. $\square$

Lemma 5.4 *Suppose $(K, \mathcal{O})$ is a valued field and L/K is algebraic. If $\mathcal{O}_1 \subseteq \mathcal{O}_2$ are valuation rings of L with $\mathcal{O}_i \cap K = \mathcal{O}$, then $\mathcal{O}_1 = \mathcal{O}_2$.*

Proof Then $\overline{\mathcal{O}}_1 = \mathcal{O}_1/\mathfrak{m}_2$ in $\mathcal{O}_2/\mathfrak{m}_2$ is a valuation ring in $\boldsymbol{k}_2$ and $\boldsymbol{k} \subset \overline{O}_1$. But $\boldsymbol{k}_2/\boldsymbol{k}$ is algebraic, thus $\overline{\mathcal{O}}_1$ is a field. Since it's a valuation ring its fraction field must be all of $\boldsymbol{k}_2$. Thus $\overline{O}_1 = \boldsymbol{k}_2$. Since $\mathfrak{m}_2 \subseteq \mathfrak{m}_1$, we must have $\mathcal{O}_1 = \mathcal{O}_2$. $\square$

The following analysis will be the key to several of our main results in this section. Let $(K, \mathcal{O})$ be a valued field. Suppose F/K be a finite Galois extension and $\mathcal{O}_1, \ldots, \mathcal{O}_m$ are distinct extensions of $\mathcal{O}$ to F. Let $G = \{\sigma \in \mathrm{Gal}(F/K) : \sigma(\mathcal{O}_1) = \mathcal{O}_1\}$ and let $L \subseteq F$ be the fixed field of G. We will make two observations.

Lemma 5.5 *Under the assumptions above with $m > 1$:*
i) $(K, \mathcal{O})$ is not henselian;
ii) $(L, \mathcal{O}_1 \cap L)$ is a proper immediate extension of $(K, \mathcal{O})$

Proof Let $\mathcal{O}'_i = \mathcal{O}_i \cap L$ for $i = 1, \ldots, m$.

claim If $i > 1$, then $\mathcal{O}'_i \neq \mathcal{O}'_1$.

If $\mathcal{O}'_i = \mathcal{O}'_1$, then $\mathcal{O}_1$ and $\mathcal{O}_i$ are extensions of $\mathcal{O}'_1$ from L to F. But then by Theorem 3.24, there is $\sigma \in \mathrm{Gal}(F/L) = G$ with $\sigma(\mathcal{O}_1) = \mathcal{O}_i$, contradicting the definition of G.

Let $A = \mathcal{O}'_1 \cap \cdots \cap \mathcal{O}'_m$. Let $\mathfrak{n}_i = \mathcal{O}_i \cap A$.

claim If $i \geq 2$, then $\mathfrak{n}_i \neq \mathfrak{n}_1$.

By Lemma 5.1, if $\mathfrak{n}_i = \mathfrak{n}_1$, then $\mathcal{O}'_1 = A_{\mathfrak{n}_1} = A_{\mathfrak{n}_i} = \mathcal{O}'_i$, a contradiction.

By Lemma 3.21 we can find $a \in A$ such that $a = 1 (\mathrm{mod}\ \mathfrak{m}_1)$ and $a \in \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_m$, where $\mathfrak{m}_i$ is the maximal ideal of $\mathcal{O}_i$.

As $\mathfrak{m}_i \cap K = \mathfrak{m}_K$ we must have $a \notin K$. Let

$$f(X) = X^n + b_{n-1}X^{n-1} + \ldots b_0 = (X - a)(X - \alpha_2) \cdots (X - \alpha_n)$$

be the minimal polynomial for a over K, where $b_0, \ldots, b_{n-1} \in K$ and $\alpha_2, \ldots, \alpha_n \in F$.

claim $\alpha_2, \ldots, \alpha_n \in \mathfrak{m}_1$.

Let $i \geq 2$. There is $\sigma \in G(F/K)$ such that $\sigma(a) = \alpha_i$. We know that $a \in A \subset L$ and any $\sigma \in G$ fixes L pointwise. Thus $\sigma \notin G$ and $\sigma^{-1}(\mathcal{O}_1) = \mathcal{O}_j$ for some $j \neq 1$. But $a \in \mathfrak{m}_j$. Thus $\alpha_i = \sigma(a) \in \mathfrak{m}_1$.

It follows that $b_{n-1} = -a - \alpha_2 - \cdots - \alpha_n = -1(\text{mod } \mathfrak{m}_1)$ and $b_0, \ldots, b_{n-2} \in \mathfrak{m}_1$.

claim $(K, \mathcal{O})$ is not henselian.

Clearly $f(1) \in \mathfrak{m}_{\mathcal{O}}$. Let $g(X) = (X - \alpha_2) \cdots (X - \alpha_n)$. Then $f'(X) = (X - a)g'(X) + g(X)$. Thus

$$f'(1)(\text{mod } \mathfrak{m}_1) = (1 - a)g'(1) + g(1)(\text{mod } m_1) = 1(\text{mod } \mathfrak{m}_1).$$

Thus $f'(1) \neq 0(\text{mod } \mathfrak{m}_{\mathcal{O}})$. If K were henselian, f would not be irreducible. Thus K is not henselian.

To show that $(L, \mathcal{O}_1')$ is an immediate extension we make some minor modifications to the proof above. Suppose c is a unit in $\mathcal{O}_1'$ we can find $a \in A$ such that $a = c(\text{mod } \mathfrak{m}_1)$ but $a \in \mathfrak{m}_i$ for $i > 1$. Let f be the minimal polynomial for a over K. Arguing as above

$$f(X) = X^d + b_{d-1}X^{d-1} + \cdots + b_0 = (X - a)(X - \alpha_2) \cdots (X - \alpha_d)$$

where $b_{d-1} = -c(\text{mod } \mathfrak{m}_1)$ and $b_0, \ldots, b_{d-2} \in \mathfrak{m}_1$. But $-(c + \alpha_2 + \cdots + \alpha_d) = b_{d-1} \in K$ and $\bar{c} = \bar{b}_{d-1}$. Thus the residue field does not extend.

We need to show the value group does not extend. We let v denoted the valuation on L. Let $x \in L$. We must find $y \in K$ with $v(x) = v(y)$. We can find $a \in A$ such that $a - 1 \in \mathfrak{m}_1$ and $a \in \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_m$. Then $v(a) = 0$ and $v(\sigma(a)) = 0$ for all $\sigma \in G$. Since $a \in \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_m$, as above, $v(\sigma(a)) > 0$ for all $\sigma \in \text{Gal}(F/K) \setminus G$. We claim that we can choose N large enough we can ensure that

$$v(a^N x) \neq v(\sigma(a^N x)) \text{ for all } \sigma \in \text{Gal}(F/K) \setminus G.$$

For any particular $\sigma \in \text{Gal}(F/K)\setminus G$, $v(a^r x) = v(x)$ and $v(\sigma(a^r x)) = rv(\sigma(a)) + v(\sigma(x))$. Since $v(\sigma(a)) > 0$, for all but one value of r these are unequal. Thus, since $\text{Gal}(F/K)$ is finite, we can choose N as desired.

Let $a^N x = \alpha_1, \ldots, \alpha_n$ be the distinct conjugates of $a^N x$ over K. Let

$$g(X) = (X - \alpha_1) \cdots (X - \alpha_n) = X^n + b_{n-1}X^{n-1} + \cdots + b_0.$$

For $1 < i \leq n$, $\alpha_i = \sigma(a^N x)$ for some $\sigma \in \text{Gal}(F/K) \setminus G$ [note that any $\tau \in G$ fixes $a^N x \in L$]. Thus $v(\alpha_i) \neq v(\alpha_1)$ for $i > 1$.

First suppose $v(\alpha_i) > v(\alpha_1)$ for all $i > 1$. Then $b_{n-1} = -\sum \alpha_i$, $v(x) = v(a^N x) = v(b_{n-1}) \in v(K)$, as desired. In general suppose that $v(\alpha_i) < v(\alpha_1)$ for $1 < i \leq k$ and $v(\alpha_i) > v(\alpha_1)$ for $k < i$. Note that

$$b_{n-j} = (-1)^j \sum_{1 \leq i_1 < \cdots < i_j \leq n} \alpha_{i_1} \cdots \alpha_{i_n}.$$

Thus

$$v(b_{n-k}) = v(\alpha_2 \cdots \alpha_k) \text{ and } v(b_{n-k-1}) = v(\alpha_1 \cdots \alpha_k).$$

Thus $v(x) = v(\alpha_1) = v(b_{n-k-1}/b_{n-k}) \in v(K)$.

Thus L is an immediate extension of K. □

Theorem 5.6 *Let $(K,\mathcal{O})$ be a valued field. The following are equivalent:*

i) $(K,\mathcal{O})$ is henselian;

ii) For any separable algebraic extension L/K there is a unique extension of $\mathcal{O}$ to a valuation ring of L;

iii) For any algebraic extension L/K there is a unique extension of $\mathcal{O}$ to a valuation ring of L

iv) If $f(X)\in\mathcal{O}[X]$ is monic irreducible and $\overline{f}(X)$ is non-constant, then there is and irreducible $\overline{g}(X)\in\boldsymbol{k}[X]$ and $n\geq 1$ such that $\overline{f}(X)=\overline{g}(X)^n$.

v) If $f,g,h\in\mathcal{O}[X]$ is monic and $\overline{f}=\overline{g}\overline{h}$ where $\overline{g}$ and $\overline{h}$ are relatively prime, then there are $g_1,h_1\in\mathcal{O}[X]$ such that $\overline{g}_1=\overline{g}$, $\overline{h}_1=\overline{h}$ and g_1 and $\overline{g}$ have the same degree.

Proof i) $\Rightarrow$ ii) Suppose not. Then we can find F/K a finite Galois extension such that $\mathcal{O}$ has multiple extensions $\mathcal{O}_1,\ldots,\mathcal{O}_m$ each of which are conjugate under $\mathrm{Gal}(F/K)$. Now we can apply Lemma 5.5 to show that $(K,\mathcal{O})$ is not henselian.

ii) $\Rightarrow$ iii) Let $K\subseteq F\subseteq L$ be the separable closure of K in L. By ii) there is a unique extension of the valuation to F. Since L/F is purely inseparable and there is a unique extension of the valuation to L.

iii) $\Rightarrow$ iv) In K^{alg} we can factor

$$f(X)=\prod_{i=1}^{d}(X-\alpha_i).$$

Let $\mathcal{O}^*$ and $\mathfrak{m}^*$ denote the valuation ring and maximal ideal of an extension to K^{alg}.

Since $f\in\mathcal{O}[X]$, $\prod\alpha_i\in\mathcal{O}$, thus we can not have $v(\alpha_i)<0$ for all i. Since any two roots are conjugate and there is a unique extension of the valuation ring to K^{alg} we must have all of the $\alpha_i\in\mathcal{O}$ or all of the $\alpha_i\notin\mathcal{O}$, but the latter option is not possible.

Thus, $\overline{f}(X)=\prod(X-\overline{\alpha}_i)$. To show that $\overline{f}$ is a power of an irreducible polynomial in $k[X]$ it is enough to show that we can not fact $\overline{f}=\overline{g}\overline{h}$ where $\overline{g}$ and $\overline{h}$ are relatively prime and monic. Suppose we can. If $\overline{g}(\overline{\alpha_i})=0$, then $g(\alpha_i)\in\mathfrak{m}^*$ and for any $\sigma\in\mathrm{Gal}(K^{\mathrm{alg}}/K)$, $g(\sigma(\alpha_i))\in\sigma(\mathfrak{m}^*)=\mathfrak{m}^*$. But all of the roots of f are conjugate. Thus they are all roots of $\overline{g}$, a contradiction.

iv) $\Rightarrow$ v) Let $f=q_1\cdot q_m$ be an irreducible factorization of f in $\mathcal{O}[X]$. into monic factors. For each i, there is a monic $p_i\in\mathcal{O}[X]$ such that $\overline{q}_i=\overline{p}_i^{n_i}$. We can find $J\subseteq\{1,\ldots,d\}$ such that $\overline{g}=\prod_{i\in J}\overline{p}_i^{n_i}$. Let

$$\overline{h}=\prod_{i\notin J}\overline{p}_i^{n_i}.$$

Let

$$g_1=\prod_{i\in J}p_i^{n_i}\text{ and }h_1=\prod_{i\notin J}p_i^{n_i}.$$

Then $\overline{f} = \overline{g}_1\overline{h}_1$ and $\overline{g}$ and g_1 have the same degree.

v) $\Rightarrow$ i) Suppose $f(X) \in \mathcal{O}[X]$ and $f(X) = X^d + X^{d-1} + \sum a_i X^i$ where $a_i \in \mathfrak{m}_i$. In $\boldsymbol{k}[X]$ we can factor $\overline{f}(X) = \overline{h}(X)(X+1)$, Since $\overline{f}'(-1) = \pm 1$, $\overline{h}(-1) \neq 0$. Thus $\overline{h}(X)$ and $(X+1)$ are relatively prime. By iv) there is $a \in K$ with $\overline{a} = -1$ such that $(X - a)$ is an irreducible factor of f. □

Exercise 5.7 Show that it $(K, \mathcal{O})$ is henselian and $(L, \mathcal{O}_L)$ is an algebraic extension, then $(L, \mathcal{O}_L)$ is henselian.

Exercise 5.8 Suppose $(K, \mathcal{O})$ is henselian, $F \subseteq K$ and F is separably closed in K. Prove that $(F, \mathcal{O} \cap F)$ is henselian.

5.2 Algebraically Maximal Fields

Definition 5.9 We say that a valued field $(K, \mathcal{O})$ is *algebraically maximal* if it has no proper separable algebraic immediate extensions.

Corollary 5.10 *An algebraically maximal valued field $(K, \mathcal{O})$ is henselian.*

Proof If $(K, \mathcal{O})$ is not henselian we can find F/K a finite Galois extension with multiple extensions of $\mathcal{O}$ to F. By Lemma 5.5, we can find an intermediate field $K \subset L \subseteq F$ with L/K immediate. □

The converse is true under some additional assumptions which will apply in many of our settings.

Definition 5.11 We say that $(K, \mathcal{O})$ has *equicharacteristic zero* if K and the residue field $\boldsymbol{k}$ have characteristic zero.

We say that $(K, \mathcal{O})$ is *finitely ramified* if $\boldsymbol{k}$ has characteristic $p > 0$ and $\{v(x) : 0 < v(x) < v(p) : x \in K^\times\}$ is finite.

Note that the later condition is true for the p-adics.

Exercise 5.12 Prove that if $(K, \mathcal{O}_K)$ is a finite algebraic extension of $(\mathbb{Q}_p, \mathbb{Z}_p)$, then $(K, \mathcal{O}_K)$ is finitely ramified.

Exercise 5.13 Suppose L/K is finitely ramified. Show that the set $\{v(x) : 0 < v(x) < v(n)\}$ is finite for all $n \in \mathbb{Z}$.

Theorem 5.14 *If $(K, \mathcal{O})$ is henselian and equicharacteristic zero or finitely ramified, then $(K, \mathcal{O})$ is algebraically maximal.*

Proof Suppose F is an algebraic immediate extension and $x \in F \setminus K$. Without loss of generality F/K is finite. There is $L \supseteq K$ such that L/K is Galois. There is a unique extension $\mathcal{O}_L$ of $\mathcal{O}$. Let v be the valuation associated with $\mathcal{O}_L$. For and $a \in K$, we have $v(x-a) = v(b)$ for some $b \in K$, but then $v(\sigma(x)-a) = v(b)$ for all $\sigma \in \mathrm{Gal}(L/K)$.

Let $d = [L : K]$ Let

$$a = \frac{1}{d} \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in K.$$

Since F/K is immediate, there is $b \in K$ such that $v((x-a)/b) = 0$ and $c \in K$ such $v(\frac{x-a}{b} - c) > 0$. Then

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

Since $(K, \mathcal{O})$ is equicharacteristic zero or finitely ramified, repeating this argument finitely many times in the case where the residue field has characteristic p we can find $\widehat{a} \in K$ such that

$$v(x - \widehat{a}) > v(x - a) + v(n)$$

(if the residue field has characteristic zero $v(n) = 0$ so we need only do this once). Then

$$\begin{aligned} v(n) + v(a - \widehat{a}) &= v(n(a - \widehat{a})) \\ &= v\left(\sum_{\sigma \in \mathrm{Gal}(L/K)} (\sigma(x) - \widehat{a}) \right) \\ &\geq \min(v(\sigma(x) - \widehat{a})) \\ &\geq v(x - \widehat{a}) \text{ since } v(w) = v(\sigma(w)) \text{ for all } w \in L \\ &> v(x - a) + v(n) \\ &= v(a - \widehat{a}) + v(n) \end{aligned}$$

a contradiction. The last line holds since $v(a - \widehat{a}) = v((a - x) + (x - \widehat{a}))$ and $v(x - \widehat{a}) > v(x - a)$. $\square$

Corollary 5.15 *If $(K, \mathcal{O})$ is henselian with divisible value group and algebraically closed residue field of characteristic zero, then K is algebraically closed.*

Proof If L/K is a proper algebraic extension, then we can extend the valuation to L and, by Lemma 3.16 it must be an immediate extension, contradicting Theorem 5.14. $\square$

Corollary 5.16 *If k is an algebraically closed field of characteristic zero, then the Puiseux series field $k\langle T \rangle$ is algebraically closed.*

This doesn't work in characteristic $p > 0$. The series solution to $f(X) = X^p - X = T^{-1}$ should be of the form

$$a + T^{-1/p} + T^{-1/p^2} + \cdots + T^{-1/p^n} + \ldots$$

where $a \in \mathbb{F}_p$, which is not a Puiseux series. This series is in the immediate extension $\mathbb{F}_p(((\mathbb{Q})))$ and thus in the separable closure of the Puiseux series in the Hahn series. This shows that henselianity alone is not enough to conclude algebraically maximal. Kedlaya in [25] gives a characterization of the algebraic closure of $\mathbb{F}_p^{\mathrm{alg}}((T))$.

If k is real closed and Γ is divisible, $k^{\mathrm{alg}}\langle T\rangle$ is a degree 2 extension of $k\langle T\rangle$. Thus $\boldsymbol{k}\langle T\rangle$ is real closed. This is true in much more generality.

Corollary 5.17 *Let $(K,<)$ is an ordered field and let $\mathcal{O}$ be the convex hull of a subring. Suppose $(K,\mathcal{O})$ is henselian with real closed residue field $\boldsymbol{k}$ and divisible value group Γ. Then K is real closed.*

Proof Let L be the real closure of $(K,<)$ and let $\mathcal{O}^*$ be the convex hull of $\mathcal{O}$ in K. Then, since the orderings agree, $(K,\mathcal{O})\subseteq(L,\mathcal{O}^*)$. The residue field $\boldsymbol{k}_L$ is real closed and algebraic over $\boldsymbol{k}$, so it must equal $\boldsymbol{k}$. Similarly, the value group of L is contained in the divisible hull of $v(K)$ and hence equals $v(K)$. Thus L/K is an immediate extension and, since $(K,\mathcal{O})$ is henselian and equicharacteristic zero, $L=K$. $\square$

5.3 Henselizations

Infinite Galois Theory

We quickly review some facts we need about the Galois Theory of infinite algebraic extensions. The reader should consult [23] §8.6 or [19] §1.

Let K be a field. The *separable closure* of K is K^s the maximal separable algebraic extension of K. When we apply these results we will be working almost exclusively in the setting where K has characteristic zero so there would be no harm in working with K^{alg} the algebraic closure of K. We let $\mathrm{Gal}(K^s/K)$ be the Galois group of all automorphisms of K^s that are the identity on K.

Suppose L/K is a finite Galois extension. If $\sigma\in\mathrm{Gal}(K^s/K)$, then $\sigma|L\in\mathrm{Gal}(L/K)$. Moreover if $\tau\in\mathrm{Gal}(L/K)$, there is $\widehat{\tau}\in\mathrm{Gal}(K^s/K)$ extending τ. Thus

$$\mathrm{Gal}(K^s/K)=\varprojlim_{L/K\text{ finite Galois}}\mathrm{Gal}(L/K)$$

is a profinite group. We topologize $\mathrm{Gal}(K^s/K)$ by taking the weakest topology such that for all finite Galois extensions L/K and $\sigma\in\mathrm{Gal}(L/K)$, $U_\sigma=\{\tau\in\mathrm{Gal}(K^s/K):\sigma\subseteq\tau\}$ is open.

If H is a subgroup of $\mathrm{Gal}(K^s/K)$, let $\mathrm{Fix}(H)=\{x\in K^s:\sigma(x)=x$ for all $\sigma\in H\}$ be the fixed field of H.

Theorem 5.18 (Fundamental Theorem of Infinite Galois Theory) *The maps $L\mapsto\mathrm{Gal}(K^s/L)$ and $H\mapsto\mathrm{Fix}(H)$ are inclusion-reversing bijections between the collection of intermediate fields $K\subseteq L\subseteq K^s$ and closed subgroups of $\mathrm{Gal}(K^s/K)$.*

Henselizations

Let $(K,\mathcal{O})$ be a valued field, let K^s be the separable closure of K and let $\mathcal{O}^s$ be an extension of $\mathcal{O}$ to K. Let $G(\mathcal{O}^s)=\{\sigma\in \mathrm{Gal}(K^s/K):\sigma(\mathcal{O}^s)=\mathcal{O}^s\}$. We call $G(\mathcal{O}^s)$ the *decomposition group.*

Lemma 5.19 *$G(\mathcal{O}^s)$ is a closed subgroup of* $\mathrm{Gal}(K^s/K)$.

Proof Suppose $\sigma\not\in G(\mathcal{O}^s)$. There is $x\in\mathcal{O}^s$ with $\sigma(x)\not\in\mathcal{O}^s$. Let L/K be finite Galois with $x\in L$ and let $\tau=\sigma|L$. Then $\sigma\in U_\tau$ and $U_\tau\cap G(\mathcal{O}^s)$ is empty. $\square$

Definition 5.20 Let $K^h(\mathcal{O}^s)$ be the fixed field of $G(\mathcal{O}^s)$ and let $\mathcal{O}^h(\mathcal{O}^s)=\mathcal{O}^s\cap K^h$. We call $(K^h(\mathcal{O}^s),\mathcal{O}^h(\mathcal{O}^s))$ a *henselization* of $(K,\mathcal{O})$.

When no confusion arises we will suppress $\mathcal{O}^s$ and write $(K^h,\mathcal{O}^h)$.

Lemma 5.21 *i) $\mathcal{O}^s$ is the unique extension of $\mathcal{O}^h$ to K^s. Thus $(K^h,\mathcal{O}^h)$ is henselian.*

ii) $(K^h,\mathcal{O}^h)$ is an immediate extension of K.

Proof i) Suppose $\mathcal{O}^s_1$ is an extension of $\mathcal{O}^h$ to K^s. By Theorem 3.24, $\mathcal{O}^s$ and $\mathcal{O}^s_1$ are conjugate under $\mathrm{Gal}(K^s/K)$. But $G(\mathcal{O}^s)$ is the Galois group of K^s/K^h, so any element of $\mathrm{Gal}(K^s/K)$ fixes $\mathcal{O}^s$. Hence $\mathcal{O}^s=\mathcal{O}^s_1$

ii) follows from Lemma 5.5. $\square$

Lemma 5.22 *If $(K_1,\mathcal{O}_1)$ is a henselian extension of $(K,\mathcal{O})$ then there is a unique embedding $j:(K^h,\mathcal{O}^h)\to(K_1,\mathcal{O}_1)$ fixing K pointwise.*

Proof Without loss of generality, by Exercise 5.8, we may assume that $K_1\subseteq K^s$. Since K_1 is henselian, there is a unique extension $\mathcal{O}^s_1$ of $\mathcal{O}_1$ to K^s. Then $\mathrm{Gal}(K^s/K_1)\subseteq G(\mathcal{O}^s_1)$. Thus $K_1\supseteq K^h(\mathcal{O}^s_1)$. By Theorem 3.24 there is $\sigma\in\mathrm{Gal}(K^s/K)$ with $\sigma(\mathcal{O}^s)=\mathcal{O}^s_1$, but then $\sigma(K^h)=K^h(\mathcal{O}^s_1)\subseteq K_1$ and $\sigma|K^h$ is the desired embedding of $(K^h,\mathcal{O}^h)$ into $(K_1,\mathcal{O}_1)$.

Suppose $j:(K^h,\mathcal{O}^h)\to(K_1,\mathcal{O}_1)$ is another embedding. We can extend j to $\tau\in\mathrm{Gal}(K^s/K)$. Then $\tau(\mathcal{O}^s)\cap\tau(K^h)=\mathcal{O}^s_1\cap\tau(K^h)$. But $(\tau(K^h),\tau(O^h))$ is henselian, so $\mathcal{O}^s_1$ is the unique extension of $\tau(\mathcal{O}^s)$ to K^s and $\tau(\mathcal{O}_s)=\mathcal{O}^s_1$. Thus $\tau^{-1}\sigma(\mathcal{O}^s)=\mathcal{O}^s$ and $\tau^{-1}\sigma\in G(\mathcal{O}^s)$. Since K^h is the fixed field of $G(\mathcal{O}_s)$, σ and τ agree on K^h. Thus $j=\sigma|K^h$. $\square$

Exercise 5.23 In particular if $\mathcal{O}^s$ and $\mathcal{O}^s_1$ are distinct extensions of $\mathcal{O}$, then there is a unique isomorphism between $(K^h(\mathcal{O}^s),\mathcal{O}^s)$ and $(K^h(\mathcal{O}^s_1),\mathcal{O}(\mathcal{O}^s_1))$ fixing K.

Summarizing we have proved:

Theorem 5.24 *Let $(K,\mathcal{O})$ be a valued field. There is a henselization $(K^h,\mathcal{O}^h)$, i.e. a henselian immediate separable algebraic extension of $(K,\mathcal{O})$ such that if $(K_1,\mathcal{O}_1)$ is a henselian extension of $(K,\mathcal{O})$ then there is a unique embedding $j:(K^h,\mathcal{O}^h)\to(K_1,\mathcal{O}_1)$ with $j|K$ the identity.*

Corollary 5.25 *a) Let (K, v) be an algebraically closed valued field of characteristic 0 and let $A \subset K$. Show that* $\mathrm{dcl}(A)$*, the definable closure of A, is exactly the henselization of the fraction field of A.*

Proof Let F be the fraction field of A. Then F^{alg} is an elementary submodel of (K, v). The valued field automorphisms of F^{alg} that fixes A are exactly the elements of the decomposition group $G(\mathcal{O}_{\mathbb{F}^{\mathrm{alg}}})$, when has fixed field F^h. It follows that $F^h = \mathrm{dcl}(A)$. $\square$

Exercise 5.26 Let (K, v) be an algebraically closed field of characteristic $p > 0$. Prove that $A = \mathrm{dcl}(A)$ if and only if A is perfect and henselian.

5.4 Pseudolimits

Let K be a valued field with valuation v. We will consider sequences $(a_\alpha : \alpha < \delta)$ where δ is a limit ordinal and $a_\alpha \in K$ for $\alpha < \delta$. Frequently, we will simplify notation by just writing (a_α).

Definition 5.27 We say that a is a *pseudolimit* of $(a_\alpha : \alpha < \delta)$ if the sequence $(v(a - a_\alpha) : \alpha < \delta)$ is eventually strictly increasing. We write $(a_\alpha) \rightsquigarrow a$. We let $\gamma_\alpha = v(a - a_\alpha)$.

Exercise 5.28 Suppose $(a_\alpha) \rightsquigarrow a$ and $b \in K$.
a) Show $(a_\alpha + b) \rightsquigarrow a + b$.
b) Show $(ba_\alpha) \rightsquigarrow ba$

Lemma 5.29 *Suppose $(a_\alpha) \rightsquigarrow a$. Then either:*
i) $(v(a_\alpha))$ is eventually constant and equal to $v(a)$;
ii) $(v(a_\alpha))$ is eventually strictly increasing and $v(a_\alpha) < v(a)$ for sufficiently large α.

Proof Suppose γ_α is increasing for $\alpha \geq \alpha_0$ and $v(a) \leq v(a_{\alpha_0})$. Then $v(a - a_{\alpha_0}) \geq v(a)$ and $\alpha > \alpha_0$, $v(a_\alpha) = v(a)$, since

$$v(a - \alpha) > v(a - a_{\alpha_0}) \geq v(a).$$

Thus we are in case i).

If this never happens then $v(a_\alpha) < v(a)$ for all sufficiently large α and for $\beta > \alpha$ Then $\gamma_\alpha = v(a_\alpha)$ and $v(a_\alpha) < v(a_\beta)$ for sufficiently large $\alpha < \beta$ and case ii) holds. $\square$

Lemma 5.30 *Suppose $(K, v) \subseteq (L, v)$ is an immediate extension and $x \in L \backslash K$. There is a sequence (a_α) in K such that $(a_\alpha) \rightsquigarrow x$ and (a_α) has no pseudolimit in K.*

Proof Let $a_0 = 0$. Suppose we have a_α. Since $v(K) = v(L)$ we can find $b \in K$ such that $v(b) = v(x - a_\alpha)$. Since $\boldsymbol{k}_K = \boldsymbol{k}_L$, there is $c \in K$ such that $0 \neq \overline{c} = \mathrm{res}(\frac{x - a_\alpha}{b})$. Thus

$$v(x - (a_\alpha + bc)) > v(b) = v(x - a_\alpha).$$

Let $a_{\alpha+1} = a_\alpha + cb$. Then $v(x - a_{\alpha+1}) > v(x - a_\alpha)$.

Suppose δ is a limit ordinal and we have constructed $(a_\alpha : \alpha < \delta)$ with $v(x - a_\alpha) < v(x - a_\beta)$ for $\alpha < \beta < \delta$. If there is $b \in K$ such that $v(x - b) > v(x - a_\alpha)$ for all $\alpha < \delta$ let $a_\delta = b$ and continue. If no such b exists (a_α) is our desired sequence. $\square$

A sequence (a_α) in K might not have a pseudolimit in K, but we can tell if it could have pseudolimit in an extension.

Definition 5.31 We say that (a_α) is *pseudocauchy* if there is α_0 such that $v(a_\delta - a_\beta) > v(a_\beta - a_\alpha)$ for $\delta > \beta > \alpha > \alpha_0$.

Lemma 5.32 *i) If $(a_\alpha) \rightsquigarrow a$, then (a_α) is pseudocauchy.*

ii) If (a_α) is pseudocauchy, there is an elementary extension $(K, v) \prec (L, v)$ such that (a_α) has a pseudolimit in L.

Proof i) If $\delta > \beta > \alpha$ are suitably large, then $a_\delta - a_\beta = (a - a_\beta) - (a - a_\delta)$. Thus $v(a_\delta - a_\beta) = v(a - a_\beta)$. Similarly, $v(a_\beta - a_\alpha) = v(a - a_\alpha)$ and, thus, $v(a_\delta - a_\beta) > v(a_\beta - a_\alpha)$ and the sequence is pseudocauchy.

ii) Consider the type $t(v) = \{v(x - a_\beta) > v(x - a_\alpha) : \text{for } \alpha_0 < \alpha < \beta\}$. Let $\Delta \subset t(v)$ be finite. Choose $\delta > \alpha$ for all a_α occurring in Δ. Then $v(a_\delta - a_\beta) > v(a_\beta - a_\alpha) = v(a_\delta - a_\beta)$ for $\delta > \beta > \alpha > \alpha_0$. Thus $t(v)$ is finitely satisfiable and thus realized in some elementary extension of K. $\square$

Corollary 5.33 *If (a_α) is pseudocauchy, then $(v(a_\alpha))$ is either eventually constant or eventually strictly increasing.*

Exercise 5.34 Prove that in a Hahn field $\boldsymbol{k}(((\Gamma)))$ every pseudocauchy sequence has a pseudolimit and conclude that Hahn fields have no proper immediate extensions. (This is essentially the same proof we gave in §1.)

The next lemma is important but not surprising and rather routine. We omit the proof and refer the reader to [12] Proposition 4.7 for the proof.

Lemma 5.35 *Suppose $(a_\alpha) \rightsquigarrow a$ and $f(X) \in K[X]$. Then $(f(a_\alpha)) \rightsquigarrow f(a)$.*

Thus if (a_α) is pseudocauchy, so is $(f(a_\alpha))$.

There is an important dichotomy among pseduocauchy sequences.

Definition 5.36 Let (a_α) be a pseudocauchy sequence in K. We say that (a_α) is of *algebraic type* if there is a nonconstant polynomial $f(X) \in K[X]$ such that $(v(f(a_\alpha)))$ is eventually strictly increasing. Otherwise we say (a_α) is of *transcendental type*.

If (a_α) is of transcendental type, then $(v(f(a_\alpha)))$ is eventually constant for all $f \in K[X]$.

Lemma 5.37 *If (a_α) is a pseudocauchy sequence over K of transcendental type, then (a_α) has no pseudolimit in K and there is an extension of v to the field of rational functions $K(X)$ with $v(f)$ = eventual value of $v(f(a_\alpha))$. Then $(K(X), v)$ is an immediate extension of K where $(a_\alpha) \rightsquigarrow X$.*

If L/K is a valued field extension of K and $(a_\alpha) \rightsquigarrow a$ in L, then sending X to a we get a valued field isomorphism between $K(X)$ and $K(a)$ fixing K.

Proof If $(a_\alpha) \rightsquigarrow a$, let $f(X) = X - a$, then $(v(f(a_\alpha)))$ is eventually strictly increasing and the sequence is of algebraic type, a contradiction. Thus (a_α) has no pseudolimit in K.

Let v be defined as above. Then, for α sufficiently large

$$v(fg) = v(f(a_\alpha)) + v(g(a_\alpha)) = v(f) + v(g)$$

and

$$v(f + g) = v(f(a_\alpha) + g(a_\alpha)) \geq \min(v(f(a_\alpha))v(g(a_\alpha))) = \min(v(f), v(g)).$$

Thus v is a valuation on $K(X)$ extending the valuation on K. Clearly, the value group of $K(X)$ is equal to the value group of K. Let $f \in K(X) \setminus K$ with $v(f) = 0$. Then $0 = v(f) = v(f(a_\alpha))$ for sufficiently large α. If $\beta > \alpha$, then $v(f - f(a_\beta)) > v(f - f(a_\alpha)) > v(f(a_\alpha)) = 0$ and $\mathrm{res}(f) = \mathrm{res}(a_\beta)$. Thus $K(X)$ is an immediate extension of K.

Suppose (L, v) is a valued field extension of K and $a \in L$ is a pseudolimit of (a_α). For nonconstant $f \in K[X]$ we have $(f(a_\alpha)) \rightsquigarrow f(a)$. Thus $v(f(a)) = v(f(a_\alpha)) = v(f)$ for sufficiently large α. In particular $f(a) \neq 0$, thus a is transcendental over K and the field isomorphism of $K(X)$ to $K(a)$ obtained by sending X to a preserves the valuation. □

Definition 5.38 If (a_α) is of algebraic type, a *minimal polynomial* of (a_α) is a polynomial g of minimal degree such $(v(g(a_\alpha))$ is eventually increasing.

Lemma 5.39 *Let (a_α) be a pseudocauchy sequence of algebraic type with minimal polynomial $g(X)$ and no pseudolimit in K. Then $g(X)$ is irreducible of degree at least 2. Let a be a zero of g in an extension field of K. Then v extends to a valuation on $K(a)$ where $v(f(a))$ = eventual value of $v(f(a_\alpha))$, where $f(X) \in K[X]$ of degree less than deg(g). Then $K(a)$ is an immediate extension of K where $(a_\alpha) \rightsquigarrow a$.*

If L/K is any valued field extension of K where $b \in K$ is a zero of g and $(a_\alpha) \rightsquigarrow b$, then the isomorphism $K(a)$ to $K(b)$ obtained by sending a to b, preserves the valuation.

Proof If $g(X) = X - a$ then $(v(g(a_\alpha))) = v(a_\alpha - a)$ is eventually strictly increasing and $(a_\alpha) \rightsquigarrow a$, a contradiction. Thus g has degree at least two. If $g = g_1 g_2$ is a nontrivial factorization of g, then, by minimality of the degree of g, $(v(g_i(a_\alpha)))$ is eventually constant for each i, but then $(v(g(a_\alpha))) = (v(g_1(a_\alpha) + g_2(a_\alpha)))$ is eventually constant, a contradiction. Thus g is irreducible of degree at least two.

Consider the extension $K(a)$ where $g(a) = 0$. Suppose $f_1, f_2 \in K[X]$ have degree less that $\deg(g)$. There are $h, r \in K[X]$ with degree less than $\deg(g)$ such that $f_1 f_2 = hg + r$. Then for α sufficiently large

$$v(f_1) = v(f_1(a_\alpha)), v(f_2) = v(f_2(a_\alpha)) \text{ and } v(f_1 f_2) = v(r) = v(r(a_\alpha)).$$

Then,

$$v(f_1) + v(f_2) = v(f_1(a_\alpha) f_2(a_\alpha)) = v(h(a_\alpha) g(a_\alpha) + r(a_\alpha)).$$

The sequence $(v(h(a_\alpha)g(a_\alpha) + r(a_\alpha))$ is eventually constant, while the sequence $(v(h(a_\alpha)g(a_\alpha))$ is eventually increasing. This is only possible if $v(h(a_\alpha)g(a_\alpha)) > v(r(a_\alpha))$ eventually. But then $v(h(a_\alpha)g(a_\alpha) + r(a_\alpha)) = v(r(a_\alpha))$ eventually and $v(f_1 f_2) = v(f_1) + v(f_2)$ as desired.

The rest of the proof closely follows the proof of Lemma 5.37. $\square$

Corollary 5.40 *Let (K, v) be a valued field. Then every pseudocauchy sequence in K has a pseudolimit in K if and only if K has no proper immediate extensions.*

Exercise 5.41 Prove that K has no proper immediate extensions if and only if K is spherically complete.

We can refine Lemma 5.30 for algebraic immediate extensions.

Lemma 5.42 *Suppose (L, v) is an immediate extension of K and $a \in L \setminus K$ is algebraic over K with minimal polynomial g. Let (a_α) be a pseudocauchy sequence over K with no pseudolimit in K such that $(a_\alpha) \rightsquigarrow a$. Then (a_α) is of algebraic type. In fact $(v(g(a_\alpha)))$ is increasing.*

Proof Let $g(X) = (X - a)h(X)$ where $h \in K(a)[X]$. Then $g(a_\alpha) = (a_\alpha - a)h(a_\alpha)$. The sequence $(v(a_\alpha - a))$ is eventually increasing and the sequence $(v(h(a_\alpha)))$ is either eventually increasing or eventually constant. Thus $v(g(a_\alpha))$ is either eventually increasing or eventually constant. $\square$

Corollary 5.43 *Let (K, v) be a valued field. If every pseudocauchy sequence (a_α) of algebraic type in K has a pseudolimit in K, then K is henselian. Moreover, the converse holds if, in addition (K, v) is either equicharacteristic zero or finitely ramified.*

Proof If every pseudocauchy sequence (a_α) of algebraic type has a pseudolimit in K, then by Lemma 5.42 (K, v) has no proper immediate algebraic extension and, by Theorem am hen, (K, v) is henselian. Note that this direction did not use the additional assumptions on (K, v).

If (K, v) is henselian and either equicharacteristic zero or finitely ramified, then by Theorem 5.10, (K, v) has no proper immediate algebraic extensions. Thus by Lemma 5.39, every pseudocauchy sequence of algebraic type in K has a pseudolimit in K. $\square$

Exercise 5.44 Suppose K is a valued field with value group Γ such that there is a lifting of the residue field $\boldsymbol{k}$ to K and there is $s : \Gamma \to K$ a section of the value group. Show there is a valuation preserving embedding of K into the Hahn field $\boldsymbol{k}(((\Gamma)))$. [Hint: View $\boldsymbol{k}$ as a subfield of K. First show that $\boldsymbol{k}(s(\Gamma))$ embeds into $\boldsymbol{k}(((\Gamma)))$. Then consider a maximal subfield $K_0 \subseteq K$ such that the embedding extends to a valuation preserving embedding of K_0 into $\boldsymbol{k}(((\Gamma)))$.]

Conclude that if K is a real closed field with valuation ring $\mathcal{O}$ a convex subring, residue field $\boldsymbol{k}$ and value group Γ, then there is a valuation preserving embedding of K into $\boldsymbol{k}(((\Gamma)))$.[8]

[8] Mourgess and Ressarye [32] proved the stronger result that we can embedding K into $k(((\Gamma)))$ such that if f is in the image so is any truncation (i.e. initial segment) of f. They used this to prove that every real closed field has an integral part (i.e. a discrete subring Z such that for all $x \in K$, $|[x, x+1) \cap Z| = 1$).

6 The Ax–Kochen Eršov Theorem

6.1 Quantifier Elimination in the Pas Language

We will be considering valued fields as three-sorted objects $(K, \Gamma, \boldsymbol{k})$ in the Pas language where we have the language of rings $\{+, -, \cdot, 0, 1\}$ on both the home sort, i.e. the field K, and the residue field sort, the language of ordered groups $\{+, -, <, 0\}$ on the value group sort, the valuation map $v : K^\times \to \Gamma$ and an angular component map $\mathrm{ac} : K^\times \to \boldsymbol{k}^\times$. Not all valued fields have angular component maps, but for any valued field we can pass to an elementary extension where there is an angular component map.

Let Δ_0 be the collection of all formulas of the form

- $\phi(\mathbf{u})$, where ϕ is a quantifier free formula in the language of rings and $\mathbf{u}$ are variables in the field sort;
- $\psi(v(f_1(\mathbf{u})), \ldots, v(f_k)(\mathbf{u})), \mathbf{v}))$ where ψ is a formula in the language of ordered groups, $\mathbf{u}$ are variables in the field sort, f_i is a term in the ring language and $\mathbf{v}$ are variables in the value groups sort;
- $\theta(\mathrm{ac}(g_1(\mathbf{u})), \ldots, \mathrm{ac}(g_k)(\mathbf{u})), \mathbf{w}))$ where ψ is a formula in the language of ordered groups, $\mathbf{u}$ are variables in the field sort, g_i is a term in the ring language, and $\mathbf{w}$ are variables in the residue sort;

Note that we are allowing quantifiers over the value group and the residue field but not over the home sort. Let Δ be the collection of finite boolean combinations of Δ-formulas. Note that each Δ formula is equivalent to a formula of the form

$$\phi(\mathbf{u}) \wedge \psi(v(f_1(\mathbf{u})), \ldots, v(f_k)(\mathbf{u})), \mathbf{v})) \wedge \theta(\mathrm{res}(g_1(\mathbf{u})), \ldots, \mathrm{res}(g_l)(\mathbf{u})), \mathbf{w})),$$

where ϕ, ψ and θ are as above.

Theorem 6.1 (Pas) *[33] Let T be the theory of henselian valued fields with angular components where the residue field has characteristic zero. Then every formula is equivalent to a Δ-formula.*

We will use the following relative quantifier elimination test.

Exercise 6.2 Suppose $\mathcal{L}$ is countable. Let Δ be a collection of formulas closed under finite boolean combinations and let T be an $\mathcal{L}$-theory with the following property.

Whenever $\mathcal{M}$ and $\mathcal{N}$ are models of T, $|\mathcal{M}| = \aleph_0$ $\mathcal{N}$ is $\aleph_1$-saturated, $A \subset \mathcal{M}$ and $f : A \to \mathcal{N}$ is a Δ-embedding (i.e, $\mathcal{M} \models \theta(\mathbf{a}) \Leftrightarrow \mathcal{N} \models \theta(f(\mathbf{a})$ for $\mathbf{a} \in A$ and $\theta \in \Delta$), then there is $\widehat{f} : \mathcal{M} \to \mathcal{N}$ that is Δ preserving.

Show that every $\mathcal{L}$-formula is equivalent to a Δ-formula. [Hint: add predicates for all formulas in Δ.]

Our main step will be proving an embedding result. We look at embeddings that preserved Δ-formulas. A map $f : (A, \Gamma_A, \boldsymbol{k}_A) \to L$ is an Δ-embedding if:

i) $f|A$ is a ring embedding;
ii) $f|\Gamma_A$ is a partial elementary embedding in the language of groups;
iii) $f|\boldsymbol{k}_A$ is a partial elementary embedding in the language of rings;
iii) f preserves v and ac.

Theorem 6.3 *Let $(K, \Gamma, \boldsymbol{k})$ and $(L, \Gamma_L,\ k_L)$ be henselian valued fields with angular component with characteristic zero residue field. Suppose K is countable, L is $\aleph_1$-saturated, $(A, \Gamma_A, \boldsymbol{k}_A)$ is a countable substructure of K, and $f : (A, \Gamma_A, \boldsymbol{k}_A) \to (L, \Gamma_L, \boldsymbol{k}_L)$ is a Δ-embedding. Then there is an extension of f to a Δ-embedding $\widehat{f} : (K, \Gamma_K, \boldsymbol{k}_K) \to (L, \Gamma_L, \boldsymbol{k}_L)$.*

Henceforth, we assume K is countable and L is $\aleph_1$-saturated. We extend our map by iterating the following lemmas.

Note that in a substructure $(A, \Gamma_A, \boldsymbol{k}_A)$, A and $\boldsymbol{k}_A$ are domains, while Γ_A is a subgroup.

Lemma 6.4 *Suppose $(A, \Gamma_A, \boldsymbol{k}_A)$ be a subring of K and $f : (A, \Gamma_A, \boldsymbol{k}_A) \to (L, \Gamma, \boldsymbol{k}_L)$ is a Δ-embeddings. Let F be the fraction field of A and let $\boldsymbol{l}$ be the fraction field of $\boldsymbol{k}_A$. We can extend f to a Δ-embedding of $(F, \Gamma, \boldsymbol{l})$ into L.*

Proof There is a unique extension of f to $(F, G, \boldsymbol{l})$. Since $v(a/b) = v(a) - v(b)$ and $\mathrm{ac}(x/y) = \mathrm{ac}(x)/\mathrm{ac}(y)$, $v_L(f(a/b)) = f(v(a/b))$ and $\mathrm{ac}_L(f(x/y)) = f(\mathrm{ac}(x/y))$, f is a Δ-embedding. $\square$

Henceforth, we will work only with substructures $(F, \Gamma_F, \boldsymbol{k}_F)$ where F and $\boldsymbol{k}_F$ are fields and Γ_F is a group, $v(F) \subseteq \Gamma_F$ and $\mathrm{ac}(F) \subseteq \boldsymbol{k}_F$.

We next show how to extend the value group.

Lemma 6.5 *Suppose $f : (F, \Gamma_F, \boldsymbol{k}_F) \to (L, \Gamma_L, \boldsymbol{k}_L)$ is a Δ-embedding. We can extend f to a Δ-embedding of $(F, \Gamma, \boldsymbol{k}_F)$.*

Proof We will prove this by iterating the following claim.

claim Let $\gamma \in \Gamma \setminus \Gamma_F$ and let G be the group generated by Γ_F and γ, then we can extend f to $(F, G, \boldsymbol{k}_F)$.

Let $p(v)$ be the type $\{\psi(v, f(g_1), \ldots, f(g_m)) : g_1, \ldots, g_m \in \Gamma_F,\ \psi$ a formula in the language of ordered groups where $\Gamma \models \psi(\gamma, g_1, \ldots, g_m)$. If $\psi_1, \ldots, \psi_n \in p(v)$ with parameters $f(g_1), \ldots, f(g_m)$, then, since f is a Δ-embedding

$$\Gamma_L \models \exists v \bigwedge_{i=1}^{n} \psi_i(v, f(g_1), \ldots, f(g_m)).$$

Thus $p(v)$ is consistent and, by $\aleph_1$-saturation, realized in Γ_L. Let γ' be a realization and extend f by $\gamma \mapsto \gamma'$. $\square$

Lemma 6.6 *If we have a Δ-embedding f defined on $(F, \Gamma, \boldsymbol{k}_F)$ we can extend it to $(F, \Gamma, \boldsymbol{k})$.*

Exercise 6.7 Prove Lemma 6.6.

We next make the residue map surjective.

Lemma 6.8 *Suppose f is a Δ-embedding of $(F, \Gamma, \boldsymbol{k})$. Then we can find $F \subseteq E \subseteq K$ such that* $\mathrm{res} : E \to \boldsymbol{k}$ *is surjective and we can extend f to a Δ-embedding of $(E, \Gamma, \boldsymbol{k})$.*

Proof We iterate the following two claims and Lemma 6.4.

claim 1 Suppose we have a Δ-embedding $f : (F, \Gamma, \boldsymbol{k}) \to (L, \Gamma_L, \boldsymbol{k}_L)$ and $b \in K$ with residue $\overline{b}$ algebraic over $\mathrm{res}(F)$ but not in $\mathrm{res}(F)$. Then we can extend f to $F(b)$.

There is $p(X) \in \mathcal{O}_F[X]$ irreducible with $\overline{p}(X)$ the minimal polynomial of $\overline{b}$ over $\mathrm{res}(F)$. Let $q(X) \in \mathcal{O}_{f(F)}[X]$be the image of p. Since the embedding of residue fields is elementary, $\overline{q}(X)$ is irreducible in $f(\mathrm{res}(F))$ and $\overline{q}(f(\overline{b})) = 0$. Moreover, since $\boldsymbol{k}_L$ has characteristic zero and $\overline{q}$ is irreducible, $\overline{q}'(f(\overline{b})) \neq 0$. Since L is henselian, there is unique $c \in L$ such that $q(c) = 0$ and $\overline{c} = f(\overline{b})$. We extend f to $F(b)$ by $b \mapsto c$.

We need to show that the valuation and angular component are preserved. Let d be the degree of p. Let $x \in F(b) = \alpha(\sum_{i=0}^{d-1} a_i b^i)$ where $\alpha \in F, a_i \in \mathcal{O}_F$ and some $v(a_i) = 0$ for some i. As $\overline{p}$ is the minimal polynomial of $\overline{b}$, $\sum \overline{a}_i \overline{b}^i \neq 0$. Thus $v(x) = v(\alpha)$ and $v(f(x)) = v(f(\alpha))$ and $\mathrm{ac}(x) = \mathrm{ac}(\alpha)(\sum \overline{a}_i \overline{b}^i)$. A similar analysis shows $\mathrm{ac}_L(f(x)) = \mathrm{ac}_L(f(\alpha))(\sum \overline{f(a_i)} \overline{c}^i)$.

claim 2 Suppose we have a Δ-embedding $f : (F, \Gamma, \boldsymbol{k}) \to (L, \Gamma_L, \boldsymbol{k}_L)$ and $b \in B$ with residue $\overline{b}$ transcendental over $\mathrm{res}(F)$. Then we can extend f to $F(b)$.

Let $c \in L$ with $\overline{c} = f(\overline{b})$. Then c is transcendental over F and we can extend f by $b \mapsto c$. We need to show that the valuation and angular component are preserved. If $x \in F[b]$ we can write $x = \alpha(\sum a_i b^i)$ where $\alpha \in F$, $a_i \in O_F$ and $v(a_i) = 0$ for some i. Then as in claim 2, $v(x) = v(\alpha)$ and $v(f(x)) = v(f(\alpha))$, $\mathrm{ac}(x) = \mathrm{ac}(\alpha)(\sum \overline{a}_i \overline{b}^i)$ and v and ac are preserved. As in Lemma 6.4, we can extend to f from $F[b]$ to $F(b)$. $\square$

Next we make the valuation surjective.

Lemma 6.9 *Suppose f is a Δ-embedding of $(F, \Gamma, \boldsymbol{k})$. There is $F \subseteq E \subseteq K$ such that $v : E \to \Gamma$ is surjective and we can extend f to $(E, \Gamma, \boldsymbol{k})$.*

Proof The lemma is proved by iterating the following two claims.

claim 1 Suppose we have a Δ-embedding f of $(F, \Gamma, \boldsymbol{k})$ where the residue map from F to $\boldsymbol{k}$ is surjective and $g \in \Gamma$ such $ng \notin v(F)$ for any $n > 0$. Let $b \in K$ with $v(b) = g$. We will extend f to $F(b)$.

Since g is not in the divisible hull of $v(F)$, b is transcendental over F. Let $c \in L$ with $v(c) = f(g)$ and $\mathrm{ac}_L(c) = f(\mathrm{ac}(b))$. We can extent f to $F(b)$ with $b \mapsto c$. Let $x = \sum a_i b^i$ recall that $v(x) = \min(v(a_i) + iv(b))$ and $v_L(f(x)) = \min v_L(f(a_i) + if(g))$. Choose i such that $v(a_i) + iv(b)$ is minimal, then $x = a_i b^i(1 + \epsilon)$ where $v(\epsilon) > 0$ and $\mathrm{ac}(x) = \mathrm{ac}(a_i)\mathrm{ac}(b)^i$. Similarly, $\mathrm{ac}_L(f(x)) = \mathrm{ac}_L(f(a_i)\mathrm{ac}(c)^i$, as desired.

claim 2 Suppose we have a Δ-embedding f of $(F, \Gamma, \boldsymbol{k})$ where the residue map from F to $\boldsymbol{k}$ is surjective and let $n > 0$ be minimal such that there is $g \in \Gamma \setminus v(F)$ such that $g > 0$ and $ng \in v(F)$. Then we can extend F to E with $F \subset E \subseteq K$ and extend f to a Δ-embedding of $(F, \Gamma, \boldsymbol{k})$ such that $g \in v(E)$.

Let $a \in F$ and $b_0 \in K$ be such that $v(b_0) = g$ and $v(a) = ng$. Since the residue field does not extend we can choose a such that $\mathrm{ac}(b_0^n) = \overline{a}$, in which case $b_0^n = a(1+\epsilon)$ where $\epsilon \in K$ and $v(\epsilon) > 0$. Since K is henselian, there is $d \in K$ with $v(d) = 0$ such that $d^n = 1 + \epsilon$. Let $b = b_0/d$. Then $b^n = a$. By the minimality of n, $X^n - a$ is the minimal polynomial of b over F.

Similarly, we can find $c \in L$ such that $c^n \in f(F)$ and $v_L(c^n) = v(f(a))$. Then $\mathrm{ac}(c)$ is algebraic over $\boldsymbol{k}_{f(F)}$. But $\boldsymbol{k}_{f(F)} \prec \boldsymbol{k}_L$, thus, $\mathrm{ac}(c_0) \in \boldsymbol{k}_{f(F)}$. Thus there is $d \in \mathcal{O}_{f(F)}$ with $\overline{d} = f(\mathrm{ac}(b))\mathrm{ac}(c_0^{-1})$. Let $c_1 = dc_0$. Then $\mathrm{ac}(c_1) = f(\mathrm{ac}(b))$ and $f(a) = f(b^n) = c_1^n(1+\epsilon)$ where $v(\epsilon) > 0$. By henselianity, there is $e \in L$ such that $e^n = (1+\epsilon)$. Let $c = c_1 e$, then $c^n = f(a)$, $v(c) = f(v(b))$ and $\mathrm{ac}(c) = f(\mathrm{ac}(b))$. We extend f to $F(b)$ by $b \mapsto c$. As in Lemma 6.5, we show that f preserves the valuation and the the angular component map. $\square$

Lemma 6.10 *Suppose the residue and valuation maps of $(F, \Gamma, \boldsymbol{k})$ are surjective and f is a Δ-embedding. Then we can extend F to $(F^h, \Gamma, \boldsymbol{k})$*

Proof There is a unique valuation preserving extension of f from F to $g : F^h \to L$. We know that F^h is an immediate extension of f. If $a \in F^h \setminus F$, there is $b \in F$, with $v(a) = v(b)$, but then $v(g(a)) = v(g(b))$. There is c a unit in $\mathcal{O}_F$ such that $\mathrm{res}(c) = \mathrm{res}(a/b)$. Thus $\mathrm{ac}(a) = \mathrm{ac}(b)\mathrm{ac}(c)$ and $\mathrm{ac}_L(g(a)) = \mathrm{ac}_L(g(b))\mathrm{ac}_L(g(c))$. $\square$

We can now finish the proof of Theorem 6.3

Thus we may assume that we have a $(F, \Gamma, \boldsymbol{k})$ such that F is henselian, $v : F \to \Gamma$ and $\mathrm{res} : F \to \boldsymbol{k}$ are surjective and f is a Δ-embedding. Then K is an immediate extension of F. By Zorn's Lemma, we may assume that $F \subseteq K$ is maximal henselian such that there is a Δ-embedding of $(F, \Gamma, \boldsymbol{k})$ into L extending f. We claim that $F = K$. If not, let $b \in K \setminus F$. We will show that we can extend f to $F(b)$. Since F is henselian and $\boldsymbol{k}_B$ has characteristic zero, by Theorem 5.14, b is transcendental over F.

We can find a pseudocauchy sequence (a_α) in F of transcendental type with no pseudolimit in F such that $(a_\alpha) \rightsquigarrow b$, (a_α) has no pseudolimit in F and $(v(p(a_\alpha))$ is eventually constant for $p \in F[T]$.

By $\aleph_1$-saturation, we can find $c \in L$ such that $(f(a_\alpha)) \rightsquigarrow c$. Extend f to $F(b)$ by $x \mapsto c$. For $p \in F[T]$,

$$v_L(f(p(b))) = v_L(f(p)(b)) = v_L(f(p)(f(a_\alpha))) = v_L(f(p(a_\alpha)) = f(v(p(a_\alpha)) = f(v(p(b)))$$

for large enough α. Similarly, $\mathrm{ac}(p(b)) = \mathrm{ac}(p(a_\alpha))$ for large enough α and it follows that $f(\mathrm{ac}(p(b))) = \mathrm{ac}_L(f(p(b)))$. But this contradicts the maximality of F.

This completes the proof.

6.2 Consequence of Quantifier Elimination

Let T_0 be the theory in the language of three sorted valued fields asserting that we have $(K, \Gamma, \boldsymbol{k})$ where K is a henselian valued field where Γ is the value group and $\boldsymbol{k}$ is a the residue field.

Corollary 6.11 (Ax-Kochen [2], Eršov[18]) *Let $(K, \Gamma, \boldsymbol{k})$ be a henselain valued field with characteristic zero residue field. Let T_Γ be the theory of the value group in the language of ordered groups and $T_{\boldsymbol{k}}$ be the theory of the residue field in the language of rings. Then $T = T_0 \cup T_\Gamma \cup T_{\boldsymbol{k}}$ is complete.*

Proof Let K and L be models of T and let $K \prec K^*$ and $L \prec L^*$ be $\aleph_1$-saturated elementary extensions. We can define angular component maps on K^* and L^*. Consider the substructure $(\mathbb{Q}, \{0\}, \mathbb{Q})$. Since T_Γ and $T_{\boldsymbol{k}}$ are complete, the identification of this structure in K^* and L^* is a Δ-embedding. Let K' be a countable elementary submodel of K^* in the Pas-language. By Theorem 6.3, we can extend this to a Δ-embedding of K into L^*. Let ϕ be any sentence in the language of valued fields. There is ψ a disjunction of Δ-sentences equivalent to ϕ. Then

$$K \models \phi \Leftrightarrow K^* \models \phi \Leftrightarrow K' \models \psi \Leftrightarrow L^* \models \psi \Leftrightarrow L^* \models \phi \Leftrightarrow L \models \phi.$$

□

Corollary 6.12 *Let $\mathcal{U}$ be an nonprinciple ultrafilter on the set of primes. Then*

$$\prod \mathbb{Q}_p/\mathcal{U} \equiv \prod \mathbb{F}_p((T))/\mathcal{U}.$$

In particular, for any sentence in the language of valued fields $\mathbb{Q}_p \models \phi$ for all but finitely many primes p if and only if $\mathbb{F}_p((T)) \models \phi$ for all but finitely many primes p.

Proof $\prod \mathbb{Q}_p/\mathcal{U}$ and $\prod \mathbb{F}_p((T))/\mathcal{U}$ are henselian valued fields with value group $\prod \mathbb{Z}/\mathcal{U}$ and characteristic zero residue field. Hence they are elementarily equivalent.

If $\mathbb{Q}_p \models \phi$ for all but finitely many primes and D is an infinite set of primes where $\mathbb{F}_p((T)) \models \neg\phi$, let $\mathcal{U}$ be an ultrafilter on the primes such that $D \in \mathcal{U}$. Then, by the Fundamental Theorem of Ultraproducts $\prod \mathbb{Q}_p/\mathcal{U} \models \phi$ and $\prod \mathbb{F}_p((T))/\mathcal{U} \models \neg\phi$, a contradiction. The converse is similar. □

Exercise 6.13 Show that if the Continuum Hypothesis is true then $\prod \mathbb{Q}_p/\mathcal{U} \cong \prod \mathbb{F}_p((T))/\mathcal{U}$.

We will discuss applications of this in the next section.

Corollary 6.14 *Suppose $(K, \Gamma, \boldsymbol{k})$ is a valued field with angular component and T_Γ and $T_{\boldsymbol{k}}$ have quantifier elimination, then every formula is equivalent to a quantifier free formula.*

Proof Every Δ-formula is equivalent to a quantifier free formula. $\square$

Exercise 6.15 Let $K \subset L$ be henselian valued fields of characteristic zero. Suppose $\Gamma_K \prec \Gamma_L$ and $\boldsymbol{k}_K \prec \boldsymbol{k}_L$. Show that $K \prec L$.

We can generalize Corollary 5.17 to drop the assumption that our field is ordered and the valuation ring is convex.

Corollary 6.16 *Let K be a henselian valued field with real closed residue field and divisible value group. Then K is real closed.*

As in ACVF in equicharacteristic zero henselian valued fields the resiude field and value group are stably embedded and orthogonal.

Exercise 6.17 Let $(K, \Gamma, \boldsymbol{k})$ be a henselian valued field with characteristic zero residue field. Any definable subset of $\Gamma^m \times \boldsymbol{k}^n$ is a finite union of rectangles $A \times B$ where $A \subseteq \Gamma^m$ is definable in the group language and $B \subset \boldsymbol{k}^n$ is definable in the ring language.

NIP

Not all theories of henselian valued fields have NIP. For example the theory of $\prod \mathbb{Q}_p/\mathcal{U}$ has the independence property since the pseudofinite field $\prod \mathbb{F}_p/\mathcal{U}$ has the independence property.

Exercise 6.18 **[Duret] [15]** Show that the theory of any infinite pseudofinite field has the independence property. In particular, show that for any distinct $a_1, \ldots, a_m$ there are b_I for $I \subseteq \{1, \ldots, m\}$ such that $a_i + b_J$ is a square if and only if $i \in J$. [Recall that in an infinite pseduofinite field every absolutely irreducible variety has a point.]

Indeed the theory of $\prod \mathbb{Q}_p/\mathcal{U}$ is NTP_2. In fact, failure of NIP in the residue field is the only obstruction to NIP. Delon [7] proved that a Henselian valued field with characteristic zero residue field has NIP if and only if the theories of the residue field and the value group have NIP. But Gurevich and Schmitt [20] showed that all theories of ordered abelian groups have NIP.

Theorem 6.19 (Delon) *Henselian valued field with characteristic zero residue fields have NIP if and only if the theory of the residue field has NIP and the theory of value group has NIP.*

Corollary 6.20 *Henselian valued field with characteristic zero residue fields have NIP if and only if the theory of the residue field has NIP.*

We will give a proof of Delon's theorem from Simon [39]. We will use an alternative characterization of the independence property (see [39] 2.7).

Lemma 6.21 *A formula $\phi(x, \mathbf{y})$ has the independence property if and only if, in a suitably saturated model, there is an indiscernible sequence $(x_0, x_1, \ldots)$ and $\mathbf{b}$ such that $\phi(x_i, \mathbf{b})$ holds if and only if i is even.*

Lemma 6.22 *Let $(K, \Gamma, \boldsymbol{k})$ be a valued field with angular component, $f(X) = a_0 + a_1 X + \cdots + a_d X^d \in K[X]$ and let $x_0, x_1, \ldots$ be a sequence of elements of K such that $v(x_0), v(x_1), \ldots$ is strictly increasing or strictly decreasing. There is $r \leq d$ and $t \in \mathbb{N}$ such that*

$$v(f(x_i)) = v(a_r x_i^r) < v(a_j x_i^j) \text{ and } \mathrm{ac}(f(x_i)) = \mathrm{ac}(a_r x_i^r)$$

for all $i \geq t$ and $j \neq r$.

Proof Consider the cut $v(x_i)$ makes with respect to the finite set $X = \{\frac{v(a_j)-v(a_k)}{k-j} : 0 \leq i < j \leq d\}$. Since $v(x_i)$ is strictly increasing or strictly decreasing, there is an t such that for all $v(x_i)$ are not in X and realize the same cut over X for $i \geq t$.

Note that if $\frac{v(a_j)-v(a_k)}{k-j} < v(x_i)$, then $v(a_j x_i^j) < v(a_k x_i^k)$. Choose r such that $v(a_r x_i^r)$ is minimal, then r is unique and works for all $i \geq t$. In this case, $v(f(x_i)) = v(a_r x_i^r)$ and $\mathrm{ac}(f(x_i)) = \mathrm{ac}(a_r x_i^r)$ for $i \geq t$, as desired. □

Lemma 6.23 *Let $(K, \Gamma, \boldsymbol{k})$ be an $\aleph_1$-saturated valued field with angular component and let $x_0, x_1, \ldots$ be a sequence of indiscernibles in K. Then there are indiscernible sequences $g_0, g_1, \ldots$ of indiscernibles in Γ and $b_0, b_1, \ldots$ of indiscernibles in $\boldsymbol{k}$ such that for any $f \in K[X]$ there is r and $\gamma \in \Gamma$ such that $v(f(x_i)) = \gamma + r g_i$ and there is $q \in \boldsymbol{k}[x]$ such that $\mathrm{ac}(f(x_i)) = q(b_i)$ for all large enough i.*

Proof
case 1 The sequence $v(x_0), v(x_1), \ldots$ is nonconstant.

We take $g_i = v(x_i)$ and $b_i = \mathrm{ac}(x_i)$. Then by indiscernibility it is either strictly increasing or strictly decreasing and we can apply the previous lemma to conclude that $v(f(x_i)) = v(a_r x_i^r)$ and $\mathrm{ac}(f(x_i)) = \mathrm{ac}(a_r x_i^r)$ for large enough i. Thus the lemma is true if we take $\gamma = v(a_r)$ and $q(X) = a_r X^r$.

From now on we assume that $v(x_0), v(x_1), \ldots$ is a constant sequence. Let $y_i = x_i - x_0$. The sequence $v(y_0), v(y_1), \ldots$ is not strictly increasing. If it were, then

$$v(x_i - x_1) = v((x_i - x_0) - (x_1 - x_0)) = v(y_i - y_1) = v(y_1).$$

But then the sequence $(v(x_i - x_1))$ is constant, while the sequence $v(x_i - x_0)$ is increasing, contradicting indiscernibility.

case 2 The sequence $v(y_1), v(y_2), \ldots$ is decreasing.

In this case we will take $g_i = v(y_{i+1})$, $a_i = \mathrm{ac}(y_{i+1}$. Let $f(X) \in K[X]$. There is $h(X) \in K[X]$ such that $f(x_i) = f(x_0 + y_i) = f(x_0) + h(y_i)$ for all $i > 0$. As in case 1, we can apply the previous lemma applied to the sequence $y_1, y_2, \ldots$.

case 3 The sequences $(v(y_i))$ and $(\mathrm{ac}(y_i))$ are constant.

Then

$$v(x_2 - x_1) = v(y_2 - y_1) > v(y_1) = v(y_2) = v(x_2 - x_0)$$

Find $x_\omega \in K$ such that $x_0, x_1, \ldots, x_\omega$ is an indiscernible sequence of order type $\omega+1$. Let $z_i = x_\omega - x_i$. By indiscernibility, $v(z_1), v(z_2), \ldots$ is an increasing sequence. Let $g_i = v(z_{i+1})$ and $a_i = \mathrm{ac}(z_i)$. For $f(X) \in K[X]$ as in case 2 there is $h(X) \in K[X]$ such that for $i > 0$ $f(x_i) = h(z_i)$ using the lemmas we proceed as in the previous cases.

case 4 The sequence $v(y_i)$ is constant but the sequence $(\mathrm{ac}(y_i))$ is not.

In this case let $g_i = v(y_0)$, a constant sequence, and let $b_i = \mathrm{ac}(y_i)$.

For any $f(X) \in K[X]$ we can find $h(X) \in K[X]$ such that

$$f(x_0 + Y) = h(y_i) = \sum_{n=0}^{d} a_n Y^n.$$

Let $A \subset \{0, \ldots, d\}$ be the set of n such that $v(a_n) + ng_0$ is minimal. Let $q(X) = \sum_{n\in A} \mathrm{ac}(a_n)X^n$. For sufficiently large i, $q(\mathrm{ac}(y_i)) \neq 0$. But then

$$v(f(x_i)) = v\left(\sum_{n=0}^{d} a_n y_i^n\right) = v\left(\sum_{n\in A} a_n y_i^n\right) = v(a_n) + ng_0 = v(a_n) + ng_i$$

and

$$\mathrm{ac}(f(x_i)) = q(\mathrm{ac}(y_i))$$

where n is any fixed element of A and i is sufficiently large. □

We are now ready to prove Delon's Theorem. By the Pas quantifier elimination and the basic facts about NIP from Lemma 4.21. it suffices to show that formulas of the following form have NIP.

1. $f(x, \mathbf{y}) = 0$, $f \in K[X, \mathbf{Y}]$ and $x, \mathbf{y}$ are variables in the home sort;

2. $\phi(x, t_1(\mathbf{y}), \ldots, t_m(\mathbf{y}))$ where ϕ is a formula in the language of ordered groups, $\mathbf{y}$ are variables from the home and value group sort and $t_1, \ldots, t_m$ are terms with values in the value group sort;

3. $\psi(x, t_1(\mathbf{y}), \ldots, t_m(\mathbf{y}))$ where ψ is a formula in the language of rings , $\mathbf{y}$ are variables from the home and residue field sort and $t_1, \ldots, t_m$ are terms with values in the residue sort;

4. $\theta(v(f_1(x, \mathbf{y})), \ldots, v(f_m(x, \mathbf{y})), \mathbf{z})$ where θ is a formula in the language ordered groups x and $\mathbf{y}$ are variables in the home sort, $f_1, \ldots, f_m \in \mathbb{Z}[X, \mathbf{Y}]$ and $\mathbf{z}$ are variables in the ordered group;

5. $\chi(\mathrm{ac}(f_1(x, \mathbf{y})), \ldots, \mathrm{ac}(f_m(x, \mathbf{y})), \mathbf{z})$ where χ is a formula in the language rings x and $\mathbf{y}$ are variables in the home sort, $f_1, \ldots, f_m \in \mathbb{Z}[X, \mathbf{Y}]$ and $\mathbf{z}$ are variables in the ring sort;

Formulas of types 1, 2 and 3 are easily seen to by NIP. If the x variable is of degree d in $f(x, \mathbf{y})$, then $f(x, \mathbf{y}) = 0$ fails to shatter a set of size $d + 2$. Thus formulas of the first type are NIP. Formulas of the second and third type are NIP by our assumptions on the theories of the residue field and the value group.

Consider $\Theta(x, \mathbf{y}, \mathbf{z}) = \theta(v(f_1(x, \mathbf{y})), \dots, v(f_m(x, \mathbf{y})), \mathbf{z})$ of type 4. If Θ has the independence property, then we can find a sequence of indiscernibles in K $(x_1, x_2, \dots)$ and $\mathbf{b}_1, \mathbf{b}_2$ such that $\Theta(x_i, \mathbf{b}_1, \mathbf{b}_2)$ holds if and only if i is even. By Lemma 6.23 there is are $g_0, g_1, \dots$ an indiscernible sequence of elements in the value group such that for $j = 1, \dots, n$ there are $h_j \in \Gamma$ and $r_j \in \mathbb{N}$ such that $v(f_j(x_i, \mathbf{b}_1) = h_j + r_j g_j$ for sufficiently large i. Consider the formula $\Theta^*(v, \mathbf{h}, \mathbf{b}_2)$ which is $\theta(h_1 + r_1 v, \dots, h_m + r_m v, \mathbf{b}_2)$ where v is a variable over the value group. Since the theory of the value group has NIP, $\Theta^*(g_i, \mathbf{h}, \mathbf{b}_2)$ is either eventually true, or eventually false for large i, but $\Theta^*(g_i, \mathbf{h}, \mathbf{b}_2)$ is equivalent to $\Theta(x_i, \mathbf{b}_1, \mathbf{b}_2)$ for large i. Thus Θ does not have the independence property.

The argument for formulas of type 5 is similar.

6.3 Artin's Conjecture

We say that a field K is a C_m*-field* if whenever $f(X_1, \dots, X_n)$ is a homogeneous polynomial of degree d where $n > d^m$, then f has a nontrivial zero in K.

Exercise 6.24 Show that K is a C_m-field if and only if every homogeneous polynomial of degree $d^m + 1$ has a nontrivial zero in K

Tsen and Lang [27] proved that if F is a finite field then $F(\!(T)\!)$ is a C_2 field and Artin conjecture that each $\mathbb{Q}_p$ is a C_2-field. This is false.

Exercise 6.25 [Terjanian] Let

$$p(X, Y, Z) = X^2YZ + XY^2Z + XYZ^2 + X^2Y^2 + X^2Z^2 - X^4 - Y^4 - Z^4$$

let

$$q(X_1, \dots, X_9) = p(X_1, X_2, X_3) + p(X_4, X_5, X_6) + p(X_7, X_8, X_9)$$

and

$$r(X_1, \dots, X_{18}) = q(X_1, \dots, X_9) + 4q(X_{10}, \dots, X_{18}).$$

a) Show that if $(x, y, z) \in \mathbb{Z}^3$ are not all even, then $p(x, y, z) = 3(\text{mod } 4)$.

b) Show that if $(x_1, \dots, x_9) \in \mathbb{Z}^9$ are not all even , then $q(x_1, \dots, x_9) \neq 0(\text{mod } 4)$.

c) If $\mathbf{x} = (x_1, \dots, x_{18}) \in \mathbb{Z}_2^{18}$ and some x_i is a unit, then $v_2(\mathbf{x}) = 0$ or 2.

d) Conclude that Artin's conjecture fails for $\mathbb{Q}_2$ with $n = 18$ and $d = 4$.

Nevertheless, the Ax, Kochen, Eršov transfer principle tell us is true for sufficiently large p.

Corollary 6.26 *Fix d. There is a prime p_0 such that for all primes $p \geq p_0$ every homogenous polynomials of degree d in $n > d^2$ variables has a nontrivial zero in $\mathbb{Q}_p$.*

Proof The statement that every homogeneous polynomial of degree d in $d^2 + 1$ variables has a nontrivial zero is a first order sentence that is true in every $\mathbb{F}_p(\!(T)\!)$ and hence true in $\mathbb{Q}_p$ for p sufficiently large. $\square$

The Tsen–Lang Theorem

We will prove that $F(\!(T)\!)$ is C_2 if F is finite.

Lemma 6.27 *If F is a finite field with $|F| = q$ and $n < q-1$, then*

$$\sum_{x \in F} x^n = 0$$

Proof Let $a \in F^\times$ with $a^n \neq 1$. Since $x \mapsto ax$ is a bijection,

$$\sum x^n = \sum (ax)^n = a^n \sum x^n.$$

Since $a^n \neq 1$, $\sum x^n = 0$. $\square$

Theorem 6.28 (Chevalley–Warning) *Let F be a finite field of characteristic p and let $f_1, \ldots, f_m \in F[X_1, \ldots, X_n]$ be polynomials of degrees $d_1, \ldots, d_m$ with $n > \sum d_i$. Then the number of zeros of $f_1 = \cdots = f_m$ in F is divisible by p.*

In particular, if the polynomials $f_1, \ldots, f_m$ are homogeneous, there is a nontrivial zero in F.

Proof Let F have characteristic p and cardinality q. Let N be the number of zeros of $f_1 = \cdots = f_m = 0$ in F^n. Note that for all $\mathbf{x} \in F^n$

$$\prod_{i=1}^{k} (1 - f_i(\mathbf{x})^{q-1}) = \begin{cases} 1 & \text{if } f_1(\mathbf{x}) = \cdots = f_k(\mathbf{x}) = 0 \\ 0 & \text{otherwise} \end{cases}.$$

Thus the number of zeros of f is

$$N = \sum_{\mathbf{x} \in F^n} \prod_{i=1}^{k} (1 - f_i(\mathbf{x})^{q-1}) = \sum_{\mathbf{x} \in F^n} \sum_{\mathbf{j} \in J} c_j \mathbf{x}^{\mathbf{j}} = \sum_{\mathbf{j} \in J} c_j \left(\sum_{\mathbf{x} \in F^n} \mathbf{x}^{\mathbf{j}} \right) (\text{mod } p)$$

where $J = \{\mathbf{j} = (j_1, \ldots, j_n) : \sum j_i \leq (q-1) \sum d_i\}$.

Fix $\mathbf{j} = (j_1, \ldots, j_n) \in J$. Note that, since $n > \sum d_i$, we must have some $j_{\hat{i}} < q-1$. Then

$$\sum_{\mathbf{x} \in F^n} \mathbf{x}^{\mathbf{j}} = \prod_{i=1}^{n} \sum_{x \in F} x^{j_i}$$

Thus, by the lemma, $\sum_{x \in F} x^{j_{\hat{i}}} = 0$ and $N = 0 (\text{mod } p)$. $\square$

We can combine this with Greenleaf's Theorem 2.27.

Corollary 6.29 *If $f_1, \ldots, f_m \in \mathbb{Z}[X_1, \ldots, X_n]$ where f_i has degree d_i and $n > \sum d_i$, then for all but finitely many primes p, $f_1 = \cdots = f_m = 0$ has a solution in $\mathbb{Z}_p$.*

Lemma 6.30 *Let $F(T)$ be the field of rational functions over a finite field F. Let $f \in F(T)[X_1, \ldots, X_n]$ be homogeneous of degree $d^2 < n$. Then f has a nontrivial zero in $F(T)^n$.*

Proof Clearing denominators, we may assume $f \in F[T][X_1, \ldots, X_n]$. We will look for a solution of the form $(x_1, \ldots, x_n)$ where for some suitably large s

$$x_i = y_{i,0} + y_{i,1}T + \cdots + y_{i,s}T^s.$$

Let r be the maximum of the degrees of the coefficients of f. Choose $s > (d(r+1) - n)/n - d^2$. Then $n(s+1) > d(ds + r + 1)$ Then

$$f(x_1, \ldots, x_n) = f_0(\mathbf{y}) + f_1(\mathbf{y})T + \cdots + f_{ds+r}(\mathbf{y})T^{ds+r}.$$

Since $n(s+1) > d(ds+r+1)$, by Chevalley-Warning, there is a nontrivial zero $\mathbf{y} = (y_{1,0}, \ldots, y_{n,s}) \in F$. $\square$

Corollary 6.31 *Let $f \in F(\!(T)\!)[X_1, \ldots, X_n]$ be homogeneous of degree d with $d^2 < n$ and F is a finite field. Then f has a nontrivial zero in $F(\!(T)\!)$.*

Proof We may assume $f \in F[[T]](X_1, \ldots, X_n)$. For k sufficiently large let $f|k(X_1, \ldots, X_n)$ be the polynomial over $F[T]$ obtained by truncating all the coefficients of f to polynomials of degree at most k. By the lemma $f_k(X_1, \ldots, X_n)$ has a nontrivial zero $\mathbf{a}_k \in F(T)^n$. We may assume that $v(a_{k,i}) \geq 0$ for all i and some $v(a_{k,i}) = 0$. Since the residue field is finite we see that $F[[T]]$ is compact so we can choose a Cauchy subsequence of the $\mathbf{a}_k$ that converges to a nonzero element of $F[[T]]^n$. $\square$

7 The Theory of $\mathbb{Q}_p$

7.1 p-adically Closed Fields

We next turn our attention to the theory of $\mathbb{Q}_p$. If $K \equiv \mathbb{Q}_p$, then $(v(G), +, <, 0, v(p)) \equiv (\mathbb{Z}, +, <, 0, 1)$. We know that the complete theory of $(\mathbb{Z}, +, <, 0, 1)$ is just Presburger arithmetic which is axiomatized by saying that we have an ordered abelian group with least positive element 1 such that for any x and $n \geq 2$ there is a y such that $x = ny$ or $x = ny + 1 \ldots$ or $x = ny + n - 1$.

We have quantifier elimination in Presburger arithmetic once we add either equivalence relation $x \equiv_n y$ for $x = y (\mathrm{mod}\ n)$ or predicates for the elements divisible by n, for all $n \geq 2$.

Definition 7.1 We say that a valued field (K, v) is p-adically closed if K is henselian of characteristic zero, the residue field is $\mathbb{F}_p$ and the value group in a model of Presburger arithmetic and $v(p)$ is the least positive element of the value group.

Lemma 7.2 *Let K be p-adically closed, $x \in K$ and $v(x) = gn + i$ where $0 \leq i < n$, then there is $m \in \mathbb{Z}$ with $0 \leq v(m) < n$ and $y \in K$ such that $x = my^n$.*

Proof Suppose K is p-adically closed and $v(x) = gn + i$. Choose z such that $v(z) = g$, then $v(\frac{x}{p^i g^n}) = 0$. There is $0 < r < p^{2v(n)+1}$ such that $\frac{x}{p^i z^n} = r (\mathrm{mod}\ p^{2v(n)+1})$ and $p \not| r$. Let $c = \frac{x}{rp^i z^n}$. Then $c = 1 (\mathrm{mod}\ p^{2v(n)+1})$. Consider $f(X) = X^n - c$, then $v(f'(1)) > 2v(n)$ and $v(f'(1)) = v(n)$. By Lemma 2.6 ii), there is $y \in F$ such that $y^n = c$. Then $x = rp^i (yz)^n$ and $0 \leq v(rp^i) < n$. $\square$

Lemma 7.3 *Suppose F is a p-adically closed field, $A \subset F$ and E is the algebraic closure of $\mathbb{Q}(A)$ in F. Then E is p-adically closed.*

Proof Since E is algebraically closed in F, E is henselian. Clearly E has characteristic zero, $\boldsymbol{k}_E = \mathbb{F}_p$ and $v(p) = 1$. So we need only show $v(E)$ is a $\mathbb{Z}$-group. Let $x \in E$. There is $y \in F$ and $m \in \mathbb{Z}$ such that $x = my^n$ and $0 \leq v(m) < n$. Since E is algebraically closed in F, $y \in E$, but then $v(x) = nv(y) + v(m)$ as desired. $\square$

We will show that the theory of p-adically closed fields has quantifier elimination in the Macintyre language $\mathcal{L}_{\mathrm{Mac}} = \{+, -, \cdot, |, P_2, P_3, \ldots, 0, 1\}$ where P_n is a predicate picking out the n^{th}-powers. The symbol $|$ is actually unnecessary as we can always define $|$ in a quantifier free way using P_2 as in Exercise 2.11.

We begin with some useful lemmas about n^{th}-powers.

Lemma 7.4 *Let K be henselian of characteristic zero. Let $a \in K^\times$ and $\gamma = v(a) + 2v(n)$. Then a is an n^{th}-power in K if and only every $b \in B_\gamma(a)$ is an n^{th}-power in K.*

Proof Suppose $b \in B_\gamma(a)$. Let $c = b/a$.

$$v(1 - c) = v(a - b) - v(a) > 2v(n).$$

Consider $f(X) = X^n - c$. Then

$$v(f(1)) = v(1-c) > 2v(n) \text{ and } v(f'(1)) = v(n).$$

Thus by Lemma 2.6 ii), there is $u \in K$ $u^n = c$. Then $au^n = b$ and a is an n^{th}-power if and only if b is. $\square$

Corollary 7.5 *In a henselian field of characteristic zero, the set of nonzero n^{th}-powers is open.*

Corollary 7.6 *Suppose K is henselian of characteristic zero with residue field $\boldsymbol{k}$ of characteristic p where $v(p)$ is the least positive element of the value group. Suppose $F \subset E \subseteq K$, E/F is immediate and $a \in E$. Then there is $b \in F$ such that $v(a-b) > v(a) + 2v(n)$ and for any such b we have that $a \in K^n$ if and only if $b \in K^n$.*

Proof Since $F(a)/F$ is immediate, there is $b_0 \in F$ such that $v(a - b_0) > v(a)$. We can then find a $b_1 \in F$ such that

$$v(a - b_1) > v(a - b_0) \geq v(a) + v(p).$$

Continuing inductively, we can find $b \in F$ such that $v(a - b) > v(a) + 2v(n)$. By the lemma, a is an n^{th}-power in K if and only any such b is. $\square$

Lemma 7.7 *Suppose K is henselian of characteristic zero and residue field $\mathbb{F}_p$ and $v(p)$ is the least positive element of the value group. Let $F \subset K$ and suppose $g \in v(K) \setminus v(F)$, $ng \in v(F)$ Then there is $b \in F$ with $v(b) = g$ such that $b^n \in F$.*

Proof Let $a \in F$ and $c \in K$ such $v(c) = g$ and $v(a) = ng$. Since K and F have the same residue field, without loss of generality we can choose a such that $c^n = a(1+\epsilon)$ where $v\epsilon > 0$. We can find $0 \leq m < p^{2v(n)+1}$ such that $m = \epsilon(\text{mod } p^{2v(n)+1})$. Then $c^n = a(1+m)(1+\delta)$ where $v(\delta) > 2v(n)$. Since K is henselian, there is $u \in K$ such that $u^n = 1 + \delta$. But then $(c/u)^n = a(1+m)$ and $v(c/u) = g$. $\square$

Quantifier elimination will follow from the following embedding result.

Theorem 7.8 (Macintyre[29]) *Suppose (K, v) and (L, w) are p-adically closed fields where K is countable and L is $\aleph_1$-saturated. Suppose A is a subring of K and $f : A \to L$ is an $\mathcal{L}_{Mac}$-embedding. Then f extends to an $\mathcal{L}_{\text{Mac}}$-embedding of K into L.*

This will be proved by iterating the following lemmas. Throughout we assume that K and L satisfy the hypotheses of the theorem. If $A \subset K$ and f is an $\mathcal{L}_{\text{Mac}}$-embedding, we will think of this as also defining a map on the value group by $f(v(a)) = w(f(b))$.

Lemma 7.9 *Suppose A is a subring of K and $f : A \to K$ is and $\mathcal{L}_{\text{Mac}}$-embedding, then we can extend f to F the fraction field of A.*

Proof Since

$$w(f(a)/f(b)) = w(f(a)) - w(f(b)) = f(v(a)) - f(v(b)) = f(v(a/b),$$

the natural extension preserves divisibility. Since

$$P_n(a/b) \Leftrightarrow P_n(ab^{n-1}),$$

the predicates P_n are preserved. $\square$

Lemma 7.10 *Suppose $F \subset K$ and $f : F \to L$ is an $\mathcal{L}_{\mathrm{Mac}}$-embedding, then f extends to an $\mathcal{L}_{\mathrm{Mac}}$-embedding of F^h into L*

Proof Let f also denote the unique extension to a valued field embedding of F^h into F. Since F^h/F is immediate, for all n and all $a \in F^h$ there is a $b \in F$ such that $v(b-a) > v(a) + 2v(n)$. Then $v(f(a) - f(b)) > v(f(a)) + 2v(n)$ and

$$P_n(a) \Leftrightarrow P_n(b) \Leftrightarrow P_n(f(b)) \Leftrightarrow P_n(f(a).$$

Hence f is an $\mathcal{L}_{\mathrm{Mac}}$-embedigin $\square$

Our next goal is to show that if we have an $\mathcal{L}_{\mathrm{Mac}}$-embedding of a subfield F of K into L, that it extends to the algebraic closure of F in K. The next lemma shows that if we can extend to a valued field embedding it will automatically be an $\mathcal{L}_{\mathrm{Mac}}$-embedding.

Lemma 7.11 *If $F \subseteq K$ is algebraically closed in K then any valuation preserving embedding of F into L preserves the predicates P_n.*

Proof Clearly if $P_n(a)$, then a is an n^{th}-power in K and, since F is algebraically closed in K there is $b \in F$ such that $b^n = a$. But then $f(b)^n = f(a)$ and $P_n(f(a))$.

Suppose $P_n(f(a))$. Suppose, for contradiction, that all of the n^{th}-roots of $f(a)$ are in $L \setminus f(K)$.

Note that Γ_K/Γ_F is torsion free. Suppose not. Let n be minimal such that there is $g \in \Gamma_K \setminus \Gamma_F$ such that $ng \in \Gamma_F$. By Lemma 7.7, we can find $a \in F$ with $v(a) = ng$ such that a has an n^{th}-root in K. Then a has an n^{th}-root in F.

It follows that $\Gamma_L/\Gamma_{f(F)}$ is also torsion free. To see this, note that if $g \in \Gamma_F$ and $n \not| \, g$ there is $1 \leq i < n$ and $b \in F$ such that $g = nv(b) + i$. Then $f(g) = w(f(b^n)) + i$ and $n \not| f(g)$.

By Exercise 2.4 F is henselian and hence $f(F)$ is henselian and, by Theorem 5.14 has no proper algebraic immediate extensions.

Let $b \in L$ with $b^n = f(a)$. Then $f(F)(b)$ is not an immediate extension of $f(F)$. Since the residue field does not extend, the value group must extend. Since the extension is algebraic, there is $g \in \Gamma_L \setminus \Gamma_{f(F)}$ such that $mg \in \Gamma_{f(F)}$ for some m, but this contradicts that $\Gamma_L/\Gamma_f(F)$ is torsion free. $\square$

Lemma 7.12 *Suppose $F \subseteq K$ is henselian and we have an $\mathcal{L}_{\mathrm{Mac}}$-embedding $f : F \to L$. Let K_0 be the algebraic closure of F in K. Then we can extend f to an $\mathcal{L}_{\mathrm{Mac}}$-embedding of K_0 into K.*

Proof By $\aleph_1$-saturation it suffices to show that we can extend f to any E where $F \subset E \subseteq K$ and E/F is a finite algebraic extension. Since F is henselian and unramified, E/F is not immediate. In particular $\Gamma_F \subset \Gamma_E \subset \mathbb{Q}\Gamma_F$. Thus Γ_E/Γ_F is finite abelian group. Suppose

$$\Gamma_E/\Gamma_F = \langle g_1/F \rangle \oplus \cdots \oplus \langle g_m/F \rangle$$

where $\langle g_i/F \rangle$is cyclic over order n_i. Then $n_i g_i \in \Gamma_F$ and n_i is minimal with this property. By Lemma 7.7, there are $a_1, \ldots, a_m \in E$ such that $v(a_i) = g_i$ and $a_i^{n_i} \in F$. Since F is henselian, so is $F(a_1, \ldots, a_m)$. But $E/F(a_1, \ldots, a_m)$ is immediate and, hence, $F(a_1, \ldots, a_m) = E$.

Since f is an $\mathcal{L}_{\mathrm{Mac}}$-embedding, there are $b_1, \ldots, b_m \in L$ such that $b_i^{n_i} = f(a_i^{n_i})$. We claim that we can extend f to a valuation preserving embedding of E into L with $a_i \mapsto b_i$.

We argue this in detail in the case $m = 1$. Suppose $a \in E$, $v(a) = g$, n is minimal such that $ng \in \Gamma_F$ and $a^n \in F$. Suppose $x = c_n a^{n-1} + \ldots c_1 a + c_0 \in E(a)$. By the minimality of n, $v(c_i) + iv(a) \neq v(c_j) + jv(a)$ for any $i < j < n$. Thus $X^n - a^n$ is irreducible over F and $v(x) = \min v(c_i) + iv(a)$. It follows that $X^n - f(a^n)$ is irreducible over $f(F)$ and that if $b \in L$ such that $b^n = f(a^m)$, then the extension of f to $F(a)$ obtained by sending a to b is valuation preserving. The general case is done similarly by induction. □

The full embedding result will follow from the next lemma.

Lemma 7.13 *Suppose $F \subset F_1 \subseteq K$ $f : F \to K$ is a valued field embedding. F and F_1 are algebraically closed in K and F_1/F is transcendence degree 1. Then we can extend f to F_1.*

Proof There are two cases to consider.

case 1 F_1/F is immediate.

Let $a \in F_1 \setminus F$. We can find a pseudocauchy sequence of transcendental type $(a_\alpha) \rightsquigarrow a$ such that (a_α) has no pseudolimit in F. We can find $b \in L$ a pseudolimit if $(f(a_\alpha))$ and can extend f to a valued field embedding of $F(a)$ into L by sending a to b. We can further extend f to a valued field embedding of $F(a)^h$ into L. But $F_1/F(a)$ is an immediate algebraic extension, thus $F_1 = F(a)^h$ and we have the desired embedding.

case 2 F_1/F is not immediate.

By $\aleph_1$-saturation, it suffices to show that we can extend the embedding to any $F \subset E \subseteq F_1$ where E/F is finitely generated. Then Γ_E/Γ_F is finitely generated and torsion free, since E/F has transcendence degree one we must have $\Gamma_E = \Gamma_F \oplus \mathbb{Z}v(a)$ for some $a \in E$ transcendental over F. We can find $b \in L$ transcendental over $f(F)$ such that the type $w(b)$ realizes over $v(\Gamma_F)$ is the image of the type $v(a)$ realizes over Γ_F. We claim that sending $a \mapsto b$ gives a valued field embedding of $F(a)$ into L. Suppose $x \in F[a]$ and $x = \sum_{c_i} a^i$ where each $c_i \in F$. By choice of a, all $v(c_i) + iv(a)$ are distinct. Choose j such that $v(c_j) + jv(a)$ is minimal. Then $v(x) = v(c_j) + jv(a)$ and, by choice of b, $w(f(c_j)) + jw(b)$

is minimal and $w(f(x)) = f(v(x))$, as desired. There is a unique valuation preserving extension of f from $F(a)^h$ into L. Since $E/F(a)$ is an immediate extension, $F(a)^h \subseteq E$. Thus we can extend f to a valuation preserving extension of E into L. By $\aleph_1$-saturation, we can extend the embedding to F_1 $\square$

Corollary 7.14 (Macintyre) *The theory of p-adically closed fields is admits quantifier elimination.*

Lemma 7.15 *Suppose K is p-adically closed and $x \in \mathbb{Q}$ then x is an n^{th}-power in K if and only if x is an n^{th}-power in $\mathbb{Q}_p$.*

Proof The algebraic closure of $\mathbb{Q}$ in K is an immediate extension of $\mathbb{Q}$ Thus the henselization $\mathbb{Q}^h$ is the algebraic closure of $\mathbb{Q}$ in K. My uniqueness of henselization, the algebraic closure of $\mathbb{Q}$ in any two p-adically closed field are isomorphic. Thus $P_n(K) \cap \mathbb{Q}$ does not depend on K. $\square$

Corollary 7.16 *The theory of p-adically closed fields is complete.*

Proof By the lemma the rational numbers with P_n interpreted as $P_n(\mathbb{Q}_p) \cap \mathbb{Q}$ is a substructure of any p-adically closed field. Thus, by quantifier elimination, the theory is complete. $\square$

Exercise 7.17 a) Show $f(x) = 0$ if and only if $P_2(pf(x)^2)$.

b) Show that if $p \neq 2$, $f(x)|g(x)$ if and only if $P_2(f(x)^2 + pg(x)^2)$.

c) Give a version of b) for $p = 2$.

d) Conclude that every definable set is a Boolean combination of sets of the form $P_k(f(x))$.

7.2 Consequences of Quantifier Elimination

Throughout this section K will be a p-adically closed field.

Lemma 7.18 *The set of nonzero n^{th}-powers in K is clopen.*

Proof By Lemma 7.4 if a is an n^{th}-power, then $B_{2v(n)+v(a)}(a)$ is contained in the n^{th} powers. Thus $P_n \setminus \{0\}$ is open. If x is not in P_n, then $x \in a(P_n \setminus \{0\}$ for some non n^{th}-power a. Thus the set of non n^{th}-powers is open. $\square$

Corollary 7.19 *If $X \subseteq K$ is definable and infinite, then X has non-empty interior.*

Proof Let X be definable. By quantifier elimination X is the union of finitely many sets of the form

$$Y = \{x \in K : f_1(x) = \cdots = f_m(x) = 0 \wedge g(x) \neq 0 \wedge \bigwedge_{i=1}^{n} (P_{k_i}(h_i(x)) \wedge h_i(x) \neq 0)$$

for some polynomials $f_i, g, h_j \in k_p[X]$. Note that we do not need conjuncts of the form $\neg P_k$ since

$$\neg P_k(x) \Leftrightarrow \bigvee_{i=1}^{m} P_k(l_i x)$$

for appropriately chosen m and $l_1, \ldots, l_m \in K$. If Y is infinite, then all of the f_i must be trivial, in which case Y is open. $\square$

Exercise 7.20 More generally, suppose $X \subseteq K_p^m$ is definable with non-empty interior. Show that if $S_1, \ldots, S_m$ is a partition of X into definable sets, then some S_i has non-empty interior.

As in Exercise 4.18, we can show that if K is a p-adically closed field and $A \subseteq K^{m+n}$ is definable, then there is an N such that A_x is finite if and only if $|A_x| \leq N$.

Exercise 7.21 Let $U \subseteq \mathbb{Q}_p$ be open and let $f : U \to \mathbb{Q}_p$ be definable.

a) Show that there is $a \in U$ such that f is continuous at a. [Hint: This is similar to the proof in [30] 3.3.24 and uses the local compactness of $\mathbb{Q}_p$.]

b) Show that $\{x : f \text{ is discontinuous at } x\}$ is finite.

c) Prove that the same is true over any p-adically closed field K.

Exercise 7.22 Let $U \subseteq K^n$ and let $f : U \to K$ be definable. Then there is $F \in \mathbb{Q}_p[\mathbf{X}, Y]$ such that $F(\mathbf{a}, f(\mathbf{a})) = 0$ for all $\mathbf{a} \in U$, i.e., f is algebraic.

There is a p-adic version of the Implicit Function Theorem (see for example [37] §II). Once we know f is algebraic and continuous except at finitely many points we can conclude it is analytic except at finitely many points.

Skolem functions

We will show that p-adically closed fields have definable Skolem functions. We start with a partial result due to Denef for functions with finite fibers.

Theorem 7.23 (Denef [8]) *Let K be p-adicaly closed. Suppose $A \subseteq K^{m+1}$ is C-definable, $B = \{x \in K^m : \exists y\ (x, y) \in A\}$ and for all $x \in B$, $|\{y \in K : (x, y) \in A\}| \leq N$. Then there is an C-definable $f : B \to K$ such that $(x, f(x)) \in A$ for all $x \in B$.*

Proof We prove this by induction on N. The result is clear if $N = 1$. Assume $N > 1$. For $x \in B$, let $A_x = \{y : (x, y) \in A\}$ Without loss of generality, we may assume that $|A_x| = N$ for all x. Replace A by

$$\{(x, y) \in A : v(y) \text{ is minimal in } \{v(z) : z \in A_x\}\}.$$

Then using induction we may, without loss of generality assume that $|A_x| = N$ and $v(y_1) = v(y_2)$ whenever $x \in B$ and $y_1, y_2 \in A_x$.

Let $k = \phi(p^{v(N)+1})$ where ϕ is Euler's phi-function.

claim For all $x \in B$, if $A_x = \{y_1, \ldots, y_N\}$ then not all the y_i are in the same coset of k^{th}-powers.

Suppose they are. Fix z such that $v(z) = v(y_1) = \cdots = v(y_N)$ and let $y_i = zy'_i$ where $p \not| y'_i$. Then all of the y'_i are in the same coset of k^{th}-powers.. Suppose $p \not| y, z$ and $y = za^k$. By Euler's theorem $a^k = 1 \text{mod } p^{v(N)+1}$. Thus y and z are congruent mod $p^{v(N)+1}$. Hence there is a c such that $p \not| c$ and $y'_i = c \text{mod } p^{v(N)+1}$ for all i/ But $\sum y'_i = 0$. Thus $Nc = 0(\text{mod } p^{v(N)+1})$, a contradiction.

Fix any ordering of the cosets of k^{th}-powers. We can assume without loss of generality that for all $(x, y) \in A$, y is in the minimal coset of k^{th}-powers represented in A_x. We are then done by induction. □

Note that the Skolem function defined in Denef's proof are invariant, i.e., if $A_x = A_z$ then $f(x) = f(z)$.

We next show that the restriction to finite fibers in unnecessary.

Theorem 7.24 (van den Dries [10]) *p-adically closed fields have definable Skolem functions.*

Proof Let $\phi(\mathbf{x}, y)$ be a formula with parameters from A. We want to show there is an A-definable function f such that if $\mathbf{a} \in K^m$ and $\exists y\ \phi(\mathbf{a}, y)$, then $\phi(\mathbf{a}, f(\mathbf{a}))$.

Consider the type

$$\Gamma(\mathbf{v}) = \{\exists y\ \phi(\mathbf{v}, y), \neg\phi(\mathbf{v}, f(\mathbf{v})) : f \text{ is an } A\text{-definable function}\}.$$

If Γ is inconsistent, then there are finitely many definable functions $f_1, \ldots, f_n$ such that

$$\{\exists y\ \phi(\mathbf{v}, y), \neg\phi(\mathbf{v}, f_1(\mathbf{v})), \ldots, \neg\phi(\mathbf{v}, f_n(\mathbf{v}))\}$$

is inconsistent. Define

$$F(\mathbf{a}) = \begin{cases} 0 & \neg\exists y\ \phi(\mathbf{a}, y) \\ f_i(\mathbf{a}) & i \text{ is least such that } \phi(\mathbf{a}, f_i(\mathbf{a})) \end{cases}.$$

Then F is the desired definable Skolem function.

Suppose for contradiction that Γ is consistent. Let $\mathbf{a}$ realize Γ in F p-adically closed. Let E be the algebraic closure of $\mathbb{Q}(A, \mathbf{a})$ in E. Then E is p-adically closed and, by model completeness $E) \prec F$. Thus there is $b \in E$ such that $\phi(\mathbf{a}, b)$. There is $f \in \mathbb{Q}(A)[\mathbf{X}, Y]$ such that $f(\mathbf{a}, Y)$ is nontrivial and $f(\mathbf{a}, b) = 0$. Let $\psi(\mathbf{x}, y)$ be

$$\phi(\mathbf{x}, y) \wedge f(\mathbf{x}, y) = 0 \wedge \exists z\ f(\mathbf{x}, z) \neq 0.$$

Then $\psi(\mathbf{a}, b)$ and $\{y : \psi(\mathbf{a}, y)\}$ is finite for all y. By Denef's theorem, there is a A-definable function g such that if $\exists y\ \psi(\mathbf{x}, y)$ then $\psi(\mathbf{x}, g(x))$. Thus $\psi(\mathbf{a}, g(\mathbf{a}))$, contradicting that $\mathbf{a}$ realizes Γ. □

Definition 7.25 Let F be a valued field. We say that K/F is a *p-adic closure* of F, if there for any p-adically closed L/F there is a unique valued field embedding of K into L fixining F pointwise.

Exercise 7.26 Suppose F is a valued field that is a substructure of a p-adically closed field. Show that F has a p-adic closure K and the there are no automorphisms of K/F. We say K/F is *rigid*.

In fact, van den Dries' result preceded Denef's. He proved the following more general result.

Exercise 7.27 Suppose T has quantifier elimination. Then T has definable Skolem functions if and only every model $\mathcal{M}$ of $T_\forall$ has an extension $\mathcal{N}$ that is algebraic and rigid over $\mathcal{M}$.

In real closed fields we have invariant definable Skolem functions, i.e., if $A \subset K^{n+m}$ is definable there is a definable Skolem function f such that if $A_x = A_y$, then $f(x) = f(y)$. This is impossible in $\mathbb{Q}_p$.

Exercise 7.28 Let $A = \{(x, y) \in \mathbb{Q}_p^2 : v(x) = v(y)\}$. Show that there is no invariant definable Skolem function.

Exercise 7.29 [Definable Curve Selection] Let $A \subseteq \mathbb{Q}_p^n$ be definable. Let a be in the closure of A but not in A. Then there for any $\epsilon > 0$ there is a definable $f : B_\epsilon(0) \to A$ such that $f(0) = a$ and for $x \neq 0$, $f(x) \in A$ and $v(f(x)) > f(x)$

Dimension

As a topological space there can be no good notion of dimension in $\mathbb{Q}_p$.

Exercise 7.30 Show that $\mathbb{Q}_p$ and $\mathbb{Q}_p^2$ are homeomorphic.

Nevertheless, there is a good notion of dimension that works for definable sets and maps.

We begin with an relatively approach to dimension due to van den Dries [11] that works in several theories of fields.

Definition 7.31 Let $\mathcal{L}$ be a language with constant symbols C and let T be an $\mathcal{L}$-theory of fields. We say that T is *algebraically bounded* if for any formula $\phi(\mathbf{x}, y)$ there are polynomials $f_1, \ldots, f_m \in \mathbb{Z}[C][\mathbf{X}, Y]$ such that if $K \models T$, $\mathbf{a}, b \in K$, $\{y \in K : \phi(\mathbf{a}, y)\}$ is finite and $\phi(\mathbf{a}, b)$, then $f_i(\mathbf{a}, b) = 0$ for some i, where $f_i(\mathbf{a}, Y)$ is not identically zero.

Exercise 7.32 Use quantifier elimination to show that algebraically closed fields, real closed fields, algebraically closed valued fields and p-adically closed fields are algebraically bounded.

Definition 7.33 Suppose $A \subseteq K^m$ is definable, say $\phi(\mathbf{v})$ is a formula with parameters from K defining A. We define $\dim A$, the *dimension* of A, to be the largest $l \leq m$ such that there is $K \prec L$ and $\mathbf{a} = (a_1, \ldots, a_m) \in L$ with $L \models \phi(\mathbf{a})$ and $\mathrm{td}(K(\mathbf{a})/K) = l$, where $\mathrm{td}(L/K)$ denotes the transcendence degree of L/K.

Exercise 7.34 Show that this definition agrees with the usual notions of dimension in algebraically closed fields and real closed fields.

Exercise 7.35 [van den Dries] Let T be an algebraically bounded theory and $K \models T$. Our notion of dimension has the following properties. Let A and B be definable sets in K^m for some m.

a) Show $\dim A = 0$ if and only if A is finite;

b) Show $\dim (A \cup B) = \max(\dim A, \dim B)$;

c) Show that if f is a definable function, then $\dim f(A) \leq \dim A$;

d) Show $A \subseteq K^{m+n}$, then $\{a \in K^m : \dim A_a = i\}$ is definable for each $i \leq n$.

Exercise 7.36 Let $A \subseteq K^{m+n}$. For $i \leq n$ let $B_i = \{\mathbf{a} \in K^m : \dim A_a = i\}$. Show that $\dim A = \max(i + \dim B_i)$.

Exercise 7.37 a) Suppose $U \subseteq \mathbb{Q}_p$ is open. Show that $\dim U = m$.

b) Suppose $A \subseteq \mathbb{Q}_p^m$ is definable, then $\dim A$ is the largest l such that there is a projection from $\pi : \mathbb{Q}_p^m \to \mathbb{Q}_p^l$ such that $\pi(A)$ has nonempty interior.

Exercise 7.38 Use quantifier elimination to show that if $A \subseteq \mathbb{Q}_p^m$ is definable and $\dim A < m$ then there is a nonzero polynomial $f \in \mathbb{Q}_p[X_1, \ldots, X_m]$ such that A is contained in the hypersurface $p(\mathbf{x}) = 0$.

In o-minimal expansions of real closed fields there is a notion of Euler characteristic for definable sets. Basically a point has Euler characteristic 1, an open cell in K^n has Euler characteristic $(-1)^n$ and if we partition a definable set into cells, then the Euler characteristic is the sum of the Euler characteristics of the cell. van den Dries [14] showed the notion is independent of the partition chosen and that two definable sets are in definable bijection if and only if they have the same dimension and Euler characteristic.

The next exercises based on results of Cluckers and Haskell [6] tells that there is no good definably invariant notion of Euler characteristic in $\mathbb{Q}_p$. Fix $p \neq 2$–though similar results can be proved for $p = 2$. Let $\mathbb{Z}_p^*$ denote $\mathbb{Z}_p \setminus 0$, let P_2 be the nonzero squares in $\mathbb{Z}_p$, let $\mathbb{Z}_p^1$ be the elements of $\mathbb{Z}_p$ with angular component 1 and let $P_2^{(1)}$ denote $P_2 \cap \mathbb{Z}_p^{(1)}$. Note that

$$\mathbb{Z}_p^* = \bigcup_{m=1}^{p-1} m\mathbb{Z}_p^{(1)}.$$

Let $X \sqcup Y$ denote the disjoint union of X and Y. Say $X \sim Y$ if there is a definable bijection between X and Y

Exercise 7.39 a) Show that $P_2 \sqcup P_2 \sim \mathbb{Z}_p^*$. [Hint: There is a definable Skolem function $f : P_2 \to \mathbb{Z}_p^*$ such that $f(x)^2 = x$.]

b) Show that $P_2 \sqcup P_2 \sqcup P_2 \sqcup P_2 \sim \mathbb{Z}_p^*$. [Hint: Recall that P_2 is an index 4 subgroup of $\mathbb{Z}_p^2$.

c) Conclude $\mathbb{Z}_p^* \sqcup \mathbb{Z}_p^* \sim \mathbb{Z}_p^*$.

Exercise 7.40 a) $\mathbb{Z}_p^{(1)}$ is definable. [Hint: First show that

$$\{x^{p-1} : x \in \mathbb{Z}_p^*\} = \{x : \mathrm{ac}(x) = 1 \wedge (p-1) | v_p(x)\}.]$$

b) Show that $\mathbb{Z}_p^{(1)} = P_2^{(1)} \cup pP_2^{(1)}$.

Exercise 7.41 Show $\mathbb{Z}_p \sqcup \mathbb{Z}_p^{(1)} \sim \mathbb{Z}_p^{(1)}$. [Hint: send $x \in \mathbb{Z}_p$ to $1 + px$ and send $x \in \mathbb{Z}_p^{(1)}$ to px.]

Definition 7.42 Let $\mathcal{M}$ be any structure. Let $\mathbb{D}(\mathcal{M})$ be the set of all definable subsets of M^n for $n \geq 1$. Let F be the free abelian group with generators

$$\lfloor X \rfloor = \{Y \in \mathbb{D}\mathcal{M}) : X \sim Y\}$$

for $X \in \mathbb{D}(\mathcal{M})$ and let R be the subgroup generated by relations $\lfloor X \cup Y \rfloor - \lfloor X \rfloor - \lfloor Y \rfloor + \lfloor X \cap Y \rfloor$. The *Grothendieck group* of $\mathcal{M}$ is the quotient F/E. We let $[X] = \lfloor X \rfloor / E$. There is a natural multiplication induced by $[X][Y] = [X \times Y]$ making it a ring which we call the *Grothendieck ring* and denote by $K_0(\mathcal{M})$.

Corollary 7.43 *$\mathcal{K}_0(\mathbb{Q}_p)$ is trivial.*

Proof By Exercise 7.39

$$[\mathbb{Z}_p^*] = [\mathbb{Z}_p^*] + [\mathbb{Z}_p^*].$$

Thus $[\mathbb{Z}_p]^* = 0$. By Exercise 7.41,

$$[\mathbb{Z}_p] + [\mathbb{Z}_p^{(1)}] = [\mathbb{Z}_p^{(1)}].$$

Thus $[\mathbb{Z}_p] = 0$. It follows that $[\{0\}] = 0$. But then for any set $X \in \mathbb{D}(\mathcal{M})$

$$[X] = [X \times \{0\}] = [X][\{0\}] = 0.$$

□

This answered a question Denef asked at a meeting in 1999. At the same meeting Bélair asked if $\mathbb{Z}_p \sim \mathbb{Z}_p^*$. The next Exercise shows the answer is yes.

Exercise 7.44 a) Define $f_1 : p^2\mathbb{Z}_p^* \sqcup (1 + p^2\mathbb{Z}_p^*) \to (1 + p^2\mathbb{Z}_p^*)$ by

$$f_1(y) = \begin{cases} 1 + p^2(mx^2) & \text{for } y = 1 + pmx, x \in \mathbb{Z}_p^{(1)}, 1 \leq m < p \\ \\ 1 + p^3mx^2 & \text{for } y = 1 + p^2mx, x \in \mathbb{Z}_p^{(1)}, 1 \leq m < p \end{cases}$$

. Show that f_1 is a bijection.

b) Define $f_2 : p\mathbb{Z}_p \sqcup (p + p^2\mathbb{Z}_p^{(1)} \to p + p^2\mathbb{Z}_p^{(1)}$ by

$$f_2(x) = \begin{cases} p + p^2(1 + px) & \text{for } x \in \mathbb{Z}_p \\ p + p^3x & \text{for } x \in \mathbb{Z}_p^{(1)} \end{cases}.$$

Show that f_2 is a bijection.

c) Let $W = (1 + p^2\mathbb{Z}_p^*) \sqcup p^2\mathbb{Z}_p \sqcup (p + p^2\mathbb{Z}_p^{(1)})$. Define $f : W \to W \setminus \{0\}$ by

$$f(x) = \begin{cases} f_1^{-1}(x) & \text{for } x \in 1 + p^2\mathbb{Z}_p^* \\ f_2(x) & \text{for } x \in p^2\mathbb{Z}_p \sqcup (p + p^2\mathbb{Z}_p^{(1)}) \end{cases}.$$

Show that f is a bijection.

d) Extend f to a definable bijection between $\mathbb{Z}_p$ and $\mathbb{Z}_p^*$.

This is the tip of the iceberg.

Theorem 7.45 (Cluckers [5]) *Two infinite subsets of $\mathbb{Q}_p$ are in definable bijection if and only if they have the same dimension.*

Cell decomposition

Lemma 7.46 *If $U \subseteq \mathbb{Q}_p^m$ is open definable and $f : U \to \mathbb{Q}_p$ is definable, then $\{x : f$ is discontinuous at $x\}$ has dimension at most $m-1$. Moreover, there is a definable open $V \subseteq U$ such that $f|V$ is analytic and* $\dim\,(U \setminus V) < m$.

Proof We first proof that if U is open, then there is $x \in U$ such that f is continuous at x. If there is an open $U_1 \subset U$ such that $f|U_1$ is constant, then we are done so we assume that there is no such set.

Let B_0 be a closed ball in U. Given B_n open, let W be the image of B_n. Then, by assumptions on f dim $f^{-1}(w)$ has dimension at most $m-1$ for all $w \in W$. If there are only finitely many fibers of dimension $m-1$, then dim $B_n \leq m-1$. So $\{w : \dim f^{-1}(w) = m-1\}$ in infinite, and hence has interior. We can find $J_n \subset W_0$ open of radius at most $1/p^n$. Then $\{x \in B_n : f(x) \in J_n\}$ has dimension m and thus contains a closed ball B_{n+1}. Since $\mathbb{Q}_p$ is locally compact, there is $x \in \bigcap B_n$ and, by construction, f is continuous at s.

Since $\{x \in U : f$ is discontinuous at $x\}$ has no interior it must have dimension at most $m-1$. We argued before that there is a non-zero polynomial F such that $F(\mathbf{x}, f(x)) = 0$. Except for a set of dimension at most $m-1$ at each x there is an open $V \subset U$ such that $x \in V$ and there is a polynomial $F(\mathbf{X}, Y)$ such that on V: f is continuous, $F(\mathbf{x}, f(x)) = 0$ and $\frac{\partial F}{\partial Y}(\mathbf{x}, f(x)) \neq 0$. Then, by the Implicit Function Theorem, f is analytic on V. $\square$

We can now prove a cell decomposition theorem due to Scowcroft and van den Dries [13].

Theorem 7.47 *Let $A \subseteq \mathbb{Q}_p^m$ and $f : A \to \mathbb{Q}_p$ be definable. There is a partition of A into definable sets $U, B_1, \ldots, B_n$ such that U is open, $f|U$ is analytic,* dim *$B_i = k_i < m$, and there is a projection $\pi_i : \mathbb{Q}_p^m \to \mathbb{Q}_p^{k_i}$ such that $\pi_i|B_i$ is a diffeomorphism and $f \circ \pi^{-1}|\pi_i(B_i)$ is analytic.*

Proof We call the above statement Φ_m and prove this by induction on m. From earlier arguments it is easy to see that Φ_1 holds.

We will also prove the following intermediate claim which we call Ψ_m. If $g_1, \ldots, g_s \in \mathbb{Q}_p[X_1, \ldots, X_m]$ are nonzero polynomials and

$$V = \{\mathbf{x} \in \mathbb{Q}_p^m : g_1(\mathbf{x}) = \cdots = g_s(\mathbf{x}) = 0\},$$

then V can be partitioned into finitely many pieces each of which is analytically homeomorphic via a projection to an open set in some $\mathbb{Q}_p^k$ with $k < m$. Note that Ψ_1 is trivially true.

We will show that from Φ_i and Ψ_i for $i \leq m$ we can prove Ψ_{m+1} and then show that from $\Phi_1, \ldots, \Phi_{m-1}$ and $\Psi_1, \ldots, \Psi_{m+1}$ we can prove Φ_{m+1}.

$\underline{\Phi_1, \ldots \Phi_m, \Psi_1, \ldots \Psi_m \Rightarrow \Psi_{m+1}}$ Let $g_1, \ldots, g_s \in \mathbb{Q}_p[X_1, \ldots, X_m, Y]$ and let

$$V = \{(\mathbf{x}, y) \in \mathbb{Q}_p^m : g_1(\mathbf{x}, y) = \cdots = g_m(\mathbf{x}, y) = 0\}.$$

Suppose

$$g_i(\mathbf{X}, Y) = \sum_{j=0}^{d_i} h_{i,j}(\mathbf{X}) Y^j$$

where $h_{i,j} \in \mathbb{Q}_p[\mathbf{X}]$. Let

$$V_0 = \{\mathbf{x} \in \mathbb{Q}_p^m : \bigwedge_{i,j} h_{i,j}(\mathbf{x}) = 0.\}$$

Then $V_0 \times \mathbb{Q}_p \subseteq V$ and there is a bound N such that if $\mathbf{x} \notin V_0$, then $|\{y : (\mathbf{x}, y) \in V\}| \leq N$ is finite. This allows us to partition $V = X_1 \cup \cdots \cup X_N \cup X_\infty$ where for $i \leq N$, $X_i = \{(\mathbf{x}, y) \in V :$ there are exactly i distinct $z \in \mathbb{Q}_p$ with $(\mathbf{x}, z) \in V\}$. and $X_\infty = V_0 \times \mathbb{Q}_p$. We deal with each X_i separately.

X_∞: We can apply Ψ_m to V_0 to partition it into finitely many sets $A_0, \ldots, A_m$ where each A_i is analytically isomorphic to an open set in sum $\mathbb{Q}_p^{k_i}$ where $k_i < m$. Let $B_i = A_i \times \mathbb{Q}_p$. This gives the desired decomposition of $X_\infty = V_0 \times \mathbb{Q}_p$.

X_k: Let

$$C = \{\mathbf{x} \in \mathbb{Q}_p^m : |\{z \in \mathbb{Q}_p : (\mathbf{x}, z) \in V\}| = k\}.$$

We can find definable Skolem functions $f_1, \ldots, f_k : C \to \mathbb{Q}_p$ such that

$$X_k = \{(\mathbf{x}, f_i(\mathbf{x})) : \mathbf{x} \in C, i = 1, \ldots, k\}.$$

By induction we can partition C into definable sets $D_0, \ldots, D_s$ such that D_0 is open (possibly empty) and all of the f_i are analytic on D_0 and otherwise D_j is analytically isomorphic via a projection π_j to an open subset of $\mathbb{Q}_p^{r_j}$ for $r_j < m$ and each $f_j \circ \pi_j^{-1} | \pi_j(D_j)$ is analytic. Then we can partition X_k into the union of the graphs of the f_i on C and the D_js and apply induction.

$\underline{\Phi_1, \ldots \Phi_m, \Psi_1, \ldots \Psi_m \Rightarrow \Phi_{m+1}}$ By the previous lemma, we can find $U \subseteq \mathbb{Q}_p^{m+1}$ open such that $f|U$ is analytic and dim $(A \setminus U) < m$. Since $A \setminus U$ has no interior, there is $g \in \mathbb{Q}_p[X_1, \ldots, X_{m+1}]$ such that $A \setminus U$ is contained in the hypersurface V given by $g(\mathbf{X}) = 0$. Apply Ψ_m to V to obtain a partition $C_1, \ldots, C_s$ where for each j, there is a projection π_j that is an analytic isomorphism to an open set in $\mathbb{Q}_p^{k_j}$. Let $D_j = \pi_j((A \setminus U) \cap C_j)$. Using Φ_{k_j} we can definably partition D_j into finitely many nice pieces, then we lift these using π_j^{-1}. $\square$

We will later state a different cell decomposition theorem due to Denef.

7.3 Rationality of Poincaré Series

Fix $f_1, \ldots, f_r \in \mathbb{Q}_p[X_1, \ldots, X_n]$. Let

$$N_k = |\{\mathbf{y} \in \mathbb{Z}/p^k\mathbb{Z} : \exists \mathbf{x} \in \mathbb{Z}_p^n \; f_1(\mathbf{x}) = \cdots = f_r(\mathbf{x}) = 0 \wedge \bigwedge x_i = y_i (\mathrm{mod}\; p^k)\}.^9$$

We will consider the *Poincaré series*

$$P(T) = \sum_{k=0}^{\infty} N_k T^k.$$

We could also consider

$$\widetilde{N}_k = |\{\mathbf{y} \in \mathbb{Z}/p^k : f_i(\mathbf{y}) = 0 (\mathrm{mod}\; p^k)\}, i = 1, \ldots, r\}$$

and $\widetilde{P}(T) = \sum_{k=0}^{\infty} \widetilde{N}_k T^k$.

Igusa [21], [22] (for $r = 1$) and Meuser [31] (for general r), proved that $\widetilde{P}(T)$ is a rational function of T. Denef answered a question of Serre and Oesterlé by proving the rationality of $P(T)$.

Theorem 7.48 (Denef [8]) *$P(T)$ is a rational function of T.*

Igusa's proof used resolution of singularities to simply certain p-adic integrals. Denef's gave two proofs, the first also using resolution of singularities but the second used quantifier elimination to avoid resolution of singularities.

p-adic integration

The p-adics under addition are a locally compact group and thus come equipped with a Haar measure μ.. Let $\mathcal{B}$ be the σ-algebra generated by the compact subsets of $\mathbb{Q}_p$. There is a unique σ-additive measure $\mu : \mathcal{B} \to \mathbb{R}$ such that:

i) $\mu(\mathbb{Z}_p) = 1$;

ii) (translation invariance) $\mu(a + A) = \mu(A)$ for $a \in \mathbb{Q}_p$, $A \in \mathcal{B}$;

iii) for every $A \in \mathcal{B}$ and $\epsilon > 0$ there is an open set U and a closed set F such that $F \subseteq X \subseteq U$ and $\mu(U \setminus F) < \epsilon$.

Exercise 7.49 $\mu(\{a\}) = 0$ for all $a \in \mathbb{Q}_p$.

Let $\mathfrak{m}$ be the maximal ideal. Then

$$\mathfrak{m} \cup (1 + \mathfrak{m}) \cup \cdots \cup ((p-1) + \mathfrak{m}) = \mathbb{Z}_p.$$

Thus by additivity and translation invariance $\mu(\mathfrak{m}) = 1/p$.

Exercise 7.50 Show that $\mu(\{x : v(x - a) \geq r\}) = p^{-r}$.

Example 7.51 Let A be the set of squares in $\mathbb{Z}_p$ where $p \neq 2$.

[9] This is a little unclear if $k = 0$, in which case we mean that $N_0 = 1$ if $f_1 = \cdots = f_m = 0$ has a zero in $\mathbb{Z}_p^n$ and otherwise $N_0 = 0$.

Let $A_k = \{x \in A : v(x) = 2k\}$. Then $A = \{0\} \cup \bigcup A_k$ and

$$\mu(A) = \sum_{k=0}^{\infty} \mu(A_k).$$

If $x \in A_k$ if and only if $x = p^{2k} y$ where $v(y) = 0$ and $\operatorname{res}(y)$ is a square in $\mathbb{F}_p$. Since there are $\frac{p-1}{2}$ squares in $\mathbb{F}_p$ we can find $z_1, \ldots, z_{\frac{p-1}{2}} \in \mathbb{Z}_p$ such that A_k is the disjoint union $B_1 \cup \cdots \cup B_{\frac{p-1}{2}}$ where

$$B_i = \{x - z_i : v_p(x) \geq 2k + 1\}.$$

We have $\mu(B_i) = p^{-2k-1}$. Thus

$$\begin{aligned}
\mu(A) &= \sum_{k=0}^{\infty} \frac{p-1}{2} p^{-2k-1} \\
&= \frac{p-1}{2p} \sum_{k=0}^{\infty} p^{-2k} \\
&= \frac{p-1}{2p} \left(\frac{1}{1-p^{-2}} \right) \\
&= \frac{p}{2(1+p)}.
\end{aligned}$$

Exercise 7.52 Calculate the Haar measure of the set of squares when $p = 2$.

There is a Haar measure μ^m on $\mathbb{Z}_p^m$. This is just the usual product measure, and we will usually write μ rather than μ^m.

Suppose $A \in \mathcal{B}$ and $f : A \to \mathbb{R}$ is a $\mathcal{B}$-measurable function, we can define the integral

$$\int_A f \, d\mu.$$

We give two illustrative examples.

Example 7.53 Suppose $p \neq 2$. Let A be the set of squares in $\mathbb{Z}_p$ and let $f(x) = |x^s|_p$.

Let $A_k = \{x \in A_k : v(x) = 2k\}$. Then

$$\begin{aligned}
\int_A |x^s|_p \, d\mu &= \sum_{k=0}^{\infty} \int_{A_k} |x^s|_p \, d\mu \\
&= \sum_{k=0}^{\infty} \int_{A_k} p^{-2sk} \, d\mu \\
&= \sum_{k=0}^{\infty} p^{-2sk} \mu(A_k).
\end{aligned}$$

We saw above that $\mu(A_k) = \frac{p-1}{2} p^{-2k-1}$. Thus

$$\begin{aligned} \int_A |x^s|_p \, d\mu &= \frac{p-1}{2p} \sum_{k=0}^{\infty} (p^{-2s-2})^k \\ &= \frac{p-1}{2p} \left(\frac{1}{1 - p^{-2s-2}} \right) \end{aligned}$$

Exercise 7.54 Calculate $\int_A |x^s| \, d\mu$ when $p = 2$.

Example 7.55 Suppose $p = 3 (\mathrm{mod}\ 4)$. Let $f(x) = |x+1|_p$ and let A again by the squares in $\mathbb{Z}_p$.

Since $p = 3(\mathrm{mod}\ 4)$, -1 is a square in $\mathbb{F}_p$ and hence in $\mathbb{Z}_p$. Let $B = \{x \in \mathbb{Z}_p : v(x+1)\}$. Then every $y \in B$ is a square. If we partition A into B and $A \setminus B$, then

$$\int_A |x+1|_p \, d\mu = \int_B |x+1|_p \, d\mu + \int_{A \setminus B} |x+1|_p \, d\mu.$$

But on $A \setminus B$, $|x+1|_p = 1$. Hence

$$\int_{A \setminus B} |x+1|_p \, d\mu = \int_{A \setminus B} 1 \, d\mu = \mu(A) - \mu(B) = \frac{p}{2(1+p)} - \frac{1}{p}.$$

Partition $B = \{-1\} \cup B_1 \cup B_2 \cup \dots$ where $B_i = \{x : v(x+1) = i\}$ Then

$$\begin{aligned} \int_B |x+1|_p \, d\mu &= \sum_{k=1}^{\infty} \int_{B_i} |x+1|_p \, d\mu \\ &= \sum_{k=1}^{\infty} \int_{B_i} p^{-k} \, d\mu \\ &= \sum_{k=1}^{\infty} p^{-k} \mu(B_i) \\ &= \sum_{k=1}^{\infty} p^{-k} \left(\frac{1}{p^k} - \frac{1}{p^{k+1}} \right) \\ &= \frac{p-1}{p^3} \sum_{k=0}^{\infty} p^{-2k} \\ &= \frac{p-1}{p^3 (1 - p^{-2})^2} \end{aligned}$$

Thus

$$\int_A |1+x|_p \, d\mu = \frac{p-1}{p^3(1-p^{-2})^2} + \frac{p}{2(1+p)} - \frac{1}{p}.$$

The next lemma is the link between integration and Poincaré series. Let $f_1, \dots, f_r \in \mathbb{Z}_p[\mathbf{X}]$, where $\mathbf{X} = (X_1, \dots, X_n)$ and let P be the associated Poincaré series. Let

$$D = \{(\mathbf{x}, y) \in \mathbb{Z}_p^{n+1} : \exists \mathbf{z} \in \mathbb{Z}_p^n \ f_1(\mathbf{z}) = \dots = f_r(\mathbf{z}) = 0 \wedge \bigwedge v(x_i - z_i) \geq v(y)\}$$

and for $s \in \mathbb{R}, s > 0$, define

$$I(s) = \int_D |y|^s \, d\mu.$$

Lemma 7.56 $I(s) = \frac{p-1}{p} P(p^{-n-1}p^{-s})$.

Proof Let $D_k = \{(x, y) \in D : v(y) = k\}$. Then

$$\begin{aligned} I(s) &= \sum_{k=0}^{\infty} \int_{D_k} |y|^s \, d\mu \\ &= \sum_{k=0}^{\infty} \int_{D_k} p^{-sk} \, d\mu \\ &= \sum_{k=0}^{\infty} p^{-sk} \mu(D_k) \end{aligned}$$

For each $\mathbf{z}(\text{mod } p^k)$ with $f_1(\mathbf{z}) = \cdots = f_r(\mathbf{z}) = 0$.

$$\mu(\{\mathbf{x} : \mathbf{z} = \mathbf{x}(\text{mod } p^k)\} = p^{-nk}$$

and

$$\mu(\{y : v(y) = k\} = \frac{p-1}{p^{k+1}}.$$

Thus

$$\mu(D_k) = N_k \frac{p-1}{p} p^{-nk-k},$$

as for each of the N_k zeros mod p^k we can find a ball (in m-space) of measure p^{-mk}. Thus

$$I(s) = \frac{p-1}{p} \sum_{k=0}^{\infty} N_k (p^{-s-n-1})^k = \frac{p-1}{p} P(p^{-s-n-1}).$$

□

We will prove that there is a rational function $Q(T)$ such that $I(s) = Q(p^{-s})$. Letting $Y = p^{-s}$ we have

$$Q(Y) = \frac{p-1}{p} P(p^{-n-1}Y).$$

Then letting $T = p^{-n-1}Y$

$$P(T) = \frac{p}{p-1} Q(p^{n+1}T).$$

Hence $P(T)$ is a rational function.

Denef proved the following general rationality theorem.

Theorem 7.57 (Denef) *Suppose $A \subseteq \mathbb{Q}_p^m$ is definable and contained in a compact set and $h : A \to \mathbb{Q}_p$ is a definable function. Suppose natural number M and $v(h(x))$ is either divisible by M or $+\infty$ for all $x \in A$. Then*

$$Z_A(s) = \int_A |h(x)|_p^{s/M} \, d\mu$$

is a rational function in p^{-s} for $s \in (0, +\infty)$.

Denef's Cell Decomposition

The proof of Theorem 7.57 needs an analysis of definable functions from $\mathbb{Q}_p^m$ to the value group and a refined cell decomposition/preparation theorem.

Definition 7.58 Suppose $A \subseteq \mathbb{Q}_p^m$ is definable. We say that a defiinable $\theta : A \to \mathbb{Z} \cup \{+\infty\}$ is *simple* if there is a finite partition of A into definable sets such that for each set B in the partition, there is an integer M and $f, g \in \mathbb{Q}_p[X_1, \ldots, X_m]$ such that $\theta(x) = \frac{1}{M}(v(f(x)) - v(g(x)))$ on B.

Lemma 7.59 *Suppose $A \subseteq \mathbb{Q}_p^{m+1}$ is definable, $B = \{\mathbf{x} \in \mathbb{Q}_p^m : \exists y \; (\mathbf{x}, y) \in A$ and for all $\mathbf{x} \in B$ v is constant on $A_{\mathbf{x}} = \{y : (\mathbf{x}, y) \in A\}$. Let $\theta : B \to \mathbb{Z} \cup \{+\infty\}$ by the function where $\theta(\mathbf{x}) = v(y)$ for all $(\mathbf{x}, y) \in A$. Then θ is simple.*

Proof Without loss of generality, assume that if $(\mathbf{x}, y) \in A$, then $y \neq 0$. If not $Z = \{(\mathbf{x}, y) \in A : y = 0\}$, then $\theta|Z$ is constant and replace A by $A \setminus Z$. Since p-adically closed fields, have definable Skolem functions there is a definable $f : B \to \mathbb{Q}_p$ such that $(\mathbf{x}, f(\mathbf{x})) \in A$ for all $\mathbf{x} \in B$. By Exercise 7.22, there is a polynomial $F(\mathbf{X}, Y)$ such that $F(\mathbf{x}, f(\mathbf{x})) = 0$ for all $x \in A$ and $F(\mathbf{x}, Y)$ is not identically zero. Let

$$F(\mathbf{X}, Y) = \sum_{i=0}^{d} g_i(\mathbf{X}) Y^i.$$

Since $F(\mathbf{x}, f(\mathbf{x})) = 0$ for each $\mathbf{x} \in A$, there is an $i < j$ such that $v(g_i(\mathbf{x})) + iv(y) = v_j(g_j(X)) + jv(y)$. For $i < j \leq d$, let

$$A_{i,j} = \{(x, y) \in A : (i, j) \text{ is minimal such that } v(y) = \frac{v(g_i(\mathbf{x})) - v(g_j)(\mathbf{x})}{j - i}\}.$$

Then $(A_{i,j} : i < j \leq d)$ is a partition of A showing that θ is simple. $\square$

Denef proved the following cell decomposition/preparation theorem. We refer the reader to [8] §7 for the proof.

Theorem 7.60 *Suppose $f_1, \ldots, f_r \in \mathbb{Q}_p[\mathbf{X}, Y]$, where $\mathbf{X} = (X_1, \ldots, X_m)$ and $N > 1$, then $\mathbb{Q}_p^{m+1}$ can be partitioned into finitely many definable sets of the form*

$$A = \{(\mathbf{x}, y) \in \mathbb{Q}_p^{m+1} : x \in C, v(a_1(\mathbf{x})) \,\square_1\, v(y - c(\mathbf{x})) \,\square_2\, v(a_2(\mathbf{x}))\}$$

where $C \subseteq \mathbb{Q}_p^m$ is definable, a_1, a_2 and c are definable functions, $\Box_i$ is either $<$, $\leq$ or no restriction, and there is are definable function $h_j : C \to \mathbb{Q}_p$ for $j = 1, \ldots, r$ such that

$$f_j(\mathbf{x}, y) = u_j(\mathbf{x}, t)^N h_i(\mathbf{x})(y - c(\mathbf{x}))^{v_j}$$

function where $u_j(\mathbf{x}, y)$ is a unit.

In the following proofs we will be interested in knowing of the value of $f_j(\mathbf{x}, y)$ or if $f_j(\mathbf{x}, y)$ is an N^{th}-power. Since $u_j(\mathbf{x}, y)^N$ is always a unit and an N^{th}-power, we have reduced the question to understanding $h_j(\mathbf{x})(y - c\mathbf{x})^{v_j}$.

The following lemma is the key step in Denef's proof.

Lemma 7.61 *Suppose $A \subseteq \mathbb{Q}_p^m$ is definable and contained in a compact set and $h : A \to \mathbb{Q}_p$ is a definable function such that for some natural number M $v(h(x))$ is either divisible by M or $+\infty$ for all $x \in A$. Then*

$$Z_A(s) = \int_A |h(x)|_p^{s/M} \, d\mu$$

is a linear combination of series of the form

$$\sum_{\substack{(k_1, \ldots, k_m) \in L \\ k_i = \lambda_i (\text{mod } N_i)}} p^{-(q_1 k_1 + \cdots + q_m k_m)s - k_1 - \cdots - k_m}$$

where $k_1, \ldots, k_m, \lambda_i \in \mathbb{Z}$, $N_i \in \mathbb{N}$, $q_1, \ldots, q_m \in \mathbb{Q}$ and L is defined by a system of linear inequalities with rational coefficients.

Any function of this form is rational in p^{-s}

Proof (Sketch) The result is trivial if $m = 0$. We write points in $\mathbb{Q}_p^{m+1}$ as $(\mathbf{x}, y)$.

Since $\int_{A \cup B} = \int_A + \int_B - \int_{A \cap B}$, we can always take Boolean combinations.

We first apply Lemma 7.59 to partition A. Without loss of generality, we may assume

$$|h(\overline{x}, y)|_p^{1/M} = \left| \frac{g_1(\mathbf{x}, y)}{g_2(\mathbf{x}, y)} \right|_p^{\frac{1}{M'}}$$

where $g_1, g_2 \in \mathbb{Q}_p[\mathbf{X}, Y]$ and $M' > 0$. Further, by quantifier elimination and Exercise 7.17 we may assume that A is defined by a conjunction

$$\bigwedge_{j=1,\ldots,r} \pm P_{n_j}(f_j(\mathbf{x}, y)).$$

We apply Theorem 7.60 to the functions $f_1, \ldots, f_r, g_1$ and g_2 where $N = \prod n_j$. So, by further partitioning, we may assume A is defined by

$$\mathbf{x} \in C \wedge v(a_1(\mathbf{x})) \,\Box_1\, v(y - c(\mathbf{x})) \,\Box_2\, v(a_2(\mathbf{x}))$$

and on A

$$|h(\mathbf{x},y)|_p^{1/M} = |h_0(\mathbf{x})|_p^{1/M'}|_p|y-c(\mathbf{x})|_p^{v/M'}$$

and $f_j(\mathbf{x},y)$ is an n_j^{th}-power if and only if $h_j(\mathbf{x})(y-c(\mathbf{x}))^{v_j}$ is.

We can further refine our partition so that the coset of N^{th}-powers of each $h_j(\overline{x})$ and $(y-c(\mathbf{x})$ is fixed on each set in the partition. Without loss of generality they are constant on A. Let $z = y - c(\mathbf{x})$. Suppose $z \in \lambda(\text{mod } P_N^{\times})$. Then

$$\begin{aligned}
\int_A |h|_p^{s/M}\, dy\, d\mathbf{x} &= \int_A |h(\mathbf{x},y)|_p^{s/M'}\, dy\, d\mathbf{x} \\
&= \int_C \left(|h_0(\mathbf{x})|_p^{s/M'} \int\limits_{\substack{v(a_1(\mathbf{x}))\square_1 v(z)\square_2 v(a_2(\mathbf{x})) \\ z=\lambda \ (\text{mod } P_N^{\times})}} |z|_p^{sv/M'} \right) dz\, d\mathbf{x} \\
&= \int_C \left(|h_0(\mathbf{x})|_p^{s/M'} \sum_{v(a_1(\mathbf{x}))\square_1 k\square_2 v(a_2(\mathbf{x}))} p^{-kvs/M'} \int\limits_{\substack{v(z)=k \\ z=\lambda \ (\text{mod } P_N^{\times})}} 1\, dz \right) d\mathbf{x}
\end{aligned}$$

Let $w = p^{-k}z$. Then

$$\int\limits_{\substack{v(z)=k \\ z=\lambda(\text{mod } P_N^{\times})}} 1\, dz = p^{-k} \int\limits_{\substack{v(w)=0 \\ w=p^{-k}\lambda \ (\text{mod } P_N^{\times})}} 1\, dw.$$

The righthand side is 0 if $k \neq v(\lambda)(\text{mod } N))$ and otherwise is $p^{-k}\gamma$ where γ does not depend on k. Thus

$$\begin{aligned}
Z_A(s) &= \gamma \int_C \left(|h_0(\mathbf{x})|_p^{s/M'} \sum_{\substack{va_1(\mathbf{x}))\square_1 k\square_2 v(a_2(\mathbf{x})) \\ k=v(\lambda)(\text{mod } N)}} p^{-(kvs)/M'-k} \right) d\mathbf{x} \\
&= \gamma \sum_{k=v(\lambda)(\text{mod } N)} \left(p^{-(kvs)/M'-k} \int\limits_{\substack{\mathbf{x}\in C \\ v(a_1(\mathbf{x}))\square_1 k\square_2 v(a_2(\mathbf{x}))}} |h_0(\mathbf{x})|_p^{s/M'}\, d\mathbf{x} \right).
\end{aligned}$$

We have succeeded in getting rid of the y variable. We next try to eliminate the variable x_m We apply cell decomposition with the functions $a_1(\mathbf{x})$ and $a_2(\mathbf{x})$. After some change of variables and further partitioning we are looking at something like $\{(v(\mathbf{x}),k) : a_1(\mathbf{x})\square_1 k\square_2 a_2(\mathbf{x})\}$. This set is defined by a Boolean combination of congruence conditions and linear inequalities. Proceeding with care we get the desired result. $\square$

The end of the proof contains quite a bit of "hand waving" that is tricky to carefully formulate as an inductive argument. We give one more hopefully illustrative example where this works out. We've chosen things so that we already done cell decompositon and don't need to partition further to get functions in the right form, but most of the other tricks in Denef's proof arise here. Also the argument given at the end to go from the power series to the rational function uses most of the ideas found in a proof of the general result.

Example 7.62

Suppose $p \equiv 1 (\mathrm{mod}\ 3)$ and let

$$A = \{(x, y) \in \mathbb{Z}_p^2 : x \text{ is a cube}, y \text{ is a square and } 0 \leq v(y) \leq v(x^3)\}$$

and let $h(x, y) = xy$. We will calculate

$$Z_A(s) = \int_A |h(x, y)|_p \, d\mu.$$

Let $D = \{x \in \mathbb{Z}_p : x \text{ is a cube}\}$. Then

$$\begin{aligned} Z_A(s) &= \int_{x \in D} |x|^s \int\limits_{\substack{y \text{ a square} \\ v(y) \leq v(x^3)}} |y|^s \, dy \, dx \\ &= \int_{x \in D} \left(|x|^s \sum_{\substack{k \geq 0 \\ k \leq v(x^3)}} p^{-ks} \int\limits_{\substack{v(y)=k \\ y \text{ a square}}} 1 \, dy \right) dx. \end{aligned}$$

We can calculate

$$\mu(\{y : v(y) = k, y \text{ a square}\}) = \begin{cases} 0 & k \text{ odd} \\ \left(\frac{p-1}{2p}\right) p^{-k} & k \text{ even} \end{cases}.$$

There are $\frac{p-1}{2}$ squares in $\mathbb{F}_p^\times$. Thus the set of squares of value k is the union of $\frac{p-1}{2}$ balls of radius p^{-k-1} and hence has measure $\frac{p-1}{2p} p^- k$. Thus

$$Z_A(s) = \frac{p-1}{2p} \sum_{k \text{ even}} \left(p^{-ks-k} \int\limits_{\substack{x \in D \\ k \leq v(x^3)}} |x|^s \, dx \right)$$

But

$$\begin{aligned} \int\limits_{\substack{x \in D \\ k \leq v(x^3)}} |x|^s \, dx &= \sum_{\substack{0 \leq l \\ k \leq 3l}} \int\limits_{\substack{v(x)=l \\ l \text{ a cube}}} 1 \, dx \\ &= \frac{p-1}{3p} \sum_{\substack{0 \leq l, 3|l \\ k \leq 3l}} p^{-ls-l} \end{aligned}$$

since there are $\frac{(p-1)}{3}$ cubes in $\mathbb{F}_p^\times$. Thus

$$Z_A(s) = \frac{(p-1)^2}{6p^2} \sum_{\substack{2|k,3|l \\ 0\leq k\leq 3l}} p^{-ls-ks-l-k}.$$

It suffices to show that

$$\sum_{\substack{2|k,3|l \\ 0\leq k\leq 3l}} p^{-ls-ks-l-k}$$

is a rational function in p^{-s}. We start by making the substitutions $k = 2i$, $l = 3j$.

$$\sum_{\substack{2|k,3|l \\ 0\leq k\leq 3l}} p^{-ls-ks-l-k} = \sum_{0\leq 2i\leq 9j} p^{-(3s+3)j-(2s+2)i}$$

Every value of j is either of the form $2r$ or $2r+1$. In the first case $2k \leq 9j$ if and only if $k \leq 9r$. In the second case

$$2k \leq 9j \Leftrightarrow 2k \leq 18r + 9 \Leftrightarrow k \leq 9r + 4.$$

Thus we can break the sum above up into

$$\sum_{0\leq i\leq 9r} p^{-(6s+6)r-(2s+2)i} + \sum_{0\leq i\leq 9r+4} p^{-6sr-3s-6r-3-(2s+2)i}$$

We will show the first summand is a rational function in p^{-s} and leave the second summand as an exercise.

$$\sum_{0\leq i\leq 9r} p^{-(6s+6)r-(2s+2)i} = \sum_{r=0}^{\infty}\left(p^{-(6s+6)r}\sum_{s=0}^{9r} p^{-(2s+2)i}\right).$$

Knowing how to sum geometric series we see that

$$\sum_{s=0}^{9r} p^{-(2s+2)i} = \frac{1-(p^{-(2s+2)})^{9r+1}}{1-p^{-(2s+2)}}$$

So

$$\begin{aligned}
\sum_{0\leq i\leq 9r} p^{-(6s+6)r-(2s+2)i} &= \frac{1}{1-p^{2s+2}}\left(\sum_{r=0}^{\infty} p^{-(6s+6)r} + \sum_{r=0}^{\infty} p^{-(6s-6)r}p^{-(2s+2)(9r+1)}\right) \\
&= \frac{1}{1-p^{2s+2}}\left(\sum_{r=0}^{\infty} p^{-(6s+6)r} + \sum_{r=0}^{\infty} p^{-24sr-2s-24r-2}\right)
\end{aligned}$$

These are both geometric series and give rise to a rational function in p^{-s}.

The tricks used in this calculation work in general to show that any series of the type arising in the proof of Lemma 7.61 is a rational function in p^{-s}.

References

[1] N. Ailling, *Foundations of Analysis over the Surreal Numbers*, North-Holland, 2012.

[2] J. Ax and S. Kochen, Diophantine problems over local fields. I. Amer. J. Math. 87 1965 605–630.

[3] J. W. S. Cassels, *Local Fields*, Cambridge University Press, 1986.

[4] Z. Chatzidakis, Théorie des Modèls des corps valués, `http://www.math.ens.fr/~zchatzid/papiers/cours08.pdf`

[5] R. Cluckers, Classification of semi-algebraic p-adic sets up to semi-algebraic bijection. J. Reine Angew. Math. 540 (2001), 105–114.

[6] R. Cluckers and D. Haskell, Grothendieck rings of $\mathbb{Z}$-valued fields, Bull. Symbolic Logic 7 (2001), no. 2, 262–269.

[7] F. Delon, Types sur $\mathbb{C}((X))$, Study Group on Stable Theories (Bruno Poizat), Second year: 1978/79, Exp. No. 5, 29 pp., Secrt́ariat Math., Paris, 1981.

[8] J. Denef, The rationality of the Poincaré series associated to the p-adic points on a variety, Invent. Math. 77 (1984), no. 1, 1–23.

[9] J. Denef, p-adic semi-algebraic sets and cell decomposition, J. Reine Angew. Math. 369 (1986), 154–166.

[10] L. van den Dries, Algebraic theories with definable Skolem functions, J. Symbolic Logic 49 (1984), no. 2, 625–629.

[11] L. van den Dries, Dimension of definable sets, algebraic boundedness and Henselian fields, Stability in model theory, II (Trento, 1987). Ann. Pure Appl. Logic 45 (1989), no. 2, 189–209.

[12] L. van den Dries, Lectures on the Model Theory of Valued Fields, *Model Theory in Algebra, Analysis and Arithmetic*, H. D. Macpherson and C. Toffalori ed., Springer, 2010.

[13] L. van den Dries and P. Scowcroft, On the structure of semialgebraic sets over p-adic fields, J. Symbolic Logic 53 (1988), no. 4, 1138-1164.

[14] L. van den Dries, *Tame topology and o-minimal structures*, London Mathematical Society Lecture Note Series, 248. Cambridge University Press, Cambridge, 1998.

[15] J.-L. Duret, Les corps pseudo-finis ont la propriété d'indépendance, C. R. Acad. Sci. Paris Sér. A-B 290 (1980), no. 21, A981–A983.

[16] D.Eisenbud, *Commutative Algebra: with a View Toward Algebraic Geometry*, Springer Graduate Texts in Mathematics 150, Springer 1995.

[17] A. J. Engler and A. Prestel, *Valued Fields*, Springer, 2005.

[18] J. Eršhov, On elementary theories of local fields, Algebra i Logika Sem. 4 1965 no. 2, 5–30.

[19] M. Fried and M. Jarden, *Field Arithmetic*, Springer, 1986.

[20] Y. Gurevich and P. Schmittt, The theory of ordered abelian groups does not have the independence property, Trans. Amer. Math. Soc. 284 (1984), no. 1, 171–182.

[21] J.-i. Igusa, Complex powers and asymptotic expansions. I, J. Reine Angew. Math. 268/269 (1974), 110–130.

[22] J.-i. Igusa, On the first terms of certain asymptotic expansions, *Complex analysis and algebraic geometry*, pp. 357–368. Iwanami Shoten, Tokyo, 1977.

[23] N. Jacobson, *Basic Algebra II*, Freeman, 1980.

[24] I. Kaplansky, Maximal fields with valuations. Duke Math. J. 9, (1942). 303–321.

[25] K. Kedlaya, The algebraic closure of the power series field in positive characteristic. Proc. Amer. Math. Soc. 129 (2001), no. 12, 3461—3470.

[26] S. Lang, *Algebra*, Addison-Wesley, 1971.

[27] S. Lang, On quasi-algebraic closure, Annals of Math. 55 (1952), 373–390.

[28] D. Macpherson, D. Marker and C. Steinhorn, Weakly o-minimal structures and real closed fields. Trans. Amer. Math. Soc. 352 (2000), no. 12, 5435–5483.

[29] A. Macintyre, On definable subsets of p-adic fields. J. Symbolic Logic 41 (1976), no. 3, 605–610.

[30] D. Marker, *Model Theory: An Introduction*, Springer, 2002.

[31] D. Meuser, On the rationality of certain generating functions. Math. Ann. 256 (1981), no. 3, 303–310.

[32] M.-H. Mourges and J.-P. Ressarye, Every real closed field has an integer part. J. Symbolic Logic 58 (1993), no. 2, 641–647.

[33] J. Pas, Uniform p-adic cell decomposition and local zeta functions. J. Reine Angew. Math. 399 (1989), 137–172.

[34] A. Robinson, *Complete theories*, North-Holland, Amsterdam, 1956.

[35] J. Ruiz,*The Basic Theory of Power Series*, Viewig, 1993.

[36] J.-P. Serre, *A Course in Arithmetic*, Springer, 1973.

[37] J.-P. Serre, *Lie Algebras and Lie Groups: 1964 lectures given at Harvard University.*,Second edition, Lecture Notes in Mathematics, 1500. Springer-Verlag, Berlin, 1992.

[38] J. Silverman, *A Friendly Introduction to Number Theory*, Pearson, 1997.

[39] P. Simon,*A Guide to NIP Theories*, Cambridge, 2015.

[40] R. Walker, *Algebraic Curves*, Springer-Verlag, 1978.