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 $x = y (\text{mod } n)$ 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 $\frac{x}{p^i z^n} = r (\text{mod } p^{2v(n)+1})$ and $p \not| r$. Let $c = \frac{x}{rp^i z^n}$. Then $c = 1 (\text{mod } p^{2v(n)+1})$. 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 $0 \leq v(rp^i) < n$. □

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. □

We will show that the theory of p-adically closed fields has quantifier elimination in the Macintyre language $\mathcal{L}_{\text{Mac}} = \{+, -, \cdot, |, P_2, P_3, \ldots, 0, 1\}$ 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. □

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. □

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 $v(c/u) = g$. □

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. □

Lemma 7.10 *Suppose $F \subset K$ and $f : F \to L$ is an $\mathcal{L}_{\text{Mac}}$-embedding, then f extends to an $\mathcal{L}_{\text{Mac}}$-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 $\mathcal{L}_{\text{Mac}}$-embedigin □

Our next goal is to show that if we have an $\mathcal{L}_{\text{Mac}}$-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 $\mathcal{L}_{\text{Mac}}$-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. □

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

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 $a^k = 1 \bmod p^{v(N)+1}$. Thus y and z are congruent mod $p^{v(N)+1}$. Hence there is a c such that $p \not| c$ and $y_i' = c \bmod p^{v(N)+1}$ for all $i/$ But $\sum y_i' = 0$. Thus $Nc = 0 (\bmod\ p^{v(N)+1})$, 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. □

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

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

We will consider the *Poincaré series*

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

We could also consider

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

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 $\text{res}(y)$ 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 $p = 3(\text{mod } 4)$. Let $f(x) = |x+1|_p$ and let A again by the squares in $\mathbb{Z}_p$.

Since $p = 3(\text{mod } 4)$, -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 $B = \{-1\} \cup B_1 \cup B_2 \cup \ldots$ 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 $f_1, \ldots, f_r \in \mathbb{Z}_p[\mathbf{X}]$, where $\mathbf{X} = (X_1, \ldots, X_n)$ and let P be the associated Poincaré series. Let

$$D = \{(\mathbf{x}, y) \in \mathbb{Z}_p^{n+1} : \exists \mathbf{z} \in \mathbb{Z}_p^n \; f_1(\mathbf{z}) = \cdots = f_r(\mathbf{z}) = 0 \wedge \bigwedge v(x_i - z_i) \geq v(y)\}$$

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 $s \in (0, +\infty)$.

7.3.1 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. □

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, $\square_i$ 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

$$\sum_{\substack{(k_1,\ldots,k_m)\in L \\ k_i = \lambda_i (\mathrm{mod}\ N_i)}} p^{-(q_1 k_1 + \cdots + q_m k_m)s - k_1 - \cdots - k_m}$$

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

$$\mathbf{x} \in C \wedge v(a_1(\mathbf{x})) \, \square_1 \, v(y - c(\mathbf{x})) \, \square_2 \, v(a_2(\mathbf{x}))$$

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

$$\begin{aligned}
\int_A |h|_p^{s/M}\,dy\,d\mathbf{x} &= \int_A |h(\mathbf{x},y)|_p^{s/M'}\,dy\,d\mathbf{x} \\
&= \int_C \left(|h_0(\mathbf{x})|_p^{s/M'} \int\limits_{\substack{v(a_1(\mathbf{x}))\square_1 v(z)\square_2 v(a_2(\mathbf{x})) \\ z=\lambda \pmod{P_N^\times}}} |z|_p^{sv/M'} \right) dz\,d\mathbf{x} \\
&= \int_C \left(|h_0(\mathbf{x})|_p^{s/M'} \sum_{v(a_1(\mathbf{x}))\square_1 k\square_2 v(a_2(\mathbf{x}))} p^{-kvs/M'} \int\limits_{\substack{v(z)=k \\ z=\lambda \pmod{P_N^\times}}} 1\,dz \right) d\mathbf{x}
\end{aligned}$$

Let $w = p^{-k}z$. Then

$$\int\limits_{\substack{v(z)=k \\ z=\lambda(\text{mod } P_N^\times)}} 1\,dz = p^{-k} \int\limits_{\substack{v(w)=0 \\ w=p^{-k}\lambda \pmod{P_N^\times}}} 1\,dw.$$

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. □

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 $p \equiv 1 (\text{mod } 3)$ 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., Secrťariat 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.