MODNET, LAROCHE APRIL 2008
Luc Bélair

NOTES ON p-ADIC NUMBERS AND p-ADICALLY CLOSED FIELDS

1 The p-adic numbers

Let p be a prime number. The p-adic numbers were introduced by Kurt Hensel at the end of the 19th century. He aimed at transposing to number theory the methods of power series expansions used in the theory of functions of a complex variable (see [5],[7]). The p-adic numbers can be defined in many ways. Fix p and consider the ring formed by infinite sums of the form $a_0 + a_1p + \ldots + a_np^n + \ldots$, with $a_i \in \mathbb{Z}, 0 \leq a_i < p$, and where addition and multiplication are performed *in base* p by carrying in the natural way. It turns out to be an integral domain of characteristic 0. It is the *ring of p-adic integers*, denoted by $\mathbb{Z}_p$. Note that any positive integer $1, 2, 3, \ldots$ can be written as such a *finite* sum; in contrast we have $-1 = (p-1) + (p-1)p + \ldots + (p-1)p^n + \ldots$. One checks that e.g. $1 - p$ is invertible in $\mathbb{Z}_p$, namely $(1-p)^{-1} = 1 + p + p^2 + p^3 + \ldots + p^n + \ldots$. The field of p-adic numbers, denoted by $\mathbb{Q}_p$, is the field of fractions of $\mathbb{Z}_p$. One sees that for any positive integer k the quotient ring $\mathbb{Z}_p/p^k\mathbb{Z}_p$ is canonically isomorphic to $\mathbb{Z}/p^k\mathbb{Z}$, the ring of integers modulo p^k. In particular $\mathbb{Z}_p/p\mathbb{Z}_p$ is canonically isomorphic to the finite field $\mathbb{F}_p$ with p elements, so the principal ideal $p\mathbb{Z}_p$ is maximal. In fact, as in the power series ring over a field, a p-adic integer $a_0 + a_1p + \ldots + a_np^n + \ldots$ is invertible in $\mathbb{Z}_p$ if and only if $a_0 \neq 0$. In other words $p\mathbb{Z}_p$ coincides with the noninvertible elements[1]. In particular note that any nonzero p-adic integer a can be expressed as $a = p^ku$ where $k \in \mathbb{N}$ and $u \in \mathbb{Z}_p$ is invertible, so that any p-adic number $x \in \mathbb{Q}_p$ can expressed as $x = p^Nu$ with $N \in \mathbb{Z}$ and $u \in \mathbb{Z}_p$ as above, in other words $x = a_Np^N + a_{N+1}p^{N+1} + \ldots$, $a_N \neq 0$. We define the map $v_p : \mathbb{Q}_p \setminus \{0\} \to \mathbb{Z}$ as follows, for $x = a_Np^N + a_{N+1}p^{N+1} + \ldots$, $a_N \neq 0$, we set $v_p(x) = N$. For $a \in \mathbb{Z}$, $v_p(a)$ is the exponent of the highest power of p which divides a. The map v_p has the following properties

(A1) $v_p(1) = 0$;

(A2) $v_p(xy) = v_p(x) + v_p(y)$;

(A3) $v_p(x + y) \geq \min(v_p(x), v_p(y))$.

[1]And hence is the only maximal ideal, so $\mathbb{Z}_p$ is a so called *local ring*.

It can be used to define a norm $|\quad|_p$ on $\mathbb{Q}_p$, namely $|x|_p = p^{-v_p(x)}$. It is a key feature that this norm is *nonarchimedean* : $|(x+y)|_p \leq \max(|x|_p, |y|_p))$. Notice that if $v_p(x) \neq v_p(y)$ then $v_p(x+y) = \min(v_p(x), v_p(y))$ so that, if $|x|_p \neq |y|_p$ then $|x+y|_p = \max(|x|_p, |y|_p)$.

One checks that $(\mathbb{Q}_p, |\quad|_p)$ is the Cauchy completion of $\mathbb{Q}$ with respect to this norm, and that $\mathbb{Z}_p$ is the projective limit of the system of natural projections $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$, when $n \geq m, n, m \in \mathbb{N}$.

Example 1 *Let $p = 3$, then 2^{3^n} is a Cauchy sequence and it converges to -1. In general for $0 < j \leq p-1, j \in \mathbb{N}$, j^{p^n} is a Cauchy sequence and it converges to a $(p-1)$-th root of 1.*

It turns out that to solve polynomial equations in the p-adic numbers, Newton's tangent method can be used systematically. This takes the form of the famous "Hensel's lemma".

Lemma 1 (Hensel's lemma) *Let $f(x) \in \mathbb{Z}_p$ and $a \in \mathbb{Z}_p$ such that $v_p(f(a)) > 0$ and $v_p(f'(a)) = 0$, then there exists $x \in \mathbb{Z}_p$ such that $f(x) = 0$ and $v_p(x-a) > 0$.*

One constructs inductively a Cauchy sequence (x_n) converging to the desired root: $x_0 = a$, $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$, with the properties $|f'(x_n)|_p = 1, |f(x_n)|_p < p^{-n}, |x_{n+1} - x_n|_p < p^{-n}$.

It is instructive to note that this allows to make $\mathbb{Z}_p$ algebraically definable in $\mathbb{Q}_p$, as follows.

Corollary 1 $\mathbb{Z}_p = \{y \in \mathbb{Q}_p : \exists t \in \mathbb{Q}_p, t^2 = 1 + p^3 y^4\}$

Let U_p be the group of units in $\mathbb{Z}_p$, and let $\mathbb{Q}_p^\times = \mathbb{Q}_p \backslash \{0\}$. Then $\mathbb{Q}_p^\times / U_p$ is isomorphic to the group $p^\mathbb{Z}$, which is order-isomorphic to the additive group of the integers, and the map v_p is essentially given by the quotient map $\mathbb{Q}_p^\times \to \mathbb{Q}_p^\times / U_p$. The subring $\mathbb{Z}_p$ of $\mathbb{Q}_p$ has the property that for any $x \in \mathbb{Q}_p$, $x \in \mathbb{Z}_p$ or $x^{-1} \in \mathbb{Z}_p$, which is enough to ensure that the divisibility relation in $\mathbb{Z}_p$ makes the quotient group $\mathbb{Q}_p^\times / U_p$ into an ordered abelian group, whose order is in fact the same as above. By the corollary, any elementary extension of $\mathbb{Q}_p$ will carry a definable ring mimicking these features of $\mathbb{Z}_p$, which will make it a field *with a valuation*, i.e. a valued field.

2 Henselian fields

For K a field, we set $K^\times = K \setminus \{0\}$. The notion of a valued field is axiomatized by the above properties (A1), (A2), (A3) for a field K together with a surjective map v from $K^\times$ to an ordered abelian group (usually expressed additively). We say that v is a *valuation* on K and that (K, v) is a *valued field*. We will denote the image of $K^\times$ under v by $valK$, and call it the *value group* of (K, v). A subring V of a field K is called a *valuation ring* if for all $x \in K$, $x \in V$ or $x^{-1} \in V$. A valued field (K, v) has the associated valuation ring $V_{(K,v)} = \{x \in K : v(x) \geq 0\}$. In a valuation ring V, the nonivertible elements form an ideal, necessarily maximal, and the quotient ring V/M is called the *residue field* of V. For a valued field (K, v), the residue field of $V_{(K,v)}$ will be denoted by $resK$ and be designated as the residue field of (K, v). We will denote the quotient map $V_{(K,v)} \to resK$ by res and call it the *residue map*. In $(\mathbb{Q}_p, v_p)$ all this translates as follows: the valuation ring of $(\mathbb{Q}_p, v_p)$ is exactly $\mathbb{Z}_p$, its residue field "is" $\mathbb{F}_p$, and its valued group is $(\mathbb{Z}, +, \leq, 0)$. We will also use the notation V_K for the valuation ring of (K, v), when there is no risk of confusion.

Definition 1 *A valued field (K, v) is called* henselian *if Hensel's lemma holds, i.e. if $f \in V_K[X]$ then the simple roots of f in $resK$ lift uniquely to roots of f in V_K.*

Theorem 1 (see [4]) *Let (K, v) be a valued field of characteristic 0. The following conditions are equivalent.*

1. *The valued field (K, v) is henselian.*
2. *The valuation of K extends uniquely to any algebraic extension.*
3. *(Hensel-Rychlik property) If $f \in V_K[X]$ is a monic polynomial with discriminant $D(f)$ and there is $a \in V_K$ such that $v(f(a)) > v(D(f))$ then there is $a \in V_K$ such that $f(a) = 0$.*
4. *(Hensel-Newton property) If $f \in V_K[X]$ and there is $a_0 \in V_K$ such that $v(f(a)) > 2v(f'(a_0))$ then there is $a \in V_K$ such that $f(a) = 0$ and $v(a - a_0) > v(f'(a_0))$.*

Theorem 2 (see [4]) *Let (K, v) be a valued field. There exists a valued field (K^h, v^h) such that*

1. *K^h is an algebraic extension of K and v^h extends v.*

2. *(K^h, v^h) is henselian.*

3. *For any valued field extension (L, v) of (K, v), if (L, v) is henselian then (K^h, v^h) embeds uniquely in (L, v) over (K, v).*

4. *(K^h, v^h) is unique up to (K, v)-isomorphism with above properties.*

Definition 2 *Let (K, v) be a valued field, the valued field (K^h, v^h) given by the previous theorem is called the* henselization *of (K, v).*

3 The p-adically closed fields

Recall that a $\mathbb{Z}$-group is an ordered abelian group, say Γ, with a least positive element, say 1, such that for each positive integer $n \geq 2$, $\Gamma/n\Gamma = \{n\Gamma, 1 + n\Gamma, \ldots, (n-1).1 + n\Gamma\}$. Recall that these properties axiomatize $(\mathbb{Z}, +, \leq, 0)$.

Definition 3 *Let p be a fixed prime. A valued field (K, v) of characteristic 0 is called p-*adically closed*, if $v(p)$ is the least positive element of $valK$, $resK = \mathbb{F}_p$, $valK$ is a $\mathbb{Z}$-group, and the valuation is henselian.*

To prove the next theorem we need to make effective a fundamental type of argument[2], relating the roots of two polynomials sufficiently close to each other, in the sense of the following valuation $\tilde{v}$: recall that that if $f(X) = \sum a_i X^i$ and $g(X) = \sum b_i X^i$, then $\tilde{v}(f - g) = \min v(a_i - b_i)$.

Theorem 3 *Let F be a p-adically closed field. Then $\tilde{F} = F\tilde{\mathbb{Q}}$.*

Proof. We have $\tilde{\mathbb{Q}} \subseteq F\tilde{\mathbb{Q}} \subseteq \tilde{F}$ and we want to show that $F\tilde{\mathbb{Q}}$ is algebraically closed. Suppose there is an irreducible monic polynomial $f(X) = a_0 + a_1 X + \ldots + X^n$. We may assume $v(a_i) \geq 0$ and $v(a_0) = 0$. Indeed since F is henselian if $f(z) = 0$ then $v(z) = v(a_0)/n$ and since $valF$ is a $\mathbb{Z}$-group there is some $x \in F\tilde{\mathbb{Q}}$ such that $v(x) = v(a_0)/n$. Let $f(X) = \prod(X - x_i)$, then $\prod(X - x_i/x)$ does the job. So we now assume

$$\begin{aligned} f(X) &= X^n + a_{n-1}X^{n-1} + \ldots + a_2 X^2 + a_0 \\ &= (X - x_1)\ldots(X - x_n) \end{aligned}$$

where $v(a_i) \geq 0, v(a_0) = 0, x_i \in \tilde{F}, v(x_i) = 0$. It follows that there is no $z$in the valuation ring of $\tilde{F}$ such that $\tilde{v}(f(X) - (X - z)^n) \leq v(n)$. For otherwise $v(z^n) = 0$ and $v(n) = v(nz) > v(n)$, which is absurd. This implies that

[2]Known as *Krasner's lemma*.

for some $i, j \leq n, v(x_i - x_j) \leq v(n)$. For suppose $v(x_i - x_j) > v(n)$ for all $i \neq j$. Note that $a_k = s_k(x_1, \ldots, x_n)$ for some symmetric polynomial s_k. For definiteness say $n = 3$. Then e.g. $a_2 = x_1x_2 + x_1x_3 + x_2x_3$ and we have

$$a_2 - 3x_1^2 = x_1(x_1 - x_2) + x_1(x_3 - x_1) + x_2(x_3 - x_1) + x_1(x_2 - x_1)$$

so that $v(a_2 - 3x_2^3) > v(3)$. Similar computations give $\tilde{v}(f(X) - (X - x_1)^n) > v(n)$, which cannot be. So let $v(x_1 - x_2) \leq v(n)$. Now, because $valF$ is a $\mathbb{Z}$-group, $res\,\tilde{F} = \tilde{\mathbb{F}}_p = res\,\tilde{\mathbb{Q}}$ and $val\,F\tilde{\mathbb{Q}}/valF$ is torsion, we can approximate f up to any prescribed finite power p^k by a polynomial g over $\tilde{\mathbb{Q}}$ in the sens that $\tilde{v}(f - g) > v(p^k)$. So let

$$\begin{aligned} g(X) &= X^n + b_{n-1}X^{n-1} + \ldots + b_0 \\ &= (X - y_1)\ldots(X - y_n) \end{aligned}$$

with

$$b_i, y_i \in \tilde{\mathbb{Q}}, \quad \tilde{v}(f - g) = \min v(a_i - b_i) > nv(n)$$

We claim that for some i, $v(x_i - y_i) > v(n)$. For otherwise $v(g(x_1)) \leq nv(n)$ and letting $h = f - g$, we get $v(h(x_1)) \geq \min v(a_i - b_i) > nv(n)$ so $nv(n) < v(h(x_1)) = v(g(x_1)) \leq nv(n)$ which is absurd. So let $v(x_1 - y_1) > v(n)$, and let $\sigma \in Gal(\tilde{F}/F\tilde{\mathbb{Q}})$ such that $\sigma(x_1) = x_2$. Then

$$\begin{aligned} v(n) < v(x_1 - y_1) &= v(\sigma(x_1 - y_1)) \\ &= v(x_2 - y_1) \\ &= \min\{v(x_1 - x_2), v(x_1 - y_1)\} \\ &= v(x_1 - x_2) \leq v(n) \end{aligned}$$

which is absurd. This completes the proof. □

Corollary 2 *Let F be a p-adically closed field and K a finite extension of F. Then there exists $x \in K$ algebraic over $\mathbb{Q}$ such that $K = F(x)$.*

Lemma 2 [3] *Let F be a valued field. The following are equivalent.*

1. *The field F is p-adically closed and valued in $\mathbb{Z}$.*
2. *The field F is p-adically closed and isomorphic to a valued subfield of $\mathbb{Q}_p$.*
3. *The field F is isomorphic to a relatively algebraically closed subfield of $\mathbb{Q}_p$.*

Proof. For (1) $\Rightarrow$ (3), the Cauchy completion of F is isometric to $\mathbb{Q}_p$. The result follows from the density of $\mathbb{Q}$ in $\mathbb{Q}_p$ and the Hensel-Rychlik property in F. $\square$

Denote by A_p the henselization of $\mathbb{Q}$ with respect to the p-adic valuation.

Lemma 3 [3] *Let F be a p-adically closed field. There is a unique embedding of $i : A_p \to F$ and $i(A_p)$ is the field of absolute algebraic numbers of F.*

Proof. The first part follows from the universal property of the henselization and the density of $\mathbb{Q}$ in A_p. Let A be the realtive algerbaic closure of $\mathbb{Q}$ in F. Then A satisfies (1) of the preceding lemma, so there is a valued field isomorphism $f : A \to B$, B a relatively algebraically closed subfield of $\mathbb{Q}_p$ algebraic over $\mathbb{Q}$. By the preceding lemma and the first part, B has to coincide with $A_p \subseteq \mathbb{Q}_p$ and A with $A_p \subseteq F$. $\square$

Lemma 4 *Let $K \subseteq E$ be fields of characteristic 0 with K algebraically closed in E. Let $K \subseteq L \subseteq \tilde{E}$ with $[L : K]$ finite. Then $[LE : E] = [L : K]$ and L is relatively algebraically closed in LE.*

We say that $(K, v) \subseteq (E, w)$ is an extension of valued fields if $K \subseteq E$ and v is the restriction of w to K, or in terms of valuation rings if $V_K = K \cap V_E$. Such an extension of valued fields induces natural inclusions at the level of residue fields and value groups. In the above notation, the degree of the extension $resE/resK$ is called the *residue degree*, and the index $[valE : valK]$ is called the *ramification index*. We say that an extension of valued fields is *immediate* when both the residue degree and ramification index are equal to 1, or in other words when both the residue field and value group stay the same. We say that a valued field (K, v) is *dimension maximal*[4], if for all valued field extensions $(K, v) \subseteq (E, w)$ such that E/K is a finite extension, the following equality holds : $[E : K] = [valE : valK] \cdot [resE : resK]$. It is a known fundamental fact that $(\mathbb{Q}_p, v_p)$ is dimension maximal.

Theorem 4 *The valued field A_p is dimension maximal.*

Proof [3] Let $A_p(x)/A_p$ be a finite extension field of degree n with ramification index e' and residue degree f'. We want to see that $n = e'f'$. we may assume $v(x) \geq 0$. Consider $A_p \subset \mathbb{Q}_p$. Now $[\mathbb{Q}_p(x) : \mathbb{Q}_p] = n$ and we know $n = ef$ for the extension $\mathbb{Q}_p(x)/\mathbb{Q}_p$, where e is the ramification index and

[3] Ax-Kochen (1965).

[4] Sometimes called *defectless*, but the terminology does not seem to have settled.

f is the residue degree. Let $z_1 = 1, z_2, \ldots, z_f \in \mathbb{Q}_p(x)$ be liftings of a basis of $res\mathbb{Q}_p(x)/\mathbb{F}_p$ to $p^f - 1$ roots of 1 in the valuation ring. Let π be a prime element in $\mathbb{Q}_p(x)$. Then $\pi^e = up$ for some $u \in \mathbb{Q}_p(x), v(u) = 0$. For the moment assume $e > 1$. Let

$$\begin{aligned} u &= u_0 + u_1 x + \ldots + u_{n-1}x^{n-1} \ , u_i \in \mathbb{Q}_p \\ u_i &= u_{i,N_i}p^{N_i} + u_{i,N_i+1}p^{N_i+1} + \ldots \ N_i \in \mathbb{Z}, \ 0 \leq u_{i,j} < p \\ S_{i,k} &= u_{i,N_i}p^{N_i} + \ldots + u_{i,k}p^k. \end{aligned}$$

Let N be large enough so that $v(u_i - S_{i,N}) > ev(e) + (e-1)v(p)$ and let $u' = S_{0,N} + \ldots + S_{n-1,N}x^{n-1}$. Then $v(u-u') \geq ev(e)+(e-1)v(p) > 0$ and in particular we have $v(u') = 0$. By the Hensel-Rychlik property there exists $y \in \mathbb{Q}_p(x)$ with $y^e = u'p$. Clearly $1, y, \ldots, y^{e-1}$ are coset representatives for $val\mathbb{Q}_p(x)/val\mathbb{Q}_p$ and algebraic over $\mathbb{Q}$. The n products $z_i y^j$ are linearly independent over $\mathbb{Q}_p$. Now they are algebraic over $\mathbb{Q}$ so they lie in $A_p(x)$, using theorem 3 and lemma 4. Thus the $z_i y^j$ form a basis for $A_p(x)/A_p$, the y^j belong to different cosets of $valA_p(x)/valA_p$, and the $res\, z_i$ still are linearly independent over $\mathbb{F}_p = res\, A_p$, and we have $n = ef \leq e'f' \leq n$. It follows that $e'f' = n$ and in fact $e' = e, f' = f$. It is now clear how to deal with $e = 1$. □

Theorem 5 *Let K be a p-adically closed field and F a relatively algebraically closed valued subfield of K. Then F is p-adically closed.*

Theorem 6 *Let K be a p-adically closed field. Then K is dimension maximal.*

Proof. Let L be a finite extension of K of degree n, $L = K(x)$ with x algebraic over $\mathbb{Q}$. recall that A_p can be identified with the the relative algebraic closure of $\mathbb{Q}$ in K. We have $[A_p(x) : A_p] = n$. Since A_p is dimension maximal we get $n = ef$ where $e = [valA_p(x) : valA_p]$ and $f = [resA_p(x) : resA_p]$. Let $a_i, b_j \in A_p(x)$ such that $resa_1, \ldots, resa_f$ is a basis for $resA_p(x)/resA_p$ and $b_1, \ldots, b_e$ is a set of representatives for $valA_p(x)/valA_p$. Since $resA_p = resK$, $resa_1, \ldots, resa_f$ are still linearly independent over $resK$. We claim that $b_1, \ldots, b_e$ yield different cosets of $valK$. Indeed suppose $v(b_i b_j^{-1}) \in valK$. Since the extension $A_p(x)/A_p$ is finite there is some $k \in \mathbb{N}$ such that $kv(b_i b_j^{-1}) \in valA_p$. Since $valA_p \subseteq valK$ are both $\mathbb{Z}$-groups with the same least positive element, it follows that $v(b_i b_j^{-1}) \in valA_p$, contradicting the choice of the b_j's. Let $e' = [valL : valK]$ and $f' = [resL : resK]$, we get $n = ef \leq e'f' \leq n$, so $n = e'f'$, in fact $e' = e, f' = f$. □

4 Exercices

The following fill in some of the details of the proof of Macintyre's theorem on the elimination of quantifiers in the p-adic numbers and p-adically closed fields, which was sketched during the talk.

1 Let p be prime and for each integer $n \geq 2$, let $\Delta_n = \{\lambda p^r : \lambda, r \in \mathbb{N}, 0 \leq r < n, 0 \leq \lambda < p^{2v_p(n)+1}, p \nmid \lambda\}$. Let K be a p-adically closed field. Show that for each $n \geq 2$ and $x \in K$ there exists $e \in \Delta_n$ such that $ex \in K^{\times n}$. (Use Hensel's lemma.)

2 Let p be prime. Let $(K_i, v_i), i = 1, 2$ be p-adically closed fields, $A_i \subseteq K_i, i = 1, 2$ be subfields and $f : A_1 \to A_2$ be an isomorphism of valued fields for the induced valuations v_i. Show that for all $n \in \mathbb{N}$ and all $a \in A_1$, **if** $v(a) = 0$ then we have that $a \in K_1^{\times n}$ if and only if $f(a) \in K_2^{\times n}$. (Use Hensel's lemma.)

Uniqueness of p-adic closures. For the next exercices, let $(K_i, v_i), i = 1, 2$ be p-adically closed fields, $A_i \subseteq K_i, i = 1, 2$ be subfields such that K_i is algebraic over A_i. Let $f : A_1 \to A_2$ be an isomorphism of valued fields for the induced valuations v_i such that for all $n \in \mathbb{N}$ and all $a \in A_1$, we have that $a \in K_1^{\times n}$ if and only if $f(a) \in K_2^{\times n}$. We will show below that f extends to a valued field isomorphism between K_1 and K_2.

U1 Show that if for all $n \in \mathbb{N}, n \cdot valA_1 = n \cdot valK_1 \cap A_1$, then $valA_1$ is a $\mathbb{Z}$-group.

U2 Show that it suffices to extend f to a subfield $A_1 \subseteq B_1 \subseteq K_1$ such that for all $n \in \mathbb{N}, n \cdot valB_1 = n \cdot valK_1 \cap B_1$.

U3 Show that in the two previous exercises it suffices to consider the case where n is a prime number.

U4 Let q be prime, $a_1 \in A_1$ such that $v(a_1)/q \in valK_1 \setminus valA_1$.

(a) Check that we may assume $a_1 \in K^{\times q}$.

(b) Check that $X^q - a_1$ is irreducible over A_1.

U5 Let q and $a_1 \in A_1$ as in U4 and $a_1 \in K_1^{\times q}$. Let $a_2 = f(a_1)$, so that $a_2 \in K_2^{\times q}$. Let $y_1 \in K_1$ such that $y_1^q = a_1$.

(a) Show that for any $c_0, \ldots, c_{q-1} \in A_1$, $v(\sum_{i=0}^{q} c_i y_1^i) = \min v(c_i y_1^i)$.

(b) Show that for *any* $y_2 \in K_2$ such that $y_2^q = a_2$, the map $\tilde{f} : A_1(y_1) \to A_2(y_2)$ defined by $\tilde{f}(\sum_{i=0}^q c_i y_1^i) = \sum_{i=0}^q c_i y_2^i$ is a valued field isomorphism.

U6 Let q and $a_1 \in A_1, y_1 \in K_1$ as in U5. Let $a_2 = f(a_1)$ and $e_n \in \Delta_n, n \geq 2$, such that $e_n y_1 \in K^{\times q}$ and **suppose** there is $y_2 \in K_2$ such that $y_2^q = a_2$ and for all $n \geq 2, e_n y_2 \in K_2^{\times n}$. Let $\tilde{f}$ as in U5 and let $x_1 \in A_1(y_1), x_2 = \tilde{f}(x_1)$. By U5 there is for some $0 \leq i < q$ and $d_1 \in A_1$ such that $v(x_1 d_1 y_1^i) = 0$. Let $d_2 = f(d_1)$, then $v(x_2 d_2 y_2^i) = 0$.

(a) Show there is some $\lambda \in \mathbb{N}$ such that $\lambda x_1 d_1 y_1^i \in K_1^{\times n}$ and $\lambda x_2 d_2 y_2^i \in K_2^{\times n}$.

(b) Show that $x_1 \in K_1^{\times n}$ iff $x_2 \in K_2^{\times n}$.

U7 Show that there is the same number of q-th roots of unity in K_1 and K_2.

U8 Let $q, a_1 \in A_1, y_1 \in K_1, y_2 \in K_2, \tilde{f}$ as in U5. Show that if 1 is the only q-th root of unity in K_1, then for all $x \in A_1(y_1), n \geq 2, x \in K_1^{\times n}$ iff $\tilde{f}(x) \in K_2^{\times n}$.

U9 Let $q, a_1 \in A_1, y_1 \in K_1$ as in U5. Suppose 1 is not the only q-th root of unity in K_1, so the same in K_2 by U7. Let $z \in K_2$ be a primitive q-th root of unity and $b \in K_2$ such that $b^q = a_2$, so that the q-th roots of a_2 are $b, bz, \ldots, bz^{q-1}$. Suppose there are $n_0, \ldots, n_{q-1} \geq 2$ such that $e_{n_j} b z^j \notin K_2^{\times n_j}, j = 1, \ldots, q-1$ and let n be the least common multiple of the n_j. Show that $(e_n b x^n)^q = 1$ for some $x \in K_2$ and deduce a contradiction.

U10 Conclude that f extends as in U2 for $n = q$.

Other exercises.

3 Let $(K, v), (K', v)$ be p-adically closed fields and suppose $K \subset K', trdeg K'/K = 1, valK \subset valK'$, and let $b \in K'$ such that $v(b) \notin valK$.

(a) Check that for any $k_i, k_j \in K$ and $i \neq j \in \mathbb{N}, v(k_i b^i) \neq v(k_j b^j)$.(Use that $n \cdot valK = valK \cap n \cdot valK'$ for all integers n.)

(b) Check that b is transcendental over K, that for any $k_0, \ldots, k_n \in K, v(\sum_i k_i b^i) = \min v(k_i b^i)$, and $valK(b) = valK \oplus \mathbb{Z}v(b)$, and that the inequalities $v(k_0) < v(b) < v(k_1), k_0, k_1 \in K$ determine $(K(b), v)$ up to (K, v)-isomorphism.

(c) For each $n \geq 2$, let $e_n \in \Delta_n$ such that $e_n b \in K'^{\times n}$. Check that the inequalities $v(k_0) < v(b) < v(k_1), k_0, k_1 \in K$, in addition to the conditions $P_n(e_n b), n \geq 2$, determine $K(b)$ up to K-isomorphism in $L_v + (P_n)_{n\geq 2}$. (Use arguments analog to U6)

4 Use Robinson's method to prove that algebraically closed (nontrivially) valued fields admit quantifier elimination in the basic language of valued fields.

References

[1] L. Bélair, Le théorème de Macintyre, un théorème de Chevalley p-adique, Annales des Sciences Mathématiques du Québec 14 (1990) 109-120.

[2] S. Kochen, The model theory of local fields, in: *Logic Conference, Kiel 1974*, (Lecture Notes in Math., 499), Springer-Verlag, 1975.

[3] A. Prestel and P. Roquette, *Formally p-adic fields*, L.N.M. 1050, Springer, 1984.

[4] P. Ribenboim, Equivalent forms of Hensel's lemma, *Expositiones Math.*, 3, 1985, 3-24.

[5] P. Roquette, History of valuation theory. Part I, in: *Valuation theory and its applications Vol II, Proceedings of the first international conference on valuation theory (Saskatoon, 1999)*, F.-W. Kuhlmann et al. eds., (Fields Inst. Commu., 32), A.M.S., 2002, 291-335. (See http://www.rzuser.uni-heidelberg.de/ ci3/ for an update.)

[6] A. Robinson, *Complete theories*, North-Holland, 1977 [1956].

[7] P. Ullrich, The genesis of Hensel's p-adic numbers, in *Charlemagne and his heritage: 1200 years of civilization and science in Europe (Aachen 1995), Vol. 2 Mathematical arts*, ed. P. L. Butzer et al. , Brepols Publishers, 1998, pp. 163-178.