p-adic \mathcal{D}'

Thomas Nowak

January 21, 2008

1 p-adic Numbers

1.1 \mathbb{Q}_p

For $n \in \mathbb{Z}$, $n \neq 0$, and p prime, let $\operatorname{ord}_p(n)$ denote the exponent of p in the prime factorization of |n| and let $\operatorname{ord}_p(0) = \infty$. For $a/b \in \mathbb{Q}$, we set $\operatorname{ord}_p(a/b) = \operatorname{ord}_p(a) - \operatorname{ord}_p(b)$. This definition is independent of the choice of representatives. We then define $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ by $|x|_p = p^{-\operatorname{ord}_p(x)}$. This is an absolute value on \mathbb{Q} which satisfies a stronger form of the triangle inequality — the $\mathit{ultrametric}$ inequality:

$$|x+y|_p \leqslant \max\left(|x|_p, |y|_p\right) \tag{UM}$$

It follows from $\operatorname{ord}_p(a/b+c/d)=\operatorname{ord}_p((ad+bc)/bd)=\operatorname{ord}_p(ad+bc)-\operatorname{ord}_p(bd)\geqslant \min(\operatorname{ord}_p(a)+\operatorname{ord}_p(d),\operatorname{ord}_p(b)+\operatorname{ord}_p(c))-\operatorname{ord}_p(b)-\operatorname{ord}_p(d)=\min(\operatorname{ord}_p(a/b),\operatorname{ord}_p(c/d)).$ We define \mathbb{Q}_p to be the completion of \mathbb{Q} with respect to the metric $d(x,y)=|x-y|_p$. This is again a field with the usual operations and the usual expansion of $|\cdot|_p$ to \mathbb{Q}_p is again an absolute value. By the continuity of $\max:\mathbb{R}^2\to\mathbb{R}$, we get the validity of (UM) for $x,y\in\mathbb{Q}_p$. It is $\mathbb{Q}_p\neq\mathbb{Q}_q$ for $p\neq q$, because $(p^n)\in 0$ in \mathbb{Q}_p , but $|p^n|_q=1$ for all n. Interesting is the following

Lemma. For all $x \in \mathbb{Q}_p \setminus \{0\}$ it is $|x|_p \in \{p^k \mid k \in \mathbb{Z}\}$.

Proof. Let (x_n) be a Cauchy sequence in $\mathbb Q$ with respect to $|\cdot|_p$ that does not converge to zero, i. e., 0 is no accumulation point. Then there exist $\varepsilon > 0$ and $N \in \mathbb N$ such that for all $n \ge N$

$$|x_n|_p \geqslant \varepsilon$$
 and $|x_n - x_N|_p < \varepsilon$.

With (UM), we get

$$|x_n|_p \leqslant \max(|x_n - x_N|_p, |x_N|_p) = |x_N|_p$$

and with the same argument

$$|x_N|_p \leqslant |x_n|_p$$

hence $|x_n|_p = |x_N|_p$ for all $n \ge N$. This shows that the sequence $(|x_n|_p)$ is eventually constant.

The elements of \mathbb{Q}_p can be represented as follows.

Proposition ($\mathbb{Q}_p \leftrightarrow \mathbb{Z}/p\mathbb{Z}((X))$). Let $x \in \mathbb{Q}_p$. Then there exist uniquely determined $0 \le a_j such that the sequence$

$$x_{n+N} = \sum_{j=-N}^{n} a_j p^j$$

is in x where $N = \max\{j \mid a_{-j} \neq 0\} \cup \{0\}$. In particular, the maximum exists.

Proof. We first consider the case $|x|_p \leq 1$, where we will have N=0. Let (c_n) be a Cauchy sequence in x. For every $k \in \mathbb{N}$ let N(k) denote a natural number such that for all $m,n \geq N(k), |c_m-c_n|_p < p^{-k-1}$ and N(k) < N(k+1). Now we set $x_{-1}=0$ and choose $x_k \in \mathbb{Z} \cap [0,p^{k+1})$ such that

$$|x_k - c_{N(k)}|_p \leqslant p^{-k-1}$$

for $k \ge 0$. These exist, because if we write $c_{N(k)} = a/b$ with (a,b) = 1 we can find $\lambda, \mu \in \mathbb{Z}$ such that $\lambda b + \mu p^{k+1} = 1$, since $\operatorname{ord}_p(a/b) \ge 0$. We can set $x_k = \lambda a + \alpha p^{k+1}$ with a suitable $\alpha \in \mathbb{Z}$ and get

$$\left|\lambda a - \frac{a}{b} + \alpha p^{k+1}\right|_p \leqslant \max(\left|\frac{a}{b}\right|_p |\lambda b - 1|_p, \left|\alpha p^{k+1}\right|_p) \leqslant \max(\left|\mu p^{k+1}\right|_p, p^{-k-1}) = p^{-k-1}.$$

We are ready to define

$$a_j = \frac{x_j - x_{j-1}}{p^j} \quad (j \geqslant 0).$$

It is $a_i \in \mathbb{Z}$ because

$$|x_j - x_{j-1}|_p \le \max(|x_j - c_{N(j)}|_p, |c_{N(j)} - c_{N(j-1)}|_p, |c_{N(j-1)} - x_{j-1}|_p) \le p^{-j}$$

hence $p^{j}|(x_{j}-x_{j-1})$ and since

$$-p^{j} < x_{i} - x_{i-1} < p^{j+1}$$

we have $0 \le a_j < p$. It is $(x_n) \sim (c_n)$, because for $n \ge N(k)$,

$$|x_n - c_n|_p \le \max(|x_n - x_k|_p, |x_k - c_{N(k)}|_p, |c_{N(k)} - c_n|_p) \le p^{-k-1}.$$

This proves the existence in our special case $|x|_p \leq 1$. Now the uniqueness. Let $\sum b_j p^j$ be another such sequence with $b_{j_0} \neq a_{j_0}$. Then

$$p^{j_0+1}
mathcal{1}
mathcal{1} \sum_{j=0}^{n} (a_j - b_j) p^j$$

for all $n \ge j_0$ and thus $(x_n) \not\sim \sum b_j p^j$.

The general case is handled by considering $p^m x$, whose p-adic absolute value is ≤ 1 for sufficiently large m.

We can thus identify a single element in \mathbb{Q}_p with a formal Laurent series over the residue field $\mathbb{Z}/p\mathbb{Z}$ considering the mapping

$$x \mapsto \sum_{j \geqslant -N} \overline{a_j} X^j$$
 (FLS)

which is a bijection, but not an isomorphism, since \mathbb{Q}_p has characteristic 0, but $\mathbb{Z}/p\mathbb{Z}((X))$ has characteristic p. It is $|x|_p = p^{-k}$ where $k = \min\{j \mid a_j \neq 0\}$.

Definition. $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leqslant 1\}.$

This is a subring of \mathbb{Q}_p with $\mathbb{Z}_p^{\times} = \{x \in \mathbb{Q}_p \mid |x|_p = 1\}$. Further, \mathbb{Z}_p is integrally closed in \mathbb{Q}_p . It is \mathbb{Q}_p the quotient field of \mathbb{Z}_p . Also, $\mathbb{Z} \subset \mathbb{Z}_p$.

1.2 Extensions of \mathbb{Q}_p

Definition. Let v be an absolute value on the field K. We call v non-Archimedean if it satisfies (UM), i. e., $v(x+y) \leq \max(v(x), v(y))$. We call v discrete if $v(K^{\times})$ is discrete in \mathbb{R}^+ . We also set

$$A_K = \{ x \in K \mid v(x) \le 1 \},$$

 $M_K = \{ x \in K \mid v(x) < 1 \}.$

Proposition. Let v be a non-Archimedean absolute value on K. Then, A_K and M_K are subrings of K and M_K is the unique maximal ideal of A_K . Thus, A_K is a local ring.

Lemma. Let L be a finite field extension of K and v non-Archimedean absolute value on L. Then A_L/M_L is a field extension of A_K/M_K .

Proof. Define $\iota: A_K/M_K \to A_L/M_L$, $\iota(x+M_K) = x+M_L$. This is well-defined and injective since $A_K \cap M_L = M_K$.

Definition. Let L be a finite field extension of K and v discrete non-Archimedean absolute value on L. Then we call the index of $v(K^{\times})$ in $v(L^{\times})$ the degree of ramification of L:K. We call

$$[A_L/M_L:A_K/M_K]$$

the degree of the residue field extension of L:K. Is the degree of ramification of L:K equal to 1, then L:K is non-ramified, is it equal to [L:K], then L:K is totally ramified.

Theorem. Let K be a with respect to the discrete non-Archimedean absolute value v complete field, L finite field extension K, e the degree of ramification and f the degree of the residue field extension of L: K. Then,

$$[L:K] = e \cdot f.$$

Proof. Let $\varphi: A_L \to A_L/M_L$ the canonical epimorphism and $y_i \in A_L$ $(i \in I)$, such that $\{\varphi(y_i) \mid i \in I\}$ is a basis of A_L/M_L over A_K/M_K . Then it is $v(y_i) = 1$ for all i. Let further $\pi \in A_L$, such that $M_L = (\pi)$. The order of $v(\pi) \cdot v(K^{\times})$ in the group $v(L^{\times})/v(K^{\times})$ is equal to e. We will show that

$$(y_i \pi^j)_{\substack{i \in I \\ 0 \leqslant j < e}}$$

is a basis of L: K. So, let

$$\sum_{\substack{i \in I \\ 0 \leqslant j < e}} \lambda_{ij} y_i \pi^j = \sum_{0 \leqslant j < e} \left(\sum_{i \in I} \lambda_{ij} y_i \right) \pi^j = 0$$

with $\lambda_{ij} \in K$ not all 0. By division by the λ_{ij} with largest absolute value, we can suppose $\lambda_{ij} \in A_K$, where $\lambda_{ij} \notin M_K$ for a λ_{ij} . By application of φ , we see that at least one $s_j \neq 0$ and that for those $s_j, v(s_j) = v(\lambda_{ij}) \in v(K^{\times})$. There have to be two $s_j \pi^j \neq 0$ with the same absolute value, $v(s_j \pi^j) = v(s_{j'} \pi^{j'})$ with j < j'. That is because $v(a) \neq v(b) \Rightarrow v(a+b) = \max(v(a), v(b))$. It follows that

$$v(\pi^{j'-j}) = \frac{v(\pi^{j'})}{v(\pi^j)} = \frac{v(s_j)}{v(s_{j'})} \in v(K^{\times}),$$

where j' - j < e. That is a contradiction to the choice of π . We now define the A_K -modules

$$X = \sum_{\substack{1 \leqslant i \leqslant f \\ 0 \leqslant j < e}} A_K y_i \pi^j, Y = \sum_{1 \leqslant i \leqslant f} A_K y_i$$

and show $X = A_L$. Obviously,

$$X = \sum_{0 \le i < e} \pi^j Y$$

and $A_L = Y + \pi A_L$. Repeated application of the last gives $A_L = \sum_{0 \leqslant j \leqslant e-1} \pi^j Y + \pi^e A_L$ and thus $A_L = X + M_K A_L$. Since $M_K X \subset X$ it follows that $A_L = X + M_K^{\nu} A_L$ for all $\nu \geqslant 1$ and since $(M_K^{\nu} A_L)_{\nu \in \mathbb{N}}$ is neighbourhood basis of 0 in A_L , it follows that $\overline{X} = A_L$. But it is X closed in A_L , because A_K is in K ist. This proves $X = A_L$.

Proposition. Let K be a non-trivially valued locally compact field and V a finite dimensional vector space over K. Then there exists at most one Hausdorff topology on V such that V becomes a topological vector space.

Proposition. Let K be a finite field extension of \mathbb{Q}_p . Then there exists exactly one absolute value on K that extends $|\cdot|_p$.

Theorem. Let K be a finite field extension of \mathbb{Q}_p . Then there exists a uniquely determined intermediate field M of $K : \mathbb{Q}_p$ such that $M : \mathbb{Q}_p$ is unramified and K : M is totally ramified.

Theorem (Hensel lemma). Let K be finite extension of \mathbb{Q}_p , π prime in A_K . Further let $f \in K[X]$, $\alpha_0 \in A_K$ with $f(\alpha_0) \equiv 0(\pi)$ and $f'(\alpha_0) \not\equiv 0(\pi)$. Then there exists an $\alpha \in A_K$ with $f(\alpha) = 0$ and $\alpha \equiv \alpha_0(\pi)$.

Theorem (Krasner lemma). Let $K : \mathbb{Q}_p$ be finite, $a, b \in \overline{\mathbb{Q}}_p$, $a = a_1, \dots, a_n$ the conjugates of a. Further let

$$|b-a|_n < |a_i-a|_n$$

for all $i \ge 2$. Then, $K(a) \subset K(b)$.

Proposition. The algebraic closure $\overline{\mathbb{Q}}_p$ of \mathbb{Q}_p is not complete.

Proof. It is $[\overline{\mathbb{Q}}_p : \mathbb{Q}_p] = \aleph_0$. This means that $\overline{\mathbb{Q}}_p = \bigcup_{i \in \mathbb{N}} K_i$ with $K_i \subset K_{i+1}$ and K_i finite over \mathbb{Q}_p , i. e., K_i complete. This shows that all K_i are closed. Also, they have empty interior. By Baire's theorem, $\overline{\mathbb{Q}}_p$ is not complete.

Definition. Let \mathbb{C}_p be the completion of $\overline{\mathbb{Q}}_p$.

Proposition. It is \mathbb{C}_p algebraically closed.

2 p-adic Analysis

We will now restrict ourselves to \mathbb{Q}_p again.

2.1 Basics

Theorem (Heine-Borel). Let $A \subset \mathbb{Q}_p$. It is A compact if and only if it is closed and bounded.

Proof. We show that \mathbb{Z}_p is compact. Let (x_n) be a sequence in \mathbb{Z}_p ,

$$x_n = \sum_{k \ge 0} x_n^k p^k.$$

For all k, the integer sequences $(x_n^k)_n$ have an accumulation point a_k , because $x_n^k \in \{0, \dots, p-1\}$. Then $a = \sum a_k p^k$ is an accumulation point of (x_n) .

Definition. For $x \in \mathbb{Q}_p^n$, we set

$$|x|_p = \max_{1 \le i \le n} |x_i|_p.$$

Let $a \in \mathbb{Q}_p^n$ and $\gamma \in \mathbb{Z}$. Then we set

$$\begin{split} B_{\gamma}(a) &=& \{x \in \mathbb{Q}_p^n \mid |x-a|_p \leqslant p^{\gamma}\}, \\ S_{\gamma}(a) &=& \{x \in \mathbb{Q}_p^n \mid |x-a|_p = p^{\gamma}\}, \\ \Delta_{\gamma} &=& \chi_{B_{\gamma}(0)}. \end{split}$$

Also, let $B_{\gamma} = B_{\gamma}(0)$ and $S_{\gamma} = S_{\gamma}(0)$.

Definition. Let $\gamma \in \mathbb{Z}$, $x_0 \in \mathbb{Q}_p$ such that

$$f(x) = \sum_{n \geqslant 0} a_n (x - x_0)^n.$$

converges for all $x \in B_{\gamma}(x_0)$. Then f is an analytic function on $B_{\gamma}(x_0)$. For $k \in \mathbb{N}$, we set

$$f^{(k)}(x) = \sum_{n \geqslant 0} (n+k) \cdots (n+1) a_{n+k} x^n,$$

$$f^{(-k)}(x) = \sum_{n \geqslant k} \frac{1}{(n-k+1) \cdots n} a_{n-k} x^n.$$

Definition. Let μ denote the unique positive regular translation-invariant Borel-measure on the locally compact group $(\mathbb{Q}_p, +)$ such that $\mu(B_0) = 1$. For μ -measurable $f : \mathbb{Q}_p^n \to \mathbb{C}$, we set

$$\int f(x)dx = \int f(x)d\mu(x).$$

Theorem (Substitution rule). Let $A, B \subset \mathbb{Q}_p^n$ open and compact, $\Phi = (\varphi_1, \dots, \varphi_n) : A \to B$ a homeomorphism such that all φ_i are analytic in A and

$$\det \frac{\partial \Phi(x)}{\partial x} \neq 0$$

for all $x \in A$. Then there holds

$$\int_{B} f(x)dx = \int_{A} f(\Phi(x)) \left| \det \frac{\partial \Phi(x)}{\partial x} \right|_{p} dx$$

for all $f \in L^1(B)$.

2.2 Distributions

Definition. Let $f: \mathbb{Q}_p^n \to \mathbb{C}$. It is called f locally constant if for every $x \in \mathbb{Q}_p^n$ there exists an $l(x) \in \mathbb{Z}$ such that $f(x + \xi) = f(x)$ for all $\xi \in B_{l(x)}$. The set of all locally constant functions on \mathbb{Q}_p^n is denoted by $\mathcal{E} = \mathcal{E}(\mathbb{Q}_p^n)$.

If f is locally constant with compact support, then $l = l(f) = \sup l(x)$ is called the degree of constancy of f. The set of all compact supported locally constant functions on \mathbb{Q}_p^n is denoted by $\mathcal{D} = \mathcal{D}(\mathbb{Q}_p^n)$. Its elements are called test functions.

We further set

$$\mathcal{D}_N^l = \mathcal{D}_N^l(\mathbb{Q}_p^n) = \{ f \in \mathcal{D} \mid l(f) \geqslant l, \operatorname{supp} f \subset B_N \}.$$

It is \mathcal{D}_N^l finite dimensional over \mathbb{Q}_p , hence complete, and $\mathcal{D}_M^k \subset \mathcal{D}_N^l$ for $M \leq N$ and $k \leq l$. We define the following notion of convergence in \mathcal{D} :

It is $\varphi_k \to 0$ iff there exist l and N such that $\varphi_k \in \mathcal{D}_N^l$ for all k and $\varphi_k(x) \to 0$ uniformly for all x. It is this the inductive limit of the spaces \mathcal{D}_N^l with the uniform convergence topology. Hence, \mathcal{D} is locally convex with this topology ([3], II, §4.4, ex. 2).

Proposition. For all compact K, it is \mathcal{D} dense in C(K).

Lemma. It is $\varphi_k \to 0$ if and only if $\varphi_k(x) \to 0$ uniformly and for all $\psi \in \mathcal{D}$, $\langle \varphi_k, \psi \rangle \to 0$.

Definition. We define $\mathcal{D}' = \mathcal{D}'(\mathbb{Q}_p^n)$ to be the set of linear forms on $\mathcal{D}(\mathbb{Q}_p^n)$. These are continuous. Convergence in \mathcal{D}' is weak convergence.

Proposition. It is \mathcal{D}' complete.

Proof. Let (f_k) be Cauchy in \mathcal{D}' . Then, $(\langle f_k, \varphi \rangle)$ is Cauchy in \mathbb{C} for all φ . Thus, there exists a $C(\varphi) \in \mathbb{C}$ with $\langle f_k, \varphi \rangle \to C(\varphi)$. By the linearity of $\langle f_k, \cdot \rangle$, we get the linearity of C and thus $C \in \mathcal{D}'$. It is $f_k \to C$.

Definition. Let $f \in \mathcal{D}'(\mathbb{Q}_p^n), g \in \mathcal{D}'(\mathbb{Q}_p^m)$. Then we define the distribution $f \times g$ by

$$\langle f(x) \times g(y), \varphi(x,y) \rangle = \langle f(x), g(y)\varphi(x,y) \rangle.$$

It is called the direct product of f and g.

For $f, g \in \mathcal{D}'(\mathbb{Q}_p^n)$, we define the convolution of f and g by

$$\langle f * g, \varphi \rangle = \lim_{k \to \infty} \langle f(x) \times g(y), \Delta_k(x) \varphi(x+y) \rangle.$$

Definition. We set

$$\delta_k = p^{nk} \Delta_{-k}.$$

Let $f \in \mathcal{D}'$. We call the sequence

$$f_k = \Delta_k(f * \delta_k)$$

the regularization of f.

It is
$$f_k \to f$$
.

Proposition. For $f \in C(\mathbb{Q}_p^n)$, it is $f_k(x) = f * \delta_k(x) \to f(x)$ for all x.

Proof. Let $\varepsilon > 0$. Since $\int \delta_k = 1$, we have

$$f_k(x) - f(x) = \int (f(x - y) - f(x))p^{nk} \chi_{B_{-k}}(y)dy$$
$$= p^{nk} \int_{B_{-k}} f(x - y) - f(x)dy.$$

Since f is continuous, there exists an $\gamma \in \mathbb{Z}$ such that $|f(x-y)-f(x)| < \varepsilon$ for $y \in B_{\gamma}$. It follows that

$$|f_k(x) - f(x)| \le \varepsilon p^{nk} \int_{B_{-k}} dy = \varepsilon$$

for $k \geqslant \gamma$.

2.3 Colombeau-type algebra of generalized functions

Definition. $\mathcal{P} = \mathcal{D}^{\mathbb{N}}$. We define addition and multiplication on \mathcal{P} componentwise (and pointwise). This forms an algebra over \mathbb{C} .

 $\mathcal{N} = \{(f_k) \in \mathcal{P} \mid \text{for all compact } K \text{ there exists an } N \text{ such that } f_k | K = 0 \text{ for } k \geqslant N \}.$

It is this an ideal of \mathcal{P} .

Definition. We call $\mathcal{G}_p = \mathcal{P}/\mathcal{N}$ the p-adic Colombeau-Egorov algebra. Its elements are called generalized functions.

Theorem. The mapping $\Phi: \mathcal{D}' \to \mathcal{G}_p$, $\Phi(f) = (f_k) + \mathcal{N}$ is a vector space monomorphism, where (f_k) denotes the regularization of f. The mapping $\Psi: \mathcal{D} \to \mathcal{G}_p$, $\Psi(f) = (f) + \mathcal{N}$ is an algebra monomorphism.

Proof. It is obvious that Φ is linear. We will now prove that $(f_k) \in \mathcal{N}$ implies f = 0. For $\varphi \in \mathcal{D}$, it is $\langle f_k, \varphi \rangle = \langle f, \delta_k * \varphi \rangle$. For all $k \geqslant -l(\varphi)$, we have $\delta_k * \varphi(x) = p^{nk} \int_{B_{-k}} \varphi(x-y) dy = \varphi(x)$ for all x. It follows that $\langle f, \varphi \rangle = \langle f_k, \varphi \rangle = 0$ for $k \geqslant \max(-l(\varphi), N(K))$, where $K = \sup \varphi$, i. e., f = 0.

Definition. We define $\mathcal{A} = \mathbb{C}^{\mathbb{N}}$ with componentwise operations, $\mathcal{I} = \{(c_k) \in \mathcal{A} \mid c_k \neq 0 \text{ for at most finitely many } k\}$. It is \mathcal{I} an ideal in \mathcal{A} . Let $\mathcal{C} = \mathcal{A}/\mathcal{I}$ be the set of Colombeau-Egorov generalized numbers.

Further, we set \mathcal{B} to be the set of bounded sequences in \mathbb{Q}_p^n and $\mathcal{J} = \{(d_k) \in \mathcal{B} \mid d_k \neq 0 \text{ for at most finitely many } k\}$. Again, \mathcal{J} is an ideal of \mathcal{B} and we set $\mathcal{M} = \mathcal{B}/\mathcal{J}$. Its elements are called generalized points.

Definition. For $f = (f_k) + \mathcal{N} \in \mathcal{G}_p$ and $x = (x_k) + \mathcal{J} \in \mathcal{M}$, we set $(f_k(x_k)) + \mathcal{I} \in \mathcal{C}$ the point value of f at x, denoted by f(x).

Lemma. The point value is well-defined.

Theorem. Let $f, g \in \mathcal{G}_p$. Suppose that for all $x \in \mathcal{M}$ we have f(x) = g(x). Then, f = g.

References

- [1] S. Albeverio, A. Yu. Khrennikov, and V. M. Shelkovich. *p*-adic colombeau-egorov type theory of generalized functions. *Math. Nachr.*, 278:3–16, 2005.
- [2] Z. I. Borevich and I.R. Shafarevich. Number Theory. Academic Press, 1986.
- [3] N. Bourbaki. Topological Vector Spaces. Springer, 1987.
- [4] N. Koblitz. p-adic Numbers, p-adic Analysis and Zeta-Functions. Springer, 1977.
- [5] E. Mayerhofer. On the characterization of p-adic colombeau-egorov generalized functions by their point values. *Math. Nachr.*, 280:1297–1301, 2007.
- [6] J. Schoißengeier. Commutative algebra (lecture notes), 2006.
- [7] V. S. Vladimorov, I. V. Volovich, and E. I. Zelenov. *p-adic Analysis and Mathematical Physics*. World Scientific, 1994.