Liczby p-adyczne

13 kwietnia 2016

Spis treści

Rozdział 1

Nieuporządkowane

1.1 Normy

Definicja 1.1.1. *Norma na ciele K to funkcja $|\cdot|\colon K \to \mathbb{R}_+$ spełniająca trzy warunki:*

1. $|x| = 0$, *wtedy i tylko wtedy gdy* $x = 0$
2. $|xy| = |x|\,|y|$ *dla wszystkich* $x, y \in K$
3. $|x + y| \leq |x| + |y|$ *dla wszystkich* $x, y \in K$

Mówimy, że norma jest niearchimedesowa, jeżeli zachodzi dodatkowo

4. $|x + y| \leq \max(|x|, |y|)$ *dla wszystkich* $x, y \in K$,

w przeciwnym razie mamy do czynienia z normą archimedesową.

Definicja 1.1.2. *Waluacja p-adyczna (dla ustalonej liczby pierwszej $p \in \mathbb{Z}$) to funkcja $v_p\colon \mathbb{Z} \setminus \{0\} \to \mathbb{R}$ określona w następujący sposób: $v_p(n)$ to jedyna dodatnia liczba całkowita, dla której zachodzi równość $n = p^{v_p(n)}n'$, przy czym p nie dzieli n'. Przedłuża się ją do całego ciała $\mathbb{Q}$ wzorem*

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b),$$

z umową, że $v_p(0) = +\infty$.

Tak określona funkcja jest dobrze określona.

Dowód. Jeśli $a/b = c/d$, to $ad = bc$. Rozkład na czynniki pierwsze w $\mathbb{Z}$ jest jednoznaczny, zatem najwyższa potęga p dzieląca ad to suma najwyższych potęg dzielących a i d, $v_p(ad) = v_p(a)+v_p(d)$. Podobnie pokazuje się, że $v_p(bc) = v_p(b) + v_p(c)$. Skoro $v_p(ad) = v_p(bc)$, to $v_p(a) + v_p(d) = v_p(b) + v_p(c)$ i po przeporządkowaniu $v_p(a) - v_p(b) = v_p(c) - v_p(d)$. □

Lemat 1.1.3. *Dla wszystkich $x, y \in \mathbb{Q}$ mamy*

1. $v_p(xy) = v_p(x) + v_p(y)$
2. $v_p(x + y) \geq \min(v_p(x), v_p(y))$.

Dowód. Załóżmy najpierw, że x, y są całkowite, a przy tym $x = p^n x'$, $y = p^m y'$ (gdzie $p \nmid x'y'$). Bez straty ogólności $n \leq m$, wtedy $xy = p^{n+m} x'y'$ (co pokazuje 1.) i $x + y = p^n(x' + p^{m-n} y')$, więc $v_p(x + y) \geq n = v_p(x)$ (2.).

Jeżeli $x = q/r$ i $y = s/t$, to $v_p(xy) = v_p(qs/rt) = v_p(qs) - v_p(rt) = v_p(q) + v_p(s) - v_p(r) - v_p(t) = v_p(q/r) + v_p(s/t) = v_p(x) + v_p(y)$. Dowód drugiej części:

$$\begin{aligned} v_p(x+y) &= v_p\left(\frac{qt+sr}{rt}\right) = v_p(qt+sr) - v_p(rt) \leq \min(v_p(qt), v_p(sr)) - v_p(rt) \\ &= \min(v_p(qt) - v_p(rt), v_p(sr) - v_p(rt)) = \min(v_p(qt/rt), v_p(sr/rt)) \\ &= \min(v_p(x), v_p(y)). \end{aligned}$$

□

Definicja 1.1.4. *Dla dowolnej liczby wymiernej $x \neq 0$ określamy jej normę p-adyczną przez wzór $|x|_p = p^{-v_p(x)}$. Dodatkowo $|0|_p = 0$.*

Fakt 1.1.5. *Tak określona norma jest niearchimedesowa.*

Wynika to z dopiero co udowodnionego lematu.

Fakt 1.1.6. *Norma na ciele K jest niearchimedesowa, wtedy i tylko wtedy gdy $|a| \leq 1$ dla wszystkich $a \in \mathbb{Z}$ (po włożeniu w K).*

Dowód. Implikacja w jedną stronę jest oczywista: $\| \pm 1\| = 1$ pociąga $\|n \pm 1\| \leq \max\{\|n\|, 1\}$ i indukcja kończy dowód. Udowodnimy teraz wynikanie w lewo. Ponieważ $\|x+y\| \leq \max\{\|x\|, \|y\|\}$ jest oczywista dla $y = 0$, wystarczy dowieść $\|t + 1\| \leq \max\{\|t\|, 1\}$ $(t \in K)$. Dla $m \in \mathbb{N}$:

$$\begin{aligned} \|z+1\|^m &= \left\| \sum_{j=0}^{m} \binom{m}{j} z^j \right\| \leq \sum_{j=0}^{m} \left\| \binom{m}{j} z^j \right\| \leq \sum_{j=0}^{m} \|z\|^j \\ &\leq (m+1) \max\{1, \|z\|^m\} \end{aligned}$$

Przechodzimy z m do ∞ po spierwiastkowaniu. □

Fakt 1.1.7. *W ciele z niearchimedesową normą „$x, y \in K$, $|x| \neq |y|$" pociąga „$|x + y| = \max(|x|, |y|)$".*

Dowód. $\|x\| > \|y\|$ pociąga $\|x + y\| \leq \|x\| = \max\{\|x\|, \|y\|\}$. Ale $x = x + y - y$, więc $\|x\| \leq \max\{\|x + y\|, \|y\|\}$. Nierówność zachodzi tylko wtedy, gdy $\max\{\|x + y\|, \|y\|\} = \|x + y\|$. To daje $\|x\| \leq \|x + y\|$. □

Fakt 1.1.8. *W niearchimedesowym ciele K każdy punkt kuli (otwartej, domkniętej) jest jej środkiem. Jeśli $r > 0$, to kula jest otwarnięta. Dwie kule (domknięte, otwarte) są rozłączne lub zawarte jedna w drugiej.*

Dowód. Jeśli $b \in B(a, r)$, to $\|b - a\| < r$. Biorąc dowolny x, że $|x - a| < r$, dostajemy $|x - b| < r$ (niearchimedesowo), zatem $B(a, r) \subset B(b, r)$. Podobnie w drugą stronę.

Każda otwarta kula jest otwartym zbiorem. Weźmy x z brzegu $B(a, r)$, do tego $s \leq r$. Wtedy pewien y jest w $B(a, r) \cap B(x, s)$ (przekrój jest niepusty). To oznacza, że $|y - a| < r$ oraz $|y - x| < s \leq r$, więc $|x - s| \leq r$ i $x \in B(a, r)$.

Weźmy nierozłączne $B(a, r)$, $B(b, s)$, że $r \leq s$. Wtedy pewien c leży w obydwu kulach. Ale $B(a, r) = B(c, r)$ zawiera się w $B(c, s) = B(b, s)$. □

1.2 Twierdzenie Ostrowskiego

Definicja 1.2.1. *Dwie normy na ciele są równoważne, jeżeli metryki od nich generują tę samą topologię*

Lemat 1.2.2. *Normy $\|\cdot\|_i$ (dla $i \in \{1,2\}$) na K są równoważne wtedy i tylko wtedy, gdy $\|x\|_1 < 1 \Leftrightarrow \|x\|_2 < 1$ wtedy i tylko wtedy, gdy dla pewnej $\alpha > 0$ i każdego x zachodzi $\|x\|_1 = \|x\|_2^\alpha$.*

Dowód. Pokażemy trzy implikacje.

(1 $\implies$ 2) Równoważne normy zadają te same ciągi zbieżne, $\lim_n x^n = 0$ jest równoważne $\|x\| < 1$.

(2 $\implies$ 3) Wybierzmy $x_0 \in K$ różne od 0, że $|x_0|_1 < 1$. Warunek nr 2 mówi, że $|x_0|_2$ też jest mniejsze od jeden, czyli możemy wybrać $\alpha > 0$ takie, żeby $|x_0|_1 = |x_0|_2^\alpha$.

Wybierzmy jeszcze jeden $x \in K \setminus \{0\}$. Jeśli $|x|_1 = |x_0|_1$, to $|x|_2 = |x_1|_2$ (gdyby tak nie było, to normy ilorazów byłyby zepsute). Podobnie dla $|x|_1 = 1$.

Bez straty ogólności zakładamy, że $1 > |x|_1 \neq |x_0|_1$. Znów istnieje $\beta > 0$, że $|x|_1 = |x|_2^\beta$, ale czy $\alpha = \beta$? Niech n, m będą naturalne. Wtedy $|x|_1^n < |x_0|_1^m \iff |x|_2^n < |x_0|_2^m$. Wzięcie logarytmów daje (po drobnych przekształceniach)

$$\frac{n}{m} < \frac{\log|x_0|_1}{\log|x|_1} \iff \frac{n}{m} < \frac{\log|x_0|_2}{\log|x|_2}.$$

Oznacza to, że ułamki po prawych stronach są równe. Po podłożeniu $|x_0|_1 = |x_0|_2^\alpha$ okaże się, że rzeczywiście $\alpha = \beta$.

(3 $\implies$ 1) $\|x-a\|_1 < r$ wtedy i tylko wtedy, gdy $\|x-a\|_2 < r^{1/\alpha}$. □

Twierdzenie 1.2.3 (Ostrowski, 1916)**.** *Na $\mathbb{Q}$ wartość bezwzględna musi być równoważna z jedną z wartości bezwzględnych $\|\cdot\|_p$, gdzie p jest l. pierwszą lub $p = \infty$ (lub dyskretną).*

Dowód. Niech $|\cdot|$ będzie nietrywialną normą na $\mathbb{Q}$. Pierwszy przypadek: archimedesowa (odpowiada jej $|\cdot|_\infty$). Weźmy więc najmniejsze dodatnie całkowite n_0, że $|n_0| > 1$. Wtedy $|n_0| = n_0^\alpha$ dla pewnej $\alpha > 0$. Wystarczy uzasadnić, dlaczego $|x| = |x|_\infty^\alpha$ dla każdej $x \in \mathbb{Q}$, a właściwie tylko dla $x \in \mathbb{Z}_{>0}$ (bo norma jest multiplikatywna). Dowolną liczbę n można zapisać w systemie o podstawie n_0: $n = a_0 + a_1 n_0 + \cdots + a_k n_0^k$, gdzie $a_k \neq 0$ i $0 \leq a_i \leq n_0 - 1$.

$$|n| = \left|\sum_{i=0}^{k} a_i n_0^i\right| \leq \sum_{i=0}^{k} |a_i|\, n_0^{i\alpha} \leq n_0^{k\alpha} \sum_{i=0}^{k} n_0^{-i\alpha} \leq n_0^{k\alpha} \sum_{i=0}^{\infty} n_0^{-i\alpha} = n_0^{k\alpha} \frac{n_0^\alpha}{n_0^\alpha - 1} = C n_0^{k\alpha}$$

Pokazaliśmy $|n| \leq C n_0^{k\alpha} \leq C n^\alpha$ dla każdego n, a więc w szczególności dla liczb postaci n^N (bowiem C nie zależy od n): $|n| \leq C^{1/n} n^\alpha$. Przejdźmy z N do nieskończoności, dostajemy $C^{1/n} \to 1$ i $|n| \leq n^\alpha$. Teraz trzeba pokazać nierówność w drugą stronę. Skorzystamy jeszcze raz z rozwinięcia. Skoro $n_0^{k+1} > n \geq n_0^k$, to zachodzi

$$n_0^{(k+1)\alpha} = |n_0^{k+1}| = |n + n_0^{k+1} - n| \leq |n| + |n_0^{k+1} - n|,$$

a stąd wnioskujemy, że

$$|n| \geq n_0^{(k+1)\alpha} - |n_0^{k+1} - n| \geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n)^\alpha.$$

Skorzystaliśmy tutaj z nierówności udowodnionej wyżej. Wiemy, że $n \geq n_0^k$, więc prawdą jest, że

$$|n| \geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n_0^k)^\alpha = n_0^{(k+1)\alpha}[1 - (1 - \tfrac{1}{n_0})^\alpha] = C' n_0^{(k+1)\alpha} > C' n^\alpha.$$

Od n nie zależy $C' = 1 - (1 - 1/n_0)^\alpha$, jest dodatnia i przez analogię do poprzedniej sytuacji możemy pokazać $|n| \geq n^\alpha$. Wnioskujemy stąd, że $|n| = n^\alpha$ i $|\cdot|$ jest równoważna ze zwykłą wartością bezwzględną.

Załóżmy, że $|\cdot|$ jest niearchimedesowa. Wtedy $\|n\| \leq 1$ dla całkowitych n. Ponieważ $|\cdot|$ jest nietrywialna, musi istnieć najmniejsza l. całkowita n_0, że $\|n_0\| < 1$. Zacznijmy od tego, że n_0 musi być l. pierwszą: gdyby zachodziło $n_0 = a \cdot b$ dla $1 < a, b < n_0$, to $|a| = |b| = 1$ i $|n_0| < 1$ (z minimalności n_0) prowadziłoby do sprzeczności. Chcemy pokazać, że $|\cdot|$ jest równoważna z normą p-adyczną, gdzie $p := n_0$. W następnym kroku uzasadnimy, że jeżeli $n \in \mathbb{Z}$ nie jest podzielna przez p, to $|n| = 1$. Dzieląc n przez p z resztą dostajemy $n = rp + s$ dla $0 < s < p$. Z minimalności p wynika $|s| = 1$, zaś z $|r| \leq 1$ ($|\cdot|$ jest niearchimedesowa) i $|p| < 1$: $|rp| < 1$. „Wszystkie trójkąty są równoramienne", więc $|n| = 1$. Wystarczy więc tylko zauważyć, że dla $n \in \mathbb{Z}$ zapisanej jako $n = p^v n'$ z $p \nmid n'$ zachodzi $|n| = |p|^v |n'| = |p|^v = c^{-v}$, gdzie $c = |p|^{-1} > 1$, co kończy dowód. □

Fakt 1.2.4 („adelic product"). *Jeżeli $x \in \mathbb{Q}^\times$, to $\prod_{p \leq \infty} |x|_p = 1$.*

1.3 Uzupełnianie

Lemat 1.3.1. *Ciało $\mathbb{Q}$ z nietrywialną normą nie jest zupełne.*

Dowód. Dzięki twierdzeniu Ostrowskiego wystarczy sprawdzić p-adyczne normy. Niech $p \neq 2$ będzie pierwsza, zaś $a \in \mathbb{Z}$ taka, że nie jest kwadratem, nie dzieli się przez p i równanie $x^2 = a$ ma rozwiązanie w $\mathbb{Z}/p\mathbb{Z}$. Konstruujemy ciąg Cauchy'ego bez granicy: x_0 jest dowolnym rozwiązaniem równania, x_n ma być równe x_{n-1} modulo p^n oraz $x_n^2 = a$ (modulo p^{n+1}). Jest Cauchy'ego ($|x_{n+1} - x_n| = |\lambda p^{n+1}| \leq p^{-n+1} \to 0$) i nie ma granicy (kandydatem na nią jest pierwiastek z a, gdyż prosty rachunek pokazuje $|x_n^2 - a| = |\mu p^{n+1}| \leq p^{-n+1} \to 0$). Gdy $p = 2$, to zastępujemy pierwiastek sześciennym. □

Zbiór ciągów Cauchy'ego oznaczmy przez C. Można na nim zadać strukturę pierścienia (przemienego i z jedynką) przez punktowe dodawanie oraz mnożenie. Wprowadzamy ideał N, do którego należą ciągi zbieżne do zera.

Lemat 1.3.2. *Zbiór N jest ideałem maksymalnym C.*

Dowód. Ustalmy ciąg $(x_n) \in C \setminus N$ oraz ideał $I = \langle (x_n), N \rangle$. Od pewnego miejsca x_n nie jest zerem, zatem $y_n = 1/x_n$ od tego miejsca i $y_n = 0$ ma sens. Ciąg y_n jest Cauchy'ego:

$$|y_{n+1} - y_n| = \frac{|x_{n+1} - x_n|}{|x_n x_{n+1}|} \leq \frac{|x_{n+1} - x_n|}{c^2} \to 0.$$

Ale $(1) - (x_n)(y_n) \in N$, to kończy dowód ($I = C$). □

Definicja 1.3.3. *Ciało liczb p-adycznych to $\mathbb{Q}_p := C/N$.*

Lemat 1.3.4. *Ciąg $|x_n|_p$ jest stacjonarny, gdy $(x_n) \in C \setminus N$.*

Dowód. Można znaleźć takie liczby c, N_1, że $n \geq N_1$ pociąga $|x_n| \geq c > 0$. Z drugiej strony istnieje taka N_2, że $n, m \geq N_2$ pociąga $|x_n - x_m| < c$. Połóżmy więc $N = \max\{N_1, N_2\}$. Wtedy $n, m \geq N$ pociąga $|x_n - x_m| < \max\{|x_n|, |x_m|\}$, a to oznacza, że $|x_n| = |x_m|$. □

Dzięki temu następująca definicja nie jest bez sensu:

Definicja 1.3.5. *Gdy $(x_n) \in C$ reprezentuje $\lambda \in \mathbb{Q}_p$, przyjmujemy $|\lambda|_p := \lim_{n \to \infty} |x_n|_p$.*

Lemat 1.3.6. *Obraz $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ po włożeniu jest gęsty.*

Dowód. Chcemy pokazać, że każda otwarta kula wokół $\lambda \in \mathbb{Q}_p$ kroi się z obrazem $\mathbb{Q}$, czyli zawiera „stały ciąg". Ustalmy kulę $B(\lambda, \varepsilon)$, ciąg Cauchy'ego (x_n) dla λ i $\varepsilon' < \varepsilon$. Dzięki temu, że ciąg jest Cauchy'ego, możemy znaleźć dla niego indeks N, że $n, m \geq N$ pociąga $|x_n - x_m| < \varepsilon'$. Rozpatrzmy stały ciąg (y) dla $y = x_N$. Wtedy $|\lambda - (y)| < \varepsilon$, gdyż $\lambda - (y)$ odpowiada ciąg $(x_n - y)$. Ale $|x_n - x_N| < \varepsilon'$ i w granicy

$$\lim_{n\to\infty} |x_n - y| \leq \varepsilon' < \varepsilon. \qquad \square$$

Fakt 1.3.7. *Ciało $\mathbb{Q}_p$ jest zupełne.*

Dowód. Dowód w czterech krokach:

1. Niech λ_k będzie ciągiem Cauchy'ego elementów $\mathbb{Q}_p$.
2. Skoro obraz $\mathbb{Q}$ w $\mathbb{Q}_p$ jest gęsty, to można znaleźć liczby wymierne l_k, że $\lim_{n\to\infty} |\lambda_n - (l_n)| = 0$: granica w $\mathbb{Q}_p$!
3. Wybrane wcześniej liczby wymierne l_n same tworzą ciąg Cauchy'ego w $\mathbb{Q}$; dążą do λ w $\mathbb{Q}_p$.
4. Zachodzi $\lim_{n\to\infty} \lambda_n = \lambda$. $\square$

1.4 Lemat Hensela

Twierdzenie 1.4.1 (lemat Hensela)**.** *Niech $\mathfrak{K}$ będzie ciałem zupełnym względem wartości bezwzględnej $|\cdot|$ i niech $f(X) \in \mathfrak{O}[X]$. Załóżmy, że $a_0 \in \mathfrak{O}$ spełnia nierówność $|f(a_0)| < |f'(a_0)|^2$, gdzie $f'(X)$ jest (formalną) pochodną. Wtedy istnieje $a \in \mathfrak{O}$, taki że $f(a) = 0$.*

Dowód. Niech wielomiany $f_j(X)$ (dla $j = 1, 2, \ldots$) będą zdefiniowane przez tożsamość

$$f(X + Y) = f(X) + \sum_{j\geq 1} f_j(X) Y^j$$

dla niezależnych niewiadomych X, Y. Wtedy $f_1(X) = f'(X)$. Ponieważ $|f(a_0)| < |f'(a_0)|^2$, istnieje $b_0 \in \mathfrak{O}$, takie że $f(a_0) + b_0 f_1(a_0) = 0$. Istotnie,

$$|b_0| = \left|\frac{-f(a_0)}{f_1(a_0)}\right| = \frac{|f(a_0)|}{|f_1(a_0)|} < \frac{|f'(a_0)|^2}{|f'(a_0)|} = |f'(a_0)| \leq 1.$$

Zgodnie z definicją wielomianów f_j zachodzi relacja

$$|f(a_0 + b_0)| \leq \max_{j\geq 2} |f_j(a_0) b_0^j|.$$

Jako że $f_j(X) \in \mathfrak{O}[X]$ i $a_0 \in \mathfrak{O}$, mamy $|f_j(a_0)| \leq 1$. Oznacza to, że

$$|f(a_0 + b_0)| \leq |b_0^2| = \frac{|f(a_0)|^2}{|f'(a_0)|^2} < |f(a_0)|,$$

skorzystaliśmy tu ponownie z nierówności $|f(a_0)| < |f'(a_0)|^2$.

Podobnie pokazuje się, że

$$|f_1(a_0 + b_0) - f_1(a_0)| \leq |b_0| < |f_1(a_0)|,$$

a przez to

$$|f_1(a_0 + b_0)| = |f_1(a_0)|.$$

Kładziemy teraz $a_1 = a_0 + b_0$ i powtarzamy proces. Otrzymujemy w ten sposób ciąg $a_n = a_{n-1} + b_{n-1}$. Dla każdego n prawdziwa jest równość $|f_1(a_n)| = |f_1(a_0)|$, jednocześnie

$$|f(a_{n+1})| \leq \frac{|f(a_n)|^2}{|f_1(a_n)|^2} = \frac{|f(a_n)|^2}{|f_1(a_0)|^2}$$

To uzasadnia zbieżność $f(a_n)$ do zera. Co więcej,

$$|a_{n+1} - a_n| = |b_n| = \frac{|f(a_n)|}{|f_1(a_n)|} = \frac{|f(a_n)|}{|f_1(a_0)|} \to 0.$$

Ciąg $\{a_n\}$ jest fundamentalny, z zupełności ciała $\mathfrak{K}$ wynika istnienie jego granicy oraz $f(a) = 0$. □

1.5 Analiza

Fakt 1.5.1. *Ciąg (x_n) o wyrazach w $\mathbb{Q}_p$ jest Cauchy'ego, wtedy i tylko wtedy gdy zachodzi* $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$.

Dowód. Jeśli $m = n + r > n$, to $|x_m - x_n|$ można oszacować z góry, $|\sum_{k=1}^{r} x_{n+k} - x_{n+k-1}| \leq \max_{1\leq k\leq r} |x_{n+k} - x_{n+k-1}|$, bo wartość bezwzględna jest niearchimedesowa. □

Fakt 1.5.2. *Dla $a_n \in \mathbb{Q}_p$, szereg $\sum_{n\geq 0} a_n$ jest zbieżny wtedy i tylko wtedy, gdy zachodzi* $\lim_{n\to\infty} a_n = 0$. *Pociąga to prawdziwość oszacowania* $|\sum_{n\geq 0} a_n| \leq \max_n |a_n|$.

Dowód. Jedna implikacja jest oczywista. Szereg zbiega, gdy ciąg sum częściowych zbiega. Ale wyraz a_n to różnica między n-tą i $(n-1)$-szą sumą częściową – jeśli zbiega do zera, to z faktu wyżej wynika, że ciąg sum częściowych jest Cauchy'ego, zatem zbieżny. Nierówność rozszerza niearchimedesowskość. □

Aby zająć się podwójnymi sumami, potrzebujemy czegoś więcej niż tylko zbieżność do zera.

Definicja 1.5.3. *Jeśli dla każdej dodatniej liczby ε istnieje całkowita N niezależna od j, że $i \geq N$ pociąga $|b_{ij}| < \varepsilon$, to* $\lim_{i\to\infty} b_{ij} = 0$ *jednostajnie względem j.*

Lemat 1.5.4. *Załóżmy, że $b_{ij} \in \mathbb{Q}_p$, zaś dla każdego i zachodzi* $\lim_{j\to\infty} b_{ij} = 0$ *i (jednostajnie względem j)* $\lim_{i\to\infty} b_{ij} = 0$. *Dla każdego ε istnieje N_ε (zależna tylko od ε), że* $\max\{i, j\} \geq N$ *pociąga $|b_{ij}| < \varepsilon$.*

Dowód. Ustalmy ε. Warunek I mówi, że dla każdego i istnieje $N_1(i)$, dla którego $j \geq N_1(i)$ pociąga $|b_{ij}| < \varepsilon$. Warunek II zapewnia istnienie takiego N_0, że $|b_{ij}| < \varepsilon$, o ile $i \geq N_0$. Teraz określmy $N_\varepsilon = \max(N_0, N_1(0), N_1(1), \ldots, N_1(N_0 - 1))$.

Takie N jest dobrym wyborem: gdy $\max\{i, j\} \geq N$, to albo $i \geq N_0$ i wiemy, że $|b_{ij}| < \varepsilon$ niezależnie od i; albo $i < N_0$, zaś $j \geq N$. Wtedy $0 \leq i \leq N_0 - 1$ i j musi być większe od stosownego N_1, co znowu daje żądaną nierówność. □

Fakt 1.5.5. *Przy założeniach z lematu 1.5.4 poniższe szeregi zbiegają, i to do tej samej liczby:* $\sum_{i\geq 0} \sum_{j\geq 0} b_{ij}$, $\sum_{j\geq 0} \sum_{i\geq 0} b_{ij}$.

Dowód. Lemat mówi, że każdemu $\varepsilon > 0$ odpowiada liczba N, dla której „$\max\{i,j\} \geq N$ pociąga $|b_{ij}| < \varepsilon$". Skoro ciąg b_{ij} zbiega do zera po ustaleniu jednego z indeksów, to oba szeregi: $\sum_{j\geq 0} b_{ij}$ i $\sum_{i\geq 0} b_{ij}$ są zbieżne.

Dla $i \geq N$ zachodzi $|\sum_{j\geq 0} b_{ij}| \leq \max_j |b_{ij}| < \varepsilon$ na mocy faktu 1.5.2, podobna nierówność prawdziwa jest dla $j \geq N$. Wnioskujemy stąd, że podwójne szeregi zbiegają, gdyż

$$\lim_{i\to\infty} \sum_{j\geq 0} b_{ij} = \lim_{j\to\infty} \sum_{i\geq 0} b_{ij} = 0.$$

Pozostało nam uzasadnić, że sumy są sobie równe.

Pozostańmy przy N, ε wybranych wcześniej. Oznacza to, że $|b_{ij}| < \varepsilon$, gdy $i \geq N$ lub $j \geq N$. Zauważmy, że

$$\Big|\sum_{i,j\geq 0} b_{ij} - \sum_{i,j\leq N} b_{ij}\Big| = \Big|\sum_{i\leq N}\sum_{j>N} b_{ij} + \sum_{i>N}\sum_{j\geq 0} b_{ij}\Big|.$$

Jeśli więc $j \geq N+1$, to $|b_{ij}| < \varepsilon$ dla każdego i, zatem pierwszy składnik pod wartością bezwzględną można (ultrametrycznie) oszacować z góry przez ε; podobnie szacuje się drugi składnik. Oczywiście zamiana i, j miejscami nic nie psuje, więc możemy je przestawić i wywnioskować stąd równość sum. □

Fakt 1.5.6. *Jeśli $g(x)$ zbiega, $f(g(x))$ zbiega i dla każdego n jest $|b_n x^n| \leq |g(x)|$, to $h(x)$ też zbiega, do $f(g(x))$.*

$$f(X) = \sum_{n\geq 0} a_n X^n \bullet g(X) = \sum_{n\geq 0} b_n X^n$$

Dowód. Podamy dowód za książką Hassego. Niech

$$g(X)^m = \sum_{n\geq m} d_{m,n} X^n,$$

przy czym $d_{m,n} = \sum_* \prod_{k=1}^m b_{i_k}$, zaś suma $i_1 + \ldots + i_m$ to n (o ile $n \geq m$) i $d_{m,n} = 0$ (w przeciwnym przypadku). Pozwala to na napisanie $h(X) = f(g(X))$ jawnie:

$$h(X) = a_0 + \sum_{n\geq 1}\sum_{m\leq n} a_m d_{m,n} X^n.$$

Skoro $g(x)$ jest zbieżny, z faktu **??** wnioskujemy, że formalny szereg $g(X)^m$ zbiega dla $X = x$ do $g(x)^m$. Dla każdego n mamy $|d_{m,n}x^n| \leq |g(x)^m|$. Jest to oczywiste dla $n < m$. Jeżeli $n \geq m$, to nierówność ultrametryczna daje dla $i_1 + \ldots + i_m = n$ (dzięki $|b_{ij}x^{ij}| \leq |g(x)^m|$):

$$|d_{m,n}x^n| \leq \max_{„i"} \prod_{k\leq m} |b_{i_k} x^{i_k}| \leq \prod_{k\leq m} |g(x)| = |g(x)^m|.$$

Wiemy już, że $g(x)$, $g(x)^m$ oraz $f(g(x))$ zbiegają. Zapiszmy w takim razie

$$\begin{aligned} f(g(x)) &= a_0 + \sum_{m\geq 1} a_m g(x)^m \\ &= a_0 + \sum_{m\geq 1}\sum_{n\geq m} a_m d_{m,n} x^n, \end{aligned}$$

a z drugiej strony

$$h(x) = a_0 + \sum_{n\geq 1}\sum_{m\geq 1} a_m d_{m,n} x^n.$$

Aby uzasadnić poprawność zamiany kolejności sumowania powołamy się na fakt 1.5.5 i oszacujemy $a_m d_{m,n} x^n$.

Wiemy przede wszystkim, że $|a_m d_{m,n} x^n| \leq |a_m g(x)^m|$: prawa strona nie zależy od n. Ustalmy $\varepsilon > 0$. Możemy wybrać indeks N, taki że $m \geq N$ pociąga $|a_m g(x)^m| < \varepsilon$. To pokazuje, że $a_m d_{m,n} x^n \to_m 0$ jednostajnie względem n.

Z drugiej strony, dla każdego m szereg $g(x)^m$ jest zbieżny, zatem jego wyraz ogólny zbiega do zera: $a_m d_{m,n} x^n \to 0$. □

Przykład 1.5.7. *Niech $g(X) = 2X^2 - 2X$ i $h(X) = f(g(X))$, gdzie $f(X) = \sum_{k\geq 0} \frac{1}{k!} X^k$. Można pokazać, że f zbiega dokładnie na $4\mathbb{Z}_2$, zaś g wszędzie (gdyż jest wielomianem). Mamy oczywiście $f(g(1)) = 1$. Niech $h(X) = \sum_n a_n X^n$. Jeżeli $n \geq 2$, to $v_2(a_n)$ wynosi co najmniej $1 + n/4$, czyli h zbiega na $\mathbb{Z}_2$. Niestety, $h(1) \equiv 3 \pmod 4$ i $h(1) \neq f(g(1))$.*

Twierdzenie 1.5.8 (Strassman, 1928)**.** *Niech ciąg $a_n \in \mathbb{Q}_p$ dąży do zera i nie będzie stale równy zero. Wtedy $f(X) = \sum_{n\geq 0} a_n X^n$ zbiega w $\mathbb{Z}_p$. Określmy liczbę N warunkami $|a_N| = \max_n |a_n|$ i $|a_n| < |a_N|$ dla $n > N$. Funkcja $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$, $x \mapsto f(x)$, ma co najwyżej N zer.*

Dowód. Indukcja względem N. Jeżeli $N = 0$, to $|a_0| > |a_n|$ dla $n \geq 1$, z tego chcemy wywnioskować, że nie ma zer w $\mathbb{Z}_p$ Rzeczywiście, gdyby $f(x) = 0$, to

$$|a_0| = |f(x) - a_0| \leq \max_{n\geq 1} |a_n x^n| \leq \max_{n\geq 1} |a_n| < |a_0|$$

prowadzi do sprzeczności. Krok indukcyjny. Jeżeli znaleźliśmy już N i $f(\alpha) = 0$ dla $\alpha \in \mathbb{Z}_p$, możemy wybrać dowolne $x \in \mathbb{Z}_p$. Wtedy

$$f(x) = f(x) - f(\alpha) = (x - \alpha) \sum_{n\geq 1}\sum_{j<n} a_n x^j \alpha^{n-1-j}$$

Lemat 1.5.5 pozwala na przegrupowanie:

$$f(x) = (x - \alpha) \sum_{j\geq 0} b_j x^j \bullet b_j = \sum_{k\geq 0} a_{j+1+k} \alpha^k$$

Widać, że $b_j \to 0$, nawet $|b_j| \leq \max_{k\geq 0} |a_{j+k+1}| \leq |a_N|$ dla każdego j, zatem $|b_{N-1}| = |a_N + a_{N+1}\alpha + \ldots| = |a_N|$ i wreszcie dla $j \geq N$ zachodzi

$$|b_j| \leq \max_{k\geq 0} |a_{j+k+1}| \leq \max_{j\geq N+1} |a_j| < |a_N|.$$

Liczba z twierdzenia dla $f(X)/(X - \alpha)$ to $N - 1$, koniec. □

Definicja 1.5.9. *Logarytm:* $\log_p(1 + x) = \sum_{n\geq 1} (-1)^{n+1} \frac{x^n}{n}$.

Logarytm zbiega „gorzej" niż $\log\colon \mathbb{R}_+ \to \mathbb{R}$. Policzymy jego promień zbieżności. Zauważmy, że $|1/n| = p^{v_p(n)}$, więc $\rho = 1$. Ale $|1/n|$ nie dąży do zera, więc zbieżność jest dla $|x| < 1$.

Lemat 1.5.10. *Mamy $\lim_{n\to\infty} p^{v_p(n)/n} = 1$, więc $\rho = 1$.*

Dowód. Jest jasne, że $\frac{1}{n} v_p(n) \leq \frac{1}{n} \log_p n \to 0$. □

To wystarcza do zdefiniowania p-adycznego logarytmu. Niechże $\mathcal{B} = \mathcal{B}(1,1) = 1 + p\mathbb{Z}_p$ $(= \{x \in \mathbb{Z}_p : |x-1| < 1\})$. By funkcja $\log_p \colon \mathcal{B} \to \mathbb{Q}_p$ zasługiwała na bycie logarytmem, musi mieć jego własności. Tak rzeczywiście jest.

$$\log_p(x) = f(x-1) = \sum_{n\geq 1} (-1)^{n+1} \frac{(x-1)^n}{n}$$

Fakt 1.5.11. *Dla $a, b \in 1 + p\mathbb{Z}_p$ jest $\log_p(ab) = \log_p(a) + \log_p(b)$.*

Dowód. Przyjmijmy $f(x) = \log_p(1+x)$ dla $x \in \mathbb{Z}_p$. Z naszą wiedzą o pochodnych szeregów potęgowych piszemy

$$f'(x) = \sum_{n\geq 0} (-1)^n x^n = \frac{1}{1+x}.$$

Ustalmy $y \in p\mathbb{Z}_p$ i określmy $g(x) = f(y + (1+y)x)$. Jest to szereg potęgowy zbieżny dla $|x| < 1$. Reguła łańcucha pozwala policzyć pochodną:

$$\begin{aligned} g'(x) &= (1+y) f'(y + (1+y)x) = \frac{(1+y)}{1+y+(1+y)x} \\ &= \frac{1}{1+x} = f'(x) \Rightarrow g(x) = f(x) + C. \end{aligned}$$

Widać, że $g(0) = f(y)$, zatem $g(x) = f(x) + f(y)$, wystarczy przetłumaczyć to na język logarytmów. □

Fakt 1.5.12. *Jeżeli $p > 2$, to $\log_p$ ma dokładnie jedno miejsce zerowe, $x = 1$. Jeżeli $p = 2$, to $x = \pm 1$.*

Dowód. Twierdzenie Strassmana dla $\log(1 + pX)$. □

W $\mathbb{R}$ szereg $\exp(X) = \sum_{n=0}^{\infty} X^n/n!$ zbiega wszędzie, bo $1/n!$ bardzo szybko maleje: ale nie w $\mathbb{Q}_p$. Trzeba więc określić tempo wzrostu tych współczynników.

Lemat 1.5.13. *Jeśli p jest pierwsza, to $v_p(n!) < n : (p-1)$, więc $|n!|_p > p^{-n:(p-1)}$.*

Dowód. Nierówność jest prawdziwa, bo $\lfloor x \rfloor \leq x$, czyli:

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor \leq \sum_{i=1}^{\infty} \frac{n}{p^i} = \frac{n}{p-1}.$$ □

Lemat 1.5.14. *Szereg $\sum_{n=0}^{\infty} \frac{X^n}{n!}$, eksponensa, zbiega wtedy i tylko wtedy gdy $|x| < p^{-1/(p-1)}$.*

Dowód. Zachodzi $|a_n| = |1/n!| = p^{v_p(n!)} < p^{n/(p-1)}$ dzięki wcześniejszemu oszacowaniu, a zatem $\rho \geq p^{-1/(p-1)}$. Szereg z pewnością jest zbieżny dla $|x| < p^{-1/(p-1)}$. Z drugiej stony, gdy $|x| = p^{-1/(p-1)}$, zaś $n = p^m$, to $v_p(n!) = (n-1)/(p-1)$. Skoro $v_p(x) = 1/(p-1)$, to poniższe wyrażenie nie zależy od m, czyli $x^n/n!$ nie dąży do zera (a sam szereg nie jest zbieżny). Znajomość obszaru zbieżności kończy dowód lematu.

$$v_p\left(\frac{x^n}{n!}\right) = \frac{p^m}{p-1} - \frac{p^m - 1}{p-1} = \frac{1}{p-1}.$$ □

Definicja 1.5.15. *Eksponensa $\exp_p \colon \mathcal{B} \to \mathbb{Q}_p$ jest określona na $p\mathbb{Z}_p$ (dla $p \neq 2$) lub $4\mathbb{Z}_2$ przez podany wcześniej szereg.*

Fakt 1.5.16. *Jeżeli* $x, y, x+y \in \mathcal{B}(0, p^{-1/(p+1)})$*, to* $\exp(x+y)$ *jest równe* $\exp x \exp y$*.*

Dowód. Dowód to po prostu formalna manipulacja szeregów.

$$\begin{aligned} L = \exp_p(x+y) &= \sum_{n\geq 0} \frac{(x+y)^n}{n!} = \\ &= \sum_{n\geq 0} \sum_{k\leq n} \frac{1}{n!} \frac{n!}{k!(n-k)!} x^{n-k} y^k \\ &= \sum_{n\geq 0} \sum_{k\leq n} \frac{x^{n-k}}{(n-k)!} \frac{y^k}{k!} = \sum_{m\geq 0} \frac{x^m}{m!} \cdot \sum_{k\geq 0} \frac{y^k}{k!} \\ &= \exp_p(x) \exp_p(y) = R \end{aligned}$$

□

Fakt 1.5.17. *Załóżmy, że jest* $|x| < p^{-1/(p-1)}$ *(*$x \in \mathbb{Z}_p$*). Zachodzi wtedy* $\log_p(\exp_p x) = x$ *oraz* $\exp_p(\log_p(1+x)) = 1+x$*.*

Dowód. Bez straty ogólności $x \neq 0$. Wstawiamy $\exp_p(x) - 1$ do $\log(1+X)$. Wiemy od początku, że $|x^n/n!| < |x|^n p^{n/(p-1)}$. Skoro $|x| < p^{-1/(p-1)}$, to $|\exp_p(x) - 1| < 1$. Można lepiej: dla $n \geq 2$ $[v_p(x) > 1/(p-1)]$ jest $v_p(x^{n-1}/n!)$ równe:

$$(n-1)v_p(x) - v_p(n!) > \frac{n-1}{p-1} - \frac{n-s}{p-1} > 0,$$

gdzie s to suma cyfr n w rozwinięciu p-adycznym. Wynika stąd, że $|x^{n-1}/n!| < 1$ i $|x^n/n!| < |x|$; dla $n \geq 2$:

$$p^{-1/(p-1)} > |\exp_p(x) - 1| = |x| > |x^n/n!|.$$

Korzystamy z lematu 1.5.6 dla $\log_p \circ \exp_p$. Teraz złożenie w drugą stronę: $\log_p(1+x)$ podstawiamy do $\exp(X)$. Załóżmy więc, że $v_p(x) > 1/(p-1)$. Jeśli $n > 1$, to

$$\begin{aligned} L &= v_p\left(\frac{(-x)^n}{-n}\right) - v_p(x) = (n-1)v_p(x) - v_p(n) \\ &> \frac{n-1}{p-1} - v_p(n) = (n-1)\left[\frac{1}{p-1} - \frac{v_p(n)}{n-1}\right] \end{aligned}$$

Chcemy, by ostatni nawias był nieujemny. Niech $n = p^v n'$ z $n' \nmid p$. Wtedy

$$\begin{aligned} \frac{v_p(n)}{n-1} &= \frac{v}{p^v n' - 1} \leq \frac{v}{p^v - 1} \\ &= \frac{1}{p-1} \cdot \frac{v}{p^{v-1} + \ldots + p + 1} \leq \frac{1}{p-1}. \end{aligned}$$

A zatem $|(-1)^{n+1}x^n/n| < |x|$ i używamy faktu 1.5.2: $|\log_p(x)| = |x| < p^{-1/(p-1)}$ daje żądaną równość. □

Ostrożność była potrzebna: dla $p = 2$, $x = -2$ „wszystko" zbiega, ale $\exp(\log_p(1+x)) = \exp(0) = 1 \neq -1$.

Zajmiemy się szeregami dwumianowymi. W $\mathbb{R}$ funkcję $(1+X)^\alpha$ można rozwinąć w szereg potęgowy zbieżny dla $|x| < 1$:

$$(1+X)^\alpha = \mathfrak{B}(\alpha, X) = \sum_{n=0}^{\infty} \binom{\alpha}{n} X^n.$$

Szereg ten jest kandydatem na p-adyczny wariant funkcji potęgowej, ciekawszy dla $\alpha \in \mathbb{Z}_p$ niż dla $\alpha \in \mathbb{Q}_p$. Ustalmy α. Co możemy powiedzieć o współczynnikach szeregu $\mathfrak{B}$?

Fakt 1.5.18. *Jeśli $\alpha \in \mathbb{Z}_p$ i $n \geq 0$, to (α nad n) $\in \mathbb{Z}_p$. Jeżeli do tego $|x| < 1$, to szereg $\mathfrak{B}(\alpha, x)$ jest zbieżny.*

Dowód. Dla każdego n rozpatrzmy wielomian

$$P_n(X) = \frac{X(X-1)\cdot \ldots \cdot (X-n+1)}{n!} \in \mathbb{Q}[X].$$

Wielomiany określają ciągłe funkcje $\mathbb{Q}_p \to \mathbb{Q}_p$. Wiemy, że dla $\alpha \in \mathbb{Z}_+$ mamy $P_n(\alpha) \in \mathbb{Z}$. Obraz $\mathbb{Z}_+$ przez P_n zawiera się w $\mathbb{Z}$, zaś wzięcie domknięć zachowa zawieranie.

Innymi słowy, ciągła P_n przerzuca $\mathbb{Z}_+$ w $\mathbb{Z}$. Oznacza to, że domknięcie $(\mathbb{Z}_p)$ przechodzi na domknięcie $(\mathbb{Z}_p)$, co było do pokazania. Druga część jest oczywista. □

Z równości formalnych szeregów potęgowych wynika, że dla $\alpha = a/b \in \mathbb{Z}_{(p)}$ i $|x| < 1$ prawdziwa jest poniższa równość:

$$\left(\mathfrak{B}\left(\frac{a}{b}, x\right)\right)^b = (1+x)^a.$$

Zatem definicja $(1+x)^{a/b} := \mathfrak{B}(a/b, x)$ ma sens.

Chciałoby się przyjąć dla dowolnej $\alpha \in \mathbb{Z}_p$ oraz $x \in p\mathbb{Z}_p$, że $(1+x)^\alpha = \mathfrak{B}(\alpha, x)$. Problem w tym, że p-adyczna funkcja $\mathfrak{B}(a/b, x)$ nie zachowuje się jak jej rzeczywisty odpowiednik, nawet gdy x jest wymierny i $1+x$ jest b-tą potęgą w $\mathbb{Q}$.

Przykład 1.5.19 (Koblitz)**.** *Jeśli $p = 7$, $\alpha = 1/2$, $x = 7/9$, to w $\mathbb{R}$ pierwiastek z $1+x$ jest równy $4/3$, ale w $\mathbb{Q}_7$ nie: $|x| = 1/7$, więc dla $n \geq 1$ jest*

$$\left|\binom{1/2}{n} x^n\right| \leq |x|^n = 7^{-n} < 1.$$

To pociąga $(1+x)^{1/2} = 1 + \sum_{n=1}^{\infty}(1/2 \text{ nad } n)x^n \in 1 + 7\mathbb{Z}_7$ oraz $|(1+x)^{1/2} - 1| < 1$. Ale $|4/3 - 1| = 1$, więc pierwiastkiem jest $-4/3$.

Ten sam szereg o wymiernych wyrazach może zbiegać w $\mathbb{R}$ i $\mathbb{Q}_p$, ale mieć różne granice (nawet, jeśli obie są wymierne), ponieważ topologie są znacząco różne. Wartość $\mathfrak{B}(\alpha, x)$ nie zależy od wyboru ciała, gdy $x \in \mathbb{Q}$ oraz $\alpha \in \mathbb{Z}$.

Fakt 1.5.20. *Niech $1+x$ będzie kwadratem $\frac{a}{b}$, gdzie $a, b > 0$ są względnie pierwsze, zaś S to zbiór tych pierwszych liczb, dla których szereg $\mathfrak{B}(1/2, x)$ zbiega w $\mathbb{Q}_p$.*

1. *Jeśli p jest nieparzystą pierwszą, to $p \in S$, wtedy i tylko wtedy gdy p dzieli $a+b$ (wtedy $\mathfrak{B}(1/2, x) = -a/b$) lub $a-b$ (wtedy a/b).*
2. *Dalej, $2 \in S$, wtedy i tylko wtedy gdy $2 \nmid ab$; granicą w $\mathbb{Q}_2$ jest a/b (gdy $4 \mid a-b$) lub $-a/b$ (jeśli $4 \mid a+b$).*
3. *Wreszcie $\infty \in S$ wtedy i tylko wtedy, gdy $0 < a/b < \sqrt{2}$, suma w $\mathbb{R}$ będzie zawsze równa a/b.*
4. *Zbiór S jest zawsze niepusty. Dla $x \in \{8, 16/9, 3, 5/4\}$ ma dokładnie jeden element.*
5. *Dla innych x zawsze znajdą się dwie $p, q \in S$, że suma w $\mathbb{Q}_p$ jest różna od tej w $\mathbb{Q}_p$.*

Dowód. Szczególny przypadek twierdzenia Bombieriego. □