Liczby $\mathfrak{p}$-adyczne

R. S.

28 marca 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* $\nu_p\colon \mathbb{Z} \setminus \{0\} \to \mathbb{R}$ *określona w następujący sposób:* $\nu_p(n)$ *to jedyna dodatnia liczba całkowita, dla której zachodzi równość* $n = p^{\nu_p(n)} n'$*, przy czym* p *nie dzieli* n'*. Przedłuża się ją do całego ciała* $\mathbb{Q}$ *wzorem*

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

z umową, że $\nu_p(0) = +\infty$*.*

Tak określona funkcja jest dobrze określona (udowodnić).

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

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

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

Fakt 1.1.5. *Tak określona norma jest niearchimedesowa.*

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*).*

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.

1. 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.

2. 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 $x \in B(a, r)$.

3. 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

Lemat 1.2.1. *Wartości bezwzględne $\|\cdot\|_i$ na K są równoważne wtedy i tylko wtedy, gdy $\|x\|_1 < 1 \Leftrightarrow \|x\|_2 < 1$ (inaczej: dla pewnej $\alpha > 0$ i każdego x zachodzi $\|x\|_1 = \|x\|_2^\alpha$). Tutaj $i = 1, 2$.*

Dowód. Dowód polegał będzie na pokazaniu ciągu implikacji.

$3 \Rightarrow 1$ $\|x-a\|_1 < r$ wtedy i tylko wtedy, gdy $\|x-a\|_2 < r^{1/\alpha}$; „otwarte kule są nadal otwarte".

$1 \Rightarrow 2$ Dla równoważnych wartości bezwzględnych mamy jedną zbieżność; $\lim_n x^n = 0$ jest równoważne $\|x\| < 1$.

$2 \Rightarrow 3$ 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 $\alpha = \beta$. □

Twierdzenie 1.2.2 (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 $0 \leq a_i \leq n_0 - 1$.

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

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

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

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 $n = p^\nu n'$ z $p \nmid n'$ zachodzi $|n| = |p|^\nu |n'| = |p|^\nu = c^{-\nu}$, gdzie $c = |p|^{-1} > 1$, co kończy dowód. □

Fakt 1.2.3 („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

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

□

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 $\lim_{n\to\infty} \lambda_n = \lambda$. □

Rozdział 2

Lemat Hensela

Twierdzenie 2.0.1 (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 $f(a) = 0$. $\square$