Almanach p-adyczny

Leon Aragones

18 sierpnia 2016

Spis treści

Przedmowa

Chociaż Kurt Hensel odkrył liczby p-adyczne ponad sto lat temu, do dzisiaj wydają się one nieco tajemnicze i niezrozumiane. Podczas sporządzania notatek im poświęconych nawet nie starałem się o formalny wydźwięk, żywię przy tym nadzieję, iż okażą się one użyteczne dla przynajmniej jednej osoby.

Dokument oparty jest na kilku książkach, jakie zdążyły się ukazać, przed zabraniem się za lekturę nie trzeba jednak znać zbyt dużo matematyki.

Najważniejsze pozycje umieszczone są w bibliografii na końcu, mniej ważne odniesienia do istniejącej literatury można znaleźć w uwagach historycznych zamykających poszczególne rozdziały.

Liczby p-adyczne do matematyki wprowadził Kurt Hensel. Oto, co chyba mogło być jego główną motywacją: pary $\mathbb{Z}$, $\mathbb{Q}$ i $\mathbb{C}[X]$, $\mathbb{C}(x)$ (pierścień – ciało ułamków) są do siebie podobne. Zarówno $\mathbb{Z}$ jak i $\mathbb{C}[X]$ są pierścieniami z jednoznacznością rozkładu: liczby pierwsze $p \in \mathbb{Z}$ odpowiadają wielomianom $X - \alpha \in \mathbb{C}[X]$. Każdemu wielomianowi $P(X) \in \mathbb{C}[X]$ można przypisać jego rozwinięcie Taylora wokół α: $P(X) = \sum_{0 \leq i \leq n} a_i (X - \alpha)^k$.

Elementy $\mathbb{N}$ również mają tę własność: jeżeli p jest l. pierwszą, to $m = a_0 + \ldots + a_n p^n$, przy czym $a_i \in \mathbb{Z} \cap [0, p-1]$ jest dobrze znanym rozwinięciem w systemie o podstawie p. Kodujemy tak lokalne informacje (rząd α jako pierwiastka P, stopień podzielności m przez p). Analogia nie umiera tak łatwo. W $\mathbb{C}(x)$ istnieją szeregi Laurenta, zazwyczaj zawierające nieskończenie wiele wyrazów.

Spróbujemy stworzyć coś na ich kształt w $\mathbb{Q}$. Oto przykład, który wyraża więcej niż tysiąc słów. Gdy $p = 3$, to $24 : 17 = (2p + 2p^2) : (2 + 2p + p^2) = p + p^3 + 2p^5 + p^7(\ldots)$. Wszystkie szeregi Laurenta w potęgach p o skończonym ogonie tworzą ciało ($\mathbb{Q}_p$). Taka definicja jest jednak do niczego. Później rozwiniemy tę analogię i uwypuklimy kilka różnic.

Oto tematyka kolejnych rozdziałów. Zaczynamy od analizy rzeczywistej i kombinatoryki, by przejść potem do topologii i algebry. Z pomocą teorii Galois algebry liniowej budujemy niearchimedesowe ciało liczb zespolonych ($\mathbb{C}_p$) oraz jego sferyczne uzupełnienie (Ω_p). W połowie kończymy zwiedzanie i wyruszamy w naukową ekspedycję, chociaż to chyba wciąż za mało, by poprowadzić poważne badania. Mam nadzieję, że Czytelnik znajdzie po lekturze tego skryptu ulubioną gałąź matematyki w p-adycznej odmianie. Oby się tylko na niej nie powiesił.

Leon Aragonés
Wrocław, Polandia
18 sierpnia 2016

Rozdział 1

Preludium (arytmetyka)

1.1 Wartości bezwzględne na ciele

Tu $\mathbb{R}_+ = \{x \in \mathbb{R} : x \geq 0\}$, zaś $\mathcal{K}$ jest ciałem.

Definicja 1.1.1. *Wartość bezwzględna to funkcja $\|\cdot\| \colon \mathcal{K} \to \mathbb{R}_+$, że $\|x\| = 0$ tylko dla $x = 0$, dla wszystkich $x, y \in \mathcal{K}$ zachodzi $\|xy\| = \|x\| \cdot \|y\|$ oraz $\|x + y\| \leq \|x\| + \|y\|$. Jeśli jest jeszcze $\|x + y\| \leq \max\{\|x\|, \|y\|\}$, to jest niearchimedesowa.*

Fakt 1.1.2. *Na skończonym ciele istnieje tylko trywialna norma.*

Dowód. Wynika to z twierdzenia Lagrange'a dla $\mathcal{K}^\times$. □

Definicja 1.1.3. *Funkcja $v_p \colon \mathbb{Z} \setminus \{0\} \to \mathbb{R}$, „największy wykładnik v, że p^v dzieli argument", to waluacja p-adyczna.*

Przedłuża się do ciała $\mathbb{Q}$: $v_p(x/y) = v_p(x) - v_p(y)$, $v_p(0)$ to „∞". Jest dobrze określona. Ogólniej przez waluację rozumie się każdą funkcję, dla której prawdziwy jest poniższy lemat.

Lemat 1.1.4. *Niech $x, y \in \mathbb{Q}$. Wtedy $v_p(xy) = v_p(x)+v_p(y)$ i $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$ z umową dla $v_p(0)$.*

Waluacja i wartość bezwzględna mają podobne własności: produkt zamienił się w sumę (logarytm), sama zaś nierówność odwróciła się. Potęgowanie i ponowne odwrócenie dowodzą:

Fakt 1.1.5. *Funkcja $|x|_p = p^{-v_p(x)}$ to niearchimedesowa norma.*

Fakt 1.1.6. *Jeśli $\mathcal{R}$ jest dziedziną całkowitości z ciałem ułamków $\mathcal{K}$, zaś $v \colon \mathcal{R} \setminus \{0\} \to \mathbb{R}$ waluacją przedłużoną do całego $\mathcal{K}$ wzorem $v(x/y) = v(x)-v(y)$, to funkcja $\mathcal{K} \to \mathbb{R}_+$, $\|z\|_v = \exp(-v(z))$ i $\|0\| = 0$ jest niearchimedesową wartością bezwzględną. Odwrotnie, gdy $\|\cdot\|$ nią jest, to $-\log\|\cdot\|$ jest waluacją.*

Fakt 1.1.7. *Norma $\|\cdot\|$ na ciele $\mathcal{K}$ jest niearchimedesowa, wtedy i tylko wtedy, gdy $\|n\| \leq 1$ dla każdego $n \in \mathbb{Z}$ (włożonego w $\mathcal{K}$).*

Dowód. Implikacja w jedną stronę jest oczywista, bo przecież $\|\pm 1\| = 1$ pociąga $\|n \pm 1\| \leq \max\{\|n\|, 1$ i indukcja kończy dowód. W lewą stronę wymagane są już czary-mary. Ponieważ $\|x+y\| \leq \max\{\|x\|, \|$ jest oczywista dla $y = 0$, wystarczy dowieść $\|z+1\| \leq \max\{\|z\|, 1\}$ ($z \in \mathcal{K}$). Dla $n \in \mathbb{N}$:

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

Przechodzimy z m do $+\infty$ po spierwiastkowaniu. □

Własność Archimedesa mówi, że $\sup\{|n| : n \in \mathbb{Z}\} = \infty$. Jeżeli supremum jest skończone, to wynosi 1 i wartość nie jest archimedesowa.

Historia 1 (Archimedes z Syrakuz)**.**

1.2 Fałszywa geometria

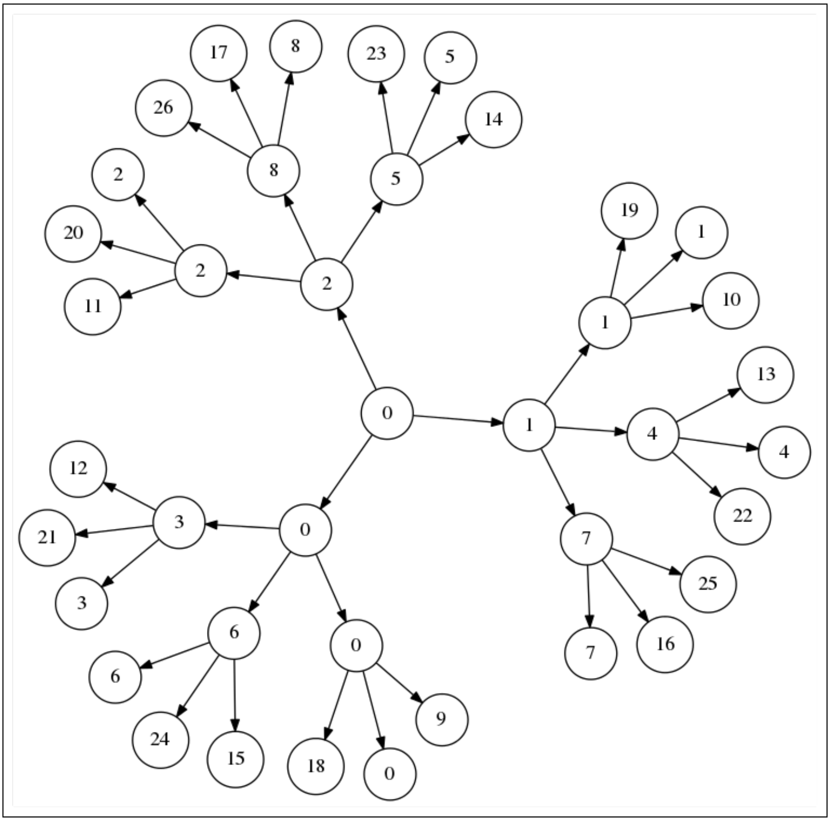
Ciało, gdzie wszystkie działania są ciągłe, nazywa się ciałem topologicznym, takie może być ciało z metryką.

Przestrzenie z taką nierównością wydają się być dziwaczne i rzeczywiście nimi są. Skoro pomiar odległości nie należy do normalnych, to i geometria będzie nie z tej Ziemi.

Fakt 1.2.1. *W niearchimedesowym ciele $\mathcal{K}$, $\|x\| \neq \|y\|$ 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 $\|x\| \leq \|x+y\|$. □

Innymi słowy, wszystkie trójkąty są równoramienne, a ich ramiona są dłuższe od podstaw. Nadszedł czas na kule.



Rysunek 1.1: Rzekomo jest to drzewiasta struktura $\mathbb{Z}_3$.

Fakt 1.2.2. *W niearchimedesowym ciele $\mathcal{K}$ 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. Wszystko jest proste, tylko nic nie jest oczywiste.

1. Jeśli $y \in \mathcal{B}(x, r)$, to $\|x - y\| < r$. Biorąc dowolny z, że $\|z - x\| < r$, dostajemy $\|z - y\| < r$ (niearchimedesowo), zatem $\mathcal{B}(x, r) \subset \mathcal{B}(y, r)$. Podobnie w drugą stronę.
2. Każda otwarta kula jest otwartym zbiorem. Weźmy y z brzegu $\mathcal{B}(x, R)$, do tego $r \leq R$. Wtedy pewien z jest w $\mathcal{B}(x, R) \cap \mathcal{B}(y, r)$ (przekrój jest niepusty). To oznacza, że $\|z - x\| < R$ oraz $\|z - y\| < r \leq R$, więc $\|x - y\| \leq R$ i $y \in \mathcal{B}(x, R)$.
3. Weźmy nierozłączne $\mathcal{B}(x, r)$, $\mathcal{B}(y, R)$, że $r \leq R$. Wtedy pewien z leży w obydwu kulach. Ale $\mathcal{B}(x, r) = \mathcal{B}(z, r)$ zawiera się w $\mathcal{B}(z, R) = \mathcal{B}(y, R)$. □

Efektem ubocznym jest to, że gdy $\mathcal{K} = \mathbb{Q}$, zaś $\| \cdot \| = | \cdot |_p$, to domknięte kula $\mathcal{B}[0, 1]$ jest sumą rozłączną otwartych $\mathcal{B}(i, 1)$ dla $0 \leq i < p$. „Sfera” ($\{x \in \mathcal{K} : \|x - y\| = r\}$) jest otwarnięta (i *nie jest* brzegiem kuli).

Nietrywialne otwarte kule niczym nie różnią się od swoich domkniętych koleżanek. To pokazuje, do jak wielu fałszywych wniosków można dojść myśląc o przestrzeniach metrycznych jak o $\mathbb{R}^n$.

Cassels nazywa nasze normy waluacjami, a przy tym upiera się przy innej nierówności: $\|x+y\| \leq C \max\{\|x\|, \|y\|\}$. Na stałą $C=2$ można sobie pozwolić zawsze (zmieniając normę, ale nie topologię) i dostać nierówność trójkąta, na $C=1$ (ultra) już niekoniecznie.

1.3 Klasyfikacja wymiernych norm

Lemat 1.3.1. *Następujące warunki są równoważne dla dwóch norm na jednym ciele $\mathcal{K}$:*

1. *topologie od norm pokrywają się*
2. $\|x\|_1 < 1$, *wtedy i tylko wtedy gdy* $\|x\|_2 < 1$
3. *istnieje stała $\alpha > 0$, że dla $x \in \mathcal{K}$ jest $\|x\|_1 = \|x\|_2^\alpha$.*

Dowód. Pokażemy ciąg implikacji.

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

$1 \Rightarrow 2$ Z każdą topologią związane jest pojęcie zbieżności, tutaj można wykorzystać równoważność $x^n \to 0$ i $\|x\| < 1$.

$2 \Rightarrow 3$ Wybierzmy $y \in \mathcal{K}$ różne od 0, że $|y|_1 < 1$. Warunek nr 2 mówi, że $|y|_2$ też jest mniejsze od jeden. Wskazujemy więc $\alpha > 0$ takie, by $|y|_1 = |y|_2^\alpha$.

Ustalmy $x \in \mathcal{K}^\times$, takie że $1 > \|x\|_1 \neq \|y\|_1$. Nie tracimy w ten sposób ogólności: jeśli jest $\|x\|_1 = \|y\|_1$, to $\|x\|_2 = \|y\|_2$ (gdyby tak nie było, to normy ilorazów byłyby zepsute). Jeżeli $\|x\|_1 = 1$, postępujemy podobnie.

Znów istnieje $\beta > 0$, że $\|x\|_1 = \|x\|_2^\beta$, ale potencjalnie może być różne od α. Weźmy dowolne naturalne n, m. Wtedy $\|x\|_1^n < \|y\|_1^m \iff \|x\|_2^n < \|y\|_2^m$. Wzięcie logarytmów daje (po drobnych przekształceniach)

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

Oznacza to, że ułamki po prawych stronach są równe. Skoro $\|y\|_1 = \|y\|_2^\alpha$, to rzeczywiście $\alpha = \beta$. □

Wniosek 1.3.2. *Norma p-adyczna nie jest równoważna q-adycznej, zaś archimedesowa – niearchimedesowej.*

Definicja 1.3.3. *Dwie normy spełniające dowolny z trzech warunków lematu nazywamy równoważnymi.*

Twierdzenie 1 (Ostrowski, 1916). *Każda norma na $\mathbb{Q}$ jest dyskretna lub równoważna z $\|\cdot\|_p$, gdzie $p \leq \infty$ jest l. pierwszą.*

Dowód. Niech $\|\cdot\|$ będzie nietrywialną normą na $\mathbb{Q}$. Pierwszy przypadek: archimedesowa (odpowiada normie $|\cdot|_\infty$). 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 $x \in \mathbb{N}$ (gdyż norma jest multiplikatywna). Dowolną liczbę n

można zapisać w systemie o podstawie n_0: $n = a_0 + a_1 n_0 + \cdots + a_m n_0^m$, gdzie $a_m \neq 0$ i $0 \leq a_j \leq n_0 - 1$.

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

Pokazaliśmy $\|n\| \leq C n_0^{m\alpha} \leq C n^\alpha$ dla każdego n, a więc w szczególności dla liczb postaci n^N (gdyż C nie zależy od n): $\|n\| \leq C^{1/n} n^\alpha$. Idziemy 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 $n_0^{m+1} > n \geq n_0^m$, to nie kłamczymy pisząc

$$\|n_0^{m+1}\| = \|n + n_0^{m+1} - n\| \leq \|n\| + \|n_0^{m+1} - n\|,$$

a stąd wnioskujemy, że

$$\begin{aligned} \|n\| &\geq n_0^{(m+1)\alpha} - \|n_0^{m+1} - n\| \\ &\geq n_0^{(m+1)\alpha} - (n_0^{m+1} - n)^\alpha. \end{aligned}$$

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

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

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 $n = ap + b$ dla $0 < b < p$. Z minimalności p wynika $\|b\| = 1$, zaś z $\|a\| \leq 1$ ($\| \cdot \|$ jest niearchimedesowa) i $\|p\| < 1$: $\|ap\| < 1$. „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 $\|n\| = \|p\|^v \|n'\| = \|p\|^v < 1$. □

Historia 2 (Ostrowski Aleksander)**.**

Zatem ∞ jest liczbą pierwszą (!).

Wniosek I.3.4 (produkt adeliczny)**.** *Gdy $x \in \mathbb{Q}^\times$, to*

$$\prod_{p=2}^\infty |x|_p = 1.$$

1.4 Łatanie podziurawionych ciał

Przypomnienie: $\mathbb{R}$ jest uzupełnieniem $\mathbb{Q}$, to znaczy norma $|\cdot|_\infty$ przedłuża się na $\mathbb{R}$, $\mathbb{R}$ jest zupełne z metryką od niej i $\mathbb{Q}$ leży gęsto w $\mathbb{R}$. Uzupełnianie jest konieczne, gdyż

Lemat 1.4.1. *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 $y \in \mathbb{Z}$ taka, że nie jest kwadratem, nie dzieli się przez p i równanie $x^2 = y$ ma rozwiązanie w $\mathbb{Z}/p\mathbb{Z}$. Stosowne y zawsze istnieje: wystarczy powiększyć jakiś kwadrat z $\mathbb{Z}$ o krotność p.

Niech y_0 będzie dowolnym rozwiązaniem równania, y_n ma być równe x_{n-1} modulo p^n oraz $y_n^2 = y$ (modulo p^{n+1}). Tak skonstruowany ciąg Cauchy'ego nie ma granicy, oto stosowne rachunki:

$$\begin{aligned} y_n &= y_{n-1} + \lambda_n p^n \\ y_n^2 &= y_{n-1}^2 + 2y_{n-1}\lambda_n p^n + \lambda_n^2 p^{2n} \\ \lambda_n &= (y - y_{n-1}^2)(2y_{n-1}p^n)^{-1} \pmod p \end{aligned}$$

Jest Cauchy'ego ($|y_{n+1} - y_n| \leq p^{-n-1}$) i nie ma granicy ($|y_n^2 - y| \leq p^{-n-1}$, ale pierwiastek z y, jedyny kandydat, nie istnieje). Gdy $p = 2$, to zastępujemy pierwiastek kwadratowy sześciennym. □

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

Lemat 1.4.2. *Ideał $N \trianglelefteq C$ jest maksymalny.*

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, 0 wcześniej ma sens. Ciąg y_n jest Cauchy'ego:

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

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

Definicja 1.4.3. *Ciało liczb p-adycznych to $\mathbb{Q}_p := C/N$.*

Lemat 1.4.4. *Ciąg $|x_n|_p$ jest stacjonarny, gdy $(x_n) \in C \setminus N$.*

Dowód. Można znaleźć takie liczby ε, N_1, że $n \geq N_1$ pociąga $|x_n| \geq \varepsilon > 0$. Z drugiej strony istnieje taka N_2, że $n, m \geq N_2$ pociąga $|x_n - x_m| < \varepsilon$. 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 1.4.5. *Gdy $(x_n) \in C$ reprezentuje $x \in \mathbb{Q}_p$, przyjmujemy $|x|_p := \lim_{n\to\infty} |x_n|_p$.*

Lemat 1.4.6. *Obraz $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ po włożeniu jest gęsty.*

Dowód. Chcemy pokazać, że każda otwarta kula wokół $x \in \mathbb{Q}_p$ kroi się z obrazem $\mathbb{Q}$, czyli zawiera „stały ciąg". Ustalmy kulę $\mathcal{B}(x, \varepsilon)$, ciąg Cauchy'ego (x_n) dla x 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 $|x - (y)| < \varepsilon$, gdyż $x - (y)$ odpowiada ciąg $(x_n - y)$. Ale $|x_n - x_N| < \varepsilon'$ i $\lim_{n\to\infty} |x_n - y| \leq \varepsilon' < \varepsilon$. □

Fakt 1.4.7. *Ciało $\mathbb{Q}_p$ jest zupełne.*

Dowód. Ustalmy x_n, ciąg Cauchy'ego elementów $\mathbb{Q}_p$. Obraz $\mathbb{Q}$ w $\mathbb{Q}_p$ jest gęsty, a zatem można znaleźć liczby wymierne q_n, że $|x_n - (q_n)| \to 0$ (w ciele $\mathbb{Q}_p$). Okazuje się, że liczby q_n same tworzą ciąg Cauchy'ego i to właśnie on jest granicą x_n. □

Fakt 1.4.8. *Własności pierścienia waluacji $\{x \in \mathbb{Q}_p : |x|_p \leq 1\}$:*

1. *pierścień „$\mathbb{Z}_p$" jest lokalny; ideał $p\mathbb{Z}_p$ jest maksymalny*
2. $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} = \{\frac{y}{z} \in \mathbb{Q} : p \nmid z\}$
3. *włożenie $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ ma gęsty obraz: jeśli $x \in \mathbb{Z}_p$ i $n \geq 1$, to istnieje jedyna $x_n \in \mathbb{Z} \cap [0, p^n - 1]$, że $|x - x_n| \leq p^{-n}$.*
4. *każdy $x \in \mathbb{Z}_p$ jest granicą ciągu Cauchy'ego $x_n \in \mathbb{Z}$, którego wyrazy spełniają $0 \leq x_n \leq p^n - 1$, $p^{n-1} \mid (x_n - x_{n-1})$.*

Dowód. Pierścień $\mathbb{Z}_p$ jest lokalny, jak inne pierścienie waluacji. Ideał waluacji ma p za generator, bo $|x| < 1$ wtedy i tylko wtedy gdy $|x/p| \leq 1$, czyli $x \in p\mathbb{Z}_p$. Ideał waluacji zawiera się w $p\mathbb{Z}_p$ i jest maksymalny, czyli jest nim po prostu $\mathbb{Z}_p$.

Niech $x \in \mathbb{Z}_p, n \geq 1$. Wskażmy $\frac{y}{z} \in \mathbb{Q}$, że $|x - \frac{y}{z}| \leq p^{-n}$. Skoro $|y/z| \leq \max(|x|, |x - y/z|) \leq 1$ (czyli $p \nmid z$), to istnieje $z' \in \mathbb{Z}$, że $zz' \equiv 1 \bmod p^n$. To oznacza, że $|y/z - yz'| \leq p^{-n}$ i $yz' \in \mathbb{Z}$. Zastąpiliśmy ułamek liczbą całkowitą.

Wybierając x_n, jedyną całkowitą, że $0 \leq x_n \leq p^n - 1$ i $x_n = yz'$ modulo p^n, dostajemy $|x - x_n| \leq p^{-n}$. Ostatni punkt wynika z przedostatniego. □

Wniosek 1.4.9. *Zbiory $p^n\mathbb{Z}_p$ to układ otoczeń dla zera kryjący $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$ ($n \in \mathbb{Z}$). Ciąg $0 \to \mathbb{Z}_p \to \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z} \to 0$ (najpierw mnożymy przez p^n, później rzutujemy) jest dokładny, a strzałki ciągłe, więc $\mathbb{Z}_p^+$ jest beztorsyjna i $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.*

1.5 Lemat Hensela o podnoszeniu

„Lemat Hensela" opisuje jedną z ważniejszych algebraicznych cech ciał udających $\mathbb{Q}_p$ (zupełnych oraz z niearchimedesową normą). Orzeka mianowicie, że w pewnych warunkach można łatwo sprawdzić, czy wielomian ma pierwiastki w $\mathbb{Z}_p$.

Twierdzenie 2 (lemat Hensela). *Każde z zer $x_1 \in \mathbb{Z}_p$ (modulo $p\mathbb{Z}_p$) dla wielomianu $f(x) \in \mathbb{Z}_p[x]$, że $f'(x_1) \not\equiv 0$ mod $p\mathbb{Z}_p$ można podnieść do prawdziwego zera x, które przystaje do x_1 mod $p\mathbb{Z}_p$. Co więcej, zero to jest jednoznacznie wyznaczone.*

Dowód. Wskażemy ciąg Cauchy'ego zbieżny do x przy użyciu „metody Newtona" (x_n), taki że $f(x_n) \equiv 0 \bmod p^n$ i $x_n \equiv x_{n+1} \bmod p^n$. Mamy x_1, chcemy $x_2 = x_1 + y_1 p$ dla $y_1 \in \mathbb{Z}_p$.

Widzimy, że $f(x_2) = f(x_1) + f'(x_1)y_1 p + p^2 \cdot r_2$ (gruz). Szukamy y_1, dla którego $f(x_1) + f'(x_1)y_1 p \equiv 0 \bmod p^2$, czyli $z_1 + f'(z_1)y_1 \equiv 0 \bmod p$, gdzie $f(x_1) = pz_1$. Rozwiązaniem jest $y_1 \equiv -z_1 f'(x_1)^{-1} \bmod p$. Uważny Czytelnik zauważy, że skoro z x_1 można dostać x_2, to z x_n można dostać x_{n+1}. □

W dowodzie skorzystaliśmy ze wzoru Taylora:

Fakt 1.5.1. *Dla wielomianu $f(x)$ nad ciałem $\mathcal{K}$ charakterystyki zero jest $f(x+h) = f(x)+f'(x)h+f''(x)h^2/$ $x, h \in \mathcal{K}$.*

Dowód. Nieustanne różniczkowanie sprawia, że wielomian f kiedyś stanie się zerem. Wystarczy porównać współczynniki przy x^j po obu stronach. □

Historia 3 (Hensel Kurt)**.**

Założenie z lematu ($f'(x) \not\equiv 0$) można osłabić, choćby do $|f(x)| < |f'(x)|^2$. Dowód podał już w 1846 Schöneman (?). Już wkrótce i tak przetłumaczymy wszystko na język waluacji.

Historia 4 (Schönemann Theodor)**.**

Wyznaczymy teraz pierwiastki jedności w $\mathbb{Q}_p$ wielomianem $f(x) = x^m - 1$ z pochodną $f'(x) = mx^{m-1}$. Aby spełnione było drugie założenie z lematu, musimy mieć $p \nmid m$ (zakładamy to) i pozostaje sprawdzić pierwsze założenie.

Lemat 1.5.2. *Niech $p \nmid m$. Istnieje taka całkowita n, że $n^m \equiv 1$ mod p (ale $n \not\equiv 1$ mod p), wtedy i tylko wtedy gdy $(m, p-1) > 1$. Dla każdego n, najmniejsza m o żądanych własnościach dzieli $p-1$.*

Dowód. Załóżmy istnienie n. Rząd n w $(\mathbb{Z}/p\mathbb{Z})^\times$ dzieli zarówno m, jak i $p-1$, zatem $(m, p-1) > 1$, chyba że $n \equiv 1 \bmod p$. Najmniejsze m musi dzielić NWD, a z nim także $p-1$.

Odwrotnie, w grupie cyklicznej rzędu $p-1$ istnieje element każdego rzędu, który dzieli $p-1$, a taka jest $(\mathbb{Z}/p\mathbb{Z})^\times$. □

Lemat Hensela daje:

Fakt 1.5.3. *Jeżeli naturalna m nie dzieli się przez pierwszą p, to w $\mathbb{Q}_p$ istnieje m-ty pierwiastek pierwotny z jedynki, wtedy i tylko wtedy gdy m dzieli $p-1$.*

Nie wykluczyliśmy jeszcze istnienia p^n-tych pierwiastków jedności w $\mathbb{Q}_p$, uda się to po poznaniu logarytmu. Pierwiastki jedności w $\mathbb{Q}_p$ dla $p \geq 3$ tworzą grupę μ_{p-1} o $p-1$ elementach.

„Jednostka urojona”, czyli kwadratowy pierwiastek z -1 w $\mathbb{Q}_p$ istnieje dokładnie wtedy, gdy $\frac{1}{2}(p-1)$ jest jeszcze parzysta, czyli dla p postaci $4k+1$.

Teraz zajmiemy się kwadratami.

Fakt 1.5.4. *Jeśli tylko $p > 2$, to każda p-adyczna jedność y, dla której istnieje z, że $z^2 \equiv y$ mod $p\mathbb{Z}_p$, jest kwadratem czegoś z $\mathbb{Z}_p^\times$.*

Dowód. Lemat Hensela dla $x^2 - y$, bo $p \neq 2$ i $y \in \mathbb{Z}_p^\times$ pociągają $2z \not\equiv 0 \bmod p$. □

Wniosek 1.5.5. *$\{x^2 : x \in \mathbb{Q}_p\} = \{p^{2n}y^2 : n \in \mathbb{Z}, y \in \mathbb{Z}_p^\times\}$, a grupa ilorazowa $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ ma rząd cztery i reprezentantów warstw $\{1, p, c, cp\}$, przy czym $c \in \mathbb{Z}_p^\times$ jest dowolnym elementem, którego redukcja mod p nie jest resztą kwadratową.*

Dowód. Własności reszt kwadratowych. □

Dla $\mathbb{R}$ jest inaczej: dokładnie nieujemne liczby to kwadraty, zaś $\mathbb{R}^\times/(\mathbb{R}^\times)^2$ odpowiada $\{-1, 1\}$. Co może się dziać w $\mathbb{Q}_2$? Potrzebna jest mocniejsza forma lematu, albowiem $f'(x) = 2x$ jest wielokrotnością dwójki.

Fakt 1.5.6. *Każda liczba $y \in 1 + 8\mathbb{Z}_2 \subseteq \mathbb{Z}_2$, jest kwadratem w $\mathbb{Z}_2$. Odwrotnie, 2-adyczna jedność i kwadrat przystaje do 1 mod 8. Zatem $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ ma rząd osiem, odpowiada jej $\{\pm 1, \pm 2, \pm 5, \pm 10\}$.*

Dowód. Wystarczy użyć wzmocnionego lematu. □

Lemat Hensela mówi, że jeżeli wielomian dzieli się przez $x - x_0$: $f(x) \equiv (x - x_0)g(x)$ mod p, to w podobny sposób daje się rozłożyć także w $\mathbb{Z}_p[x]$. Warunek nałożony na pochodną dopuszcza jedynie pojedyncze pierwiastki. Teraz osłabimy to założenie do względnej pierwszości.

Przez $\overline{w}$, oznaczymy redukcję współczynników wielomianu $w \in \mathbb{Z}_p[x]$ modulo p.

Definicja 1.5.7. *Wielomiany q, r są względnie pierwsze modulo p, gdy $(\overline{q}, \overline{r}) = 1$ w $\mathbb{F}_p[x]$.*

Istnieją wtedy $a, b \in \mathbb{Z}_p[x]$, że $aq + br \equiv 1 \bmod p$.

Twierdzenie 3. *Niech dla wielomianu $f(x) \in \mathbb{Z}_p[x]$ istnieją dwa względnie pierwsze mod p wielomiany: $g_1, h_1 \in \mathbb{Z}_p[x]$, przy czym g_1 jest unormowany i $f(x) \equiv (g_1 h_1)(x)$ mod p. Wtedy istnieją takie $g(x), h(x) \in \mathbb{Z}_p[x]$, że g jest unormowany, g i g_1 oraz h i h_1 przystają do siebie mod p oraz $f(x) = (gh)(x)$.*

Dowód. Postępujemy jak wcześniej: znajdujemy przybliżone rozwiązanie i próbujemy przejść do granicy.

Niech d będzie stopniem f, zaś m: stopniem g_1. Możemy założyć, że $\deg h_1 \leq d - m$. Potrzebne są nam dwa ciągi, g_n i h_n (wielomiany), że: każdy g_n jest unormowany, $g_{n+1} \equiv g_n$ mod p^n oraz $h_{n+1} \equiv h_n$ mod p^n, a przy tym $f \equiv g_n h_n$ mod p^n. Wielomiany h, g otrzymamy przez przejście do granicy.

Mamy już g_1, h_1. Musi zachodzić $g_2 = g_1 + pr_1$, a przy tym $h_2 = h_1 + ps_1$. Po podstawieniu do równania $f \equiv g_2 h_2$ mod p^2 i uproszczeniu otrzymamy $f - g_1 h_1 = pk_1$ dla $k_1 \in \mathbb{Z}_p[x]$. Dalsze uproszczenie do $pk_1 \equiv pr_1 h_1 + ps_1 g_1$ mod p^2 sprawia, że chcemy podzielić przez p.

Skoro g_1, h_1 są względnie pierwsze mod p, to istnieją a, b (wielomiany nad $\mathbb{Z}_p$), że $ag_1 + bh_1 \equiv 1$ mod p. Rozpatrzmy nowe wielomiany, $\overline{r}_1 = bk_1$ i $\overline{s}_1 = ak_1$. Wiemy już, że

$$\overline{r}_1 h_1 + \overline{s}_1 g_1 \equiv k_1 \pmod{p}.$$

Podzielmy $\overline{r}_1$ przez g_1; niech r_1 będzie resztą: $r_1 = g_1 q + r_1$. Rzecz jasna $\deg r_1 < \deg g_1$. Ale jeśli położymy $s_1 = \overline{s}_1 + h_1 q$, to wszystko będzie grać:

$$\begin{aligned} \ldots = r_1 h_1 + s_1 g_1 &\equiv (\overline{r}_1 - g_1 q) h_1 + (\overline{s}_1 + h_1 q) g_1 \\ &\equiv \overline{r}_1 h_1 - g_1 h_1 q + \overline{s}_1 g_1 + g_1 h_1 q \equiv \overline{r}_1 h_1 + \overline{s}_1 g_1 \\ &\equiv k_1 \pmod{p}. \end{aligned}$$

Tak pokazaliśmy, że g_2 oraz h_2 istnieją. Skoro przystają do g_1 i h_1 mod p, to również są względnie pierwsze mod p i możemy wykonać kolejny krok „indukcyjny". □

1.6 Regionalnie czy wszechstronnie?

Jednym z wniosków lematu Hensela jest to, że dla wielomianu o współczynnikach całkowitych łatwo sprawdzić, czy ma zera w $\mathbb{Z}_p$ (bo wystarczy szukać ich w $\mathbb{Z}/p\mathbb{Z}$), podobnie w $\mathbb{R}$. Istnienie pierwiastka w $\mathbb{Q}$ pociąga „to samo" w każdym $\mathbb{Q}_p$ ($p \leq \infty$). Trzeba o tym myśleć tak: ciała p-adyczne są odpowiednikami ciał rozwinięć Laurenta i dają „lokalną" informację „blisko" p. Fakt, że pierwiastki przenoszą się z $\mathbb{Q}$ do $\mathbb{Q}_p$ oznacza bowiem, że „globalny" pierwiastek jest też „lokalnym" dla każdego p, czyli „wszędzie". Ciekawe pytanie brzmi, kiedy można to odwrócić.

Fakt 1.6.1. *Liczba $x \in \mathbb{Q}$ jest kwadratem wtedy i tylko wtedy, gdy jest kwadratem w każdym $\mathbb{Q}_p$, $p \leq \infty$.*

Zbyt niejasne, żeby nazwać twierdzeniem:

Fakt 1.6.2 (reguła lokalno-globalna)**.** *Istnienie rozwiązań w $\mathbb{Q}$ (lub ich brak) dla równania diofantycznego można stwierdzić na podstawie istnienia (lub nie) rozwiązań w $\mathbb{Q}_p$.*

Niestety, $(x^2-2)(x^2-17)(x^2-34) = 0$ ma pierwiastki w każdym z $\mathbb{Q}_p$, ale nie w $\mathbb{Q}$. Inny przykład: $x^4 - 17 = 2y^2$. Na szczęście nie wszystko stracone.

Twierdzenie 4 (Hasse, Minkowski)**.** *Forma kwadratowa F nad $\mathcal{K}$ (ciałem liczbowym jak $\mathbb{Q}$) reprezentuje nietrywialnie zero w $\mathcal{K}$, wtedy i tylko wtedy gdy reprezentuje je w każdym uzupełnieniu $\mathcal{K}$.*

Dowód. Zbyt trudny (przez wyrwy w wiedzy o kwadratowych formach), nawet dla samego $\mathcal{K} = \mathbb{Q}$. Można go jednak znaleźć w pierwszej połowie książki Serre'a ([5]) □

Historia 5 (Hasse Helmut)**.**

Historia 6 (Minkowski Hermann)**.**

Ograniczymy się do rozwiązania tylko jednego równania: $ax^2 + by^2 + cz^2 = 0$ dla wymiernych a, b, c. Poczynimi kilka założeń: $abc \neq 0$ jest bezkwadratowa oraz $a, b, c \in \mathbb{Z}$, gdyż możemy. Wynika stąd, że a, b, c są parami względnie pierwsze i różnych znaków (patrz $p = \infty$!).

Fakt 1.6.3. *Jeśli liczba pierwsza $p > 2$ nie dzieli abc, to istnieją liczby $x_0, y_0, z_0 \in \mathbb{Z}$, że $ax_0^2+by_0^2+cz_0^2 = 0$, a przy tym p nie dzieli wszystkich trzech (x_0, y_0, z_0).*

Dowód. Gdy x, y, z przebiegają przez całkowite od 0 do $p-1$, to istnieje p^3 trójek (x, y, z). Ile z nich pasuje do równania? Brudna sztuczka: $(ax^2 + by^2 + cx^2)^{p-1}$ jest równe 1, gdy trójka nie jest rozwiązaniem (i 0 w przeciwnym przypadku), wynika to z MTF. Liczba nierozwiązań to $\sum_{p^3}(ax^2 + by^2 + cz^2)^{p-1}$ (ale modulo p!). Rozwijamy potęgi i dostajemy sumy postaci $\sum \lambda x^{2i}y^{2k}z^{2l}$ z $2i + 2k + 2l = 2(p-1)$ i $\lambda \in \mathbb{Z}$. Każda z nich jest zerem modulo p: przynajmniej jedna z $2i, 2k, 2l$ jest mniejsza od $p-1$ (powiedzmy, $2i$). Wtedy nasza suma to

$$\sum_{(y,z)} \left(\lambda y^{2k} z^{2l} \sum_x x^{2i} \right).$$

Przywołujemy poniższy lemat. Skoro p dzieli N (liczbę nierozwiązań), to dzieli także $p^3 - N$. Znamy jedno rozwiązanie (trywialne), zatem istnieją inne. Był to specjalny przypadek tw. Chevalleya i Warninga. □

Lemat 1.6.4. *Jeśli* $0 \leq n \leq p-1$*, to* p *dzieli* $\sum_{i=0}^{p-1} i^n$.

Dowód. Wybierzmy takie y, że $y^n \not\equiv 1 \bmod p$. Wtedy

$$0 \equiv \sum_{i=0}^{p-1} i^n - \sum_{i=0}^{p-1} (yi)^n = (1-y^n) \sum_{i=0}^{p-1} i^n$$

□

Znając rozwiązanie (x_0, y_0, z_0) „mod p" wiemy, że $p \nmid x_0$ (bez straty ogólności). Znamy rozwiązanie wielomianowego $aX^2 + by_0^2 + cz_0^2 = 0$ modulo p, x_0. Z naszymi założeniami lemat Hensela wskaże $x \in \mathbb{Z}_p$, pierwiastek równania, a także rozwiązanie pierwotnego: (x, y_0, z_0).

To jeszcze nie koniec. Załóżmy teraz, że $p = 2$, ale a, b, c są nieparzyste. Gdy istnieje rozwiązanie $(x, y, z) \in \mathbb{Q}_2^3$, to możemy założyć, że nie wszystkie leżą w $2\mathbb{Z}_2$ (innymi słowy, $\max\{|x|_2, |y|_2, |z|_2\} = 1$). Po redukcji mod $2\mathbb{Z}_2$ widzimy, że y, z są jednościami 2-adycznymi, x dzieli się przez 2. Kwadrat 2-adycznej jedności leży w $1 + 4\mathbb{Z}_2$, zaś kwadrat czegoś z $2\mathbb{Z}_2$ leży w $4\mathbb{Z}_2$. Redukując modulo $4\mathbb{Z}_2$ dostajemy więc: $b + c \equiv 0 \bmod 4$. Okazuje się, że warunek ten jest nie tylko konieczny, ale też wystarczający.

Lemat 1.6.5. *Równanie* $aX^2 + bY^2 + cZ^2 = 0$ *ma nietrywialne rozwiązanie w* $\mathbb{Q}_2$*, gdy* $2 \nmid abc$ *i* 4 *dzieli sumę dwóch z* a, b, c.

Dowód. Szukamy początkowego rozwiązania (x_0, y_0, z_0), dla którego $8 \mid ax_0^2 + by_0^2 + cz_0^2$. Jeśli $8 \mid a + b$, to kładziemy $x_0 = 1$, $y_0 = 1$, $z_0 = 0$. Jeśli nie, to $z_0 = 2$, $x_0 = y_0 = 1$. Stosujemy lemat Hensela. □

Lemat 1.6.6. *Równanie* $aX^2 + bY^2 + cZ^2 = 0$ *ma nietrywialne rozwiązanie w* $\mathbb{Q}_2$*, gdy jedna z* a, b, c *jest parzysta, zaś suma dwóch lub trzech z nich dzieli się przez 8.*

Dowód. Załóżmy, że 2 dzieli tylko a oraz że $ax^2 + by^2 + cz^2 = 0$. Możemy przyjąć, że któraś z x, y, z jest 2-adyczną jednością, zaś wszystkie leżą w $\mathbb{Z}_2$. Kwadrat 2-adycznej jedności leży w $1 + 8\mathbb{Z}_2$, zatem $0 = ax^2 + by^2 + cz^2 \equiv b + c \pmod 8$, jeśli $x \in 2\mathbb{Z}_2$ (wtedy y, z muszą być 2-adycznymi jednościami).

Jeśli x jest 2-adyczną jednością, to y, z i tak też muszą nimi być, co prowadzi do $a+b+c \equiv 0$ mod 8. Twierdzenie odwrotne jest prawdziwe na mocy uogólnionego lematu Hensela. □

Lemat 1.6.7. *Jeżeli* $p \neq 2$ *dzieli* a*, to równanie ma nietrywialne rozwiązanie dokładnie wtedy, gdy* $-b/c$ *to kwadratowa reszta mod* p.

Dowód. Ponownie, lemat Hensela. □

Fakt 1.6.8. *Niech liczby* $a, b, c \in \mathbb{Z}$ *będą parami względnie pierwsze, bezkwadratowe. Równanie* $ax^2 + by^2 + cz^2 = 0$ *posiada w* $\mathbb{Q}$ *nietrywialne rozwiązania, wtedy i tylko wtedy gdy:*

1. *(a, b, c nie są tego samego znaku)*
2. *każdy nieparzysty dzielnik pierwszy liczby* a *posiada* $r \in \mathbb{Z}$*, że* $p \mid b + r^2c$*, podobnie dla* b *i* c
3. *jeśli* $2 \nmid abc$*, to* 4 *dzieli sumę pewnych dwóch z* a*,* b*,* c.
4. *jeśli* $2 \mid a$*, to* 8 *dzieli* $b + c$ *lub* $a + b + c$ *(podobnie* b *i* c*).*

Pierwszy warunek wynika z pozostałych.

Bezpośredni dowód można znaleźć w rozdziałach 3 – 5 książki [Cas91]. Strategią jest użycie trzech warunków, a także „geometrii liczb" Minkowskiego do pokazania, że możliwe jest znalezienie rozwiązania (x, y, z) spełniającego nierówność

$$|a|x^2 + |b|y^2 + |c|z^2 < 4|abc|.$$

1.7 Normowa niezależność

Zaprezentujemy teraz pogląd Casselsa na temat niezależności nierównoważnych norm. Co dokładnie przez to rozumiemy, stanie się jasne natychmiast po udowodnieniu lematu.

Lemat 1.7.1. *Niech nietrywialne normy $|\cdot|_1, \ldots, |\cdot|_m$ będą parami nierównoważne (na ciele $\mathcal{K}$). Istnieje wtedy $x \in \mathcal{K}$, że $|x|_1 > 1$, ale $|x|_2, \ldots, |x|_m < 1$.*

Dowód. Indukcyjny względem m. Gdy $m = 2$, istnieją $y, z \in \mathcal{K}$, takie że $|y|_1, |z|_2 < 1$ oraz $|y|_2, |z|_1 \geq 1$. Poszukiwanym jest wtedy $x = zy^{-1}$.

Jeżeli $m > 2$, to z założenia indukcyjnego mamy $y \in \mathcal{K}$, że $|y|_1 > 1$, $|y|_i < 1$ $(2 \leq i \leq m-1)$. Z drugiej strony istnieje $z \in \mathcal{K}$, że $|z|_1 > 1$, $|z|_m < 1$. Rozpatrujemy trzy przypadki.

Jeżeli $|y|_m < 1$, to $x = y$. Jeżeli $|y|_m = 1$, to $x = y^n z$ dla dużego n. Jeżeli $|y|_m > 1$, to $x = y^n z(1 + y^n)^{-1}$ dla dużego n. Mamy bowiem

$$\frac{y^n}{1+y^n} \to \begin{cases} 1 & \text{dla } |\cdot|_1 \text{ oraz } |\cdot|_m, \\ 0 & \text{w przeciwnym razie.} \end{cases}$$ □

Fakt 1.7.2. *Przy założeniach lematu, $x_1, \ldots, x_m \in \mathcal{K}$ oraz $\varepsilon > 0$ (rzeczywistym), istnieje $x \in \mathcal{K}$, że jednocześnie spełniona jest każda z nierówności $|x - x_i|_i < \varepsilon$.*

Dowód. Z lematu wynika istnienie takich $y_i \in \mathcal{K}$, że $|y_i|_i > 1$, $|y_i|_k < 1$ $(k \neq i)$. Wystarczy położyć

$$x = \lim_{n\to\infty} \sum_{i=1}^{m} \frac{y_i^n}{1+y_i^n} x_i.$$ □

Związane jest to z chińskim twierdzeniem o resztach. Mówi ono, że gdy $x_i \in \mathbb{Z}$ są dane, p_i parami różne (i pierwsze), zaś m_i naturalne, to układ „kongruencji"

$$|x - x_i|_i \leq p_i^{-m(i)}$$

ma rozwiązanie nie tylko w $\mathbb{Q}$, ale także $\mathbb{Z}$. Nasz fakt można jednak wzmocnić, gdy $\mathcal{K}$ jest algebraicznym ciałem liczbowym (uczynimy to, ale jeszcze nie teraz).

Przedstawimy teraz obrazowo niezależność.

Fakt 1.7.3. *Odwzorowanie przekątniowe ma gęsty obraz, kiedy $\mathcal{K}_i$ uzupełnia $\mathcal{K}$ względem nierównoważnych parami norm.*

$$\Delta : \mathcal{K} \hookrightarrow \prod_i \mathcal{K}_i$$

Dowód. Ustalmy elementy $x_i \in \mathcal{K}_i$ dla $1 \leq i \leq n$. Istnieją wtedy $y_i \in \mathcal{K}$, że $|x_i - y_i|_i < \varepsilon$ dla ustalonego $\varepsilon > 0$. Mamy takie $z \in \mathcal{K}$, że $|z - y_i|_i < \varepsilon$, zatem $|z - x_i|_i < 2\varepsilon$ (na mocy poprzedniego faktu). □

Rozdział 2

Analiza

2.1 Ciągi oraz szeregi

W ciele $\mathbb{Q}_p$ marzenia stają się prawdziwe:

Fakt 2.1.1. *Ciąg* (x_n) *o wyrazach w* $\mathbb{Q}_p$ *jest Cauchy'ego, wtedy i tylko wtedy gdy zachodzi* $\lim_{n\to\infty} |x_{n+1} - x_n| =$

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

Zbieżność absolutna szeregu pociąga jego zbieżność, w ciele liczb p-adycznych zachodzi jednak jeszcze mocniejszy fakt.

Fakt 2.1.2. *Zbieżność szeregu* $\sum_n x_n$ *o wyrazie ogólnym z* $\mathbb{Q}_p$ *jest równoważna zbieżności* x_n *do* 0. *Prawdziwe jest wtedy oszacowanie* $|\sum_{n\geq 0} x_n| \leq \max_n |x_n|$.

Dowód. Implikacja w prawo jest oczywista. Dla dowodu w lewo wynikania wystarczy zauważyć, że wyraz x_n to różnica między dwoma sumami częściowymi i powołać się na poprzedni fakt.

Nierówność wynika z

$$\left| \sum_{n=0}^{N-1} x_n + \sum_{n=N}^{\infty} x_n \right| \leq \max_{n<N} |x_n| + \left| \sum_{n=N}^{\infty} x_n \right|,$$

gdzie drugi składnik znika w nieskończoności. □

Wniosek 2.1.3. *Szereg z poprzedniego faktu zbiega bezwarunkowo, ale niekoniecznie bezwzględnie.*

Dowód. Nałożenie permutacji na wyrazy szeregu nie psuje ich zbieżności do zera.

Nie każdy szereg zbiega jednak bezwzględnie, wystarczy dodać do siebie p^k sztuk liczby p^k dla $k \geq 0$. Nałożenie normy zmusza do wysumowania $1 + 1 + 1 + \ldots$, ale zwykłą sumą graniczną jest odwrotność $1 - p^2$, żyjąca w każdym $\mathbb{Q}_p$. □

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

Definicja 2.1.4. *Jeśli dla każdej dodatniej liczby ε istnieje całkowita N niezależna od k, że $i \geq N$ pociąga $|x_{ik}| < \varepsilon$, to $\lim_{i\to\infty} x_{ik} = 0$ jednostajnie względem k.*

Lemat 2.1.5. *Załóżmy, że $x_{ik} \in \mathbb{Q}_p$, $\lim_{k\to\infty} x_{ik} = 0$ (dla każdego i), $\lim_{i\to\infty} x_{ik} = 0$ jednostajnie względem k. Wtedy każdemu $\varepsilon > 0$ odpowiada N, że $\max\{i,k\} \geq N$ pociąga $|x_{ik}| < \varepsilon$.*

Dowód. Ustalmy ε. Drugi warunek zapewnia N_0 (zależne tylko od ε), że $|x_{ik}| < \varepsilon$ dla $i \geq N_0$. Pierwszy zaś dla każdego i daje N_1, dla którego $k \geq N_1$ pociąga $|x_{ik}| < \varepsilon$. Wystarczy przyjąć $N = \max\{N_0, N_1(0), N_1(1), \ldots, N_1(N_0-1)\}$. □

Fakt 2.1.6. *Przy założeniach z lematu 2.1.5 poniższe szeregi zbiegają do tej samej liczby: $\sum_{i=0}^{\infty}\sum_{k=0}^{\infty} x_{ik} = \sum_{k}$*

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

Dla $i \geq N$ mamy $|\sum_{k\geq 0} x_{ik}| \leq \max_k |x_{ik}| < \varepsilon$ na mocy faktu 2.1.2, podobna nierówność prawdziwa jest dla $k \geq N$.

Wnioskujemy stąd, że podwójne szeregi także zbiegają, bo

$$\lim_{i\to\infty} \sum_{k\geq 0} x_{ik} = \lim_{k\to\infty} \sum_{i\geq 0} x_{ik} = 0.$$

Pozostało nam uzasadnić, że sumy są sobie równe.

Pozostańmy przy N, ε wybranych wcześniej. Oznacza to, że $|x_{ik}| < \varepsilon$, gdy $i \geq N$ lub $k \geq N$. Zauważmy, że

$$\Big|\sum_{i,k\geq 0} x_{ik} - \sum_{i,k\leq N} x_{ik}\Big| = \Big|\sum_{i\leq N}\sum_{k>N} x_{ik} + \sum_{i>N}\sum_{k\geq 0} x_{ik}\Big|.$$

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

Fakt 2.1.7. *Załóżmy zbieżność szeregów $\sum_i x_i$, $\sum_i y_i$. Zachodzi wtedy: $\sum_i x_i + y_i = \sum_i x_i + \sum_i y_i$, a także*

$$\sum_{i=0}^{\infty}\sum_{k=0}^{i} x_k y_{i-k} = \Big[\sum_{i=0}^{\infty} x_i\Big] \cdot \Big[\sum_{i=0}^{\infty} y_i\Big].$$

Wyznaczymy teraz wartość kilku szeregów p-adycznych. Fenomen związany z ich nieoczekiwanymi granicami wyjaśnić się może po lekturze ostatniego ustępu w tym rozdziale, gdzie przytoczymy zaskakujący wynik Burgera i Struppecka.

Fakt 2.1.8. *Jeżeli $k > 0$, to $\sum_{n\geq 0} n^k p^n$ jest wymierne w $\mathbb{Q}_p$.*

Dowód. Wynika to z równości szeregów formalnych

$$\sum_{n=0}^{\infty} n^k x^n = (x \cdot \partial_x)^k \frac{1}{1-x}.$$

Szereg stojący po lewej stronie to specjalny przypadek funkcji ζ Hurwitza-Lercha, ale nam wystarczy wiedza o wielomianach Eulera. Okazuje się (skoro $|p| = 1/p < 1$), że

$$\sum_{n=0}^{\infty} n^k p^n = \sum_{n=1}^{k} \left\{ {k \atop n} \right\} \cdot \frac{p \cdot n!}{(p-1)^{n+1}},$$

gdzie $\{\cdot, \cdot\}$ to (nieznakowana) druga licza Stirlinga. □

Łatwo pokazać jest, że $\sum_{n \geq 0} n \cdot n! = -1$ w każdym z ciał $\mathbb{Q}_p$, gdyż suma ta jest „teleskopowa": $n \cdot n! = (n+1)! - n!$. Nieco więcej wysiłku wymaga powtórzenie osiągnięć van Hamme'a, któremu Schikhof przypisuje równości: $\sum_{n \geq 1} n^2 (n+1)! = 2$, $\sum_{n \geq 1} n^5 (n+1)! = 26$, $\sum_{n \geq 1} 4^{-n-1} \cdot n^2 (n+1)! = -1$.

Fakt 2.1.9. *Wszystkie one są prawdziwe w $\mathbb{Q}_p$, przy czym ostatnia wymaga $p \neq 2$.*

Dowód. Ostatnia równość jest fałszywa (u Schikhofa), musiała więc zostać delikatnie poprawiona. Dla $p = 2$ szereg po lewej stronie nie jest nawet zbieżny. Podamy jedynie sumy częściowe (do $n = m$), które uważny Czytelnik może zweryfikować:

$$\begin{aligned} 2 &+ (m+2)!(m-1) \\ 26 &+ (m+2)!(m^4 - m^3 - 3m^2 + 12m - 13) \\ -1 &+ (m+2)!(m+2) : 4^{m+1}. \end{aligned}$$

□

Spróbujemy teraz związać dwa ostatnie szeregi ze światem poza-p-adycznym. Dla każdego n istnieją (jedyne) liczby a_n, b_n oraz wielomian $p_n(x)$, że (przy niefortunnej notacji!)

$$\sum_{i=1}^{k} i^n (i+1)! = (k+2)! \cdot p_n(k) + b_n + \sum_{i=1}^{k} a_n (i+1)!.$$

Jeżeli $a_n = 0$, to lewa strona dąży do b_n w $\mathbb{Q}_p$, ale niestety nie są znane żadne n inne niż 2 i 5, które spełniają ten warunek. Ciągi 074051 i 074052 w bazie danych OEIS zawierają więcej informacji. Wykładnicza tworząca a_n to $\exp(1 - 2x - e^{-x})$.

Problem wymierności liczby $x = \sum_n n!$ pozostaje otwarty w każdym ciele $\mathbb{Q}_p$. Wymierna wszędzie nie może jednak być: po pierwsze, nie zależałaby od p, po drugie, byłaby całkowita.

Fakt 2.1.10. *Mamy* $x_k := \sum_{n \geq 1} n^k \cdot n! = v_k - u_k x$, $v_k, u_k \in \mathbb{Z}$.

Lemat 2.1.11. $\sum_{n \geq 1} (n+k)! - n! = -\sum_{n \leq k} n!$.

Wykorzystamy notację Murty'ego i Sumner.

Dowód. Rozwinięcie obu stron lematu daje $\sum_n n^2 \cdot n! = -x$ (dla $k = 2$), przypadek $k = 1$ rozważaliśmy wcześniej. Teraz wystarczy zastosować indukcję. □

Fakt 2.1.12. *Zachodzi* $u_k = \sum_{i=1}^{k+1} (-1)^{k+i} \cdot \{k+1, i\}$.

Wzór ten pozwala szybciej wyznaczać współczynniki u_k, wcześniej Dragovich sugerował rozwiązanie układu liniowych $k + 1$ równań.

Fakt 2.1.13. *Jeśli $k \in 3\mathbb{N}+1$, to $u_k \neq 0$, wtedy x_k i x są tak samo niewymierne.*

Wrócimy teraz do rzeczy przyziemnych i p-adycznej analizy „numerycznej".

Fakt 2.1.14. *Niech $x \in \mathbb{Z}$ nie dzieli się przez p, zaś $x_0 \in \mathbb{Z}$ będzie takie, że $|1-x_0x|_p < 1$. Formuła $1 - x_{n+1}x = (1-x_nx)^2$, to znaczy $x_{n+1} = x_n(2-x_nx)$ zadaje ciąg liczb x_n, które szybko zbiegają do odwrotności x: $v_p(x_n - 1 : x) \geq 2^n$.*

2.2 Bezmyślne różniczkowanie

Metryka zadaje ciągłość. Niestety, w $\mathbb{Q}_p$ nie można pracować z przedziałami (bo ich nie ma); można jednak definiować funkcje na kulach (otwar...niętych). Upośledzona definicja pozwoli nam udawać, że różniczkujemy, chociaż do przyszłego rozdziału nie będziemy tego potrafić.

Definicja 2.2.1. *Niech $U \subseteq \mathbb{Q}_p$ będzie zbiorem otwartym. Funkcja $f\colon U \to \mathbb{Q}_p$ jest ciągła w punkcie $y \in U$, jeśli dla każdego $\varepsilon > 0$ istnieje $\delta > 0$, że „$|x-y| < \delta$ pociąga $|f(x)-f(y)| < \varepsilon$".*

Pochodna takiej funkcji to granica ilorazów różnicowych, by zachować analogię z rzeczywistym przypadkiem. Użyteczność pochodnej jest jednak ograniczona. Wszystko przez fałszywość twierdzenia o wartości średniej w $\mathbb{Q}_p$.

Fakt 2.2.2 (fałszywy). *Jeśli funkcja f jest różniczkowalna na $\mathbb{Q}_p$ i ma ciągłą pochodną, zaś $x, y \in \mathbb{Q}_p$, to istnieje taka liczba $z \in \mathbb{Q}_p$ postaci $\lambda x + (1-\lambda)y$ z $|\lambda| \leq 1$, że $f(y) - f(x) = f'(z)(y-x)$.*

Dowód. Niech $f(t) = t^p - t$, $x = 0$, $y = 1$. Nie ma takiego $z_\lambda = 1 - \lambda$ z $\lambda \in \mathbb{Z}_p$, żeby $f'(z_\lambda) = 0$: w takiej stuacji pochodna się odwraca (!) i nie może być zerem. □

Fakt 2.2.3. *Istnieje różniczkowalna funkcja $\mathbb{Q}_p \to \mathbb{Q}_p$ o pochodnej wszędzie równej zero, która nie jest lokalnie stała („prawie stała").*

Pewnym wyjaśnieniem tego, skąd biorą się takie funkcje jest poniższy fakt (w $\mathbb{Q}_p$ prawdziwa jest reguła łańcucha).

Fakt 2.2.4. *Jeśli pochodna funkcji f wszędzie znika, zaś g jest ciągle różniczkowalna, to pochodne złożeń $f \circ g$, $g \circ f$ są zerem (wszędzie). Funkcje o tej samej pochodnej nie muszą różnić się o stałą.*

Twierdzenie o wartości średniej uratujemy później, w ślad za Robertem (po delikatnym wzmocnieniu założeń).

2.3 Szeregi potęgowe

Będziemy rozważać szeregi potęgowe, $f(x) = \sum_n a_n x^n$. Dla $x \in \mathbb{Q}_p$ wyrażenie $f(x)$ ma sens, o ile $|a_n x^n| \to 0$. Nie mamy przy tym zamiaru odróżniać x od X!

Fakt 2.3.1. *Szereg $\sum_n a_n x^n$ zbiega na różnych dyskach, których promień zależy od R, odwrotności* $\limsup |a_n|^{1:n}$.

1. *jeśli $R = 0$, to f zbiega tylko w $x = 0$.*
2. *jeśli $R = \infty$, to f zbiega wszędzie na $\mathbb{Q}_p$.*

3. *jeśli* $R > 0$ *i* $\lim_{n\to\infty} |a_n|R^n = 0$, *to* f *zbiega dla* $|x| \leq R$.
4. *w przeciwnym przypadku* f *zbiega dokładnie dla* $|x| < R$.

Dowód. Wiadomo dobrze, jaki zbiór jest obszarem zbieżności: $\{x \in \mathbb{Q}_p : \lim_{n\to\infty} |a_n x^n| = 0\}$. Oczywiście $f(0)$ jest zbieżny. Jeśli $|x| < R$, to (rzeczywisty) szereg potęgowy $\sum_n |a_n||x|^n$ jest zbieżny. Jeśli zaś $|x| > R$, to $|a_n||x|^n$ nie może zbiegać do zera przy n dążącym do nieskończoności: nieskończenie często $|a_n|$ jest blisko R^{-n}, więc $(|x|/R)^n$ może być dowolnie duże. Przypadek $|x| = R$ jest konsekwencją faktu 2.1.2. $\square$

Szeregi p-adyczne szeregi zachowują się porządniej niż ich zespoleni koledzy. Tam zbieżność na brzegu dysku $\{|x| = R\}$ jest nieprzewidywalna, tutaj brzegu po prostu nie ma.

Formalne szeregi potęgowe można dodawać i mnożyć.

Fakt 2.3.2. *Jeżeli szeregi potęgowe* f, g *nad* $\mathbb{Q}_p$ *zbiegają w punkcie* x, *to* $f + g$ *oraz* fg *również – odpowiednio do* $f(x) + g(x)$ *i* $f(x)g(x)$.

Przyjrzymy się teraz formalnym złożeniom, które (o dziwo) zachowują się zaskakująco często gorzej niż źle. Będziemy więc pracować z szeregami: $f(x) = \sum_n a_n x^n$ i $g(x) = \sum_n b_n x^n$, przy czym $b_0 = 0$, by napis $f(g(x))$ miał sens (niezależnie od topologii). Przez formalne złożenie rozumiemy

$$h(x) = (f \circ g)(x) = \sum_{n=0}^{\infty} a_n g(x)^n = \sum_{n=0}^{\infty} c_n x^n.$$

Współczynniki c_n są jawnie opisane przez wielomiany Bella, ale te akurat nie będą dla nas przesadnie przydatne.

Fakt 2.3.3 (złoty). *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* $f(g(x))$.

Dowód. Podamy dowód za [3], książką Hassego (rozdział 17). Niech $g(x)^m = \sum_{n=m}^{\infty} d_{m,n} x^n$. Pozwala to na napisanie $h(x)$ jawnie: $h(x) = a_0 + \sum_{n=1}^{\infty} \sum_{m=1}^{n} a_m d_{m,n} x^n$.

Niestety, ale musimy: $d_{m,n} = \sum_{i_1+\ldots+i_m=n} \prod_{k=1}^{m} b(i_k)$.

Szereg $g(x)$ jest zbieżny, więc fakt 2.3.2 pozwala powiedzieć, że $g(x)^m$ zbiega do $g(x)^m$ (jeden szereg jest formalny, drugi nie!). Co ciekawsze, dla każdego n mamy $|d_{m,n} x^n| \leq |g(x)^m|$. Jeżeli $n \geq m$, to nierówność ultrametryczna daje

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

kiedy $i_1 + \ldots + i_m = n$ (dzięki $|b_{ij} x^{ij}| \leq |g(x)^m|$). Jeżeli $n < m$, to nie ma czego dowodzić: $d_{m,n} x^n = 0$. Wiemy już, że $g(x)$, $g(x)^m$ oraz $f(g(x))$ zbiegają. Zapiszmy w takim razie

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

Aby uzasadnić poprawność zamiany kolejności sumowania powołamy się na fakt 2.1.6 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: $a_m d_{m,n} x^n \to 0$. □

Leniwi mogą nie sprawdzić założeń i nadepnąć na minę, co świetnie ilustruje poniższy przykład. To ciekawe, że zwykła analiza łatwiej radzi sobie z tym problemem: jeśli promieniem zbieżności $f(x)$ jest R i $|g(x)| < R$, to $h(x)$ zbiega do $f(g(x))$.

Przykład 2.3.4. *Niech $g(x) = 2x^2 - 2x$ i $h(x) = (f \circ g)(x)$, 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 $h(1) \neq f(g(1))$.

Fakt 2.3.5. *Formalna pochodna (czyli $\sum a_n x^n \mapsto \sum_n n a_n x^{n-1}$) współpracuje z dodawaniem, mnożeniem i składaniem: jest operatorem liniowym, prawdziwe są dla niej reguły: Leibniza oraz łańcuchowa.*

Przy pomocy szeregów potęgowych można zdefiniować na ich obszarze zbieżności funkcje. Dowód poniższego lematu jest analogiczny do przypadku „$\mathbb{R}$".

Lemat 2.3.6. *Jeśli szereg potęgowy $f(x) \in \mathbb{Q}_p[[x]]$ jest zbieżny na $D \subseteq \mathbb{Q}_p$, to funcja $f\colon D \to \mathbb{Q}_p$, $x \mapsto f(x)$, jest ciągła.*

Niestety, nie istnieje p-adyczny odpowiednik analitycznego przedłużania. Obszar zbieżności można zwiększyć (dla funkcji $\mathbb{R} \to \mathbb{R}$) przez rozwinięcie w innym miejscu; tutaj ta sztuczka się nie uda.

Fakt 2.3.7. *Funkcje od szeregów potęgowych f i g mają ten sam obszar zbieżności, jeśli $f(x) = \sum_n a_n x^n \in \mathbb{Q}_p[$ istnieje dla $x = x_0$.*

$$g(x) = \sum_{m \geq 0} \sum_{n \geq m} \underbrace{C^n_m a_n x_0^{n-m}}_{b_m} \cdot (x - x_0)^m$$

Dowód. Liczby b_m są dobrze określone: dla ustalonego m mamy

$$\left| \binom{n}{m} a_n x_0^{n-m} \right| \leq |a_n x_0^{n-m}| = \frac{|a_n x_0^n|}{|x_0|^m} \to 0.$$

Niech x leży w obszarze zbieżności $f(x)$. Wtedy zachodzi $f(x) = f(x - x_0 + x_0)$, co daje się rozpisać:

$$\sum_{n \geq 0} a_n x^n = \sum_{n \geq 0} \sum_{m \leq n} a_n \binom{n}{m} x_0^{n-m} (x - x_0)^m$$

Ostatnia suma wygląda jak częściowa $g(x)$ po przegrupowaniu. Sprawdzimy założenia faktu 2.1.6.

Niech $\beta_{n,m} = 0$ dla $m > n$ i (n nad m)$a_n x_0^{n-m}(x-x_0)^m$ dla $m \leq n$. Trzeba ograniczyć $|a_n x_0^{n-m}(x - x_0)^m| \geq |\beta_{nm}|$.

Skoro x, x_0 leżą w kole zbieżności o jakimś promieniu R, to obszar ten zawiera domknięty dysk o promieniu r, równym co najmniej $\max\{|x|, |x_0|\}$.

Z konstrukcji wynika nierówność $|x_0|^{n-m} \leq r^{n-m}$ oraz $|x-x_0|^m \leq \max\{|x|, |x_0|\}^m \leq r^m$. Kluczową obserwacją jest niearchimedesowość ciała.

Podsumowując, $|\beta_{mn}| \leq |a_n| r^n$, co nie zależy od m i daje jednostajną zbieżność. □

Nasze życie nie jest usłane różami tak bardzo jak w analizie zespolonej. Indykator $\mathbb{Z}_p$ w $\mathbb{Q}_p$ jest lokalnie analityczny, jednak czujemy opory przed nazwaniem go analitycznym. Te i inne problemy można obejść, lecz wymaga to wiele wysiłku. Chodzi tu o podstawy *sztywnej geometrii analitycznej*, której fundamenty wyłożył Tate.

Zamiast tego zajmiemy się innymi, prostszymi rzeczami. Zbieżny ciąg nazwiemy stacjonarnym, jeśli jest od pewnego miejsca stały. Jeśli funkcja jest zadana rozwinięciem w szereg potęgowy, to przedstawienie jest jednoznaczne.

Fakt 2.3.8. *Istnienie niestacjonarnego ciągu $x_m \in \mathbb{Q}_p$ zbieżnego do zera dla formalnych szeregów potęgowych f, g, że $f(x_m) = g(x_m)$, pociąga ich równość: $f \equiv g$.*

Dowód. Bez straty ogólności $x_m \neq 0$. Popatrzmy na różnicę, $h(x) = f(x) - g(x) = \sum_n a_n x^n$. Wiemy, że $h(x_m) = 0$, ale czy $a_n = 0$? Załóżmy, że nie, niech r będzie najmniejszym indeksem, dla którego $a_r \neq 0$, by $h(x) = x^r h_1(x)$. Przy tym $h_1(0) = a_r \neq 0$ i funkcja h_1 jest ciągła, więc $h_1(x_m) \to a_r$ gdy $m \to \infty$, w szczególności $h_1(x_m)$ jest niezerem dla dużych m. Wtedy $h(x_m) = x_m^r h_1(x_m)$ nie jest zerem, sprzeczność. □

Jeżeli funkcja jest zdefiniowana jako szereg potęgowy, to niech lepiej jej pochodna odpowiada „formalnej" pochodnej dla formalnego szeregu potęgowego.

Fakt 2.3.9. *Formalne zróżniczkowanie szeregu nie zmniejsza jego promienia zbieżności, a przy tym pokrywa się z „analityczną" definicją pochodnej (jako granicy ilorazów): $f(x) = \sum_n a_n x^n$.*

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}.$$

Dowód. Pokażemy najpierw, że granica nie jest bez sensu. Gdy $x = 0$, to każde h z $|h| < R$ jest w porządku. Jeżeli tak nie jest, to $|h| < |x|$ też nie będzie takie złe.

Załóżmy, że $f(x)$ zbiega, zatem $a_n x^n \to 0$. Jeżeli $x \neq 0$, to $|n a_n x^{n-1}| \leq |a_n x^{n-1}| = |a_n x^n| / |x| -$ co wystarcza do zbieżności pochodnej.

Szereg $f(x)$ zbiega w domkniętej lub otwartej kuli $\mathcal{B}(0, R)$. W pierwszym przypadku niech $r = R$; w drugim bierzemy dowolne r, że $|x| \leq r < R$. Możemy do tego założyć, że jeśli $x \neq 0$, to $|h| < |x| \leq r$, bo interesują nas tylko h bliskie zera. W przeciwnym razie, $x = 0$ i po prostu $|h| \leq r$. Teraz,

$$f(x+h) = \sum_{n=0}^{\infty} a_n \sum_{m=0}^{n} \binom{n}{m} x^{n-m} h^m$$

$$\frac{f(x+h) - f(x)}{h} = \sum_{n=1}^{\infty} \sum_{m=1}^{n} a_n \binom{n}{m} x^{n-m} h^{m-1}.$$

Wiemy dobrze, że $|x|, |h| \leq r$, zatem:

$$\left| a_n \binom{n}{m} x^{n-m} h^{m-1} \right| \leq |a_n| r^{n-1},$$

Dzięki $|a_n| R_1^n \to 0$ możemy wywnioskować jednostajną zbieżność względem h, co pozwala wzięcie granicy wyraz po wyrazie (to znaczy: $h = 0$). □

Otrzymany wynik ma „efekty uboczne", gdyż wynika z niego ciekawe twierdzenie o pochodnych. Dwie p-adyczne funkcje mogą mieć tę samą pochodną i nie różnić się o stałą. Szeregi nigdy nas jednak nie zawiodą.

Fakt 2.3.10. *Jeśli szeregi potęgowe $f(x)$ oraz $g(x)$ są zbieżne dla $|x| < R$ oraz $f'(x) = g'(x)$ dla $|x| < R$, to istnieje stała $c \in \mathbb{Q}_p$, że $f(x) = g(x) + c$ jako szeregi potęgowe (więc oba mają jeden obszar zbieżności).*

Dowód. Jeżeli $f(x) = \sum_{n=0}^{\infty} a_n x^n$ i $g(x) = \sum_{n=0}^{\infty} b_n x^n$ mają formalne pochodne $f'(x)$ i $g'(x)$, to z faktów 2.3.8 oraz 2.3.9 wnioskujemy równości $a_n = b_n$ dla $n \geq 1$. □

Twierdzenie 5 (Strassman, 1928). *Jeżeli niezerowy ciąg $a_n \in \mathbb{Q}_p$ zbiega do zera, to funkcja od szeregu $f(x) = \sum_{n \geq 0} a_n x^n$ ma za dziedzinę co najmniej $\mathbb{Z}_p$, gdzie ma co najwyżej N zer: N to ostatni indeks n, dla którego $|a_n|$ jest maksymalne.*

Dowód. Dla dowodu warto znać p-adyczne tw. Weierstraßa o *preparacji,* ale nie trzeba. 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, nie może być $f(x) = 0$, bo

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

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

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

Lemat 2.1.6 pozwala na przegrupowanie:

$$f(x) = (x - y) \sum_{m \geq 0} b_m x^m \quad \bullet \quad b_m = \sum_{k \geq 0} a_{m+1+k} y^k$$

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

$$|b_m| \leq \max_{k \geq 0} |a_{m+k+1}| \leq \max_{m \geq N+1} |a_m| < |a_N|.$$

Liczba z twierdzenia dla $(x - y)^{-1} f(x)$ to $N - 1$, koniec. □

Twierdzenie Strassmana jest pierwszym potężnym o zerach szeregów potęgowych na $\mathbb{Q}_p$. Jeśli $f(x) = \sum_n a_n x^n$ nie jest zerem i zbiega na $p^m \mathbb{Z}_p$ dla pewnego m, to ma tam skończenie wiele zer (dowód: $g(x) = f(p^m x)$). Dwa szeregi zbieżne w $p^m \mathbb{Z}_p$ i pokrywające się dla ∞-wielu wartości są sobie równe (dowód: patrz na $f(x) - g(x)$). Niespodzianka!

Fakt 2.3.11. *Okresowa funkcja $p^m\mathbb{Z}_p \to \mathbb{Q}_p$ określona zbieżnym na $p^m\mathbb{Z}_p$ szeregiem potęgowym $\sum_n a_n x^n$ jest stała.*

Dowód. Niech $t \in p^m\mathbb{Z}_p$ będzie okresem. Szereg $f(x) - f(0)$ ma zera w nt dla $n \in \mathbb{Z}$. To daje nieskończenie wiele zer, więc różnica musi być zerem, czyli $f(x)$ jest stały. □

To zupełnie nie przypomina przypadku $\mathbb{R}$: sinus i kosinus są okresowe i entiére! Powodem jest to, że w $\mathbb{R}$ nie może być tak, że wszystkie wielokrotności okresu leżą w przedziale (ale w $\mathbb{Q}_p$ już tak). Chociaż okresowość w $\mathbb{R}$ nie pokrywa się z tą w $\mathbb{Q}_p$, to zera entiére są podobnie rozłożone.

Fakt 2.3.12. *Zbieżny na $\mathbb{Q}_p$ szereg potęgowy $f(x) = \sum_n a_n x^n$ ma co najwyżej przeliczalnie wiele zer. Tworzą one ciąg x_n z $|x_n| \to \infty$, jeśli jest ich nieskończenie wiele.*

Dowód. Liczba zer w każdym ograniczonym dysku $p^m\mathbb{Z}_p$ jest skończona. □

Rozdział 3

Analiza z plusem

Jakie własności mają ciągłe funkcje określone na podzbiorach p-adycznego ciała $\mathbb{Q}_p$ o wartościach w rozszerzeniach $\mathbb{Q}_p$? To pytanie, na które spróbujemy odpowiedzieć. $\mathbb{Q}_p$ rozbija się na otwarnięte kule $x + \mathbb{Z}_p$ dla $x \in \mathbb{Q}_p/\mathbb{Z}_p = \mathbb{Z}[1/p]/\mathbb{Z}$, można ograniczyć się do ciągłych funkcji określonych na $\mathbb{Z}_p$.

W $\mathbb{R}$-analizie ciągłe funkcje na odcinku są jednostajnymi granicami wielomianów. W analizie p-adycznej wielomiany te można kanonicznie wybrać (to zasługa Mahlera). Van Hamme zastąpił współczynniki dwumianowe innymi wielomianami, tak zrodził się rachunek cienisty.

Ziarnista struktura $\mathbb{Z}_p$ sprawia, że lokalnie stałe funkcje są gęstą podprzestrzenią $\mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$ i zastępują funkcje skokowe z $\mathbb{R}$-analizy.

3.1 Ciągi, różnice, sploty

Wielomian $f \in \mathbb{Q}[x]$ może spełniać zależność $f[\mathbb{N}] \subseteq \mathbb{Z}$, nawet gdy nie ma całkowitych współczynników. Taki jest na przykład $\frac{1}{p}(x^p - x)$.

Definicja 3.1.1. $(\nabla f)(x) = f(x+1) - f(x)$ *określa operator skończonej różnicy.*

Elementarne rachunki pokazują, że $\nabla(x \text{ nad } 0) = 0$ oraz $\nabla(x \text{ nad } i) = (x \text{ nad } i-1)$. Przypomina to zwykłą pochodną i wielomiany $f_n = x^n/n!$, $f_n' = f_{n-1}$, $f_0' = 0$. Analogię ze wzorem Taylora rozwija następujący fakt.

Fakt 3.1.2. *Jeśli $f : \mathbb{N} \to M$ jest funkcją w grupę abelową (czyli $\mathbb{Z}$-moduł), to istnieje dokładnie jeden ciąg $m_i \in M$, że*

$$f(x) = \sum_{i \geq 0} m_i \binom{x}{i} = \sum_{i \geq 0} \frac{\nabla^i f(0)}{i!} \cdot (x)_i$$

Dowód. Łatwo widać, że $m_k = \nabla^k f(0)$ są w porządku. Choć nieskończenie wiele z nich będzie niezerami, to ustalenie x czyni sumę skończoną. $\square$

Nadmieńmy: $\Delta^k f(0) = \sum_{i \le k} (-1)^{k-i} (k \text{ nad } i) f(i)$ jest formułą odpowiadającą funkcjom tworzącym:

$$\sum_{k=0}^{\infty} \Delta^k f(0) \frac{x^k}{k!} = e^{-x} \sum_{n=0}^{\infty} f(n) \cdot \frac{x^n}{n!}.$$

Fakt 3.1.3. *$\mathbb{Z}$-moduł $\mathcal{L} \subseteq \mathbb{Q}[x]$ wszystkich funkcji spełniających warunek $f[\mathbb{N}] \subseteq \mathbb{Z}$ jest wolny, ma bazę złożoną z $(\cdot$ nad $i)$.*

Powinniśmy rozpatrzyć przypadek, gdzie $\mathbb{Z}$-moduł M jest przestrzenią wektorową nad ciałem $\mathbb{F}_p$.

Lemat 3.1.4. *Przestrzeń funkcji $\mathbb{Z} \to \mathbb{F}_p$, których okres to $T = p^t$, ma bazę złożoną z $x \mapsto (x$ nad $i)$ mod p dla $0 < i < T$.*

Fakt 3.1.5. *Każda p^t-okresowa funkcja $f\colon \mathbb{Z} \to \mathbb{F}_p^n$ zapisuje się jednoznacznie jako $f(x) = \sum_{i \le T} (x$ nad $i) m_i$ dla $m_i \in \mathbb{F}_p^n$.*

Jeżeli $\mathcal{R}$ jest przemiennym pierścieniem, zaś $f, g\colon \mathbb{N} \to \mathcal{R}$ funkcjami, to ich przesuniętym splotem jest $(f \oslash g)(0) = 0$, $(f \oslash g)(n) = \sum_{i=0}^{n-1} f(i) g(n-i-1)$. Iterowaną różnicę splotu opisuje: $\nabla^n (f \oslash g) = f \oslash \nabla^n g + \sum_{k=0}^{n-1} \nabla^k f \, \nabla^{n-k-1} g(0)$.

Skoro operator różnicy udaje pochodną, to co może być dobrym kandydatem na całkę? Dla każdej funkcji $f\colon \mathbb{N} \to \mathcal{R}$ istnieje jedyna *pierwotna* $F\colon \mathbb{N} \to \mathcal{R}$, że $\nabla F = f$, $F(0) = 0$.

Definicja 3.1.6. *Operator sumy nieoznaczonej Ƨ to $f \mapsto 1 \oslash f$, to znaczy $(\text{Ƨ} f)(0) = 0$ oraz $(\text{Ƨ} f)(n) = \sum_{i=0}^{n-1} f(i)$.*

Przykład 3.1.7. $\text{Ƨ}(x$ *nad* $i) = (x$ *nad* $i+1)$.

Jeżeli przez $P_0\colon A^{\mathbb{N}} \to A$ oznaczymy rzut na funkcje stałe ($f \mapsto f(0) \cdot 1$), to będziemy mogli zapisać trzy nowe zależności.

Fakt 3.1.8. $\nabla \circ \text{Ƨ} = \mathrm{id}$, $\text{Ƨ} \circ \nabla = \mathrm{id} - P_0$, $\nabla \circ \text{Ƨ} - \text{Ƨ} \circ \nabla = P_0$.

Druga tożsamość przepisana do $f(x) = f(0) + \text{Ƨ} \nabla f(x)$ daje nam ograniczone rozwinięcie f pierwszego rzędu. Właśnie tak van Hamme uzyskał następujący wynik.

Twierdzenie 6 (van Hamme)**.** *Funkcje f zmiennej całkowitej mogą zostać rozwinięte (dla całkowitego $n \ge 0$) z resztą van Hamme'a, $R_{n+1} f(x) = \nabla^{n+1} f \oslash (x$ nad $n)$.*

$$f(x) = f(0) \cdot 1 + R_{n+1} f(x) + \sum_{k=1}^{n} \nabla^k f(0) \cdot \binom{x}{k}.$$

3.2 Ciągłość na $\mathbb{Z}_p$

Przed lekturą tego ustępu warto przypomnieć sobie definicję i podstawowe własności jednostajnej zbieżności.

Punktowa granica ciągłych funkcji z X (topologicznej) w M (zupełną metryczną) jest ciągła, jeśli jednostajna.

Jeśli ustalimy ciągłą injekcję $\varphi\colon \mathbb{Z}_p \to \mathbb{R}$ (choćby liniowy model $\mathbb{Z}_p$), to możemy przybliżać jednostajnie wielomianami od φ ciągłą $f\colon \mathbb{Z}_p \to \mathbb{R}$. Istotnie, algebra wielomianów od

φ jest podalgebrą wszystkich ciągłych $\mathbb{Z}_p \to \mathbb{R}$, która rozdziela punkty ($\mathbb{Z}_p$ jest zwarta). Tw. Stone'a-Weierstraßa orzeka, że ta podalgebra jest gęsta z jednostajną zbieżnością.

Niech $f\colon \mathbb{Z}_p \to \mathbb{C}_p$ będzie ciągła. Funkcja $|f|\colon \mathbb{Z}_p \to \mathbb{R}$ też jest ciągła i osiąga supremum. Dokładniej, zbiór $f[\mathbb{Z}_p] \subseteq \mathbb{C}_p$ jest zwarty, zaś $\{|f(x)| \neq 0 : x \in \mathbb{Z}_p\} \subseteq \mathbb{R}_+$: dyskretny.

Definicja pierścienia topologicznego $\mathcal{R}$ pokazuje, że każdy wielomian $f \in \mathcal{R}[x]$ zadaje ciągłą funkcję $\mathcal{R} \to \mathcal{R}$. Kolejnymi źródłami ciągłych funkcji są:

1. wielomiany z $\mathbb{C}_p[x]$ po obcięciu do $\mathbb{Z}_p$
2. szeregi potęgowe $\sum_{i\geq 0} a_i x^i$ z $a_i \in \mathbb{C}_p$, $|a_i| \to 0$.

Definicja 3.2.1. *Dla ciągłej funkcji $f\colon \mathbb{Z}_p \to \mathbb{C}_p$ przyjmijmy, że $\|f\| = \sup_{x\in\mathbb{Z}_p} |f(x)| = \max_{x\in\mathbb{Z}_p} |f(x)|$.*

Jest jasne, że wielomiany dwumianowe wyznaczają ciągłe funkcje $f_k\colon \mathbb{Z}_p \to \mathbb{Z}_p, x \mapsto (x \text{ nad } k)$. Zbiór $\mathbb{N}$ jest gęsty w $\mathbb{Z}_p$, zatem $\|f_k\| = \sup_{\mathbb{N}} |(n \text{ nad } k)| \leq 1$. Ponieważ $(k \text{ nad } k) = 1$, mamy nawet równość.

Zanim pójdziemy śladami Mahlera, żeby odwrócić proste spostrzeżenie sprzed akapitu, określimy użyteczne szeregi, które nazwano zresztą jego nazwiskiem.

Definicja 3.2.2. *Szereg Mahlera dla $a_k \in \mathbb{C}_p$ (Ω_p), że $|a_k| \to 0$ to $\sum_{k\geq 0} a_k(x \text{ nad } k)$.*

Jeśli szereg dwumianowy zbiega dla wszystkich $x \in \mathbb{Z}_p$ (lub dla samego $x = -1$), to czyni to jednostajnie. Ze zbieżności w -1 wynika, że $a_k(-1 \text{ nad } k) = \pm a_k \to 0$ i $|a_k| \to 0$.

Twierdzenie 7 (Mahler). *Niech funkcja $f\colon \mathbb{Z}_p \to \mathbb{C}_p$ będzie ciągła, $a_k = \nabla^k f(0)$. Wtedy $|a_k| \to 0$, zaś szereg $\sum_{k\geq 0} a_k(x \text{ nad } k)$ zbiega jednostajnie do $f(x)$. Co więcej, $\|f\| = \sup_{k\geq 0} |a_k|$.*

Dowód. Bez straty ogólności, zastąpmy $f \neq 0$ przez $f/f(x_0)$, gdzie $x_0 \in \mathbb{Z}_p$ maksymalizuje $|f(x)|$. Teraz obraz f leży w $\mathcal{O}$.

Rozważmy iloraz $E = \mathcal{O}/p\mathcal{O}$ jako przestrzeń liniową nad ciałem prostym $\mathbb{F}_p$. Złożenie $\varphi = f \bmod p\colon \mathbb{Z}_p \to \mathcal{O}_p \to E$, jest ciągłe (przyjmuje skończenie wiele wartości, jest lokalnie stałe), ale nie jest stale zerem. Jest jednostajnie ciągłe, a także jednostajnie lokalnie stałe ($\mathbb{Z}_p$ jest zwarte).

To oznacza, że φ jest stała na warstwach modulo $p^t\mathbb{Z}_p$ dla dużych t, czyli p^t-okresowa na $\mathbb{Z}$. Skorzystamy więc z faktu 3.1.4. Niech $T = p^t$. Zapiszmy φ tak, jak niżej, przy czym znaczenie sztyletu † jest nieznane: $\varphi(x) = \sum_{k<T} \alpha_k(x \text{ nad } k)^\dagger$.

Weźmy reprezentantów $a_k^0 \in \mathcal{O}$ dla α_k. Przynajmniej raz $|a_k^0| = 1$, gdyż różnica $\sum_{k<T} a_k^0 f_k - f$ przyjmuje wartości w $p\mathcal{O}$. Wiemy, że $|a_k^0| \leq 1$. Z naszej konstrukcji wynika, że jest $\|f(x) - \sum_{k<T} a_k^0(x \text{ nad } k)\| = r \leq |p|$. Jeśli różnica nie jest 0, możemy powtórzyć proces: znaleźć $S > T$ i współczynniki a_k^1, że $|a_k^1| \leq r$, $\max|a_k^1| = r$. Drobne nagięcie oznaczeń prowadzi przez $a_k^0 = 0$ dla $k \geq T$ do

$$\left| f(x) - \sum_{k=0}^{S-1} (a_k^0 + a_k^1) \cdot \binom{x}{k} \right| = r' \leq |p^2|.$$

Jest jasnym, że po nieskończenie wielu krokach otrzymamy zbieżne szeregi $a_k = a_k^0 + a_k^1 + \ldots \in \mathbb{C}_p$, że $|a_k^n| \leq |p^n| \to 0$. Zachodzi przy tym $\sup_{k>0} |a_k| = \sup_{k<T} |a_k| = 1 = \|f\|$ i to już koniec: $\|f(x) - \sum_{k\geq 0} a_k(x \text{ nad } k)\| < |p|^m$, $m \in \mathbb{N}$. □

Wniosek 3.2.3. *Ciągłe funkcje $\mathbb{Z}_p \to \mathbb{C}_p$ to dokładnie jednostajne granice wielomianów z $\mathbb{C}_p[X]$.*

Znajomość jednostajnej zbieżności, zwartych przestrzeni metrycznych, funkcji ciągłych i twierdzenia Mahlera pozwala przeprowadzić częściowo indukcyjny dowód następującego faktu.

Fakt 3.2.4. *Następujące warunki są sobie równoważne dla funkcji $f : \mathbb{N} \to \mathbb{C}_p$ oraz $a_k = \nabla^k f(0)$: $|a_k| \to 0$; $\| \nabla^k f\| \to 0$; f ma ciągłe przedłużenie do $\mathbb{Z}_p \to \mathbb{C}_p$; f jest jednostajnie ciągła (na $\mathbb{N}$ z topologią od $\mathbb{Z}_p$); szereg Mahlera dla f zbiega jednostajnie.*

Twierdzenie Mahlera ma ciekawe zastosowania dla splotów (przesuniętych). Okazuje się, że dzięki temu można oszacować resztę w skończonym rozwinięciu Mahlera. Przypomnijmy,

$$|(f \oslash g)(n)| \leq \max |f(i)g(n-i-1)| \leq \|f\| \cdot \|g\|$$

Fakt 3.2.5. *Przesunięty splot $f \oslash g$ ciągłych funkcji $\mathbb{Z}_p \to \mathbb{C}_p$ daje się przedłużyć do ciągłej funkcji $\mathbb{Z}_p \to \mathbb{C}_p$.*

Dowód. Pokażemy, że $\nabla^k (f \oslash g)(0) \to 0$. Wróćmy do

$$\nabla^{2n+1}(f \oslash g) = \sum_{i+j=2n} \nabla^i f \cdot \nabla^j g(0) + f \oslash \nabla^{2n+1} g$$

Dla ograniczonej funkcji h ultrametryka daje $\| \nabla h\| \leq \|h\|$. Rozbijemy lewą stronę powyższego równania na trzy człony.

$$\begin{aligned}
\left| \sum_{i=n}^{2n} \nabla^i f(0) \cdot \nabla^{2n-i} g(0) \right| &\leq \| \nabla^n f\| \cdot \|g\| \\
\left| \sum_{i=0}^{n-1} \nabla^i f(0) \cdot \nabla^{2n-i} g(0) \right| &\leq \|f\| \cdot \| \nabla^n g\| \\
\left| (f \oslash \nabla^{2n+1} g)(0) \right| &\leq \|f\| \cdot \| \nabla^{2n+1} g\| \\
&\leq \|f\| \cdot \| \nabla^n g\|
\end{aligned}$$

Prawe strony nierówności dążą do 0, gdy n rośnie. Można podać podobne oszacowania dla ∇^{2n} miast ∇^{2n+1}. $\square$

Wniosek 3.2.6. *Twierdzenie van Hamme'a jest prawdziwe także dla $f : \mathbb{Z}_p \to \mathbb{C}_p$, z oszacowaniem $\|R_{n+1}f\| \leq \| \nabla^{n+1} f\| \to 0$.*

Wniosek 3.2.7. *Jedyną liniowa formą $C(\mathbb{Z}_p, \mathcal{K}) \to \mathcal{K}$, która jest odporna na przesuwanie, jest forma zerowa: $\varphi \equiv 0$.*

Dowód. Ustalmy $f \in C(\mathbb{Z}_p, \mathcal{K})$ z pierwotną $F = \text{Ƨ}\, f$. Wtedy $\varphi(f(x)) = \varphi(F(x+1)) - \varphi(F(x)) = 0$. $\square$

Przykład 3.2.8. *Funkcja $f : \mathbb{Z}_p \backslash \{1\} \to \mathbb{Q}_p$ jest nieograniczona, ale ciągła: $f(x) = \sum_{n \geq 0} (x$ nad $p^{2n} - 1) p^{-}$*

Człowiek może się zastanawiać, dlaczego w definicje szeregu Mahlera pojawiają się symbole Newtona, a nie zwykłe potęgi x.

Fakt 3.2.9. *Funkcje $f_n(x) = x^n$ nie tworzą ortonomalnej bazy p. funkcji ciągłych, ograniczonych z $\mathcal{O} \subseteq \mathcal{K}$ (zupełnego) w L, „BC".*

Dowód. Liniowo niezależne funkcje f_n mają normę 1. Jeśli L nie jest lokalnie zwarta, zbiór $\{f_n\}$ jest ortonormalny, ale jego L-liniowa powłoka nie jest gęsta w „BC".

Jeśli jednak jest, to f_n nie są zbiorem ortogonalnym (!), choć ich L-powłoka jest gęsta wśród ciągłych $X \to L$. □

3.3 Lokalna stałość

Definicja 3.3.1. *Funkcja $X \to Y$ jest stała lokalnie, jeśli jest ciągła (z dyskretną topologią na Y).*

Funkcje $X \to \mathcal{K}$ (w ciało) tworzą przestrzeń wektorową nad $\mathcal{K}$, $\mathcal{F}(X)$. Jeżeli X jest zwarta i ultrametryczna, to lokalnie stałe $X \to \mathcal{K}$ stanowią podprzestrzeń $\mathcal{F}^{lc}(X)$, generowaną przez indykatory otwarniętych kul w X.

Przyjrzyjmy się lokalnie stałym funkcjom $f\colon \mathbb{Z}_p \to \mathcal{G}$ (w grupę abelową), takim że $|x-y| \leq p^{-j}$ pociąga $f(x) = f(y)$ dla ustalonej liczby całkowitej $j \geq 0$. Na domkniętych kulach o promieniu p^{-j} są one stałe. Ponieważ to są warstwy $p^j\mathbb{Z}_p$ w $\mathbb{Z}_p$, wybrane przez nas funkcje należą do $F_j = \mathcal{F}(\mathbb{Z}_p/p^j\mathbb{Z}_p)$. Tak naprawdę mamy partycję $\mathbb{Z}_p = \coprod_{i<p^j}(i+p^j\mathbb{Z}_p)$ na kule. Indykatory kul $\mathcal{B}(i, p^{-j})$ dla $0 \leq i < p^j$ tworzą bazę F_j, która jest p. wektorową skończonego wymiaru. Choć zwiększenie j zwiększa F_j: $\mathcal{F}^l(\mathbb{Z}_p, \mathcal{K}) = \bigcup_{j\geq 0} F_j$, to bazy dla F_j i F_{j-1} nie mają ze sobą wiele wspólnego.

Van der Put był sprytniejszy w szukaniu baz. Zdefiniujmy funkcję $\psi_i = \varphi_{i,j}$ jako indykator $i + p^j\mathbb{Z}_p$, gdy $p^{j-1} \leq i < p^j$.

Wartości bezwzględne elementów $\mathbb{Z}_p$ to potęgi p, zatem $|x| < 1/i$, wtedy i tylko wtedy gdy $|x| \leq p^{-j}$. Długością liczby całkowitej $i \geq 1$jest liczba $v \geq 1$, że w rozwinięciu i w systemie o podstawie p „ostatnia" cyfra to $i_{v-1} \neq 0$.

Fakt 3.3.2 (i definicja)**.** *Ciąg van der Puta $\{\psi_i\}_{i=0}^{p^j-1}$ jest bazą F_j, gdzie $j \geq 1$ i $\psi_i = \varphi_{i,v(i)}$.*

Można powiedzieć więcej o takiej bazie. Mianowicie jeżeli $f = \sum_i a_i\psi_i \in F_j$, to $a_0 = f(0)$ i dla każdego $n \geq 1$ zachodzi $a_n = f(n) - f(n_-)$. Tutaj przez n_- rozumiemy $n - n_{v-1}p^{v-1}$, liczbę powstałą z n przez wymazanie najstarszej cyfry. Zanim przejdziemy do dużego twierdzenia, podsumujmy to, co mamy.

Fakt 3.3.3. *Niech $f\colon \mathbb{Z}_p \to \mathcal{K}$ będzie lokalnie stałą funkcją. Połóżmy $a_n = f(n) - f(n_-)$ i $a_0 = f(0)$. Wtedy $\|f\| = \sup_i |a_i|$, zaś samą f można zapisać jako skończoną sumę $\sum_i a_i\psi_i$.*

Twierdzenie, do którego małymi krokami się zbliżaliśmy, podałoby reprezentację każdej funkcji w zupełne rozszerzenie $\mathbb{Q}_p$, gdyby nie luki wielkie jak kanion.

Twierdzenie 8 (van der Put)**.** *Funkcja $f\colon \mathbb{Z}_p \to \mathcal{K}$ niechaj będzie ciągła. Jeśli $a_0 = f(0)$, $a_n = f(n) - f(n_-)$, to ciąg $|a_n|$ dąży do zera, szereg $\sum_i a_i\psi_i$ zbiega jednostajnie do f i $\|f\| = \sup_i |a_i|$.*

3.4 Rachunek cienisty

Niech ciało $\mathcal{K}$ ma charakterystykę 0. Będziemy teraz pracować w $\mathcal{V} = \mathcal{K}[x]$. Określmy $\mathcal{V}_n = \{f \in \mathcal{K}[x] : \deg f \leq n\} \leq \mathcal{V}$.

Definicja 3.4.1. *Translacje to liniowe operatory w $\mathcal{K}[x]$ dane wzorem $(\tau_a f)(x) = f(x+a)$.*

Definicja 3.4.2. *Operator dorzecza to liniowy endomorfizm δ dla $\mathcal{K}[x]$, który komutuje z translacjami i spełnia $\delta(x) = c \in \mathcal{K}^\times$.*

Fakt 3.4.3. *Operatory dorzecza spełniają $\delta[\mathcal{K}] = \{0\}$. Jeśli f jest niestałym wielomianem, to* $\deg f - \deg(\delta f) = 1$.

Dowód. Mamy $c = \tau_a c = \tau_a \delta x = \delta \tau_a x = \delta(x+a) = c + \delta a$, więc $\delta a = 0$ dla stałych $a \in \mathcal{K}$. Pokażemy, że $\deg \delta x^n = n - 1$ dla $n \geq 1$. Niech $\delta x^n = f(x)$. Wtedy

$$\begin{aligned} f(x+a) &= \tau_a f(x) = \delta \tau_a (x^n) = \delta(x+a)^n \\ &= \sum (n \text{ nad } k) a^k \delta x^{n-k}. \end{aligned}$$

Podstawmy w tym wzorze najpierw $x = 0$, a potem $a = x$. Tak otrzymamy $f(x) = \sum (n \text{ nad } k) \delta(x^{n-k}$
Widać, że f jest wielomianem stopnia $\leq n$, którego współczynnik przy x^n to $\delta(1)(0) = 0$. Kolejny, wiodący, to $n \delta x(0) = nc \neq 0$, gdyż $\mathcal{K}$ było charakterystyki zero. □

Wniosek 3.4.4. *Mamy $\delta[\mathcal{V}_n] = \mathcal{V}_{n-1}$.*

Tuż za rogiem czai się cała gromadka operatorów dorzecza.

Przykład 3.4.5. *Operator różniczkowania $\mathfrak{D}$, ogólniej $\tau_a \mathfrak{D}$.*

Przykład 3.4.6. *Operator różnicy $\tau_a \nabla$ (w szczególności $a = 0$).*

Przykład 3.4.7. *Formalny szereg od $\mathfrak{D}$ rzędu 1, $\sum_i c_i \mathfrak{D}^i \in \mathcal{K}[[\mathfrak{D}]]$: na przykład* $\log 1 + \mathfrak{D}$, $-1 + \exp \mathfrak{D}$ *albo* $\mathfrak{D}^2 / (\exp \mathfrak{D} - 1)$.

Definicja 3.4.8. *Układ podstawowy dla operatora dorzecza δ to ciąg wielomianów, że* $\deg p_n = n$, $\delta p_n = n p_{n-1}$, $p_n(0) = [n = 0]$.

Prosty arguent indukcyjny pokazuje, że jest wyznaczony jednoznacznie. Pozwala to na napisanie „wzoru Taylora".

Fakt 3.4.9. *Dla operatora dorzecza δ z ciągiem podstawowym p_n w $\mathcal{K}[X]$ mamy rozwinięcie dla $f \in \mathcal{K}[X]$:*

$$f(x+y) = \sum_{k=0}^{\infty} \frac{\delta^k f(x)}{k!} \cdot p_k(y).$$

To pierwsza inkarnacja rachunku ciernistego, z jaką się spotykamy. Jeśli za f wstawimy p_n, dostaniemy:

$$p_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} p_k(x) \cdot p_{n-k}(y)$$

Definicja 3.4.10. *Operator kompozytowy to endomorfizm $\mathcal{K}[x]$, który komutuje z translacjami.*

Fakt 3.4.11. *Operatory kompozytowe wśród endomorfizmów T dla $\mathcal{K}[x]$ scharakteryzowane są przez następujęce warunki: T komutuje z translacją jednostkową, każdą, derywacją $\mathfrak{D}$, operatorami dorzecza; jest formalnym szeregiem potęgowym od $\mathfrak{D}$ lub operatora dorzecza δ (nad $\mathcal{K}$).*

Niech T będzie ciągłym endomorfizmem $C(\mathbb{Z}_p, \mathcal{K})$, gdzie $\mathcal{K}$ to zupełne rozszerzenie $\mathbb{Q}_p$. Jeśli komutuje z translacjami, to nie rusza $\ker \nabla^n \subseteq C(\mathbb{Z}_p)$.

Lemat 3.4.12. $\ker \nabla^n \subseteq C(\mathbb{Z}_p)$ *to wielomiany stopnia* $\leq n$.

Z trochę większą wiedzą można uogólnić wynik Mahlera tak, jak zrobił to van Hamme. Zapiszmy

$$T = \sum_{n \geq v} \alpha_n \nabla^n \in \mathcal{K}[[\nabla]].$$

Fakt 3.4.13. *Ciągły endomorfizm* T *dla* $C(\mathbb{Z}_p)$ *komutujący z* ∇ *z* $T(1) = 0$ *i* $\|T\| = |\alpha_1| = 1$ *indukuje operator dorzecza na* $\mathcal{K}[x]$ *z układem* p_n: $\deg p_n = n$, $T(p_n) = np_{n-1}$, $p_n(0) = [n = 0]$, *a przy tym* $\|p_n\| = n!$.

Dowód. Po normalizacji układu $q_n = p_n/n!$ chcemy pokazać, że $\|q_n\| = 1$. Być może T też wymaga zmiany na T/α_1, ale i tak ostatecznie napiszemy (z $\alpha_1 = 1$):

$$1 = \|q_0\| = \|Tq_1\| \leq \|q_1\| = \|Tq_2\| \leq \cdots.$$

Z założenia, $T = \nabla + \alpha_2 \nabla^2 + \cdots = \nabla U$, kompozytowy operator U odwraca się ($V = U^{-1}$) i $\|U\| = 1$. Twierdzimy, że istnieje S, odwracalny i ciągły operator kompozytowy, $\|S\| = 1$, że $q_n = SV^n(f_n)$, gdzie przez f_n tymczasowo oznaczamy współczynniki dwumianowe nad n ($\nabla f_n = f_{n-1}$).

Niezależnie od S (jeśli jest rzędu 0), ta definicja prowadzi do wielomianów stopnia $\deg q_n = n$ i $Tq_n = \nabla U \circ SV^n(f_n)$, a skoro $UV = 1$ i operatory komutują, $Tq_n = q_{n-1}$.

Pozostało znaleźć takie S, by $q_n(0) = 0$ dla $n \geq 1$. Niech $S = I - \nabla V'U$, gdzie V' jest formalną pochodną V. Wtedy

$$\begin{aligned} SV^n(f_n) &= (I - \nabla(V'/V)) \circ V^n(f_n) \\ &= (V^n - \nabla V^{n-1}V')(f_n). \end{aligned}$$

Operatory są szeregami formalnymi w ∇ i $\nabla^k f_n = f_{n-k}$ znika w początku dla $k < n$. Jedyny interesujący człon to w takim razie jednomian zawierający $\nabla^n f_n$. Ale jeśli $\varphi(t)$ jest formalnym szeregiem, to współczynnik w $\varphi^n - t\varphi^{n-1}\varphi'$ (czyli $\varphi^n - (t/n)(\varphi^n)'$) przy t^n jest zerem. Wynika stąd, że zerem jest też wyraz wolny $SV^n(f_n)$ i $q_n(0) = 0$.

Operatory z definicji S miały normy ≤ 1, zatem $\|S\| \leq 1$ i $\|q_n\| \leq \|S\|\|V^n\|\|f_n\| = 1$. $\square$

Fakt 3.4.14. *Przy założeniach z poprzedniego faktu, każda ciągła funkcja* f *z* $C(\mathbb{Z}_p)$ *daje się rozwinąć w uogólniony szereg Mahlera z* $c_n = (T^n f)(0) \to 0$ *i* $\|f\| = \sup_{n \geq 0} |c_n|$: $f(x) = \sum_n c_n q_n$.

Dowód. Przy oznaczeniach z poprzedniego faktu, $T = \nabla U$ pociąga $|T^n f(0)| \leq \|U^n \nabla^n f\| \leq \| \nabla^n f$ (na mocy tw. Mahlera). Wystarczy ograniczyć się do wielomianów, ogólny przypadek wyniknie z gęstości i ciągłości. Wzór Taylora dla f przybiera postać $f = \sum_{n \geq 0} (T^n f)(0) q_n$. Skoro $\|q_n\| = 1$, to $\|f\| \leq \sup |c_n|$. Prawdziwa jest również nierówność w drugą stronę: $|c_n| \leq \|T^n f\| \leq \|T^n\|\|f\| \leq \|T\|^n \|f\| \leq \|f\|$. $\square$

Uogólnione rozwinięcie Mahlera nie jest prawdziwe dla $\mathfrak{D}$ (różniczkowania): operator ten nie rozszerza się ciągle na całe $C(\mathbb{Z}_p)$. Cokolwiek to nie znaczy, wygląda niepokojąco. Nawet jeśli $f(x) = \sum_n c_n x^n/n!$ zbiega jednostajnie, zazwyczaj $\|f\|$, $\sup |f(x)|$ nie jest równe $\sup |c_n|$.

Zilustrujemy teraz ważną zasadę, o której to mowa będzie dopiero później.

Przykład 3.4.15. *Ciąg podstawowy dla* $\tau_a \mathfrak{D}$ *to* $p_n : x(x-an)^{n-1}$.

Lemat 3.4.16. *Jeżeli* $T = \varphi(\mathfrak{D})$ *jest kompozytowym operatorem, zaś* M_x *mnoży przez* x, *to* $TM_x - M_xT = \varphi'(D)$.

Pochodna Pincherle, khm.

Fakt 3.4.17. *Dla operatora dorzecza* $\delta = \mathfrak{D}\varphi(\mathfrak{D})$ *(z odwracalnym szeregiem potęgowym* φ*) ciągiem podstawowym (wielomianów) jest* $p_n = x\varphi(\mathfrak{D})^{-n}(x^{n-1})$.

Dowód. Skoro $\varphi(\mathfrak{D})$ i $\varphi(\mathfrak{D})^{-n}$ są odwracalne, $\varphi(\mathfrak{D})^{-n}(x^{n-1})$ jest wielomianem stopnia $n-1$ i $\deg p_n = n$. Oczywiście $p_n(0) = 0$. Pozostało sprawdzić, czy $\delta p_n = np_{n-1}$.

Z definicji, $\delta p_n = \mathfrak{D}\varphi(\mathfrak{D})M_x\varphi(\mathfrak{D})^{-n}(x^{n-1})$, więc teraz użyjemy lematu.

$$\begin{aligned}
\ldots &= M_x\varphi(\mathfrak{D})^{-n}(x^{n-1}) \\
&= \varphi(\mathfrak{D})^{-n}M_x(x^{n-1}) - [\varphi(\mathfrak{D})]'(x^{n-1}) \\
&= \varphi(\mathfrak{D})^{-n}(x^n) + n[\varphi(\mathfrak{D})^{-n-1}](x^{n-1}).
\end{aligned}$$

Zatem

$$\begin{aligned}
\delta p_n &= \mathfrak{D}\varphi(\mathfrak{D})M_x\varphi(\mathfrak{D})^{-n}(x^{n-1}) \\
&= \mathfrak{D}\varphi(\mathfrak{D})[\varphi(\mathfrak{D})^{-n}(x^n) + n[\varphi(\mathfrak{D})^{n-1}](x^{n-1})] \\
&= \varphi(\mathfrak{D})^{1-n}(\mathfrak{D}x^n) + n\varphi(\mathfrak{D})^{-n}(\mathfrak{D}x^{n-1}) \\
&= \varphi(\mathfrak{D})^{1-n}(nx^{n-1}) + (n^2-n)\varphi(\mathfrak{D})^{-n}(x^{n-2}) \\
&= [n\varphi(\mathfrak{D})^{1-n}M_x + (n^2-n)\varphi(\mathfrak{D})^{-n}](x^{n-2}).
\end{aligned}$$

Teraz lemat wyciągnie M_x z opresji.

$$\begin{aligned}
\delta p_n &= [M_x n\varphi(\mathfrak{D})^{1-n} + (n\varphi(\mathfrak{D})^{1-n})' \\
&\quad + (n^2-n)\varphi(\mathfrak{D})^{-n}](x^{n-2}) \\
&= nM_x\varphi(\mathfrak{D})^{-(n-1)}(x^{n-2}) = np_{n-1}
\end{aligned}$$

□

Fakt 3.4.18 (doktryna tłumacza)**.** *Układ podstawowy dla operatora dorzecza* $\tau_a\delta$ *to* $p_0 = 1$, $\widehat{p}_n(x) = xp_n(x-na)/(x-na)$.

Dowód. Niech $\delta = \mathfrak{D}\varphi(\mathfrak{D})$, wtedy $\widehat{p}_n = x[\tau_a\varphi(\mathfrak{D})]^{-n}(x^{n-1}) = x\tau_{-na}\varphi(\mathfrak{D})^{-n}(x^{n-1}) = x\tau_{-na}[p_n/x$

□

3.4.1 Funkcje tworzące

Ustalamy raz na zawsze operator dorzecza δ, którego układ podstawowy to p_k.

Definicja 3.4.19. *Ciąg Sheffera dla* δ *to taki ciąg wielomianów* s_n *stopni* n, *że (od* $n = 1$*) prawdą jest* $\delta s_n = ns_{n-1}$.

Wzór Taylora daje $s_n(x+y) = \sum \binom{n}{k} p_k(x)s_{n-k}(y)$

Definicja 3.4.20. *Ciąg Appella to ciąg Sheffera* p_n *dla operatora* $\mathfrak{D}$.

Fakt 3.4.21. *Endomorfizm S dla $\mathcal{K}[x]$ jest odwracalnym operatorem kompozytowym, wtedy i tylko wtedy gdy posyła bazę (p_n) na (s_n).*

Ustalmy taki endomorfizm S. Układ wielomianów $S^{-1}p_n$ (s_n) jest ciągiem Sheffera, a my wyznaczymy jego wykładniczą funkcję tworzącą: $F_s(x,z) = \sum_{n\geq 0} s_n(x)z^n/n!$

Niech $\delta = \varphi(\mathfrak{D})$, $S = \psi(\mathfrak{D})$ będą elementami $\mathcal{K}[[\mathfrak{D}]]$, że $\varphi(0) = 0$, $\varphi'(0), \psi(0) \neq 0$. Rozwińmy szereg dla

$$\begin{aligned} \tau_x S^{-1} &= \sum \tau_x S^{-1}(p_n)(0)\frac{\delta^n}{n!} = \sum S^{-1}(p_n)(x)\frac{\delta^n}{n!} \\ &= \sum s_n(x)\frac{\delta^n}{n!} = F_s(x,\delta). \end{aligned}$$

Po pierwsze wiemy, że $\tau_x = \sum p_n(x)\delta^n/n! = \sum x^n\mathfrak{D}^n/n!$, czyli $\exp(x\mathfrak{D})$. Z drugiej strony, $\tau_x S^{-1}S = F_s(x,\delta) \circ \psi(\mathfrak{D})$. Te dwa wyrażenia są sobie równe. Podstawmy $\mathfrak{D} = \varphi^{-1}(\delta)$:

$$F_s(x,z) = \frac{\exp(x\varphi^{-1}(z))}{\psi(\varphi^{-1}(z))}$$

Stąd dla $s_n = p_n$ ($S = \mathrm{id}$) mamy $\psi \equiv 1$, a to pozwala nam wygodnie szukać ciągu p_n.

Przykład 3.4.22. *Niech $\nabla = -1 + \exp\mathfrak{D} = \varphi(\mathfrak{D})$, wtedy*

$$\exp(x\varphi^{-1}(z)) = \exp(x\log 1 + z) = (1+z)^x,$$

co ze wzorem Newtona daje $p_n(x) = x \cdot \ldots \cdot (x-n+1)$.

Rozdział 4

Imperium topologii

Rozdział 5

Kalifat algebry

Rozdział 6

Rozszerzenia ciał

6.1 Rozszerzenia kwadratowe

Rozszerzymy teraz $\mathbb{Q}_p$ o pierwiastek z $\varepsilon \notin \mathbb{Q}_p^\times$. Otrzymany tak zbiór, $\mathbb{Q}_p(\sqrt{\varepsilon})$, jest ciałem równym $\{x + y\sqrt{\varepsilon} : x, y \in \mathbb{Q}_p\}$. Vlad. 1.4

Lemat 6.1.1. *Równanie $x^2 = a \in \mathbb{Z}_p^\times$, ma rozwiązanie $x \in \mathbb{Q}_p$, wtedy i tylko wtedy gdy a_0 jest kwadratem w $\mathbb{F}_p$ (dla $p \neq 2$) lub a_1 i a_2 są zerami (dla $p = 2$): $a = a_0 + a_1 p + a_2 p^2 + \ldots$.*

Volovich z kolegami podaje nie do końca właściwy dowód, jako że nie chce skorzystać z lematu Hensela. Ustalmy jedność η, która nie jest kwadratem.

Wniosek 6.1.2. *Dla $p \neq 2$, liczby η, p, $p\eta$ nie są kwadratami.*

Wniosek 6.1.3. *Liczby p-adyczne są postaci εy^2, gdzie $y \in \mathbb{Q}_p$, zaś $\varepsilon = 1, \eta, p$ lub $p\eta$ ($p \neq 2$). Istnieją trzy nieizomorficzne rozszerzenia stopnia dwa dla $\mathbb{Q}_p$: o pierwiastek z η, p i $p\eta$.*

Wniosek 6.1.4. *Liczby 2-adyczne są postaci εy^2, gdzie $y \in \mathbb{Q}_p$, zaś $\varepsilon = \pm 1, \pm 2, \pm 3$ lub ± 6. Istnieje zatem siedem nieizomorficznych rozszerzeń kwadratowych: o pierwiastki z -1, ± 2, ± 3 lub ± 6.*

Wniosek 6.1.5. *Dla $p = 4k + 3$, $|x^2 + y^2|_p = \max\{|x|_p^2, |y|_p^2\}$.*

Definicja 6.1.6. *Współrzędne kartezjańskie to para $(x, y) \in \mathbb{Q}_p \times \mathbb{Q}_p$ dla $x + y\sqrt{\varepsilon}$.*

Definicja 6.1.7. *Pseudookrąg to zbiór punktów z spełniających $z\overline{z} = c$.*

Niech $\mathbb{Q}_p^\varepsilon \leq \mathbb{Q}_p^\times$ składa się z liczb postaci: r^2 lub κr^2, gdzie $r \in \mathbb{Q}_p^\times$, $\kappa \in \mathbb{Q}_p^\varepsilon$ nie jest kwadratem.

Definicja 6.1.8. *Współrzędne biegunowe to para (ρ, σ), gdzie $\rho = r$ lub $\rho = \nu r$, $\nu \neq 0$, $z = \rho\sigma$ i $\sigma\overline{\sigma} = 1$.* Vlad. 1.5

„Okrąg” $z\overline{z} = 1$ to $\{(1 + \varepsilon t^2, 2t)/(1 - \varepsilon t^2) : t \in \mathbb{Q}_p\}$, jest on zbiorem zwartym.

Fakt 6.1.9. *Obraz funkcji $\varphi\colon \mathbb{Q}_p \to \mathbb{R}_+$, $\varphi(x) = |x|_p \sum_{k=0}^{\infty} x_k p^{-2k}$ jest przeliczalną unią rozłącznych, nigdzie gęstych zbiorów o mierze Lebesgue'a zero, które są doskonałe.* Vlad. 1.6

6.2 Przestrzenie unormowane

Przyjmujemy, że mamy jakieś ciało $\mathcal{K}$ z wartością bezwzględną, z którą (to ciało $\mathcal{K}$) jest zupełne. Dla świętego spokoju do listy założeń dopisujemy „charakterystyka ciała to zero”. Weźmy przestrzeń wektorową $\mathcal{V}$ nad $\mathcal{K}$.

Definicja 6.2.1. *Norma to funkcja* $\|\cdot\|\colon \mathcal{V} \to \mathbb{R}_+$ *spełniająca:*

1. $\|v\| = 0$*, wtedy i tylko wtedy gdy* $v = 0$.
2. *jeśli* $v, w \in \mathcal{V}$*, to* $\|v + w\| \leq \|v\| + \|w\|$.
3. *jeśli* $v \in \mathcal{V}$*,* $\lambda \in \mathcal{K}$*, to* $\|\lambda v\| = |\lambda| \cdot \|v\|$.

Nie wprowadzamy pojęcia niearchimedesowej przestrzeni liniowej, gdyż taka definicja byłaby równie skomplikowana co bezużyteczna. Każda $\mathcal{V}$ przestrzeń nad niearchimedesowym ciałem $\mathcal{K}$ sama taka jest.

Definicja 6.2.2. *Dwie normy na jednej przestrzeni są równoważne, gdy istnieją rzeczywiste stałe* C *i* D*, że* $\|v\|_1 \leq C\|v\|_2 \leq CD\|v\|_1$.

Fakt 6.2.3. *Dwie normy są równoważne, wtedy i tylko wtedy gdy zadają tę samą topologię. Wtedy ciągi Cauchy'ego względem nich pokrywają się.*

Dowód. By pokazać, że równoważne normy zadają taką samą topologię, wystarczy pokazać, że kula otwarta względem jednej normy jest też otwarta względem drugiej. Można ograniczyć się do jednej kuli, bo to wektorowa przestrzeń z normą.

Dla $x \in \mathcal{B} = \{x \in \mathcal{V} : \|x\|_1 < 1\}$ przyjmijmy, że $r = \|x\|_1$ i weźmy $R < (1-r)/C$. Zbiór $N = \{y \in \mathcal{V} : \|y - x\|_2 < R\}$, otwarta względem $\|\cdot\|_2$ kula, zawiera się w $\mathcal{B}$, która (dzięki temu) jest otwarta względem $\|\cdot\|_2$.

W drugą stronę można zaszaleć. Identyczność $i\colon \mathcal{V} \to \mathcal{V}$ (obie z różnymi normami) oraz odwrotna do niej są ciągłe i liniowe. □

Fakt 6.2.4. *Przestrzeń wektorowa* $\mathcal{V}$ *nad zupełnym ciałem z normą i bazą* $v_1, \ldots, v_m$ *jest zupełna (z normą supremum). Ciąg jej wektorów* $w_n = \sum_{k=1}^m a_{kn} v_k$ *jest Cauchy'ego, wtedy i tylko wtedy gdy takie są ciągi jego współczynników* (a_{kn}) *w ciele* $\mathcal{K}$.

Dowód. Norma to największy ze współczynników „bazowych”, zatem $\|w_{n_1} - w_{n_2}\|$ dąży do zera dokładnie wtedy, gdy do zera dążą wszystkie $a_{in_1} - a_{in_2}$. □

Fakt 6.2.5. *Weźmy* $\mathcal{V} = \mathbb{Q}_p[X]$ *i ustalmy rzeczywiste* $c > 0$*. Wtedy* $\|\cdot\|$ *jest (multiplikatywną) normą na* $\mathcal{V}$*, z którą ta jest zupełna.*

$$\left\| \sum_{k=0}^{n} a_k X^k \right\| = \max_{0 \leq i \leq n} |a_i| c^i$$

Dowód. „Ciało $\mathbb{C}_p$”. □

6.3 Przestrzenie skończonego wymiaru

Pokażemy, że w pewnym sensie jeżeli przestrzeń wektorowa ma skończony wymiar, to wiemy o niej wszystko, co tylko można wiedzieć.

Fakt 6.3.1. *Niech $\mathcal{V}$ będzie p. wektorową nad zupełnym ciałem $\mathcal{K}$ z normą, że $\dim_{\mathcal{K}} \mathcal{V} < \infty$. Wszystkie normy na $\mathcal{V}$ są równoważne, a sama $\mathcal{V}$ jest zupełna „z metryką supremum".*

To nie takie proste w dowodzie, więc podzielimy go na kilka części. Niechaj $v_1, \ldots, v_n$ będzie bazą dla $\mathcal{V}$, $\|\cdot\|_0$ supremum normą, zaś $\|\cdot\|_1$ jakąś inną normą. Chcemy pokazać istnienie C, D, że $\|v\|_1 \leq C\|v\|_0$ oraz $\|v\|_0 \leq D\|v\|_1$.

Lemat 6.3.2. *Gdy $C = n \max_{1 \leq i \leq n} \|v_i\|_1$, to $\|v\|_1 \leq C\|v\|_0$ dla każdego $v \in V$.*

Dowód. Ustalmy wektor $v \in V$ i zapiszmy go w bazie:

$$\begin{aligned} \|v\|_1 = \left\| \sum_{k=1}^{n} a_i v_i \right\|_1 &\leq \sum_{k=1}^{n} \|a_i v_i\|_1 = \sum_{k=1}^{n} |a_i| \, \|v_i\|_1 \\ &\leq n \max |a_i| \max \|v_i\|_1 = C\|v\|_0 \end{aligned}$$

□

Druga nierówność jest trudniejsza. Będziemy indukować po wymiarze $\mathcal{V}$.

Lemat 6.3.3. *Dla pewnej stałej $D > 0$ zachodzi $\|v\|_0 \leq D\|v\|_1$ dla każdego $v \in \mathcal{V}$, w szczególności: $\mathcal{V}$ jest zupełna z $\|\cdot\|_1$.*

Dowód. Druga część wynika z pierwszej, która to jest trywialna, gdy $\dim \mathcal{V} = 1$. Pokażemy sam krok indukcyjny z $n-1$ do n. Załóżmy, że teza jest fałszywa, wtedy iloraz $\|w\|_1/\|w\|_0$ dla $w \in \mathcal{V}$ jest dowolnie mały. Oznacza to, że dla całkowitej m można znaleźć $w_m \in \mathcal{V}$, żeby $\|w_m\|_1 < \|w_m\|_0/m$.

Zauważmy, że norma supremum $\|w_m\|_0$ to największy ze współczynników w bazie. Pewien indeks jest największy dla ∞-wielu m. Możemy założyć, że jest to ostatni indeks. Weźmy ciąg $m_1 < m_2 < \ldots$ „tych m" właśnie, zaś przez β_k oznaczmy n-ty współczynnik w_{m_k}. Wektory $\beta_k^{-1} w_{m_k}$ mają dwie ładne własności: ich n-ta współrzędna to 1, więc są postaci $u_k + v_n$, gdzie u_k należy do podprzestrzeni rozpiętej przez $v_1, \ldots, v_{n-1}$, $\mathcal{W}$. Po drugie,

$$\|u_k + v_n\| = |\beta_k|^{-1} \|w_{m_k}\|_1 = \frac{\|w_{m_k}\|_1}{\|w_{m_k}\|_0} < \frac{1}{m_k}.$$

Dostaliśmy ciąg wektorów u_k takich, że normy $\|u_k + v_n\|_1$ dążą do zera. Oczywiście tworzą ciąg Cauchy'ego (w $\mathcal{W}$, które jest zupełne), więc istnieje $u \in W$, że $u_k \to u$. Problem w tym, że wtedy $\|u_k + v_n\|_1 \to \|u + v_n\|_1 = 0$, więc $u = -v_n \notin \mathcal{W}$. □

Fakt 6.3.4. *Unormowana p. wektorowa $\mathcal{V}$ o skończonym wymiarze nad lokalnie zwartym, zupełnym ciałem $\mathcal{K}$ jest lokalnie zwarta (na $\mathcal{K}$ jest wartość bezwzględna).*

Dowód. Weźmy $\mathcal{B} = \{v \in \mathcal{V} : \|v\| \leq 1\}$, zwarte otoczenie zera. Ustalmy bazę v_i dla $\mathcal{V}$. Normą jest supremum. Wektor v postaci $\sum_{k=1}^{n} a_k v_k$ należy do $\mathcal{B}$ dokładnie wtedy, gdy a_k należą do domkniętej kuli jednostkowej w $\mathcal{K}$. Chcemy pokazać, że $\mathcal{B}$ jest zupełne (owszem: jest domknięte w zupełnej $\mathcal{V}$) i całkowicie ograniczone. Pokryjmy w $\mathcal{K}$ jednostkową kulę N kulami (środki w $c_1, \ldots, c_N$, promień ε ustalony). Kule wokół n^N wektorów w $\mathcal{V}$ o współrzędnych „z c_i" o promieniu ε kryją $\mathcal{B}$. □

Udowodnimy twierdzenie częściowo do powyższego faktu odwrotne (za Robertem, a nie Gouveą).

Fakt 6.3.5. *Lokalnie zwarta p. unormowana $\mathcal{V}$ nad $\mathbb{Q}_p$ ma skończony wymiar.*

Dowód. Ustalmy zwarte otoczenie Ω dla zera w $\mathcal{V}$ oraz skalar $a \in \mathbb{Q}_p^\times$, taki że $|a| < 1$ (na przykład $a = p$). Unia wszystkich wnętrz przesunięć $x + a\Omega$ dla $x \in \mathcal{V}$ kryje całą przestrzeń. Zbiór Ω można pokryć skończenie wieloma $a_i + a\Omega$.

Rozpatrzmy podprzestrzeń $L = \langle a_i \rangle$. Jest izomorfizczna z $\mathbb{Q}_p^d$, a przez to zupełna. Dalej, L jest domknięta, zaś w ilorazie Hausdorffa V/L obraz A zbioru Ω jest zwartym otoczeniem zera, które spełnia $A \subseteq aA$. Prosta indukcja pokazuje, że dla $n \geq 1$ jest nawet $a^{-n}A \subseteq A$.

Stąd $A \subseteq V/L \subseteq \bigcup_{n\geq 1} a^{-n}A \subseteq A$ (gdyż $|a^{-n}| \to \infty$), $V/L = 0$ jest zwarty, zaś $V = L$ skończonego wymiaru. □

Przy użyciu miary Haara można ominąć jedno z założeń (to, że topologia pochodzi od normy), po raz pierwszy pokazał to bodajże Weil.

Być może dowód można nieznacznie skomplikować tak, by był poprawny dla dowolnego ciała ultrametrycznego, nie tylko $\mathbb{Q}_p$. Zwartych przestrzeni nad $\mathbb{Q}_p$ zbyt wiele nie ma: każdy niezerowy jej element rozpina prostą, na której norma nie jest ograniczona, więc jedyną (zwartą) jest $\{0\}$.

Wniosek 6.3.6. *W lokalnie zwartej p. unormowanej nad $\mathbb{Q}_p$, zbiory zwarte to dokładnie te, które są domknięte i ograniczone.*

Dowód. W każdej p. metrycznej zbiory zwarte są domknięte i ograniczone (ze względu na ciągłość metryki).

Odwrotnie, lokalnie zwarta p. unormowana nad $\mathbb{Q}_p$ ma skończony wymiar, więc możemy założyć bez utraty ogólności, że normą jest supremum. Ale w $\mathbb{Q}_p^n$ ograniczone zbiory leżą w produktach kul z $\mathbb{Q}_p$, a domkniętość pociąga zwartość. □

6.4 Skończone rozszerzenia ciał

Nadciało $\mathcal{K}$ dla $\mathbb{Q}_p$, które jest nad nim przestrzenią wymiarową i ma skończony wymiar (zwany stopniem) to właśnie skończone rozszerzenie. Chcemy rozszerzyć wartość bezwzględną z $\mathbb{Q}_p$ do całego $\mathcal{K}$. Będzie to jednocześnie niearchimedesowa norma („wektorowa"). Pokażemy, jakie jeszcze własności musiałaby mieć, gdyby istniała.

Fakt 6.4.1. *Gdyby funkcja $|\cdot|$ istniała, to $\mathcal{K}$ byłoby z nią zupełne. Topologia na $\mathcal{K}$ nie zależy od bazy, gdyż jest „jedyna": to topologia unormowanej przestrzeni $\mathbb{Q}_p$-wektorowej. Granica ciągu o wyrazach z $\mathcal{K}$ to granice współrzędnych w bazie (dowolnej).*

Pomijamy oczywisty dowód tego stwierdzenia. Z samego faktu wynika ważny wniosek:

Fakt 6.4.2. *Co najwyżej jedna wartość bezwzględna na $\mathcal{K}$ przedłuża p-adyczną wartość bezwzględną na $\mathbb{Q}_p$.*

Dowód. Załóżmy, że mamy dwie: $|\cdot|$, $\|\cdot\|$. Pokażemy najpierw, że są równoważne (jako wartości bezwzględne!) i identyczne. Chcemy pokazać, że dla $x \in \mathcal{K}$ zachodzi $|x| < 1 \Leftrightarrow \|x\| < 1$. Oznacza to, że $x^n \to 0$ w każdej z topologii. Wiemy już, że zarówno $|\cdot|$, jak i $\|\cdot\|$ są równoważne (jako normy na $\mathcal{K}$!), więc zadają tę samą topologię. Oznacza to, że istnieje liczba $\alpha > 0$, że $|x| = \|x\|^\alpha$. Wystarczy podstawić $x = p$, by przekonać się o równości $\alpha = 1$. □

Przypuśćmy, że mamy dwa rozszerzenia $\mathcal{K}, \mathcal{L}$, powiedzmy, $\mathbb{Q}_p \subset \mathcal{L} \subset \mathcal{K}$. Gdy znajdziemy wartości bezwzględne na nich, które przedłużają p-adyczną wartość bezwzględną, to obcięcie $|\cdot|_{\mathcal{K}}$ do $\mathcal{L}$ jest po prostu $|\cdot|_{\mathcal{L}}$, czyli wartość bezwzględna „nie zależy od kontekstu".

Definicja 6.4.3. *Rozszerzenie $\mathcal{K}/\mathcal{F}$ jest normalne, jeśli wszystkie włożenia σ z $\mathcal{K}$ w algebraiczne domknięcie $\mathcal{F}$, trzymające punktowo $\mathcal{F}$, spełniają $\sigma[L] = L$.*

Automorfizmy rozszerzenia normalnego, charakterystyki zero tworzą skończoną grupę (grupę Galois), której rząd jest wymiarem rozszerzenia.

Dla każdego skończonego rozszerzenia $\mathcal{K}/\mathcal{F}$ istnieje inne, skończone i normalne rozszerzenie dla $\mathcal{F}$, które zawiera $\mathcal{K}$, zwane normalnym domknięciem $\mathcal{K}/\mathcal{F}$. Warto wiedzieć. To, że istnieje funkcja $N_{\mathcal{K}/\mathcal{F}} \colon \mathcal{K} \to \mathcal{F}$, zwana normą z $\mathcal{K}$ do $\mathcal{F}$, jest kluczem do sukcesu. Nazewnictwo troszkę niefortunne…

Funkcja nie jest byle jaka, a do tego można określić ją na kilka równoważnych sposobów. Oto trzy z nich.

Definicja 6.4.4. *$N_{\mathcal{K}/\mathcal{F}}(\alpha)$ to wyznacznik macierzy $\mathcal{F}$-liniowego mnożenia przez α (jako endomorfizm $\mathcal{K}$, przestrzeni wektorowej nad $\mathcal{F}$ skończonego wymiaru).*

Definicja 6.4.5. *$N_{\mathcal{K}/\mathcal{F}}(\alpha) = (-1)^{nr} a_0^r$, gdzie r to stopień $\mathcal{K}$ nad $\mathcal{F}(\alpha)$, zaś $x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{F}[$ jest minimalny dla elementu α.*

Definicja 6.4.6. *$N_{\mathcal{K}/\mathcal{F}}(\alpha)$ to produkt $\sigma(\alpha)$, przy czym σ przebiega automorfizmy $\mathcal{K}/\mathcal{F}$.*

Zanim zajmiemy się ich równoważnością, zwrócimy uwagę na kilka ważnych rzeczy. Jeśli $\alpha \in \mathcal{F}$, to $N(\alpha) = \alpha^n$, gdzie $n = [\mathcal{K} : \mathcal{F}]$. „Norma" jest multiplikatywna, tzn. dla dowolnych $\alpha, \beta \in \mathcal{K}$ mamy: $N_{\mathcal{K}/\mathcal{F}}(\alpha\beta) = N_{\mathcal{K}/\mathcal{F}}(\alpha) N_{\mathcal{K}/\mathcal{F}}(\beta)$. „Norma" sumy nie ma wiele wspólnego z normami składników.

Lemat 6.4.7. *Definicje A i B są równoważne dla $\mathcal{K} = \mathcal{F}(\alpha)$.*

Dowód. Rozpatrz bazę dla $\mathcal{K}$ postaci $\{1, \alpha, \ldots, \alpha^{n-1}\}$. □

A jeżeli $\mathcal{K}$ jest większe od $\mathcal{F}(\alpha)$? W takiej sytuacji skorzystać można z następującego faktu: gdy mamy trzy ciała $\mathcal{F} \subseteq \mathcal{L} \subseteq \mathcal{K}$, to dla $\alpha \in \mathcal{K}$ prawdą jest $N_{\mathcal{L}/\mathcal{F}}(N_{\mathcal{K}/\mathcal{L}}(\alpha)) = N_{\mathcal{K}/\mathcal{F}}(\alpha)$. Także definicje B i C są równoważne. Rozpatruje się dwa przypadki: $\mathcal{K}/\mathcal{F}$ jest normalne i $\mathcal{K} = \mathcal{F}(\alpha)$ albo nie. W tym pierwszym obrazy $\sigma(\alpha)$ dla różnych σ, automorfizmów $\mathcal{K}/\mathcal{F}$, to dokładnie pierwiastki wielomianu minimalnego.

Dla nienormalnego rozszerzenia $\mathcal{K}/\mathcal{F}$ wzięcie produktu w normalnym domknięciu być może jest akceptowalne.

Dlaczego „norma" miałaby być ważna? Niech $\mathcal{K}/\mathbb{Q}_p$ będzie normalnym rozszerzeniem, zaś σ automorfizmem. Weźmy więc wartość bezwzględną $|\cdot|$ na $\mathcal{K}$. Wtedy $x \mapsto |\sigma(x)|$ też jest wartością bezwzględną, więc $|\sigma(x)| = |x|$ dla $x \in \mathcal{K}$. Wiemy, że $|\prod_\sigma \sigma(x)| = |x|^n$, zatem

$$|x| = |N_{\mathcal{K}/\mathbb{Q}_p}(x)|^{1/n}.$$

Co prawda ograniczyliśmy się do rozszerzeń normalnych, ale nie jest tak źle, jak mogło się by wydawać.

Lemat 6.4.8. *Niech $\mathcal{L}, \mathcal{K}$ będą skończonymi rozszerzeniami $\mathbb{Q}_p$, które tworzą wieżę: $\mathbb{Q}_p \subseteq \mathcal{L} \subseteq \mathcal{K}$. Ustalmy $x \in \mathcal{L}$. Jeżeli m, n to stopnie $\mathcal{L}$, $\mathcal{K}$ nad $\mathbb{Q}_p$, to*

$$\sqrt[m]{\left|N_{\mathcal{L}/\mathbb{Q}_p}(x)\right|_p} = \sqrt[n]{\left|N_{\mathcal{K}/\mathbb{Q}_p}(x)\right|_p}.$$

Dowód. $N_{\mathcal{K}/\mathcal{F}}(x) = N_{\mathcal{L}/\mathbb{Q}_p}(N_{\mathcal{K}/\mathcal{L}}(x)) = N_{\mathcal{L}/\mathbb{Q}_p}(x^{[\mathcal{K}:\mathcal{L}]})$. A teraz wystarczy $[\mathcal{K} : \mathbb{Q}_p] = [\mathcal{K} : \mathcal{L}][\mathcal{L} : \mathbb{Q}$ □

Założenie o normalności rozszerzenia przestaje być nam już potrzebne: wystarczy przejść do normalnego domknięcia i zauważyć, że wartość pierwiastka „nie zależy" od ciała. Tym samym pokazaliśmy prawdziwość następującego:

Fakt 6.4.9. *Przedłużenie p-adycznej bezwzględnej wartości z $\mathbb{Q}_p$ do $\mathcal{K}$ musi być dane wzorem*

$$|x| = |N_{\mathcal{K}/\mathbb{Q}_p}(x)|_p^{1:[\mathcal{K}:\mathbb{Q}_p]}.$$

Dowód. Po pierwsze, $|x| = 0$ tylko wtedy, gdy $N_{\mathcal{K}/\mathbb{Q}_p} = 0$, więc mnożenie przez x się nie odwraca, tzn. $x = 0$, bo $\mathcal{K}$ to ciało. Multiplikatywność $|\cdot|$ jest oczywista. Jeśli wreszcie $x \in \mathbb{Q}_p$, to $N_{\mathcal{K}/\mathbb{Q}_p} = x^n$, więc $|x| = |x|_p$.

Nierówność niearchimedesowa $|x + y| \leq \max\{|x|, |y|\}$ dla $x, y \in \mathcal{K}$: wystarczy, że pokażemy ją dla $y = 1$, a wynika wtedy z „jeśli $|x| \leq 1$, to $|x - 1| \leq 1$". Dlaczego jednak wynika?

Mamy $x+1 = -(-x-1)$, więc jeśli implikacja wyżej jest prawdziwa, to dostajemy ciąg wynikań: $|x| \leq 1$; $|-x| \leq 1$, $|-x-1| \leq 1$, $|x+1| \leq 1$. Jeżeli $|x| \leq 1$, to $\max\{|x|, 1\} = 1$, jeśli nie, to $|1/x| < 1$, więc $|1 + 1/x| \leq 1$, czyli $|x+1| \leq |x|$.

Nierówność $|x| \leq 1$ ma miejsce dokładnie wtedy, gdy $|N_{\mathcal{K}/\mathbb{Q}_p}|_p \leq 1$. Zatem tak naprawdę pokazujemy wynikanie: jeśli $N_{\mathcal{K}/\mathbb{Q}_p}(x) \in \mathbb{Z}_p$, to $N_{\mathcal{K}/\mathbb{Q}_p}(x-1) \in \mathbb{Z}_p$.

Z poniższego lematu wynika, że możemy przyjąć, że $\mathcal{K} = \mathbb{Q}_p(x)$ jest najmniejszym ciałem zawierającym x. Zawsze mamy $\mathbb{Q}_p(x) = \mathbb{Q}_p(x-1)$. Niech $f(x) = x^n + \ldots + a_1x + a_0$ będzie wielomianem minimalnym dla x. Wtedy minimalnym dla $x - 1$ jest $f(x+1)$. Zatem $N_{\mathcal{K}/\mathbb{Q}_p}(x) = (-1)^n a_0$ oraz $N_{\mathcal{K}/\mathbb{Q}_p}(x-1) = (-1)^n(1 + a_{n-1} + \cdots + a_0)$. To, co chcemy pokazać, wyniknie z: jeśli $f(x)$ (jak wyżej) jest nierozkładalny i $a_0 \in \mathbb{Z}_p$, to $f(1) \in \mathbb{Z}_p$. □

Lemat 6.4.10. *Jeżeli $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ jest nierozkładalnym wielomianem (o współczynnikach z $\mathbb{Q}_p$) i $a_0 \in \mathbb{Z}_p$, to wszystkie współczynniki są w $\mathbb{Z}_p$.*

Dowód. Załóżmy zatem nie wprost, że któryś $a_i \notin \mathbb{Z}_p$. Niech m będzie najmniejszym wykładnikiem, dla którego $p^m a_i \in \mathbb{Z}_p$ (dla każdego i), połóżmy $g(x) = p^m f(x)$. Mamy $b_n = p^m$ i $b_0 = p^m a_0$, wszystkie b_i należą do $\mathbb{Z}_p$, ale przynajmniej jeden nie dzieli się przez p. Niech k będzie najmniejszym i, że $p \nmid b_i$. Wtedy $g(x) \equiv (b_n x^{n-k} + \cdots + b_k)x^k$ modulo p, łatwo widać, że czynniki są względnie pierwsze modulo p. Z drugiej formy lematu Hensela wnioskujemy, że $g(x)$ jest rozkładalny, więc $f(x)$ też (dowód za Neukirchem). □

Prawdziwsze jest ogólniejsze stwierdzenie.

Twierdzenie 9 (Krull)**.** *Waluację niearchimedesową z ciała $\mathcal{K}$ na nadciało L można zawsze przedłużyć.*

Wszystkie jego znane dowody są trudne, ale my ominemy rozszerzenia i grupy Galois. Ideą przewodnią jest „wygładzanie dowolnej normy" na L.

Dowód. Na mocy lematu Zorna jedynym rozszerzeniem, jakie należy rozpatrzyć, jest $L = \mathcal{K}(z)$.

Jeżeli z nie jest algebraiczny nad $\mathcal{K}$, to ciała $\mathcal{K}(z)$ oraz $\mathcal{K}(x)$ są izomorficzne. Dla $f = \sum_{i \le n} a_i x^i$ (wielomianu) kładziemy $\|f\| := \max\{|a_j| \colon 0 \le j \le n\}$. Oczywiście przedłuża to naszą wartość bezwzględną. Pokażemy multiplikatywność. Jasnym jest to, że $\|fg\| \le \|f\| \cdot \|g\|$.

Dla dowodu nierówności w drugą stronę wystarczy nam sprawdzić w produkcie współczynnik c_{s+t}, gdzie s dobrany jest wg przepisu $s = \min\{j : |a_j| = \|f\|\}$, t analogicznie.

Formuła $\|f : g\| = \|f\| : \|g\|$ daje żądane przedłużenie.

Jeżeli z jest algebraiczny, ustalamy bazę $e_1, \ldots, e_n$ dla L. Definiujemy dla $x \in L$: $\| \sum_{k=1}^n \xi_k e_k \|_1 = \max\{|\xi_k| : k \le n\}$. Funkcja ta ma własności normy, ale nie wiemy jeszcze, czy jest multiplikatywna. Weźmy zatem dwa elementy $x = \sum_{i \le n} \xi_i e_i$, $y = \sum_{i \le n} \eta_i e_i$ ($\xi, \eta \in \mathcal{K}$), wtedy $\|xy\|_1$, „norma" ich iloczynu, to $\| \sum_{i,j \le n} \xi_i \eta_j e_i e_j \|_1 \le \max_{i,j} |\xi_i||\eta_j|\|e_i e_j\|_1$, oszacujemy z góry jeszcze przez $C\|x\|_1\|y\|_1$.

Funkcja $\|x\|_2 = C\|x\|_1 \colon L \to \mathbb{R}$ to nadal za mało, zatem podrabiamy normę spektralną (z $\mathbb{C}$-algebr Banacha) $L \to \mathbb{R}$ wzorem $\nu(x)^n = \limsup_{n \to \infty} \|x^n\|_2$, a skoro $\|x^n\|_2 \le \|x\|_2^n$, ma to ręce i nogi. Twierdzimy przy tym, że funkcja ν ma pewne własności dla $\lambda \in \mathcal{K}$ oraz $x, y \in L$: $\nu(1) = 1$, $\nu(x^k) = \nu(x)^k$, $\nu(xy) \le \nu(x)\nu(y)$, $0 \le \nu(x) \le \|x\|_2$, $\nu(\lambda x) = |\lambda|\nu(x)$ oraz $0 \le \nu(x) \le \|x\|_2$. Ich dowody są łatwe i przyjemne.

Udowodnimy dwie kolejne, trudniejsze (patrz: najbliższe lematy). Pokazaliśmy dopiero, że zbiór S funkcji $\nu \colon L \to \mathbb{R}$, które spełniają powyższe warunki i dwa lematy, nie jest pusty. Porządkujemy go częściowo: $\nu_1 \le \nu_2$, gdy $\nu_1(x) \le \nu_2(x)$ dla każdego $x \in L$.

Jeżeli $T \subseteq S$ jest łańcuchem, to $x \mapsto \inf\{\nu(x) : \nu \in T\}$ jest znowu elementem S. Lemat Zorna zapewnia nas, że w S istnieje element minimalny τ, kandydat na przedłużenie.

$1 = \tau(1) = \tau(xx^{-1}) \le \tau(x)\tau(x^{-1})$ dla $x \in L^\times$ pokazuje, że (wtedy) $\tau(x) > 0$. Niech $a \in L^\times$.

Funkcja $\rho(x) = \lim_n \tau(a^n x)\tau(a)^{-n}$ ma sens (istnieje dla każdego x) oraz $\rho \le \tau$, gdyż $\tau(x) \ge \tau(a^k x)\tau(a)^{-k}$. Nadal posiada pożądane cechy, więc należy do S, z minimalności τ mamy równość $\rho = \tau$.

Ale to już koniec: $\tau(x) = \tau(ax)\tau(a)^{-1}$ równoważne jest $\tau(xy) = \tau(x)\tau(y)$ (wobec dowolności a). Nierówności trójkąta dowód przebiega prosto:

$$\begin{aligned}\tau(x+y) &= \tau(x(1 + x^{-1}y)) = \tau(x)\tau(1 + x^{-1}y) \\ &\le \tau(x)\max(1, \tau(x^{-1}y)) \\ &= \max(\tau(x), \tau(y)).\end{aligned}$$ □

Lemat 6.4.11. $\nu(x) = \lim_n \|x^n\|_2^{1:n} = \inf_n \|x^n\|_2^{1:n} =: a$

Dowód. Ustalmy $\varepsilon > 0$ i takie n, by $\|x^n\|_2 < (a+\varepsilon)^n$. Niech $m = qn + r$ (dzielenie z resztą). Wtedy

$$\begin{aligned}\|x^m\|_2 &\le \|x^n\|_2^q \|x\|_2^r \le (a+\varepsilon)^{nq}\|x\|_2^r \\ &= (a+\varepsilon)^m(\|x\|_2 : (a+\varepsilon))^r,\end{aligned}$$

skąd wynika już, że granica górna (!) nie przekracza $a + \varepsilon$. □

Lemat 6.4.12. $\nu(1+x) \le \max(1, \nu(x))$.

Dowód. Nierówność $\|(1+x)^n\|_2 \leq \max_{0\leq k\leq n} \|x^k\|_2$ jest wnioskiem z rozwinięcia dwumianowego. Jeśli mamy $k = 0$, to $\|x^k\|_2 = \|1\|_2$. Dla $1 \leq k \leq m$ i $m^2 = n$ jest $\|x^k\|_2 \leq 1$ lub $\|x\|_2^m$. Jeśli $m < k \leq n^2$, $\|x^k\|_2 \geq 1$, to prawdziwe jest inne oszacowanie: $\|x^k\|_2 \leq \sup_{s^2>n} \|x^s\|_2^{n:s}$.

Połączenie tych przypadków mówi, że $\|(1+x)^n\|_2$ z góry jest ograniczony przez największy z: $\sup_{s^2>n} \|x^s\|_2^{n:s}$, $\|x\|_2^m$, $\|1\|_2$, 1, co kończy dowód. $\square$

Fakt 6.4.13 (Gelfand, Mazur?). *Z dokładnością do izomorfizmu, nie ma żadnych zupełnych ciał z metryką archimedesową poza $\mathbb{R}$ lub $\mathbb{C}$.*

Pokazaliśmy dla dowolnego skończonego rozszerzenia $\mathcal{K}$ dla $\mathbb{Q}_p$ istnienie jedynej wartości bezwzględnej, która przedłuża p-adyczną na $\mathbb{Q}_p$. Na koniec zajmiemy się $\mathbb{Q}_p^a$, algebraicznym domknięciem $\mathbb{Q}_p$. Ciało to zawiera pierwiastki wielomianów o współczynnikach z $\mathbb{Q}_p$ i można je dostać w łatwy sposób: biorąc sumę skończonych rozszerzeń $\mathbb{Q}_p$.

Wartość bezwzględną na tymże domknięciu już dobrze znamy. Jeżeli $x \in \mathbb{Q}_p^a$, to rozszerzenie $\mathbb{Q}_p(x)$ jest skończone. Żyje w nim x, więc możemy określić $|x|$ dzięki jednoznacznemu przedłużeniu p-adycznej wartości bezwzględnej z $\mathbb{Q}_p$ do $\mathbb{Q}_p(x)$. Wiemy, że $|x|$ nie zależy od ciała, tylko od x. Zatem p-adyczna wartość bezwzględna na $\mathbb{Q}_p^a$ też jest jednoznaczna.

Dlaczego $\mathbb{Q}_p^a$ nie jest skończonym rozszerzeniem $\mathbb{Q}_p$? Bo istnieją nierozkładalne wielomiany nad $\mathbb{Q}_p$ wysokiego stopnia. Potrzebny będzie lemat.

Lemat 6.4.14. *Jeżeli $f \in \mathbb{Z}_p[x]$ rozkłada się nietrywialnie: $f = gh$, $g, h \in \mathbb{Q}_p[x]$, to istnieją także dwa niestałe $g_0, h_0 \in \mathbb{Z}_p[x]$, że $f = g_0h_0$.*

Dowód. Jeżeli $k(x) = \sum_i a_ix^i \in \mathbb{Q}_p[x]$ jest wielomianem, to przez $w(k)$ rozumiemy $\min_{i\leq n} v_p(a_i)$, największą potęgę p, która dzieli każdy współczynnik.

Jeżeli lemat jest prawdziwy dla $w(f(x)) = 0$, to jest prawdziwy zawsze (dla $w(f(x)) \geq 0$).

Istotnie, $w(f(x)) = -v_p(a)$, gdzie $a \in \mathbb{Q}_p$ to odwrotność najmniejszego współczynnika dla $f(x)$. Wiemy, że $f \in \mathbb{Z}_p[x]$, zatem $a^{-1} \in \mathbb{Z}_p$. Jest oczywistym, że $w(af(x)) = 0$. Teraz wystarczy położyć $f^*(x) = af(x)$ oraz $g^*(x) = ag(x)$, wtedy $f^* = g^*h$ i $w(f^*) = 0$

Wiara w szczególny przypadek lematu pozwala rozłożyć $f^*(x)$ w pierścieniu $\mathbb{Z}_p[x]$, jeden z czynników musi teraz tylko wchłonąć a^{-1}.

Lemat jest prawdziwy dla $w(f(x)) = 0$.

Rozumując analogicznie można znaleźć liczby $b, c \in \mathbb{Q}_p$, że $w(bg(x)) = w(ch(x)) = 0$. Niech $g_1 = bg$, $h_1 = ch$, a do tego $f_1 = g_1h_1$, zaś $k \mapsto k_r : \mathbb{Z}_p[x] \to \mathbb{F}_p[x]$ oznacza redukcję współczynników modulo p.

Z naszych założeń ($g_{1,r}$ i $h_{1,r}$ są niezerowe) wynika, że $f_{1,r}$ nie jest zerem. Zatem $w(f_1(x)) = w(f(x)) = 0$, czyli $v_p(bc) = 0$.

Można przyjąć $g_0(x) = (bc)^{-1}g_1(x)$, $h_0(x) = h_1(x)$. $\square$

Wniosek: gdy $f(x) \in \mathbb{Z}_p[x]$ ma nierozkładalną redukcję modulo p w $\mathbb{F}_p[x]$ i jest unormowany, to jest też nierozkładalny nad $\mathbb{Q}_p$. Gdyby tak nie było, to rozkładałby się nad $\mathbb{Z}_p$ (lemat), a po zredukowaniu także nad $\mathbb{F}_p$.

Algebraicy wiedzą, że zawsze można znaleźć wielomian (stopnia $n \in \mathbb{N}$, nierozkładalny) w $\mathbb{F}_p[x]$, którego pierwiastki generują jedyne rozszerzenie stopnia n dla $\mathbb{F}_p$. Wielomian ten podnosi się naturalnie do $\mathbb{Z}_p[x]$. Zatem:

Fakt 6.4.15. *Dla każdego $n \geq 1$ istnieje rozszerzenie $\mathbb{Q}_p$ stopnia n, które „pochodzi" od jedynego rozszerzenia stopnia n dla ciała $\mathbb{F}_p$. Są one normalne i mają taką samą grupę Galois jak rozszerzenia $\mathbb{F}_p$.*

Wniosek 6.4.16. *$\mathbb{Q}_p^a$ jest nieskończonym rozszerzeniem $\mathbb{Q}_p$.*

Zanim zajmiemy się algebraicznym domknięciem bliżej, potrzeba nam lepszej znajomości skończonych rozszerzeń $\mathbb{Q}_p$. Trochę wcześniej dowiemy się jednak, jak dostać jeszcze więcej skończonych rozszerzeń dla tego ciała.

Twierdzenie 10 (kryterium Eisensteina)**.** *Jeżeli wielomian*

$$f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}_p[x],$$

spełnia: $|a_n| = 1$, $|a_i| < 1$ dla $0 \leq i < n$ i $|a_0| = 1/p$, to jest on nierozkładalny nad ciałem $\mathbb{Q}_p$.

Dowód. Załóżmy nie wprost, że $f(x)$ jednak jest rozkładalny. Z lematu wiemy, że rozkłada się nawet nad $\mathbb{Z}_p$. Weźmy więc $g(x), h(x) \in \mathbb{Z}_p[x]$, takie że $g(x)h(x) = f(x)$. Zapiszmy $g(x) = b_r x^r + \cdots + b_0$, $h(x) = c_s x^s + \cdots + c_0$, $r + s = n$. Jest $|b_r| = |c_s| = 1$, bo $|b_r c_s| = |a_n| = 1$.

Mamy $f^*(x) = g^*(x)h^*(x)$. Z drugiej strony, założenia pociągają $f^*(x) = a_n^* x^n$. W takim razie $g^*(x) = b_r^* x^r$ oraz $h^*(x) = c_s^* x^s$, a zatem b_0, c_0 dzielą się przez p i $|a_0| \leq 1/p^2$, sprzeczność. □

6.5 Własności skończonych rozszerzeń

Tutaj $\mathcal{K}$ jest skończonym rozszerzeniem stopnia n dla $\mathbb{Q}_p$. W $\mathbb{Q}_p$ wartość bezwzględna niezerowego elementu była postaci p^v, $v \in \mathbb{Z}$. Teraz widzimy (gdyż norma to pierwiastek „normy"), że dla $x \in \mathcal{K} \setminus \{0\}$, wartość bezwzględna jest postaci p^v, gdzie $v \in \frac{1}{n}\mathbb{Z}$. To naprowadza nas na definicję.

Definicja 6.5.1. *Waluacja p-adyczna dla $x \in \mathcal{K}^\times$ jest jedyną liczbą wymierną, która spełnia $|x| = p^{-v_p(x)}$. Oprócz tego $v_p(0) = +\infty$ ($\mathcal{K}$ to skończone rozszerzenie $\mathbb{Q}_p$).*

Jej znajomość wymaga tylko „normy", gdyż

$$v_p(x) = \frac{1}{n} v_p(N_{\mathcal{K}/\mathbb{Q}_p}(x)).$$

Wiemy już, że obraz v_p jest zawarty w $\frac{1}{n}\mathbb{Z}$, ale wciaż nie znamy jego prawdziwego oblicza. Pora to zmienić.

Fakt 6.5.2. *Waluacja p-adyczna jest homomorfizmem z grupy $\mathcal{K}^\times$ w $\mathbb{Q}$. Jego obraz to $\frac{1}{e}\mathbb{Z}$, gdzie e dzieli $n = [\mathcal{K} : \mathbb{Q}_p]$.*

Dowód. To, że v_p jest homomorfizmem, już wiemy (wiemy?). Zatem jego obraz to addytywna podgrupa $\mathbb{Q}$. Wiemy też, że obraz ten zawiera się w $(1/n)\mathbb{Z}$ i zawiera co najmniej $\mathbb{Z}$, gdyż obraz v_p w $\mathbb{Q}_p^\times$ taki jest. Niech d/e (ułamek skrócony) należy do obrazu, zaś mianownik e

będzie największy z możliwych. Możemy znaleźć takie r, s, że $rd = 1 + se$. To oznacza jednak, że

$$r\frac{d}{e} = \frac{1+se}{e} = \frac{1}{e} + s$$

jest w obrazie, a skoro $s \in \mathbb{Z}$ tam jest, to $1/e$ także. Skoro e było największe z możliwych, to obrazem jest dokładnie $\frac{1}{e}\mathbb{Z}$. $\square$

Liczba e (wyznaczona przez $v_p(\mathcal{K}^\times) = \frac{1}{e}\mathbb{Z}$) jest na tyle ważna, że ma specjalną nazwę. Do tego określamy $f = n/e$.

Definicja 6.5.3. *Liczba e to indeks rozgałęzienia $\mathcal{K}$ nad $\mathbb{Q}_p$.*

Rozszerzenie może być rozgałęzione (gdy $e > 1$, dla $e = n$: całkowicie) lub nie ($e = 1$).
W ciele $\mathbb{Q}_p$ liczba p była ważna, gdyż jej waluacja $v_p(p) = 1$ była najmniejszą spośród dodatnich. Elementy $x \in \mathbb{Z}_p$, które spełniają $v_p(x) > 0$, są podzielne przez p. Zatem waluacja to „krotność”: każdy $y \in \mathbb{Q}_p$ zapisuje się jako $p^{v_p(y)}u$, gdzie $v_p(u) = 0$. Znowu potrzeba nam czegoś takiego.

Definicja 6.5.4. *Jeżeli $\mathcal{K}/\mathbb{Q}_p$ jest skończonym rozszerzeniem, to $\pi \in \mathcal{K}$ jest jednolitością, jeżeli $ev_p(\pi) = 1$.*

Jest wiele jednolitości, tak jak jest wiele liczb w $\mathbb{Z}_p$, których waluacja to 1. Ustalmy jedną z nich (możemy wybrać $\pi = p$ w nierozgałęzionym przypadku). Mamy wszystko, co chcieliśmy mieć, by opisać algebraiczną strukturę $\mathcal{K}$. Przypomnienie: $\mathcal{O}$ to pierścień waluacji z ideałem maksymalnym $\mathfrak{m}$, $\mathfrak{K} = \mathcal{O}/\mathfrak{m}$ to ciało residuów.

Fakt 6.5.5. *Ustalmy jednolitość π w $\mathcal{K}$ i powyższe oznaczenia.*

1. *Ideał $\mathfrak{m} \subseteq \mathcal{O}$ jest główny, generuje go π.*
2. *Każdy element $x \in \mathcal{K}$ można zapisać w postaci $u\pi^{ev_p(x)}$, gdzie $u \in \mathcal{O}^\times$ to jedność ($v_p(u) = 0$); więc $\mathcal{K} = \mathcal{O}[1/\pi]$.*
3. *Ciało residuów $\mathfrak{K}$ to skończone rozszerzenie $\mathbb{F}_p$, którego stopień to co najwyżej $[\mathcal{K} : \mathbb{Q}_p]$.*
4. *Elementy $\mathcal{O}$ to dokładnie $x \in \mathcal{K}$, zerujące (jakiś) unormowany wielomian o współczynnikach z $\mathbb{Z}_p$.*
5. *$\mathcal{O}$ to zwarty pierścień topologiczny. Zbiory $\pi^n\mathcal{O}$, $n \in \mathbb{Z}$, to fundamentalny układ otoczeń zera w $\mathcal{K}$ (które jest $\mathcal{T}_2$ całkowicie niespójną i lokalnie zwartą p. topologiczną).*
6. *Dla ustalonego zbioru reprezentantów A, $\{0, c_1, \ldots, c_f\}$, warstw $\mathfrak{m}$ w $\mathcal{O}$, każdy $x \in \mathcal{K}$ jednoznacznie zapisuje się jako $\pi^{-m}\sum_0^\infty a_i\pi^i$ ($a_i \in A$).*

Dowód. (3) Gdy zbiór elementów $\mathcal{O}$ jest liniowo niezależny nad $\mathbb{Q}_p$, to jego redukcja jest liniowo niezależna nad $\mathbb{F}_p$. Następne punkty są oczywiste dla każdego, kto zna konstrukcję wartości bezwzględnej oraz $\mathbb{Q}_p$. $\square$

Okazuje się, że liczba f ma naturalną interpretację.

Fakt 6.5.6. *Mamy $[\mathfrak{K} : \mathbb{F}_p] = n/e$, więc $|\mathfrak{K}| = p^f$.*

Dowód. Niech $m = [\mathfrak{K} : \mathbb{F}_p]$; indeksem rozgałęzienia jest e. Wybierzmy $\alpha_1, \ldots, \alpha_m \in \mathcal{O}$ tak, by ich obrazy w $\mathfrak{K}$ były bazą (nad $\mathbb{F}_p$) tego ciała. Wtedy z pewnością α_i są liniowo niezależne nad $\mathbb{Q}_p$.

(Gdyby były zależne, moglibyśmy je przeskalować do całkowitych, niektóre stałyby się jednościami. Redukcja do $\mathbb{F}_p$ daje relację zależności w tym ciele, sprzeczność.)

Musimy pokazać, jak dopełnić ten zbiór do bazy $\mathcal{K}$ nad $\mathbb{Q}_p$. Przyda się jednolitość π. Rozpatrzmy elementy $\pi^j a_i$ dla $0 \le j < e$, $1 \le i \le m$. Udowodnimy tezę, gdy pokażemy, że tworzą bazę, bo $n = e \cdot m$.

Jeśli każdy element $\mathcal{O}$ jest $\mathbb{Q}_p$-liniową kombinacją $\pi^j \alpha_i$, to także każdy element $\mathcal{K}$ jest taki (każdy $x \in \mathcal{K}$ ma takie r, że $p^r x \in \mathcal{O}$). Ustalmy $x \in \mathcal{O}$ i zredukujmy go do $\overline{x}$ (modulo π). Mamy $x = x_{0,1}\alpha_1 + \cdots + x_{0,m}\alpha_m +$ krotność π, przy czym $x_{0,j}$ leży w $\mathbb{Z}_p$. Powtarzając rozumowanie dostaniemy z kolei: $x = x_{0,1}\alpha_1 + \cdots + x_{0,m}\alpha_m + x_{1,1}\pi\alpha_1 + \cdots + x_{1,m}\pi\alpha_m +$ krotność π^2. Po e powtórzeniach spostrzegamy, że π^e oraz p różnią się o jedność, bo mają tę samą waluację. Zatem:

$$x = px' + \sum_{l=0}^{e-1} \sum_{k=1}^{m} x_{l,k} \pi^l \alpha_k,$$

gdzie $x_{i,j} \in \mathbb{Z}_p$ oraz $x' \in \mathcal{O}$. Stosując tę samą technikę wobec x' dostaniemy nowe współczynniki $x_{j,i} + px'_{j,i}$, dla których równość jest prawdziwa modulo p^2. Kontynuowanie prowadzi do ciągu Cauchy'ego w $\mathbb{Q}_p$ dla każdego współczynnika. Biorąc granicę, dostaniemy wyrażenie x jako liniowa kombinacja $\pi^j \alpha_i$. Te ostatnie rozpinają więc naszą przestrzeń.

Ustalmy kombinację $\sum x_{j,i}\pi^j \alpha_i = 0$ dla $x_{j,i} \in \mathbb{Q}_p$. Po ewentualnym skalowaniu, wszystkie $x_{j,i}$ leżą w $\mathbb{Z}_p$, ale pewien nie jest podzielny przez p. Redukcja równania modulo π daje relację zależności dla $\overline{\alpha}_i$ nad $\mathbb{F}_p$. Musi być ona trywialna, $x_{j,0}$ redukują się do zer, więc są podzielne przez p. Cała relacja dzieli się przez π, podzielmy. Przez analogię uzasadnia się, że także $x_{j,1}$ (a także „wyższe") współczynniki dzielą się przez p, co jest sprzeczne z założeniami (mamy liniową niezależność). □

Rozszerzenie ciała o charakterystyce zero powstaje przez dołączanie pierwiastków nierozkładalnego wielomianu. Teoria ciał dostarcza nam tej wiedzy. Jaki dokładnie jest to wielomian, można powiedzieć na przykład w całkowicie rozgałęzionym przypadku.

Fakt 6.5.7. *Jeżeli $\mathcal{K}/\mathbb{Q}_p$ jest rozszerzeniem skończonym dla $\mathbb{Q}_p$, zaś $e = n = [\mathcal{K} : \mathbb{Q}_p]$ (całkowite rozgałęzienie), to $\mathcal{K} = \mathbb{Q}_p(\pi)$, gdzie π jest jednolitością. Jednolitość π jest pierwiastkiem $f(X)$, wielomianu $X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$, który spełnia założenia dla kryterium Eisensteina (11).*

Dowód. Niech $f(X)$ będzie minimalnym wielomianem dla π, jednolitości ($v_p(\pi) = 1/n$, $|\pi| = p^{-1/n}$) nad $\mathbb{Q}_p$. Bezwzględną wartość π można wyznaczyć na podstawie jej normy. Jeżeli stopień f to s (musi być $s \mid n$), zaś ostatni współczynnik to a_0, to normą π jest $(-1)^n a_0^r$, gdzie $r = n/s$. Z tą wiedzą piszemy:

$$p^{-1/n} = |\pi| = \sqrt[n]{|a_0^r|} = \sqrt[s]{|a_0|}.$$

Skoro a_0 leży w $\mathbb{Q}_p$, to jego wartość bezwzględna jest całkowitą potęgą p. Wtedy musi być $s = n$ oraz $|a_0| = p^{-1}$.

Stopień f to n, zatem $\mathcal{K} = \mathbb{Q}_p(\pi)$. Fakt, że $|a_0| = p^{-1}$ mówi nam, że p^2 nie dzieli a_0. Pozostało pokazać, że $p \mid a_i$ dla $1 \le i < n$. Przez $\pi_1 = \pi, \pi_2, \ldots, \pi_n$ oznaczmy pierwiastki $f(X)$. Wszystkie mają ten sam wielomian minimalny, zatem także tę samą normę (i wartość bezwzględną). Oznacza to, że $|\pi_i| < 1$. Współczynniki $f(X)$ to kombinacje pierwiastków, zatem $|a_i| < 1$ dla $1 \le i \le n$ i po wszystkim. □

To całkiem ciekawy wynik, bo daje precyzyjny opis pewnej klasy rozszerzeń. Chcielibyśmy udowodnić coś podobnego, ale dla rozszerzeń nierozgałęzionych. Okazuje się, że to jeszcze prostsze, lecz wymaga dodatkowego narzędzia.

Twierdzenie 11 (lemat Hensela). *Dane są skończone rozszerzenie $\mathcal{K}/\mathbb{Q}_p$, jednolitość π oraz wielomian $F(X)$ z $\mathcal{O}[X]$. Gdy istnieje taka „całkowita" $\alpha_1 \in \mathcal{O}$, że $F(\alpha_1) \equiv 0 \pmod{\pi}$, zaś $F'(\alpha_1) \not\equiv 0 \pmod{\pi}$ (gdzie F' to formalna pochodna), to istnieje $\alpha \in \mathcal{O}$, że $\alpha \equiv \alpha_1$ i $F(\alpha) = 0$.*

Dowód. Identyczny z dowodem zwykłego lematu Hensela. □

Lemat Hensela pozwala uzyskać pierwiastki jedności w $\mathcal{K}$. Niezerowe elementy ciała residuów $\mathfrak{K}$ (jest ich $p^f - 1$) tworzą grupę cykliczną. Oznacza to, że gdy m dzieli $p^f - 1$, wielomian $F_(X) = X^m - 1$ ma dokładnie m pierwiastków w $\mathfrak{K}^\times$. Wybór dowolnego podniesienia tychże do $\mathcal{O}^\times$ daje m nieprzystających „przybliżonych pierwiastków". Pochodna $F'_m(X) = mX^{m-1}$ nie jest zerem, jak w lemacie; daje on więc m różnych (bo nieprzystających) m-tych pierwiastków z jedności w $\mathcal{O}^\times$. To prawda dla dowolnego m dzielącego $p^f - 1$, udowodniliśmy więc

Fakt 6.5.8. *Jeżeli $\mathcal{K}$ jest skończonym rozszerzeniem $\mathbb{Q}_p$, to $\mathcal{O}^\times$ ma w sobie cykliczną grupę $(p^f - 1)$-ych pierwiastków jedności.*

Jeżeli m dzieli $p^f - 1$ i ciało $\mathcal{K}$ zawiera $(p^f - 1)$-e pierwiastki jedności, to ma w sobie także m-te. Można to odwrócić. Jeżeli p nie dzieli m, to istnieje f takie że $p^f \equiv 1 \bmod m$, to znaczy: m dzieli $p^f - 1$. Przechodząc do ciał z coraz większym f dostajemy wszystkie pierwiastki jedności o stopniu względnie pierwszym z p.

Poza pierwiastkami jedności stopnia p^i (i naturalne), opis jest już kompletny. Jeżeli $\mathcal{K}$ zawiera jakieś inne (m-te dla m względnie pierwszego z $p^f - 1$), to muszą być 1-jednościami, gdyż ich redukcja modulo π musi być równa 1. Dokładniej: gdy $x \in \mathcal{K}$ spełnia $x^m = 1$, to $x \in \mathcal{O}^\times$ oraz $x \equiv 1 \pmod{\pi}$, czyli prawdą jest $x \in 1 + \mathcal{P}$.

Jak znam życie, 1-jedność może być m-tym pierwiastkiem jedności tylko wtedy, gdy m jest potęgą p. Pokażemy to wprost, ale poprzedzimy ciekawym spostrzeżeniem.

Lemat 6.5.9. *Jeżeli $x \equiv 1 \pmod{\pi}$, to $x^{p^r} \equiv 1 \pmod{\pi^{r-1}}$.*

Dowód. Proste użycie twierdzenia o dwumianie (dla $r = 1$) oraz indukcja (dla $r > 1$). □

Teraz jest już łatwo. Gdy ζ jest 1-jednością i $\zeta^m = 1$ dla m względnie pierwszego z p, to zaczynamy od $\zeta \equiv 1 \pmod{\pi}$. Zauważyliśmy wcześniej, że istnieje liczba r, dla której $p^r \equiv 1 \pmod{m}$. Wykorzystamy ją teraz: $\zeta = \zeta^{p^r} \equiv 1 \pmod{\pi^{r-1}}$. Zastępując r przez jej wielokrotność widzimy, że ζ przystaje do 1 modulo dowolnie wysokie potęgi π, więc $\zeta = 1$ (gdyby nie, jaka byłaby waluacja $\zeta - 1$?).

Powyższe akapity pozwalają spojrzeć na nowo na strukturę 1-jedności, czyli elementów $U_1 = 1 + \pi\mathcal{O}$. To zdecydowanie grupa: $(1 + \pi x)^{-1} = 1 - \pi x + (\pi x)^2 - (\pi x)^3 + \dots$ zbiega i do U_1 należy, podobnie $(1 + \pi x)(1 + \pi y) = 1 + \pi(x + y) + \pi^2 xy$. Tak samo pokazuje się, że zbiory $U_n = 1 + \pi^n \mathcal{O}$ są podgrupami.

Wniosek 6.5.10. *Dla każdego n iloraz U_n/U_{n+1} jest p-grupą.*

Dowód. Lemat 6.5.9 pokazuje, że $x \in U_n$ pociąga $x^p \in U_{n+1}$. Zatem każdy element abelowego ilorazu ma rząd p. Dlaczego jednak jest skończony? Bo funkcja $U_n \to \mathcal{O}, 1 + \pi^n x \mapsto x$ dla ustalonej jednolitości π. □

Mamy prawie gotowy opis pierwiastków jedności. Ciało $\mathcal{K}$ zawiera $p^f - 1$ nieprzystające $(p^f - 1)$-e oraz jakieś p^i-sze, które są 1-jednościami. Wracamy do nierozgałęzionych rozszerzeń $\mathbb{Q}_p$, naszego pierwotnego celu.

Fakt 6.5.11. *Dla każdej f istnieje nierozgałęzione rozszerzenie $\mathbb{Q}_p$ stopnia f (dokładnie jedno!). Powstaje ono przez dołączenie do $\mathbb{Q}_p$ pierwotnego $(p^f - 1)$-ego pierwiastka jedności.*

Dowód. Niech $q = p^f$. Gdy $\overline{\alpha}$ generuje cykliczną grupę $\mathbb{F}_q^\times$, to $\mathbb{F}_q = \mathbb{F}_p(\overline{\alpha})$ jest rozszerzeniem stopnia f. Niech

$$\overline{g}(X) = X^f + \overline{a}_{f-1}X^{f-1} + \ldots + \overline{a}_1 X + \overline{a}_0$$

będzie minimalnym wielomianem dla $\overline{\alpha}$ nad $\mathbb{F}_p$. Podnosząc $\overline{g}(X)$ do $g(X) \in \mathbb{Z}_p[X]$ w taki sposób, w jaki się nam podoba, dostajemy nierozkładalny wielomian nad $\mathbb{Q}_p$. Jeżeli α zeruje $g(X)$, to $\mathcal{K} = \mathbb{Q}_p(\alpha)$ jest rozszerzeniem stopnia f. Residuów ciało $\mathfrak{K}$ dla $\mathcal{K}$ musi zawierać pierwiastek $\overline{g}(X)$ (redukcja α mod $\mathfrak{P}$), zatem $[\mathfrak{K} : \mathbb{F}_p] \geq f$. Z drugiej strony stopień $\mathfrak{K}$ nad $\mathbb{F}_p$ nie przekracza stopnia $\mathcal{K}$ nad $\mathbb{Q}_p$, f, więc jest równy dokładnie f. Ciało $\mathcal{K}/\mathbb{Q}_p$ jest nierozgałęzione i $\mathfrak{K} = \mathbb{F}_{p^f}$.

Pokażemy jeszcze jedyność. Z faktu 6.5.8 wiemy, że w $\mathcal{K}$ żyją $(p^f - 1)$-sze pierwiastki jedności. Musimy pokazać, że najmniejsze rozszerzenie $\mathbb{Q}_p$ o te pierwiastki jest już stopnia f i pokrywa się z $\mathcal{K}$. Niech β będzie takim pierwiastkiem.

Mamy $\mathbb{Q}_p \subseteq \mathbb{Q}_p(\beta) \subseteq \mathcal{K}$. Potęgi β są (różnymi modulo π) pierwiastkami jedności ($p^f - 1$-szymi). Ciało residuów $\mathbb{Q}_p(\beta)$ nad $\mathbb{Q}_p$ zawiera $\mathfrak{K} = \mathbb{F}_{p^f}$. Z całą pewnością stopień tego ciała nie przekracza stopnia rozszerzenia, więc $[\mathbb{Q}_p(\beta) : \mathbb{Q}_p] \geq f$. Wiemy, że $\mathcal{K}/\mathbb{Q}_p$ ma stopień f, skąd wynika $\mathcal{K} = \mathbb{Q}_p(\beta)$. ☐

Definicja 6.5.12. *$\mathbb{Q}_p^{unr}$ to maksymalne nierozgałęzione rozszerzenie $\mathbb{Q}_p$, unia wszystkich nierozgałęzionych.*

Fakt 6.5.13. *Jeżeli p nie dzieli m, to w $\mathbb{Q}_p^{unr}$ istnieją m-te pierwiastki z jedności, przez dołączenie których do $\mathbb{Q}_p$ to rozszerzenie powstaje.*

Dowód. Dla każdego m istnieje r, że $m \mid (p^r - 1)$. ☐

Fakt 6.5.14. *Obrazem $\mathbb{Q}_p^{unr}$ przez v_p jest $\mathbb{Z}$, gdyż nic się jeszcze nie rozgałęziło. Ciało residuów to algebraiczne domknięcie $\mathbb{F}_p$.*

Fakt 6.5.15. $v_p[\mathbb{Q}_p^a] = \mathbb{Q}$.

Koblitz twierdzi, że wszystkie rozszerzenia powstają przez wzięcie najpierw nierozgałęzionego, a następnie całkowicie rozgałęzionego.

Definicja 6.5.16. *Rozszerzenie $\mathcal{K}/\mathbb{Q}_p$ jest poskromione, gdy jest ono całkowicie rozgałęzione i p nie dzieli stopnia e.*

Fakt 6.5.17. *Poskromione rozszerzenia otrzymuje się z $\mathbb{Q}_p$ poprzez dołączenie pierwiastka wielomianu postaci $x^e - pu$ dla $u \in \mathbb{Z}_p^\times$.*

Fakt 6.5.18. *Niech $\mathcal{K}$ będzie niedyskretnym ciałem ultrametrycznym, które nie jest zupełne. Uzupełnienie $\mathcal{K}'$ jest topologiczną przestrzenią wektorową nad $\mathcal{K}$. Ustalmy liniowo niezależne $a, b \in \mathcal{K}'$. $\mathcal{K}^2$ oraz $\mathcal{K}a + \mathcal{K}b$ nie są izomorficzne jako liniowe p. topologiczne.*

Dowód. $\mathcal{K}^2$ nie ma gęstej podprzestrzeni wymiaru jeden. □

Fakt 6.5.19. *Niech X będzie p. ultrametryczną, dla której każdy ze zbiorów $\{d(x,y) : y \in X\}$ jest gęsty w $\mathbb{R}_+$. Rodzina domkniętych kul zamienia się w drzewo z częściowym porządkiem od zawierania. Dla ośrodkowej X, funkcja „średnica" ma przeliczalne włókna.*

6.6 Analiza

Tak jak w $\mathbb{Q}_p$, gdy mamy już ciało z wartością bezwzględna, można zacząć uprawianie analizy. Wiele z dotychczasowych osiągnięć przenosi się bez problemów na ogólny przypadek, bo nie korzystaliśmy z magicznych własności $\mathbb{Q}_p$. Jedyne zmiany, o których trzeba pamiętać, mają związek z rozgałęzieniem: być może trzeba będzie użyć jednolitości π zamiast p. Oto lista:

1. Ciąg (a_n) w $\mathcal{K}$ jest Cauchy'ego, wtedy i tylko wtedy gdy $|a_{n+1} - a_n| \to 0$.
2. Jeśli ciąg zbiega, ale nie do zera, to jest stacjonarny.
3. Szereg $\sum_n a_n$ w $\mathcal{K}$ zbiega, wtedy i tylko wtedy, gdy a_n zbiega do zera.
4. *Fakt 4.1.4 zachodzi dla podwójnych szeregów w $\mathcal{K}$.* [X]
5. Szereg potęgowy $\sum_n a_n X^n$ z $a_n \in \mathcal{K}$ jest ciągły w kuli otwartej o promieniu $1/\limsup |a_n|^{1/n}$ i przedłuża się do domkniętej, jeśli $|a_n|\rho^n \to 0$.
6. *Fakt 4.3.2 i twierdzenie 4.3.3 są prawdziwe dla szeregów z $\mathcal{K}[x]$.*
7. Szeregi potęgowe są różniczkowalne. [X]
8. Jeśli f i g są szeregami potęgowymi (współczynniki są z $\mathcal{K}$), x_m jest zbieżny, leży w przecięciu ich obszarów zbieżności i $f(x_m) = g(x_m)$, to $f \equiv g$.
9. Twierdzenie Strassmana działa dla K zamiast $\mathbb{Q}_p$ i $\mathcal{O}_k$ zamiast $\mathbb{Z}_p$. Wnioski z niego zachowują sens.
10. Zwykły szereg potęgowy definiuje p-adyczny logarytm, $\log_p \colon B \to K$, gdzie $B = 1+\pi\mathcal{O}_k$. Ten spełnia nadal $\log_p(xy) = \log_p(x) + \log_p(y)$ dla $x, y \in B$.
11. Zwykły szereg potęgowy definiuje p-adyczną eksponensę, $\exp_p \colon D \to K$, gdzie D to te $x \in \mathcal{O}_k$, że $|x| < p^{1/(1-p)}$. Ta spełnia $\exp_p(x + y) = \exp_p(x)\exp_p(y)$ dla $x, y \in D$.
12. Jeśli $X \in D$, to $\exp_p(x) \in B$ i $\log_p(\exp_p(x)) = x$.
13. Jeśli $x \in 1 + D$, to $\log_p(x) \in D$ i $\exp_p(\log_p(x)) = x$.
14. Logarytm p-adyczny to homomorfizm z $B = 1 + \pi\mathcal{O}_{\mathcal{K}}$ z mnożeniem w $\mathcal{P}_{\mathcal{K}} = \pi\mathcal{O}_{\mathcal{K}}$ z dodawaniem, a przy tym $\log_p \colon 1 + D \cong D$ (ta grupa jest izo-kopią $\mathcal{O}_{\mathcal{K}}$).
15. Dla każdego $\alpha \in \mathbb{Z}_p$ i $|x| < 1$ szereg $(1 + x)^\alpha$ zbiega.
16. Numeracja trochę kłamie!

6.7 Dołączanie p-tego pierwiastka

Wcześniejsze osiągnięcia teoretyczne tylko czekają, by użyć ich do czegoś konkretnego. Rozpatrujemy ciało $\mathcal{K} = \mathbb{Q}_p(\zeta)$, gdzie ζ to p-ty pierwiastek jedności, zaś p nie jest dwójką. Przypadek $p = 2$ jest, delikatnie mówiąc, trywialny. Zatem ζ zeruje

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = \sum_{k=0}^{p-1} X^k,$$

„p-ty wielomian cyklotomiczny".

Lemat 6.7.1. *Wielomian $\Phi_p(X)$ jest nierozkładalny nad $\mathbb{Q}_p$.*

Dowód. Niech $F(X) = \Phi_p(X+1)$. Jest on nierozkładalny tak samo jak $\Phi_p(X)$; sprawdzimy założenia kryterium Eisensteina. Mamy

$$F(X) = \frac{(X+1)^p - 1}{X} = \frac{X^p + 1 - 1}{X} \overset{p}{\equiv} X^{p-1},$$

więc wszystkie (poza pierwszym) współczynniki $F(X)$ dzielą się przez p. Ostatni współczynnik to $F(0) = \Phi_p(1) = p$ i z całą pewnością nie dzieli się przez p^2. □

Możemy stąd wywnioskować kilka rzeczy.

1. $\mathcal{K} = \mathbb{Q}_p(\zeta)$ jest rozszerzeniem $\mathbb{Q}_p$ stopnia $p-1$.
2. $\mathfrak{N}_{\mathcal{K}/\mathbb{Q}_p}(\zeta) = 1$, więc $|\zeta| = 1$.
3. Wielomian $F(X) = \Phi_p(X+1)$ jest minimalny dla $\zeta - 1$, zatem $\mathfrak{N}_{\mathcal{K}/\mathbb{Q}_p}(\zeta - 1) = p$ i $|\zeta - 1| = p^{1/(1-p)}$.
4. $\mathcal{K}$ jest całkowicie rozgałęzione, z jednolitością $\pi = \zeta - 1$.
5. $\zeta \equiv 1 \pmod{\pi}$; tzn. ζ jest 1-jednością w $\mathcal{O}_{\mathcal{K}}$.
6. $\mathbb{Z}_p[\zeta] \subseteq \mathcal{O}_{\mathcal{K}}$.

Skoro $\mathcal{K}$ jest całkowicie rozgałęzione, to $e = p-1$, $f = 1$ i ciało residuów $\mathcal{O}_{\mathcal{K}}/\pi\mathcal{O}_{\mathcal{K}}$ dla $\mathcal{K}$ to $\mathbb{F}_p$. Wybieramy liczby $0, 1, \ldots, p-1$ jako reprezentantów warstw. Wynika stąd, że elementy $\mathcal{K}$ mają π-adyczne rozwinięcia postaci

$$a_{-n}\pi^{-n} + a_{-n+1}\pi^{-n+1} + \ldots + a_0 + a_1\pi + \ldots,$$

gdzie $a_i \in [0, p-1] \cap \mathbb{Z}$. Jest tylko jeden mały kłopot: jak z p-adycznego rozwinięcia $x \in \mathbb{Q}_p$ uzyskać rozwinięcie π-adyczne? Już $x = p$ zapewnia koszmarne rachunki.

Fakt 6.7.2. *Tak naprawdę $\mathbb{Z}_p[\zeta] = \mathcal{O}_{\mathcal{K}}$.*

Dowód. Pokazaliśmy kiedyś, że elementy $\mathcal{O}_{\mathcal{K}}$ to $\mathbb{Z}_p$-liniowe kombinacje $\pi^l\alpha_i$ dla $0 \leq l < e$ oraz $1 \leq i \leq f$, gdzie α_i to elementy $\mathcal{O}_{\mathcal{K}}$, które redukują się do bazy dla $\mathfrak{K}$ nad $\mathbb{F}_p$.

W naszym przypadku $f = 1$, więc wystarcza nam $\alpha_1 = 1$, a przy tym $e = p-1$. Przypomnijmy sobie, że $\pi = \zeta - 1$, to koniec. □

A teraz niespodzianka, własne uogólnienie dla $\zeta = 2$.

Fakt 6.7.3. $\sum_{n \geq 1}(1-\zeta)^n : n = 0$.

Dowód. Skoro $|\zeta - 1| < 1$, szereg dla logarytmu zbiega. Z drugiej strony $\zeta^p = 1$, więc $p \log_p \zeta = \log_p 1 = 0$, co można zapisać w postaci

$$\sum_{n=1}^{\infty} (-1)^{n+1} \frac{(\zeta - 1)^n}{n} = 0.$$ □

Co jeszcze dziwniejsze, w $\mathcal{O}_{\mathcal{K}}$ można doszukać się takiego π_1, że $\pi_1^{p-1} + p = 0$. Jest to możliwe dzięki współpracy algebry z analizą.

6.8 Na drodze do $\mathbb{C}_p$

Dobrze jest znać teorię Galois, ale bez niej też można przeżyć. Elementy $x, y \in \mathbb{Q}_p^a$ nazywamy sprzężonymi (nad podciałem $\mathcal{K} \subseteq \mathbb{Q}_p^a$), jeżeli zerują ten sam nierozkładalny wielomian z $\mathcal{K}[X]$, którego współczynnik wiodący to jeden. Lemat Krasnera powie nam, że jeśli b jest „bliski" a, to jest od niego bardziej „skomplikowany".

Twierdzenie 12 (lemat Krasnera). *Gdy liczba $b \in \mathbb{Q}_p^a$ leży bliżej $a \in \mathbb{Q}_p^a$ niż jej sprzężenia ($|b-a| < |a-a_i|$ dla $i = 1, 2, \dots, n$, sprzężenia nad $\mathbb{Q}_p^a$), to $\mathbb{Q}_p(a) \subseteq \mathbb{Q}_p(b)$.*

Dowód. Niech $L = \mathbb{Q}_p(b)$, załóżmy, że $a \notin L$. W takim razie stopień $m = [L(a) : L]$ jest większy od jeden. Musi istnieć m homomorfizmów $\sigma\colon L(a) \to \mathbb{Q}_p^a$, które posyłają L na L (siebie). Załóżmy, że jeden z nich, σ_0, nie przerzuca a na a. Z jednoznaczności rozszerzenia wartości bezwzględnej wiemy, że $|\sigma(x)| = |x|$ dla $x \in \mathbb{Q}_p^a$. Zatem $|\sigma_0(b) - \sigma_0(a)| = |b-a|$. Ale wiemy też, że σ_0 trzyma L, a z nim b, więc $|b - \sigma_0(a)| = |b-a|$. To początek końca, bo

$$\begin{aligned}|a - \sigma_0(a)| &\leq \max\{|a-b|, |b-\sigma_0(a)|\}\\ &= \max\{|b-a|, |a-b|\} = |a-b|,\end{aligned}$$

a to niedopuszczalne. □

Z powyższego lematu płynie ważny wniosek.

Fakt 6.8.1. *Jeżeli $f(X) = X^n + \ldots + a_1X + a_0 \in \mathbb{Q}_p[X]$ jest nierozkładalny, $f(\lambda) = 0$ i $L = \mathbb{Q}_p(\lambda)$, to istnieje liczba rzeczywista $\varepsilon > 0$ o następującej własności: jeśli współczynniki $g(X) = X^n + \ldots + b_1X + b_0$ leżą „blisko": $|a_i - b_i| < \varepsilon$, to $g(X)$ jest nierozkładalny nad $\mathbb{Q}_p$ i ma pierwiastek w L.*

Dowód. Niech $\lambda_1 = \lambda, \lambda_2, \dots, \lambda_n$ będą pierwiastkami $f(X)$ w domknięciu $\mathbb{Q}_p^a$. Określmy $r = \min_{i\neq j} |\lambda_i - \lambda_j|$. Weźmy $g(X)$ taki, jak w fakcie. Wtedy (jeżeli jego pierwiastki w $\mathbb{Q}_p^a$ to $\mu_1, \dots, \mu_m$) ma on postać $g(X) = \prod(X - \mu_j)$. Przyjmijmy $D = \prod_i g(\lambda_i) = \prod_{i,j}(\lambda_i - \mu_j)$.

Jeśli $|D| < r^{n^2}$, to wielomian $g(X)$ jest nierozkładalny nad $\mathbb{Q}_p$ i ma pierwiastek w $L = \mathbb{Q}_p(\lambda)$. Wtedy istnieje para i, j, że $|\lambda_i - \mu_j| < r$. Definicja r pozwala na użycie lematu Krasnera, by pokazać, że $\mathbb{Q}_p(\lambda_i) \subseteq \mathbb{Q}_p(\mu_j)$. Oznacza to, że $\mathbb{Q}_p(\mu_j)$ jest stopnia co najmniej n nad $\mathbb{Q}_p$. Tak może być tylko wtedy gdy wielomian jest nierozkładalny i stopnia dokładnie n (bo μ_j „taki" zeruje?). Wtedy oba ciała mają stopień n i są zawarte jedno w drugim, zatem równe sobie.

Mamy nierozkładalność $g(X)$ oraz to, że $\mathbb{Q}_p(\lambda_i) = \mathbb{Q}_p(\mu_j)$. Gdyby okazało się, że $i = 1$, to byłby już koniec dowodu. Jeśli nie, to istnieje automorfizm $\mathbb{Q}_p^a$, który posyła λ_i na λ, zaś μ_j na jakiś inny pierwiastek $g(X)$. Po nałożeniu tego automorfizmu na równość $\mathbb{Q}_p(\lambda_i) = \mathbb{Q}_p(\mu_j)$ daje $L = \mathbb{Q}_p(\mu)$. Wtedy $g(X)$ ma pierwiastek μ w L.

Istnieje liczba $\varepsilon > 0$, że gdy $|a_i - b_i| < \varepsilon$, to $|D| < r^{n^2}$. □

Z tym dowodem nie wszystko jest w porządku, dlatego warto zapoznać się z problemami 258 – 262.

Fakt 6.8.2. *Ciało $\mathbb{Q}_p^a$ nie jest zupełne.*

Dowód. Wiemy, że nierozgałęzione rozszerzenie $\mathbb{Q}_p$ powstaje przez dołączenie pierwiastka rzędu względnie pierwszego z p. Wybierzmy $\zeta_1 = 1$, a potem ciąg $\zeta_2, \zeta_3, \dots$, że: $\zeta_i^{m_i} = 1$ (i $p \nmid m_i$), $\mathbb{Q}_p(\zeta_{i-1}) \subseteq \mathbb{Q}_p(\zeta_i)$ oraz $[\mathbb{Q}_p(\zeta_i) : \mathbb{Q}_p(\zeta_{i-1})] > i$.

Niech $c_n = \sum_{i=0}^{n} \zeta_i p^i$ będą sumami częściowymi szeregu. Tworzą w $\mathbb{Q}_p^a$ ciąg Cauchy'ego bez granicy. Załóżmy nie wprost, że jednak $c_n \to c \in \mathbb{Q}_p^a$. Liczba c to pierwiastek wielomianu nad $\mathbb{Q}_p$, powiedzmy, że stopnia d, który nie jest rozkładalny. Zatem $[\mathbb{Q}_p(c) : \mathbb{Q}_p] = d$. Rozważmy d-tą sumę częściową.

Skoro $c - c_d = \sum_{i=d+1}^{\infty} \zeta_i p^i$, zaś ζ_i są jednościami, to mamy $|c - c_d| \leq p^{-(d+1)}$. Ustalmy automorfizm $\sigma \colon \mathbb{Q}_p^a \to \mathbb{Q}_p^a$, który indukuje identyczność na $\mathbb{Q}_p$. Musi on zachować bezwzględną wartość, zatem $|\sigma(c) - \sigma(c_d)| \leq p^{-(d+1)}$.

Dążymy do sprzeczności, więc trzeba trzeba wybrać dobre σ. Pamiętając, że wybraliśmy ζ tak, by $[\mathbb{Q}_p(\zeta_i) : \mathbb{Q}_p(\zeta_{i-1})] > i$, możemy użyć tego dla $i = d$. Istnieje $d+1$ automorfizmów $\sigma_1, \dots, \sigma_{d+1}$, które obcięte do $\mathbb{Q}_p(\zeta_{d-1})$ są identycznością (więc trzymają $\zeta_1, \dots, \zeta_{d-1}$), ale różnią się parami na ζ_d.

Teraz, jeśli $i \neq j$, to $\sigma_i(c_d) - \sigma_j(c_d) = (\sigma_i(\zeta_d) - \sigma_j(\zeta_d))p^d$. Zauważmy, że $\sigma_i(\zeta_d)$ oraz $\sigma_j(\zeta_d)$ to różne m_d-te pierwiastki z jedynki, nie mogą przystawać do siebie modulo p. To oznacza, że p nie może dzielić ich różnicy i $|\sigma_i(c_d) - \sigma_j(c_d)| = p^{-d}$.

Prawie koniec: nakładamy (wszystkie) σ na c:

$$\begin{aligned} |\sigma_i(c_d) - \sigma_i(c)| &\leq p^{-(d+1)} \\ |\sigma_j(c_d) - \sigma_j(c)| &\leq p^{-(d+1)} \\ |\sigma_i(c_d) - \sigma_j(c_d)| &= p^{-d}. \end{aligned}$$

Zatem $|\sigma_i(c) - \sigma_j(c)| = p^{-d}$ (trójkąty są równoramienne), czyli $\sigma_i(c) \neq \sigma_j(c)$.

Innymi słowy, znaleźliśmy $d+1$ automorfizmów σ_i dla $\mathbb{Q}_p^a$, które są identycznością na $\mathbb{Q}_p$. Dodatkowo przerzucają c na różne elementy, zatem wielomian minimalny dla c ma $d+1$ (co najmniej) pierwiastków i nie może być stopnia d. Skoro c nie zeruje wielomianów z $\mathbb{Q}_p[X]$, to nie ma go w $\mathbb{Q}_p^a$. □

Skoro wszystkie ζ_i są pierwiastkami jedności rzędu, który jest względnie pierwszy z p, to pokazaliśmy coś jeszcze:

Fakt 6.8.3. *Maksymalne nierozgałęzione rozszerzenie $\mathbb{Q}_p^{unr}$ dla $\mathbb{Q}_p$ nie jest zupełne.*

Ponieważ $\mathbb{Q}_p^a$ nie jest zupełne, trzeba ponownie zbudować uzupełnienie, podobnie jak dla $\mathbb{Q}$ i $\mathbb{Q}_p$. Wnioskujemy stąd, że „ciało $\mathbb{C}_p$ istnieje".

Definicja 6.8.4. *$\mathbb{C}_p$ to uzupełnienie $\mathbb{Q}_p^a$ z normą $|\cdot|_p$.*

Jeśli tylko mamy zbieżny ciąg $x_n \to x \neq 0$ w ciele, które nie jest archimedesowe, to $|x_n| = |x|$ dla odpowiednio dużych wartości n. Oznacza to, że zbiór wartości bezwzględnych w $\mathbb{C}_p$ pokrywa się ze swoim odpowiednikiem w $\mathbb{Q}_p^a$: $v_p[\mathbb{C}_p^\times] = \mathbb{Q}$, zaś pojęcie jednolitości straciło wszelki sens.

Fakt 6.8.5. *Każdy element $x \in \mathbb{C}_p$ to iloczyn trzech liczb: ułamkowej potęgi p, pierwiastka jedności oraz 1-jedności.*

Dowód. Załóżmy, że $x \in \mathbb{C}_p$, zaś $v_p(x) = r = a/b$. Wybierzmy pierwiastek π dla $X^b - p^a$ w $\mathbb{Q}_p^a$; wtedy $v_p(\pi) = a/b$ i $y = x/\pi$ jest jednością. □

$\mathbb{C}_p$ to ogromny obiekt. Wreszcie uzyskaliśmy ciało, które nie dość, że jest zupełne, to jeszcze algebraicznie domknięte. Nie jest niestety sferycznie domknięte (stąd bierze się potrzeba powiększania go do Ω_p, o czym mowa będzie później).

Fakt 6.8.6. *$\mathbb{C}_p$ jest algebraicznie domknięte.*

Dowód. Ustalmy wielomian $f(X)$ o współczynnikach w $\mathbb{C}_p$, który nie jest rozkładalny. $\mathbb{Q}_p^a$ jest gęste w $\mathbb{C}_p$, możemy zatem znaleźć wielomiany o tym samym stopniu i współczynnikach w $\mathbb{Q}_p^a$ tak, by były bliskie „tym z $\mathbb{C}_p$".

Z faktu 6.8.1 wynika, że „odpowiednio bliski" $f_0(X)$ będzie nierozkładalny nad $\mathbb{C}_p$, nad $\mathbb{Q}_p$ zatem też. To ciało jest jednak algebraicznie domknięte, więc stopień f_0 (a więc także f) to jeden. □

Fakt 6.8.7. *$\mathbb{C}_p$ nie jest lokalnie zwarte.*

Prawdą jest mocniejszy fakt: każde lokalnie zwarte (więc też zupełne) ciało charakterystyki zero jest izomorficzne z $\mathbb{R}$, $\mathbb{C}$ lub skończonym rozszerzeniem $\mathbb{Q}_p$. Ciało $\mathbb{C}_p$ (mocy continuum) można traktować jak algebraiczne $\mathbb{C}$ z egzotyczną metryką, a przez to także topologią. Nie znamy izomorfizmu $\mathbb{C}_p \to \mathbb{C}$ z powodu użycia (w dowodzie istnienia) Aksjomatu Wyboru.

Co ciekawe, można zacząć od „końca": lokalnie zwartego ciała o charakterystyce zero i odtworzyć normę z miary Haara.

Fakt 6.8.8. *Jeżeli $n = hp^m$, $p \nmid h$, to rozszerzeń $\mathbb{Q}_p$ stopnia n w $\mathbb{Q}_p^a$ jest dokładnie (przynajmniej dla $p \leq 5$)*

$$\sum_{d|h} d \sum_{s=0}^{m} \frac{(p^{m+1} - p^s)(p^{n\varepsilon(s)} - p^{n\varepsilon(s-1)})}{(p-1)p^{-s}},$$

gdzie $\varepsilon(-1) = -\infty$, $\varepsilon(0) = 0$ i $\varepsilon(s) = \sum_{i=1}^{s} p^{-i}$, zaś

$$n(\sum_{s=0}^{m} p^s(p^{n\varepsilon(s)} - p^{n\varepsilon(s-1)}))$$

jest totally ramified.

6.9 Konstrukcja uniwersalnego ciała Ω_p

Niech $\mathcal{R}$ będzie pierścieniem $\ell^\infty(\mathbb{Q}_p^a)$ ograniczonych ciągów $x = (x_i)$ w $\mathbb{Q}_p^a$ z normą $\|x\| = \sup_i |x_i|$. Ustalmy ultrafiltr $\mathcal{U}$ na $\mathbb{N}$ zawierający zbiory $[n, \infty)$ (n naturalne). Ponieważ każdy ograniczony ciąg liczb rzeczywistych ma granicę pośród $\mathcal{U}$ (?), kładziemy $\varphi(x) = \lim_{\mathcal{U}} |x_i| \geq 0$.

Krótkie powtórzenie wiadomości o filtrach znajduje się na końcu sekcji.

Fakt 6.9.1. *Zbiór $\mathcal{I} = \varphi^{-1}(0)$ jest maksymalnym ideałem w $\mathcal{R}$. Ciało $\Omega_p = \mathcal{R}/\mathcal{I}$ jest rozszerzeniem $\mathbb{Q}_p^a$.*

Dowód. Pokażemy dla każdego $x \notin \mathcal{I}$ odwracalność modulo $\mathcal{I}$. Granica $r = \varphi(x)$ nie znika dla takiego x, więc istnieje zbiór $A \in \mathcal{U}$, że $r < 2|x_i| < 4r$ dla $i \in A$. Określamy ciąg y przez $y_i x_i = 1$ dla $i \in A$ i $y_i = 0$ w pozostałych przypadkach.

Jest on ograniczony: $|y_i| < 2/r$ dla $i \in A$, więc należy do $\mathcal{R}$. Z konstrukcji wynika, znikanie $1 - x_i y_i = 0$ na A, więc $1 - xy \in \mathcal{I}$. To pokazuje, że $x \mod \mathcal{I}$ odwraca się w ilorazie Ω_p, więc ten jest ciałem, zaś ideał $\mathcal{I} \triangleleft \mathcal{R}$ jest maksymalny. Stałe ciągi dają zanurzenie $\mathbb{Q}_p^a \to \Omega_p$. □

Funkcja φ zadaje na Ω_p wartość bezwzględną. Kładziemy $|\alpha| = \varphi(x)$ dla $\alpha = (x \bmod \mathcal{I})$.

Fakt 6.9.2. *Tak zdefiniowana wartość bezwzględna pokrywa się z normą ilorazową dla $\mathcal{R}/\mathcal{I}$, mianowicie dla $\alpha = (x \bmod \mathcal{I})$ mamy*

$$|\alpha|_\Omega = \|x \bmod \mathcal{I}\|_{\mathcal{R}/\mathcal{I}} := \inf_{y \in \mathcal{I}} \|x - y\|.$$

Dowód. Mamy $\lim_{\mathcal{U}} |z_i| \leq \sup |z_i|$ dla każdego $z \in \mathcal{R}$, a zatem $\lim_{\mathcal{U}} |x_i| = \lim_{\mathcal{U}} |x_i - y_i| \leq \sup |x_i - y$
oraz $|\alpha|_\Omega \leq \|x - y\|$ dla $y \in \mathcal{I}$, co dowodzi nierówności $|\alpha|_\Omega \leq \|\alpha\|_{\mathcal{R}/\mathcal{I}}$.

Jeśli $\alpha = x \bmod \mathcal{I}$, to dla każdego podzbioru $A \in \mathcal{U}$ można określić ciąg y wzorem $y_i = x_i \cdot [i \notin A]$. Wtedy ciąg y leży w ideale I oraz $\|x - y\| = \sup_{i \in A} |x_i|$, a do tego

$$\|\alpha\|_{\mathcal{R}/\mathcal{I}} \leq \inf_{A \in \mathcal{U}} \sup_{i \in A} |x_i| = \limsup |x_i| = |\alpha|_\Omega.$$

□

Fakt 6.9.3. $|\Omega_p^\times| = \mathbb{R}_{>0}$.

Dowód. Wynika to z gęstości $|\mathbb{Q}_p^a|$ w $\mathbb{R}_{\geq 0}$. □

Ciało Ω_p ma wiele intrygujących własności.

Fakt 6.9.4. *Ciało Ω_p jest algebraicznie domknięte.*

Dowód. Ustalmy $f \in \Omega_p[x]$ postaci $x^n + \alpha_{n-1}x^{n-1} + \ldots + \alpha_0$ i rodziny reprezentantów współczynników: $\alpha_k = (a_{ki})_i \bmod \mathcal{I}$. Rozważmy $f_i(x) = x^n + \sum_{k<n} a_{ki} x^i \in \mathbb{Q}_p^a[X]$. Każdy z nich ma naturalnie pierwiastki w $\mathbb{Q}_p^a$. Oznacza to, że produkt (tych pierwiastków) jest równy (co do znaku) a_{0i}, więc istnieje taki pierwiastek ξ_i, który jest mniejszy od $|a_{0i}|^{1/n}$. Ciąg ξ, (ξ_i), jest ograniczony: $\|\xi\| \leq \|\alpha_0\|^{1/n}$, $\xi \in \mathcal{R}$, klasa abstrakcji dla ξ zeruje f w Ω_p. □

Rozważmy zstępujący ciąg kul $\mathcal{B}[a_n, r_n]$ ($d(a_i, a_n) \leq r_n$ dla $i \geq n$) w przestrzeni ultrametrycznej X. Kiedy r_n dąży do zera, ciąg a_n jest Cauchy'ego i ma granicę (dla zupełnych X), zatem przekrój kul jest niepusty.

Definicja 6.9.5. *Przestrzeń ultrametryczną, w której nie istnieje ciąg zstępujący domkniętych kul o pustym przekroju, nazywamy sferycznie zupełną.*

Fakt 6.9.6. *Sferyczna zupełność pociąga zupełność.*

Dowód. Niech x_n będzie ciągiem Cauchy'ego. Jego granicą jest jedyny element przekroju zstępującego ciągu kul $\mathcal{B}[x_n, r_n]$; tu $r_n = \sup_{m>n} |x_m - x_n|$ maleje do zera. □

Odwrotna implikacja jest fałszywa.

Przykład 6.9.7. *$\mathbb{C}_p$ jest zupełne, ale nie sferycznie zupełne.*

Dowód. Niech r_n będzie ściśle malejącym ciągiem z $\Gamma = p^{\mathbb{Q}}$, którego granica nie jest zerem. W kuli $\mathcal{B}[0, r_0]$ znajdziemy dwie rozłączne kule domknięte o tym samym promieniu r_1, $\mathcal{B}_0$ i $\mathcal{B}_1$. W każdej z nich dwie następne (o promieniu r_2), $\mathcal{B}_{i0}$, $\mathcal{B}_{i1}$. Kule o różnych wieloindeksach tej samej długości są rozłączne, gdy przedłużymy indukcyjnie ten proces.

Kładziemy $\mathcal{B}_{(i_1, i_2, \ldots)} = \bigcap_{n \geq 1} \mathcal{B}_{i_1 \ldots i_n}$ (po lewej stronie (i_n) jest dowolnym ciągiem binarnym). Tak otrzymane kule są albo puste, albo domknięte, o promieniu $r = \lim_n r_n$. Skoro $r > 0$, to wszystkie są otwarte i parami rozłączne.

Przestrzeń $\mathbb{C}_p$ jest ośrodkowa, więc tylko przeliczalnie wiele spośród nich może być niepusta. □

Fakt 6.9.8. *Ciało Ω_p jest (sferycznie) zupełne.*

Dowód. Ustalmy zstępujący ciąg domkniętych kul $\mathcal{B}_n[\alpha_n, r_n]$, wtedy $|\alpha_{n+1} - \alpha_n| \leq r_n$, zaś ciąg r_n jest malejący (wynika to z ultranierówności).

Podnieśmy środki α_n do elementów $a_n \in \mathcal{R}$: skoro wartość bezwzględna jest normą ilorazową i $|a_{n+1} - a_n| \leq r_n < r_{n-1}$, wybieramy takie a_{n+1}, że $\|a_{n+1} - a_n\| < r_{n-1}$. Wtedy prawdą jest także $\|a_k - a_n\| < r_{n-1}$ oraz $|a_{ki} - a_{ni}| < r_{n-1}$ dla $k \geq n$ i i-tych składowych. Niech $\xi_i = a_{ii}$. Ciąg ξ leży w $\mathcal{R}$.

Oszacowanie $\|\xi - a_n\| \leq \sup_{i \geq n} |\xi_i - a_{ni}| \leq r_{n-1}$ wynika z należenia przedziałów $[n, \infty)$ do ultrafiltru $\mathcal{U}$. Wnioskujemy stąd, że dla $x = \xi \bmod \mathcal{I}$, $n > 0$ zachodzą nierówności:

$$|x - a_n| \leq \|\xi - \alpha_n\| \leq r_{n-1}$$
$$|x - a_{n-1}| \leq \max(|x - a_n|, |a_n - a_{n-1}|) \leq r_{n-1},$$

czyli $x \in \mathcal{B}_{n-1}$ jest świadkiem niepustości zbioru $\bigcap_n \mathcal{B}_n$. □

Mając Ω_p możemy określić $\mathbb{C}_p$ inaczej, jako domknięcie $\mathbb{Q}_p^a$ w Ω_p.

Fakt 6.9.9. *Ciało $\mathbb{C}_p$ jest ośrodkową przestrzenią metryczną.*

Dowód. Algebraiczne domknięcie $\mathbb{Q}_p^a$ dla $\mathbb{Q}_p$ jest ośrodkową przestrzenią metryczną, gęstą w $\mathbb{C}_p$. Przeliczalny zbiór $\mathbb{Q}^a$ jest ośrodkiem $\mathbb{C}_p$. □

Fakt 6.9.10. *Z algebraicznego punktu widzenia, $\mathbb{C} \cong \mathbb{C}_p$.*

Skąd się biorą takie potwory jak niedomknięte sferycznie przestrzenie? Okazuje się, że wcale nie są nie z tego świata.

Fakt 6.9.11. *Każda zupełna p. ultrametryczna X z gęstą metryką ma podprzestrzeń, która jest zupełna, ale nie sferycznie.*

Dowód. Ustalmy ciąg zstępujących kul $\mathcal{B}_n$, których ciąg średnic dąży do niezera. Wycięcie otwarniętego zbioru $\bigcap_n \mathcal{B}_n$ z X nie zmienia jej zupełności. W tej podprzestrzeni „kule $\mathcal{B}_i$" zstępują do zbioru pustego. □

Fakt 6.9.12. *Zupełna przestrzeń z dyskretną metryką (ultra-) jest sferycznie zupełna.*

Przykład 6.9.13. *Unormowana przestrzeń skończonego wymiaru nad zupełnym ciałem z dyskretną waluacją (takie są lokalnie zwarte) albo $B(X \to \mathcal{K})$.*

To, że ciało $\mathbb{C}_p$ nie jest sferycznie zupełne, wynika (inaczej) z następującego faktu.

Fakt 6.9.14. *Ośrodkowa p. ultrametryczna X z gęstą metryką nie jest zupełna sferycznie.*

Dowód. Ustalmy ośrodek $\{a_1, a_2, \ldots\}$ dla X oraz l. rzeczywiste $r_0, r_1, \ldots \in \mathbb{R}$, takie że $r_0 > r_1 > \ldots > r_0/2$ i $r_0 = d(a, b)$ dla pewnych $a, b \in X$. Formuła $d(x, y) \leq r_1$ rozbija X (przez relację równoważności) na co najmniej dwie kule. Niech $\mathcal{B}_1$ nie zawiera a_1, wtedy $d(\mathcal{B}_1) = r_1$.

Metryka na tej kuli też jest gęsta, więc możemy (tak samo) dostać kulę $\mathcal{B}_2 \subseteq \mathcal{B}_1$ średnicy r_2, która nie zawiera a_2, i tak dalej. Gdyby przekrój $\bigcap_n \mathcal{B}_n$ był niepusty, zawierałby kulę $\mathcal{B}$ dodatniej średnicy, w której nie leżałby żaden a_n. Ale te punkty tworzą ośrodek, sprzeczność. □

Przypomnijmy że lokalnie zwarte albo zupełne przestrzenie są Baire'a: przeliczalna suma domkniętych zbiorów o pustym wnętrzu ma puste wnętrze. Przestrzeń $\mathbb{Q}_p^a$ nie jest Baire'a.

Definicja 6.9.15. *Filtr to rodzina $\mathcal{A}$ podzbiorów X, która zawiera X (ale nie $\varnothing$) oraz jest zamknięta na dopełnienia i skończone przekroje.*

Definicja 6.9.16. *Filtr wolny to taki, który pusto się kroi.*

Definicja 6.9.17. *Rodzina $\mathcal{B} \subseteq \mathcal{A}$ jest bazą filtru, gdy każdy $A \in \mathcal{A}$ zawiera $B \in \mathcal{B}$.*

Lemat 6.9.18. *Niech $\mathcal{B}$ będzie rodziną niepustych podzbiorów X, taką że jeśli $A, B \in \mathcal{B}$, to istnieje $C \in \mathcal{B}$ zawarty w przekroju A i B. Nadzbiory elementów $\mathcal{B}$ tworzą filtr, którego $\mathcal{B}$ jest bazą.*

Filtr z lematu nazywamy generowanym przez $\mathcal{B}$.

Lemat 6.9.19. *Wolny filtr na nieskończonym X zawiera zbiory o skończonych dopełnieniach.*

Zbiory koskończone tworzą tak zwany filtr Frecheta.

Definicja 6.9.20. *Ultrafiltr to filtr maksymalny względem inkluzji.*

Fakt 6.9.21. *Filtr $\mathcal{A}$ na X jest ultrafiltrem, wtedy i tylko wtedy gdy dla każdego $A \subseteq X$, $A \in \mathcal{A}$ lub $X \setminus A \in \mathcal{A}$.*

Definicja 6.9.22. *Filtr $\mathcal{A}$ na przestrzeni topologicznej X zbiega do $x \in X$, gdy każde otoczenie x zawiera pewien $A \in \mathcal{A}$.*

Fakt 6.9.23. *Każdy ultrafiltr na zwartej przestrzeni zbiega.*

Przykład 6.9.24. *Ustalmy ograniczony ciąg liczb rzeczywistych a_n oraz ultrafiltr $\mathcal{U}$ na $\mathbb{N}$. Wtedy $\inf_n a_n \leq \lim_{\mathcal{U}} a_n \leq \sup_n a_n$.*

Wrócimy do Ω_p. Przypomnijmy, że jego ciało residuów jest nieskończone, zaś $|\Omega_p^\times| = \mathbb{R}_+$. Każdej domkniętej kuli $\mathcal{B}[a, r]$ zawartej w Ω_p przypiszemy teraz filtr okrężny $\mathcal{F}_\mathcal{B}$ (na Ω_p).

Jeśli $\mathcal{B}$ jest jednym punktem, za $\mathcal{F}_\mathcal{B}$ bierzemy filtr otoczeń generowany przez małe kule wokół a, $\mathcal{B}(a, \varepsilon)$. Jeśli jednak $\mathcal{B}$ ma dodatni promień, generatory to $\mathcal{B}[a, r+\varepsilon] \setminus \bigcup_{i=1}^n \mathcal{B}(a_i, r-\varepsilon)$. Im mniejszy $\varepsilon > 0$ lub większy n, tym mniejsze zbiory; istotnie stanowią one bazę pewnego filtru.

Łatwo widać, że generatory zawierają $x \in \Omega_p$, takie że jest $r < |x - a| < r + \varepsilon$. Jednocześnie każdy $b \in \mathcal{B}$ ma $\delta > 0$, że $\{x : r - \delta < |x - b| < r\}$ leży w pewnym generatorze, skąd natychmiastowo dostajemy lemat:

Lemat 6.9.25. *Niech $\mathcal{B}$ oznacza jakąś kulę o dodatnim promienu r, $a \in \mathcal{B}$. Poniższe zbiory są bazą filtru $\mathcal{F}_{\mathcal{B}}$, gdzie a_i brane są ze sfer $S_r(a) : |x-a| = r$, zaś $0 < \varepsilon < r$.*

$$\{r - \varepsilon < |x - a| < r + \varepsilon\} \setminus \bigcup_{k=1}^{n} \mathcal{B}(a_i, r - \varepsilon)$$

Zastępując ε czymś mniejszym możemy nawet zakładać, że $i \neq j$ pociąga $|a_i - a_j| = r$.

Powyższe definicje przenoszą się na podzbiory $X \subseteq \Omega_p$. Załóżmy, że $X \cap A \neq \varnothing$ dla wszystkich $A \in \mathcal{F}_{\mathcal{B}}$. Wtedy $\mathcal{F}_{\mathcal{B}}$ indukuje filtr na X, nadal nazywany okrężnym.

Przykład 6.9.26 ($X = \mathbb{C}_p$)**.** *Jeśli domknięta kula $\mathcal{B}$ w Ω_p nie tnie $\mathbb{C}_p$, zaś $\delta(\mathcal{B}) = d(\mathcal{B}, \mathbb{C}_p)$, to ślad $\mathcal{F}_{\mathcal{B}}$ na $\mathbb{C}_p$ jest okrężnym filtrem bezśrodkowym.*

Bibliografia

[1] BOVEY, J. D. A note on Waring's problem in p-adic fields. *Acta Arithmetica 29* (1976), 343–351.

[2] BURGER, E. B., AND STRUPPECK, T. Does $\sum_{n\geq 0} n!^{-1}$ really converge? Infinite series and p-adic analysis. *The American Mathematical Monthly 103* (1996), 565–577.

[3] HASSE, H. *Number Theory*. Springer, 1980.

[4] PARVARDI, A. Lifting the exponent lemma (LTE). *Art of problem solving 103*, 7 (2011), 565–577.

[5] SERRE, J. P. *A Course in Arithmetic*. Springer, 1973.

[6] VOLOCH, J. F. On the p-adic Waring's problem. *Acta Arithmetica XC*, 1 (1999), 92–95.