Spis treści

Od autora

Dobry Bóg stworzył liczby naturalne, reszta jest dziełem człowieka, ale p-adyczne szkarady mają jeszcze inny rodowód. Nie należą bowiem do standardowej matematyki poznawanej na studiach, choć odgrywają ważną rolę we współczesnej teorii liczb. Stanowią wygodny język do opisu kongruencji, a jednocześnie umożliwiają stosowanie typowo analitycznych narzędzi (jak szeregi potęgowe).

Rozdziały: pierwszy, drugi, szósty, a także częściowo: czwarty z piątym przypominają bardziej zwiedzanie niż naukową ekspedycję i nie są wystarczające do prowadzenia poważnych badań. Ich treść oparta jest na książce F. Gouvea [**?**], podaje ona rozsądny przepis na rozszerzanie ciał, a przy tym nie odstrasza mniej doświadczonych podróżników formalizmem.

Bardziej wymagające jest dzieło Roberta [**?**], które nadal podąża za analogiami z klasyczną analizą. Fałszywość twierdzenia o wartości średniej utrudnia życie, ale nowa wartość bezwzględna nie jest bezużyteczna. Autor opisuje bardziej skomplikowane struktury: solenoidy, „właściwsze" ciała $\mathbb{C}_p$ i Ω_p, a także przedstawia analizę zespoloną, funkcjonalną i niektóre funkcje specjalne. Chodzi tu o funkcję Γ Mority, eksponens Artina-Hassego i logarytm Iwasawy. Bez niego rozdziały: czwarty z piątym, siódmy, ósmy i dziewiąty wyglądałyby zupełnie inaczej.

Jeszcze trudniejsza w lekturze jest „Analytic Elements in p-adic Analysis" spod pióra Escassuta; w tych notatkach nie ma jednak odniesień do niej. Dołączyłem jednak opis analogonu funkcji ζ Riemanna, to znaczy p-adycznego przedłużenia Kuboty-Leopoldta do $\mathbb{Q}_p$ w oparciu o książkę Koblitza [**?**] (który to korzysta z nieopublikowanych notatek Mazura). Brakuje w niej twierdzenia Hassego-Minkowskiego (można je znaleźć w „Number Theory" Borewicza i Szafarewicza), pracy dyplomowej Tate'a (do znalezienia w podręczniku „Algebraic Number Theory" Langa). Temat p-adycznych L-funkcji odpowiadających charakterom Dirichleta też jest nie do końca zgłębiony.

Zajmujący tylko jedną stronę (ale nadal zajmujący!) rozdział dziesiąty to zachęta do przeczytania jedynej w swoim rodzaju monografii trzech rosyjskich uczonych ([**?**]). Tu i ówdzie widać też inspirację Schikhofem ([**?**]). W przyszłości planuję dopisanie dodatkowych ustępów o zastosowaniu metod p-adycznych w kombinatoryce czy teorii macierzy (na przykład w oparciu o nieco przestarzałą „Local fields" Casselsa, [**?**]), nie wiem jednak, kiedy to nastąpi.

Liczby p-adyczne do matematyki wprowadził Kurt Hensel. Oto, co chyba było 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 liczbą 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. Jest to dobre, gdyż zawiera 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. Niech $p = 3$. Wtedy $24 : 17 = (2p + 2p^2) : (2 + 2p + p^2) = p + p^3 + 2p^5 + p^7 + p^8 + 2p^9 + \ldots$. Wszystkie szeregi Laurenta w potęgach p o skończonym ogonie tworzą ciało ($\mathbb{Q}_p$). Taka definicja jest jednak do niczego.

Mam nadzieję, że Czytelnik znajdzie po lekturze tego skryptu ulubioną gałąź matematyki w p-adycznej odmianie. Oby się tylko na niej nie powiesił.

Notacja. Oznaczamy ciała przez $\mathcal{K}$, pierścienie: $\mathcal{R}$, grupy: $\mathcal{G}$, przestrzenie liniowe: $\mathcal{V}$, kule: $\mathcal{B}$. Indeks sumowania to zazwyczaj k lub i, pod literą j zawsze kryje się jednostka urojona, zaś m i n to najczęściej jakieś liczby całkowite. Elementy ciała to x, y, z, promienie kul: r, R, bliżej nieokreślone stałe: C. Kule domknięte odróżniamy od otwartych nawiasami ($\mathcal{B}[\cdot, \cdot]$ kontra $\mathcal{B}(\cdot, \cdot)$), jako że domknięcie kuli otwartej zazwyczaj nie jest kulą domkniętą o tym samym promieniu. Wykładnikami są greckie litery: α, β, niekoniecznie naturalnymi, ale λ to tylko mnożnik.

Leon Aragonés
Wrocław, Polandia
17 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 nieархimedesowa.*

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 $\|x + y\| \leq \max\{\|x\|, \|y\|\}$ jest oczywista dla $y = 0$, wystarczy dowieść $\|z + 1\| \leq \max\{\|z\|, 1\}$ ($z \in \mathcal{K}$). Dla $n \in \mathbb{N}$:

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

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

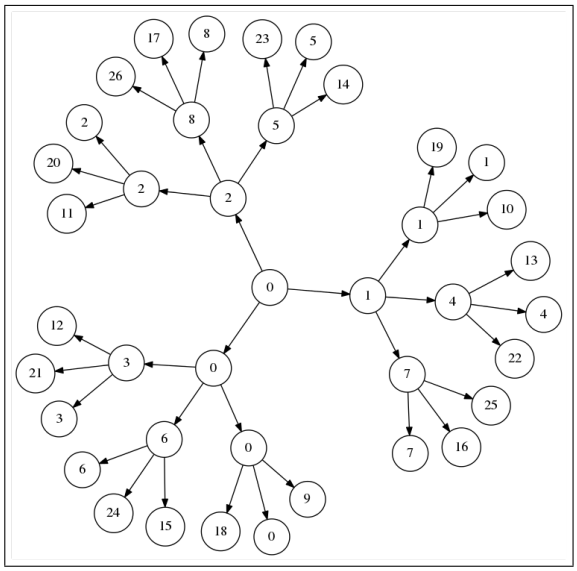
Ciało, gdzie wszystkie działania są ciągłe, nazywa się ciałem topologicznym, takie może być ciało z metryką.

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 $0 \leq a_j \leq n_0 - 1$.

$$\|n\| = \left\| \sum_{i=0}^{m} a_i n_0^i \right\| \leq \sum_{i=0}^{m} \|a_i\| \, n_0^{i\alpha} \leq n_0^{m\alpha} \sum_{i=0}^{m} n_0^{-i\alpha}$$

$$\leq n_0^{m\alpha} \sum_{i=0}^{\infty} n_0^{-i\alpha} = n_0^{m\alpha} \frac{n_0^\alpha}{n_0^\alpha - 1} = C n_0^{m\alpha}$$

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

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

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

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

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 1.3.4 (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:

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

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* $f(x + h) = f(x) + f'(x)h + f''(x)h^2/2 + \ldots$, $x, h \in \mathcal{K}$.

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 $\{\pm1, \pm2, \pm5, \pm10\}$.*

Dowód. Wystarczy użyć wzmocnionego lematu. □

Lemat Hensela mówi, że jeżeli wielomian dzieli się przez $x - x_0$: $f(x) \equiv (x - x_0)g(x) \bmod p$, 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 $f(x) \equiv (g_1h_1)(x)$ 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, $g_{n+1} \equiv g_n \bmod p^n$ oraz $h_{n+1} \equiv h_n \bmod p^n$, a przy tym $f \equiv g_nh_n \bmod p^n$. 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 $f \equiv g_2h_2 \bmod p^2$ i uproszczeniu otrzymamy $f - g_1h_1 = pk_1$ dla $k_1 \in \mathbb{Z}_p[x]$. Dalsze uproszczenie do $pk_1 \equiv pr_1h_1 + ps_1g_1 \bmod p^2$ 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 $ag_1 + bh_1 \equiv 1 \bmod p$. Rozpatrzmy nowe wielomiany, $\overline{r}_1 = bk_1$ i $\overline{s}_1 = ak_1$. Wiemy już, że

$$\overline{r}_1h_1 + \overline{s}_1g_1 \equiv k_1 \pmod p.$$

Podzielmy $\overline{r}_1$ przez g_1; niech r_1 będzie resztą: $r_1 = g_1q + r_1$. Rzecz jasna $\deg r_1 < \deg g_1$. Ale jeśli położymy $s_1 = \overline{s}_1 + h_1q$, to wszystko będzie grać:

$$\begin{aligned}\ldots &= r_1h_1 + s_1g_1 \equiv (\overline{r}_1 - g_1q)h_1 + (\overline{s}_1 + h_1q)g_1\\ &\equiv \overline{r}_1h_1 - g_1h_1q + \overline{s}_1g_1 + g_1h_1q \equiv \overline{r}_1h_1 + \overline{s}_1g_1\\ &\equiv k_1 \pmod p.\end{aligned}$$

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 ([**?**]) □

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

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

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. $\square$

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 $a+b+c \equiv 0 \bmod 8$. Twierdzenie odwrotne jest prawdziwe na mocy uogólnionego lematu Hensela. $\square$

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. $\square$

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 $p \mid b + r^2 c$, 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

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

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

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

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). $\square$

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* $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$.

Dowód. Jeśli $m = n + r > n$, to $|x_m - x_n|$ można oszacować z góry, $|\sum_{k=1}^{r} x_{n+k} - x_{n+k-1}| \le \max_{1\le k\le r} |x_{n+k} - x_{n+k-1}|$, 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 $|\sum_{n\ge 0} x_n| \le \max_n |x_n|$.*

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

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

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 $k \ge 0$. 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 $i \ge N$ 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 $\max\{i, k\} \ge N$ pociąga $|x_{ik}| < \varepsilon$.*

Dowód. Ustalmy ε. Drugi warunek zapewnia N_0 (zależne tylko od ε), że $|x_{ik}| < \varepsilon$ dla $i \ge N_0$. Pierwszy zaś dla każdego i daje N_1, dla którego $k \ge N_1$ 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: $\sum_{i=0}^{\infty}\sum_{k=0}^{\infty} x_{ik} = \sum_{k=0}^{\infty}\sum_{i=0}^{\infty} x_{ik}$.*

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

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

Wnioskujemy stąd, że podwójne szeregi także zbiegają, bo

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

Pozostało nam uzasadnić, że sumy są sobie równe.

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

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

Jeśli więc $k \ge N+1$, 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 $\sum_{n\ge 0} n^k p^n$ 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 $\sum_{n\ge 0} n\cdot n! = -1$ 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: $\sum_{n\ge 1} n^2(n+1)! = 2$, $\sum_{n\ge 1} n^5(n+1)! = 26$, $\sum_{n\ge 1} 4^{-n-1}\cdot n^2(n+1)! = -1$.

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

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

Fakt 2.3.1. *Szereg $\sum_n a_nx^n$ 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: $\{x\in\mathbb{Q}_p : \lim_{n\to\infty}|a_nx^n|=0\}$. 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. □

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: $f(x)=\sum_n a_nx^n$ i $g(x)=\sum_n b_nx^n$, przy czym $b_0=0$, by napis $f(g(x))$ miał sens (niezależnie od topologii). Przez formalne złożenie rozumiemy

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

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 $|b_nx^n|\leq|g(x)|$, to $h(x)$ też zbiega, do $f(g(x))$.*

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

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

$$f(g(x))=a_0+\sum_{m\geq 1}\sum_{n\geq m}a_md_{m,n}x^n,$$

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

Aby uzasadnić poprawność zamiany kolejności sumowania powołamy się na fakt 2.1.6 i oszacujemy $a_md_{m,n}x^n$.

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 $f(x) = \sum_n a_n x^n \in \mathbb{Q}_p[[x]]$ istnieje dla $x = x_0$.*

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

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 $(n \text{ nad } m) a_n x_0^{n-m} (x - x_0)^m$ 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 $|n a_n x^{n-1}| \leq |a_n x^{n-1}| = |a_n x^n|/|x| \to 0$, 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:

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

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. □

2.4 Wielozbieżność

Czy istnieje szereg o wymiernych wyrazach, który jest zbieżny w $\mathbb{Q}_p$ dla wszystkich $p \leq \infty$? Pytanie to zadali Edward Burger oraz Thomas Struppeck w pracy [**?**]. Okazuje się, że tak:

$$\sum_{n=0}^{\infty} n! \rightsquigarrow \sum_{n=0}^{\infty} \frac{n!}{(n!)^2} \rightsquigarrow \sum_{n=0}^{\infty} \frac{n!}{(n!)^2 + 1}.$$

Naturalne pytanie o algebraiczność granicy szeregu jest trudne. Pomimo to przeprowadzimy teraz konstrukcję, która pozornie stanowi dużo większe wyzwanie: wskażemy szereg zbieżny do liczby wymiernej w każdym z ciał $\mathbb{Q}_p$ (dla $p \leq \infty$).

Definicja 2.4.1. $X_m = \{\frac{1+am}{1+bm} : a, b \in \mathbb{Z}\} \subseteq \mathbb{Q}$ *dla* $m \geq 2$.

Lemat 2.4.2 (III)**.** *Zbiór X_m leży gęsto na prostej $\mathbb{R}$.*

Dowód. Niech $\varepsilon > 0$, $a/b \in \mathbb{Q}$. Gdy $b^2mn\varepsilon > |a - b|_\infty - b\varepsilon$, $|a/b - (1 + amn)/(1 + bmn)|_\infty < \varepsilon$. □

Każdej ze skończenie wielu liczb pierwszych $p \in P$ niech odpowiada $\delta_p \in \mathbb{Q}_p^\times$ równa $\sum_n d_{p,n}p^n$ dla $n \geq l_p$, gdzie cyfra początkowa jest niezerem, a kolejne leżą między 0 oraz $p - 1$. Niech $\Upsilon = \prod_p |\delta_p|_p^{-1}$.

Lemat 2.4.3 (IV)**.** *Przy tych oznaczeniach istnieje całkowita $M > 0$, że $|\delta_p - M\Upsilon|_p < |\delta_p|_p$ dla wszystkich $p \in P$.*

Dowód. Dla każdej $p \in P$ definiujemy $\Upsilon_p = \Upsilon|\delta_p|_p = m_p/n_p$, gdzie całkowite m_p, n_p są względnie pierwsze z p. Rozpatrzmy jednocześnie wszystkie kongruencje $m_p x \equiv n_p d_{p,l_p} \bmod p$. Chińskie twierdzenie o resztach daje nam jakieś rozwiązanie $M > 0$. Każdemu $p \in P$ odpowiada całkowita t_p, że

$$\frac{m_p}{n_p} M = d_{p,l_p} + p\frac{t_p}{n_p},$$

co pociąga $M\Upsilon = d_{p,l_p}p^{l_p} + p^{1+l_p} \cdot t_p/n_p$.

Skoro $n_p \not\equiv 0 \bmod p$, to pierwszy człon rozwinięcia dla $M\Upsilon$ to $d_{p,l_p}p^{l_p}$, dokładnie taki sam jak dla δ_p. To kończy dowód. □

Wniosek 2.4.4 (V)**.** $|\delta_p - M\Upsilon x|_p < |\delta_p|_p$*, jeśli $p \in P$ i $x \in X_p$.*

Dowód. Silna nierówność trójkąta razem z lematem pokazują, że

$$\begin{aligned} \ldots = |\delta_p - M\Upsilon x|_p &= |\delta_p - M\Upsilon + M\Upsilon - M\Upsilon x|_p \\ &\leq \max\{|\delta_p - M\Upsilon|_p, |M\Upsilon - M\Upsilon x|_p\} \\ &< \max\{|\delta_p|_p, |M\Upsilon|_p|1 - x|_p\} \\ &\leq \max\{|\delta_p|_p, |\delta_p|_p/p\} = |\delta_p|_p, \end{aligned}$$

co uzasadnia żądaną nierówność. □

Twierdzenie 6. *Dane są liczby $x_p \in \mathbb{Q}_p$ dla wszystkich $p \leq \infty$. Istnieje szereg $\sum y_n$ o wymiernych wyrazach, $y_n > 0$ dla $n \geq 1$, którego granicą w $\mathbb{Q}_p$ jest x_p.*

Dowód. Definiujemy y_n rekursywnie: $y_0 = [x_\infty - 1]$. Niechaj P_n będzie zbiorem pierwszych n liczb pierwszych. Zakładamy, że mamy już $y_0, \ldots, y_n$ i spełnione są dla $p \in P_n$:

1. $y_n \in \mathbb{Q}_+$ dla $n > 0$, $y_0 \in \mathbb{Q}$
2. jeśli $S_n := \sum_{k=0}^n y_k$, to $0 < x_\infty - S_n < 2^{1-n}$
3. $S_{n-1} = x_p$ albo $|x_p - S_n|_p < |x_p - S_{n-1}|_p$.

Łatwo widać, że założenia są spełnione w kroku bazowym. Dla każdej liczby pierwszej $p \in P_{n+1}$ napiszmy $\delta_p = x_p - S_n$, $P_{n+1}^\delta = \{p \in P_{n+1} : \delta_p \neq 0\}$. Gdy $P_{n+1}^\delta = \varnothing$, to kładziemy $M\Upsilon := 1$. W przeciwnym razie lemat IV daje całkowitą $M > 0$, że $|\delta_p - M\Upsilon|_p < |\delta_p|_p$ dla wszystkich $p \in P_{n+1}^\delta$. Niechaj Π będzie produktem pierwszych $n + 1$ liczb pierwszych.

Lemat III orzeka o istnieniu takiej wymiernej $u \in X_\Pi$, dla której $0 < u < (x_\infty - S_n)/(M\Upsilon)$, a przy tym

$$\left|\frac{x_\infty - S_n}{M\Upsilon} - u\right|_\infty < \frac{|S_n - x_\infty|_\infty}{2M\Upsilon}.$$

Zauważmy, że $X(\Pi) = \bigcap_p X_p$ (przekrój po $p \in P_{n+1}$). To pozwala $*$-wyciągnąć z wniosku V: $|\delta_p - uM\Upsilon|_p < |\delta_p|_p$. Teraz kładziemy $y_{n+1} := uM\Upsilon$, wszystkie warunki są spełnione.

Pokażemy, że szereg $\sum_n y_n$ zbiega do x_p w $\mathbb{Q}_p$. Z założenia drugiego wynika, że jest tak dla $p = \infty$. A jeśli $p < \infty$? Wtedy S_n jest monotonicznie rosnącym ciągiem liczb wymiernych,

$x_p = S_i$ dla co najwyżej jednego i. Razem z $*$-nierównością daje nam to informację, że $0 < |x_p - S_{n+1}|_p < |x_p - S_n|_p$ (dla dużych n). Ciąg $|x_p - S_n|$ od pewnego miejsca jest ściśle malejący, więc dąży do zera (gdyż składa się z potęg p), zatem sam szereg zbiega w $\mathbb{Q}_p$ do x_p. □

Spostrzeżenie: przez zmianę górnego ograniczenia w IV lemacie (z $|\delta_p|_p$) a także w drugim założeniu (o 2^{1-N}) uzyskać można szeregi zbieżne dużo szybciej.

2.5 Przestępność

Definicja 2.5.1 (lokalna)**.** *Niech $a, b \in \mathbb{Z}$ będą względnie pierwsze. Wtedy $h(a/b) := \max\{|a|_\infty, |b|_\infty\}$.*

Definicja 2.5.2. *Dla $X \subseteq \mathbb{Q}$, $h(X) := \max\{h(x) : x \in X\}$.*

Przypomnimy teraz twierdzenie, które jest użyteczne samo w sobie.

Twierdzenie 7 (Liouville'a)**.** *Dla każdej liczby pierwszej $p \leq \infty$ i algebraicznej $x \in \mathbb{Q}_p$ stopnia $d \geq 1$ nad $\mathbb{Q}$ istnieje stała $c > 0$, że dla wymiernych liczb $a/b \neq \alpha$ mamy*

$$\frac{c}{h(a/b)^d} \leq \left|x - \frac{a}{b}\right|_p.$$

Wybierzemy taki ciąg $\beta_i \in \mathbb{Q}$, że spełnione są nierówności $0 < |\beta_n|_p \cdot n^n \cdot h(\{\beta_0, \ldots, \beta_{n-1}\})^{n^2-2n+1} \leq 1$ i $\gamma \in \mathbb{Q}^\times$, przy czym te pierwsze chyba mogą być prawdziwe prawie zawsze.

Definicja 2.5.3. *Niech $q_n = \sum_{k=0}^n \beta_k \gamma^k \in \mathbb{Q}$.*

Definicja 2.5.4. *Niech $f(x) = \sum_{k \geq 0} \beta_k x^k$.*

Jeśli $m = h(\gamma)$, to $h(q_n) \leq (n+1)h(\{\beta_0, \ldots, \beta_n\})^{n+1} m^n$. Z pierwszej nierówności mamy dla $\lambda_k = 1 : h(\{\beta_0, \ldots, \beta_k\})$, $n > m$ i $\Delta = |f(\gamma) - q_n|_p$:

$$\begin{aligned}\Delta &\leq \sum_{k=n+1}^{\infty} |\beta_k|_p |\gamma|_p^k \leq \sum_{k=n+1}^{\infty} \frac{m^k}{k^k} \cdot \lambda_{k-1}^{(k-1)^2} \\ &\leq \sum_{k=n+1}^{\infty} \lambda_{k-1}^{(k-1)^2} \leq \sum_{k=n+1}^{\infty} \lambda_n^{(k-1)^2} \\ &\leq \lambda_n^{n \cdot n} \sum_{k=0}^{\infty} \lambda_n^k \leq \lambda_n^{n \cdot n} \sum_{k=0}^{\infty} 2^{-n} = 2\lambda_n^{n \cdot n}.\end{aligned}$$

Jeżeli założymy teraz, że $f(\gamma)$ jest algebraiczna, stopnia d, to twierdzenie Liouville'a zapewnia nam stałą $c > 0$, taką że $ch(q_n)^{-d} \leq |f(\gamma) - q_n|_p$. Stąd ciąg nierówności

$$\begin{aligned}0 < c/2 &\leq h(q_n)^d \lambda_n^{n \cdot n} \leq (n+1)^d m^{dn} \lambda_n^{-dn-d} \lambda_n^{n \cdot n} \\ &= [(n+1)^d \lambda^{n^2:3}][m^{dn} \lambda^{n^2:3}] \lambda_n^{n^2:3-dn-d}.\end{aligned}$$

Im większe n, tym bliższa zeru prawa strona, ale to nie jest możliwe, gdyż ogranicza ją $c/2$. Zatem $f(\gamma)$ jest przestępna w $\mathbb{Q}_p$ i pozostało wskazać stosowne β_i.

Przez $A_p(n)$ oznaczmy (tylko lokalnie) sumę cyfr $n \in \mathbb{N}$ w rozwinięciu przy podstawie p.

Lemat 2.5.5 (VI)**.** *Gdy n jest naturalna, zaś p pierwsza, to*

$$v_p(n!) = \frac{n - A_p(n)}{p-1}.$$

Wniosek 2.5.6 (VII)**.** *Dla liczby pierwszej p oraz prawie każdej n (naturalnej) mamy $v_p(n!) \geq n/(2p-2)$.*

Dowód. Niech $n = a_0 + \ldots + a_k p^k$, gdzie $a_k \neq 0$, zaś same cyfry a_i spełniają $0 \leq a_i \leq p-1$. Wtedy $n \geq p^k$ i $k \leq \log n / \log p$, zatem

$$A_p(n) \leq (p-1)\left(1 + \frac{\log n}{\log p}\right),$$

co dla dużych n daje $A_p(n) \leq n/2$. Lemat VI z wcześniejszą nierównością kończą dowód. □

Fakt 2.5.7. *Jeśli $q \in \mathbb{Q}^\times$, to dla każdego $p \leq \infty$ liczba $f(q) \in \mathbb{Q}_p$ jest przestępna:*

$$f(x) = \sum_{n=0}^{\infty} \left(\frac{n!}{n!^2 + 1}\right)^{n! \cdot n! \cdot n!} x^n.$$

Dowód. Zdefiniujmy wreszcie ciąg β:

$$\beta_n = \left[\frac{n!}{(n!)^2 + 1}\right]^{n!^3}$$

Wystarczy sprawdzić, że dla dużych wartości n stosowne nierówności są spełnione.

Jeśli $p = \infty$, to $|\beta_n|_\infty \leq (n!)^{-n!^3}$. Z drugiej strony, dla n odpowiednio dużych (i $m = n-1$) mamy

$$\begin{aligned}\frac{\lambda_m^{m \cdot m}}{n^n} &= \frac{1}{n^n (1 + m!^2)^{m^2 \cdot m!^3}} \geq_\diamondsuit (n!)^{-n - m^2 \cdot m!^3} \\ &\geq (n!)^{-n!^3} \geq |\beta_n|_\infty.\end{aligned}$$

Niech teraz p będzie pierwsza. Z wniosku VII wnioskujemy, że dla dużych n: $v_p(\beta_n) = v_p(n!^i) \geq in/(2p-2)$, $i = n!^3$.

Jak już zauważyliśmy, mamy („$\diamondsuit$", wyciągnięte z przypadku $p = \infty$):

$$\frac{\lambda_m^{m \cdot m}}{n^n} \geq \left(\frac{1}{n!}\right)^{n + m^2 m!^3}.$$

Prawa strona przekracza $p^{-in/(2p-2)}$, koniec. □

2.6 Lemat o podnoszeniu wykładnika

Przytoczymy teraz mało znany, użyteczny lemat z pracy [**?**].

Lemat 2.6.1. *Załóżmy, że liczby x, y (całkowite), n (naturalna) i p (pierwsza) zostały dobrane tak, by $p \nmid nxy$ oraz $p \mid x \pm y$. Wtedy $v_p(x^n \pm y^n) = v_p(x \pm y)$.*

Podamy teraz pierwsze dwie formy lematu, w zależności od znaku w „$p \mid x \pm y$".

Fakt 2.6.2. *Załóżmy, że liczby x, y (całkowite), n (naturalna) i $p > 2$ (pierwsza) zostały dobrane tak, by $p \mid x \pm y$ i $p \nmid xy$. Wtedy $v_p(x^n \pm y^n) = v_p(x \pm y) + v_p(n)$.*

Przypadek $p = 2$ jak zwykle wymaga więcej uwagi.

Fakt 2.6.3. *Niech nieparzyste liczby całkowite x, y dają tę samą resztę z dzielenia przez 4. Wtedy*

$$v_2(x^n - y^n) = v_2(x - y) + v_2(n).$$

Fakt 2.6.4. *Niech dane będą nieparzyste liczby całkowite x, y oraz parzysta $n > 0$. Wtedy*

$$v_2(x^n - y^n) = v_2(x - y) + v_2(x + y) + v_2(n) - 1.$$

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 $f\colon \mathbb{N} \to M$ 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. □

Nadmieńmy: $\Delta^k f(0) = \sum_{i\leq k}(-1)^{k-i}(k \text{ nad } i) f(i)$ 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 $(\cdot \text{ nad } i)$.*

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 $x \mapsto (x \text{ nad } i) \bmod p$ 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 $f(x) = \sum_{i\leq T}(x \text{ nad } i) m_i$ 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 $\mathfrak{Z}$ to $f \mapsto 1 \oslash f$, to znaczy $(\mathfrak{Z} f)(0) = 0$ oraz $(\mathfrak{Z} f)(n) = \sum_{i=0}^{n-1} f(i)$.*

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

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. $\nabla \circ \mathfrak{Z} = \mathrm{id}$, $\mathfrak{Z} \circ \nabla = \mathrm{id} - P_0$, $\nabla \circ \mathfrak{Z} - \mathfrak{Z} \circ \nabla = P_0$.

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

Twierdzenie 8 (van Hamme)**.** *Funkcje f zmiennej całkowitej mogą zostać rozwinięte (dla całkowitego $n \geq 0$) z resztą van Hamme'a, $R_{n+1} f(x) = \nabla^{n+1} f \oslash (x \text{ nad } n)$.*

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

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 9 (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 $f\colon \mathbb{N} \to \mathbb{C}_p$ 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.

$$\left| \sum_{i=n}^{2n} \nabla^i f(0) \cdot \nabla^{2n-i} g(0) \right| \leq \|\nabla^n f\| \cdot \|g\|$$

$$\left| \sum_{i=0}^{n-1} \nabla^i f(0) \cdot \nabla^{2n-i} g(0) \right| \leq \|f\| \cdot \|\nabla^n g\|$$

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

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

Wniosek 3.2.6. *Twierdzenie van Hamme'a jest prawdziwe także dla $f\colon \mathbb{Z}_p \to \mathbb{C}_p$, 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 $F = \mathfrak{d} f$. Wtedy $\varphi(f(x)) = \varphi(F(x+1)) - \varphi(F(x)) = 0$. □

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

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 10 (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 $\mathcal{V}_n = \{f \in \mathcal{K}[x] : \deg f \le n\} \le \mathcal{V}$.

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 $n \ge 1$. Niech $\delta x^n = f(x)$. Wtedy

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

Podstawmy w tym wzorze najpierw $x = 0$, a potem $a = x$. Tak otrzymamy $f(x) = \sum (n \text{ nad } k) \delta(x^{n-k})(0) \cdot x^k$. Widać, że f jest wielomianem stopnia $\le n$, 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 następujące 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 $\le n$.*

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

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

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: $\deg p_n = n$, $T(p_n) = n p_{n-1}$, $p_n(0) = [n = 0]$, 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 $\alpha_1 = 1$):

$$1 = \|q_0\| = \|T q_1\| \le \|q_1\| = \|T q_2\| \le \cdots.$$

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 $T q_n = \nabla U \circ SV^n(f_n)$, a skoro $UV = 1$ i operatory komutują, $T q_n = q_{n-1}$.

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

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

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 $\|S\| \le 1$ i $\|q_n\| \le \|S\| \|V^n\| \|f_n\| = 1$. □

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 $\|f\| = \sup_{n \ge 0} |c_n|$: $f(x) = \sum_n c_n q_n$.*

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

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 $TM_x - M_x T = \varphi'(D)$.*

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 $p_n(x) = x\cdot\ldots\cdot(x-n+1)$.

3.5 Różniczki i pochodne

Niech $X \subseteq \mathcal{K}$ będzie pozbawiony izolatorów, zaś $\mathcal{K}$ stanowi zupełne rozszerzenie $\mathbb{Q}_p$ (jak $\mathbb{C}_p$ lub Ω_p).

Definicja 3.5.1. *Funkcja $f\colon X \to \mathcal{K}$ jest różniczkowalna w punkcie a, gdy istnieje granica*

$$\lim_{x\to a}\frac{f(x)-f(a)}{x-a} =: f'(a)$$

Równoważnie możemy żądać rozwinięcia rzędu jeden (dla $\phi(x)\to 0$): $f(x) = f(a) + (x-a)f'(a) + (x-a)\phi(x)$.

Przykład 3.5.2. *Niech otwarta kula $\mathcal{B}_n \subseteq \mathbb{Z}_p$ ma swój środek w p^n i promień $|p^{2n}|$. Funkcja $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ dana wzorem*

$$f(x) = \sum_{n=1}^{\infty} p^{2n}\cdot 1_{x\in\mathcal{B}_n}$$

jest stała na otwartych kulach, zatem lokalnie stała poza zerem. Jej pochodna zeruje się, ale ilorazy różnicowe $[f(y)-f(x)] : (y-x)$ dla $x = p^n$, $y = p^n - p^{2n}$ są stale równe jeden!

Przykład 3.5.3. *Ciągła funkcja $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ zadana wzorem*

$$f(x) = x - \sum_{n\geq 1} p^{2n}\cdot[|x-p^n|_p < p^{-2n}]$$

jest różniczkowalna dla wszystkich $x\in\mathbb{Z}_p$ z $f'(x) = 1$; pomimo to f nie jest injekcją, bo $f(p^n) = f(p^n - p^{2n})$.

Przykład 3.5.4. *Ciągła funkcja $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ zadana wzorem*

$$x = \sum_{n=0}^{\infty} a_n p^n \mapsto f(x) = \sum_{n=0}^{\infty} a_n p^{2n}$$

jest różniczkowalna dla wszystkich $x\in\mathbb{Z}_p$ z $f'(x) = 0$; pomimo to f nie jest lokalnie stała (przez injektywność).

Przykład 3.5.5. *Niech $x = \sum_{n\geq 0} a_n p^n \in \mathbb{Z}_p$. Jeśli $|x|_p = p^{-m}$, niech $f(x)$ powstaje z x przez przestawienie a_{2m} i a_{2m+1}, $f(0) := 0$. Funkcja f jest różniczkowalną bijekcją $\mathbb{Z}_p \to \mathbb{Z}_p$, $f' = 1$, ale w zerze nie jest lokalną izometrią.*

Powyższy przykład można poprawić tak, żeby funkcja f nie była wcale Lipschitza.

Przykład 3.5.6. *Istnieje $\mathcal{C}^\infty$-bijekcja $\mathbb{Z}_p \to \mathbb{Z}_p$ o pochodnej jeden, która nie jest izometrią.*

Klasyczna definicja bycia różniczkowalnym (ciągle) nie jest więc przystosowana do liczb p-adycznych.

Definicja 3.5.7. *Funkcja $f\colon X \to \mathcal{K}$ jest ściśle różniczkowalna w punkcie a („$f\in\mathcal{S}^1(a)$"), jeśli dla $(x,y)\to(a,a)$ istnieje granica*

$$\lim_{(x,y)}(\Phi f)(x,y) := \lim_{(x,y)}\frac{f(x)-f(y)}{x-y}$$

Jeżeli pochodna funkcji $f\colon (a,b)\to\mathbb{R}$ istnieje i jest ciągła, to f jest ściśle różniczkowalna w każdym $x\in(a,b)$. Nie jest to ultrametryczną prawdą: tu interesujące wyniki wymagają równie interesujących założeń.

Fakt 3.5.8. *Niech funkcja $f\colon X\to\mathcal{K}$ będzie ściśle różniczkowalna w punkcie a i ma tam niezerową pochodną. Funkcja $f/f'(a)$ obcięta do pewnego otoczenia V dla a jest izometrią.*

Dowód. Skoro $f\in\mathcal{S}^1(a)$, dla każdego $\varepsilon > 0$ istnieje otoczenie V_ε dla a, że $x\in V_\varepsilon, y\in V_\varepsilon$ daje $|\Phi f(x,y) - f'(a)| < \varepsilon$. Weźmy $\varepsilon = |f'(a)|$. Wtedy dla $x,y\in V$ zachodzi $|\Phi f(x,y)| = |f'(a)|$, a to pociąga $|f(x)-f(y)| = |f'(a)|\cdot|x-y|$. □

Podamy teraz zaskakujące uogólnienie lematu Hensela: funkcja $f-c$ ma zero $x\in\mathcal{B}$, $f(x)=c$, gdy tylko $|f(b)-c|$ jest małe dla pewnego $b\in\mathcal{B}$, chociaż f nie musi być wielomianem.

Fakt 3.5.9. *Niech funkcja f z otoczenia punktu $a\in\mathcal{K}$ będzie ściśle różniczkowalna w a, $f'(a)\neq 0$. Wybierzmy otwartą kulę $\mathcal{B}$, w której leży a, że*

$$\sigma := \sup_{x\neq y\in\mathcal{B}}\left|\frac{f(x)-f(y)}{x-y}-f'(a)\right| < |f'(a)|.$$

Wtedy f przerzuca otwarte kule na otwarte kule: obrazem $\mathcal{B}(b,\varepsilon)$ jest kula $\mathcal{B}(f(b),|f'(a)|\varepsilon)$.

Dowód. Niech $s=f'(a)\neq 0$. Funkcja f/s jest izometrią, więc $f[\mathcal{B}(b,\varepsilon)]\subseteq\mathcal{B}(f(b),|s|\varepsilon)$.

Dla dowodu drugiej inkluzji wybierzmy c z drugiej kuli: że $|f(b)-c|<|s|\varepsilon$. Pokażemy, że równanie $f(x)=c$ ma pewne rozwiązanie z $|x-b|<\varepsilon$ (funkcja $\varphi(x)=x-(f(x)-c)/s$ ma punkt stały). Zauważmy, że $\varphi[\mathcal{B}(b,\varepsilon)]\subseteq\mathcal{B}(b,\varepsilon)$.

Funkcja φ jest kontrakcją ze stałą $\sigma/|s|<1$ na lewej kuli (domkniętej w zupełnym K), zatem ma tam dokładnie jeden punkt stały. □

Jeżeli funkcja f spełnia któryś z poniższych warunków, to powiemy, że jest **ściśle różniczkowalna** ($f\in\mathcal{S}^1(X)$).

Fakt 3.5.10. *Dla funkcji $f\colon X\to\mathcal{K}$ te warunki są równoważne:*

1. *$f\in\mathcal{S}^1(a)$ dla $a\in X$.*
2. *funkcja Φf przedłuża się ciągle z $X^2\setminus\triangle_X$ do X^2.*
3. *f jest różniczkowalna w $a\in X$, istnieje ciągła funkcja α na X^2, która znika na $\triangle_X$ z*
$$f(y)=f(x)+(y-x)(f'(x)+\alpha(x,y)).$$

Twierdzenie o przerzucaniu kul staje się wyjątkowo ciekawe dla lokalnie zwartych ciał $\mathcal{K}$ (skończonych rozszerzeń $\mathbb{Q}_p$). Tam mamy klasyczne oznaczenia: $\mathfrak{p}=\pi\mathcal{O}$, $\mathcal{O}/\mathfrak{p}=\mathbb{F}_q$.

Jeśli $r\in|\mathcal{K}^\times|$, każda kula $\mathcal{B}[a,r]$ jest rozłączną sumą q otwartych kul $\mathcal{B}_i$ (o promieniach r), czyli domkniętych kul $\mathcal{B}_i$ (o promieniach θr z $\theta=|\pi|<1$). Dowolny zbiór zawierający q różnych punktów $x_i\in\mathcal{B}[a,r]$, że $i\neq j$ implikuje $|x_i-x_j|\geq r$ zawiera co najwyżej po jednym punkcie z $\mathcal{B}_i$, zatem dokładnie po jednym.

Fakt 3.5.11. *Izometria f z G, zwartego, otwartego podzbioru K, w K, skończone rozszerzenie $\mathbb{Q}_p$, przerzuca kule na kule.*

Dowód. Jeśli $\mathcal{B}[a,r]\subseteq G$, to $f[\mathcal{B}[a,r]]\subseteq\mathcal{B}[f(a),r]$, pokażemy drugie zawieranie. Rozbijmy $\mathcal{B}[a,r]$ na mniejsze rozłączne kule o środkach w a_i oraz promieniach $\varepsilon=|\pi|^v r$. Obrazy punktów $x_i=f(a_i)$ tworzą układ q^v punktów spełniający $|x_i-x_j|>\varepsilon$ dla $i\neq j$, zatem obraz $f[\mathcal{B}[a,r]]$ zawiera punkt z każdej z mniejszych kul rozkładu (czyli kroi wszystkie kule domknięte dodatniego promienia). Wynika stąd, że $f[\mathcal{B}[a,r]]$ leży gęsto w $\mathcal{B}[f(a),r]$; jest też zwarty, przez co domknięty. □

Definicja 3.5.12. *Granulat otwarto-zwartego $G\subseteq\mathcal{K}$ to skończone rozbicie na domknięte kule tego samego promienia.*

Granulaty są porównywalne (kule są rozłączne lub zawarte jedna w drugiej). Kula w uboższej jest sumą rozłączną pewnej potęgi q^v kul z bogatszej. Zauważmy, że $q^v\equiv 1 \bmod p-1$, więc liczba kul w dwóch granulatach różni się o wielokrotność $p-1$. To uzasadnia poprawność takiej definicji:

Definicja 3.5.13. *Typ otwarto-zwartego $G\subseteq\mathcal{K}$ to $\tau(G)$, liczba kul w dowolnym granulacie modulo $p-1$.*

Dopuszczamy rozbicia na kule o różnych promieniach, gdyż $\tau(G\sqcup G')=\tau(G)+\tau(G')$, typ rozłącznej sumy jest addytywny. Podsumujmy.

Fakt 3.5.14. *Otwarty i zwarty $G\subset\mathcal{K}$ oraz jego obraz przez ściśle różniczkowalną injekcję $f\colon G\to\mathcal{K}$ o nieznikającej pochodnej mają ten sam typ.*

Dowód. Z $f\in\mathcal{S}^1(a)$ i $f'(a)\neq 0$ wnioskujemy, że punkt a ma otoczenie V w G, takie że f przerzuca otwarte kule na kule w $f[V]$. □

Wniosek 3.5.15. *Dla $p>2$ nie istnieje ściśle różniczkowalna bijekcja $f\colon\mathbb{Z}_p\to\mathbb{Z}_p^\times$, której pochodna nie znika.*

Zajmiemy się teraz funkcjami bardziej różniczkowalnymi. Przyjmijmy

$$\Phi_2 f(x,y,z)=\frac{\Phi f(x,z)-\Phi f(y,z)}{x-y}.$$

Definicja 3.5.16. *Jeśli dla $(x,y,z)\to(a,a,a)$ istnieje granica $\Phi_2 f(x,y,z)$, to funkcja $f\colon X\to\mathcal{K}$ jest dwukrotnie różniczkowalna (ściśle) w puncie a, co zapisujemy $f\in\mathcal{S}^2(a)$.*

Fakt 3.5.17. *Jeśli $f\in\mathcal{S}^2(a)$, to $f\in\mathcal{S}^1(a)$.*

Definicja 3.5.18. *Funkcję $\Phi_2 f$ można przedłużyć ciągle do X^3, wtedy i tylko wtedy gdy $f\in\mathcal{S}^2(a)$ dla każdego a.*

Fakt 3.5.19. *Jeśli $f\in\mathcal{S}^2$, to $f'\in\mathcal{S}^1$.*

Uwaga: twierdzenie odwrotne nie jest prawdziwe (choćby dla niektórych funkcji z $f'\equiv 0$).

Spróbujemy teraz zróżniczkować szereg Mahlera. Ustalmy f, ciągłą funkcję na $\mathbb{Z}_p$ oraz $y\in\mathbb{Z}_p$. Możemy wtedy rozwinąć: $f(x+y)=\sum_{k\geq 0}c_k(y)(x \text{ nad } k)$, $c_k(y)=(\nabla^k f)(y)$ dąży do zera.

Fakt 3.5.20. *Ciągła funkcja f na $\mathbb{Z}_p$ jest różniczkowalna w y, wtedy i tylko wtedy gdy $|(\nabla^k f)(y)/k|\to 0$ dla $k\to\infty$. Wtedy*

$$f'(y)=-\sum_{k=1}^{\infty}\frac{(-1)^k}{k}\cdot(\nabla^k f)(y).$$

Dowód. Bez straty ogólności, $y=0$, gdyż funkcję $f(x)$ możemy zastąpić przez $f(x+y)$. Wtedy $c_0=f(0)$ i

$$\frac{f(x)-f(0)}{x}=\sum_{k=1}^{\infty}\frac{c_k}{k}\binom{x}{k}=\sum_{k=1}^{\infty}\frac{c_k}{k}\binom{x-1}{k-1}.$$

Jeśli $|c_k/k|$ zbiega do zera, szereg Mahlera zadany przez $g(y)=\sum_{k\geq 1}(y \text{ nad } k-1)\cdot c_k/k$ reprezentuje ciągłą funkcję na $\mathbb{Z}_p$ i w szczególności $f'(0)$ istnieje, jest równe $g(-1)$, czyli $\sum_{k\geq 1}(-1)^{k-1}c_k/k$.

Odwrotnie, gdy $f'(0)$ istnieje, to funkcja g równa $f'(0)$ w zerze i $(f(x)-f(0))/x$ poza nim jest ciągła. Współczynniki Mahlera dla niej to $\gamma_k=\nabla^k g(0)$ (dążą do zera). Zapiszmy więc g jako $\sum_{k\geq 0}\gamma_k(x \text{ nad } k)$.

Mamy $x(x \text{ nad } k)=(k+1)(x \text{ nad } k+1)+k(x \text{ nad } k)$ (jak łatwo sprawdzić bezpośrednim rachunkiem), co upoważnia do $f(x)=f(0)+xg(x)=c_0+\sum_{k\geq 1}k(\gamma_{k-1}+\gamma_k)(x \text{ nad } k)$. Z jednoznaczności współczynników Mahlera dla f możemy wywnioskować, że $c_k=k(\gamma_k+\gamma_{k-1})$, więc $c_k/k\to 0$. □

Fakt 3.5.21. *Dla ciągłej funkcji $f(x)=\sum_{k\geq 0}c_k\binom{x}{k}$ klasy $\mathcal{C}(\mathbb{Z}_p)$ ograniczoność $k|c_k|$ jest równoważna z lipschitzowskością f.*

Wniosek 3.5.22. *$\|\Phi f\|:=\sup_{x\neq y}|\Phi f(x,y)|=\sup_{n\geq 1}\kappa_n|c_n|$ jest skończona, gdzie κ_n to największa potęga p nie większa od n.*

Wielkość $\|\Phi f\|$ nie jest normą, lecz półnormą, gdyż znika na stałych. Aby dostać normę możemy położyć $q_0 = 1$ i napisać $\|f\|_* = \sup(|f(0)|, \|\Phi f\|)$.

Wniosek 3.5.23. *Gdy f jest Lipschitza, to $\|f\|_* \le \|\wr f\|_* \le p\|f\|_*$, więc $\wr f$ też jest Lipschitza.*

Wniosek 3.5.24. *$(Lip(\mathbb{Z}_p), \|\cdot\|_*)$ oraz ℓ^∞ są izomorficzne dzięki f. Funkcje 1 i $\kappa_n(x \text{ nad } n)$ odpowiadają „kanonicznej bazie" ℓ^∞.*

$$f\colon \sum_{n=0}^{\infty} c_n \binom{x}{n} \mapsto \left(\frac{c_n}{\kappa_n}\right).$$

Fakt 3.5.25. *Ustalmy $f(x) = \sum_{k\ge 0} c_k(x \text{ nad } k) \in \mathcal{C}(\mathbb{Z}_p)$. Ciąg $k^n|c_k|$ dąży do zera, wtedy i tylko wtedy gdy f jest klasy $\mathcal{S}^n$.*

Fakt 3.5.26. *Funkcja $\sum_{k\ge 0} c_k(x \text{ nad } k) \in \mathcal{C}(\mathbb{Z}_p)$ jest analityczna, wtedy i tylko wtedy gdy $c_n/n!$ dąży do zera.*

Następne stwierdzenie jest szokujące.

Przykład 3.5.27. *Suma ($\wr f$) analitycznej funkcji na $\mathbb{Z}_p$ nie musi taka być!*

Podobne charakteryzacje istnieją także w terminach bazy van der Puta. Przypomnijmy, $e_0 \equiv 1$, zaś dla $n \ge 1$ funkcja e_n jest indykatorem kuli $\mathcal{B}(n, 1/n) \subseteq \mathbb{Z}_p$.

Niech $f = \sum_{n\ge 0} a_n e_n \in \mathcal{C}(\mathbb{Z}_p, \mathcal{K})$.

Fakt 3.5.28. *Funkcja f jest a-lipschitzowska, wtedy i tylko wtedy gdy $\sup_n |a_n|n^a < \infty$, $a > 0$.*

Fakt 3.5.29. *Funkcja f jest a-lipschitzowska, wtedy i tylko wtedy gdy $\sup_n |a_n|n^a < \infty$. Jeśli $a > 1$, pociąga to zerowanie pochodnej, ale implikacja w drugą stronę jest fałszywa.*

Fakt 3.5.30. *Funkcja f ma zerową pochodną, wtedy i tylko wtedy gdy $|a_n|n$ (albo $a_n/(n - n_-)$) dąży do zera.*

Fakt 3.5.31. *Funkcja f ma zerową pochodną i jest $\mathcal{C}^n$, wtedy i tylko wtedy gdy $|a_m|m^n$ dąży do zera.*

Zajmiemy się teraz ratowaniem twierdzenia o wartości średniej, które nie zawsze jest prawdziwe.

Fakt 3.5.32. *Niech szereg $f \in \mathcal{K}\{x\}$ wyznacza funkcję f na kuli $\mathcal{B}_[0, 1]$. Ustalmy $h, t \in \mathcal{K}$, takie że $|t| \le 1$ i $|h| \le r_p = |p|^{1/(p-1)}$. Wtedy $|f(t + h) - f(t)| \le |h| \cdot \|f'\|$.*

Wynika z niego inne, o punkcie stałym.

Fakt 3.5.33. *Niech $\mathcal{K}$ będzie skończonym rozszerzeniem $\mathbb{Q}_p$, zaś $\mathcal{B}$ jednostkową kulą domkniętą. Ustalmy szereg $f \in \mathcal{K}\{x\}$, że $\|f\| \le 1$, $\|f'\| < 1$ oraz $\inf_{x\in\mathcal{B}} |f(x) - x| \le r_p$. Wtedy f ma punkt stały na kuli $\mathcal{B}$.*

Sekcja 73 książki Schikhofa porusza:

Twierdzenie 11 (Łuzin)**.** *Niech funkcja $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ posiada pochodną. Wtedy to obrazem zbioru zerowego jest zbiór zerowy, zaś $\{f(x) : f'(x) = 0\}$ jest zerowy.*

Istnieje jednak ciągła funkcja $\mathbb{Z}_p \to \mathbb{Z}_p$, obrazem przez którą pewnego zbioru zerowego jest całe $\mathbb{Z}_p$.

Przykład 3.5.34. *Niech $X := \{\sum_n a_n p^n : a_1 = a_3 = \ldots = 0\}$, zaś $t(x)$ będzie najmniejszym nieparzystym indeksem n, że $a_n \ne 0$. Wtedy dla $g(x) = \sum_{j<t(x)} a_j p^{j:2}$ (suma po parzystych j) mamy równość $g[X] = \mathbb{Z}_p$.*

Skończymy na izometriach.

Fakt 3.5.35. *Jeśli ciało residuów jest nieskończone, to „domknięta" kula jednostkowa i sfera są izometrycznie izomorficzne.*

Wniosek 3.5.36. *Wtedy istnieje izometria $\mathcal{K} \to \mathcal{K}$ nie „na".*

Fakt 3.5.37. *Każda izometria $\mathcal{K} \to \mathcal{K}$ jest „na", wtedy i tylko wtedy gdy $\mathcal{K}$ jest sferycznie zupełne i ma skończone ciało residuów.*

Fakt 3.5.38. *Każda funkcja 1-Lipschitza z $X \subseteq \mathcal{K}$ w ciało $\mathcal{K}$ jest $\mathcal{K}$-liniową kombinacją dwóch izometrii.*

Dowód. Jedną z nich jest identyczność. □

Fakt 3.5.39. *Jeśli zbiory $A, B \subseteq \mathbb{Z}_p$ są przeliczalne i gęste, to istnieje izometria f dla $\mathbb{Z}_p$, taka że $f[A] = B$.*

Fakt 3.5.40. *Ciągły endomorfizm $\mathbb{C}_p$ jest surjektywną izometrią.*

3.6 Algebra Tate'a

Pierścień szeregów formalnych $\mathcal{K}[[X]]$ zawiera podprzestrzeń wektorową złożoną z szeregów, których współczynniki zbiegają do zera, zwaną $\mathcal{K}\{X\}$.

Podprzestrzeń ta jest izomorficzna z p. Banacha $c_0(\mathcal{K})$ i jest uzupełnieniem $\mathcal{K}[x]$ z normą Gaußa (to znaczy supremum współczynników). Zachodzi nierówność $\|fg\| \le \|f\| \cdot \|g\|$, z której wynika (jednostajna) ciągłość mnożenia w $\mathcal{K}[x]$ i jego ciągłość w $\mathcal{K}\{x\}$.

Z tego względu $\mathcal{K}\{x\}$ jest pierścieniem i algebrą Banacha, algebrą Tate'a jednej zmiennej nad $\mathcal{K}$. **Algebra Tate'a** pozostaje chwilowo poza naszym zasięgiem.

3.7 Całka Volkenborna

Zdefiniujemy całkę z funkcji $f\colon \mathbb{Z}_p \to \mathcal{K}$, gdzie $\mathcal{K}$ to zupełne rozszerzenie $\mathbb{Q}_p$. Niestety, fakt 3.2.7 pokazuje, że nie można zdefiniować formy liniowej φ na przestrzeni $\mathcal{C}(\mathbb{Z}_p)$, ciekawej i niezmienniczej na przesunięcia.

Można tego dokonać dla $\mathcal{F}^{lc}(\mathbb{Z}_p)$. Przyjmijmy, że $\varphi(1) = 1$. Odporność na przesuwanie wymusza tę samą wartość p^{-n} dla indykatorów warstw $p^n\mathbb{Z}_p$. Supremum tych funkcji wynosi 1, ale $|\varphi(f)|$ jest dowolnie duże, gdyż równe p^n, co odbiera formie φ ciągłość.

Zdefiniujmy „objętość" kuli $\mathcal{B}[j, |p^n|]$ w $\mathbb{Z}_p$ jako $p^{-n} \in \mathbb{Q}_p$. Zaraz przedstawiona konstrukcja nie jest niezmiennicza na przesunięcia i wymaga istnienia przynajmniej $(\wr f)'(0)$, choć nie ma nic złego w ograniczaniu się do $f \in \mathcal{S}^1(\mathbb{Z}_p)$. Zacznijmy od wyrażenia

$$S(f, n) := \frac{1}{p^n} \sum_{j=0}^{p^n-1} f(j) = \sum_{j=0}^{p^n-1} f(j) m(j + p^n\mathbb{Z}_p).$$

Reprezentuje ono sumę Riemanna dla f. Nieoznaczona suma F dla funkcji f była zdefiniowana tak, by $\nabla F = f$ ($F(0) = 0$). Zachodzi wtedy

$$S(f, n) = \frac{F(p^n) - F(0)}{p^n}.$$

Widać więc, że jeśli F różniczkuje się w początku, to granica z $n \to \infty$ istnieje.

Kiedy f ma współczynniki Mahlera c_n, współczynniki $\wr f$ są „przesunięte", zaś różniczkowalność w początku ma miejsce dokładnie gdy $|c_{n-1}/n| \to 0$ (ale tak jest dla $f \in S^1(\mathbb{Z}_p)$).

Definicja 3.7.1. ***Całką Volkenborna*** *dla funkcji $f \in S^1(\mathbb{Z}_p)$ jest:*

$$\int_{\mathbb{Z}_p} f(x)\,dx = \lim_{n\to\infty} \frac{1}{p^n} \sum_{j=0}^{p^n-1} f(j) = (\mathfrak{2}\, f)'(0)$$

Przykład 3.7.2. *Jeśli b_k są liczbami Bernoulliego, to*

$$\int_{\mathbb{Z}_p} x^k\,dx = b_k \qquad\qquad \frac{t}{\exp t - 1} = \sum_{m=0}^{\infty} b_m \frac{t^m}{m!}.$$

Fakt 3.7.3. *Dla $f \in S^1(\mathbb{Z}_p)$ prawdziwe jest poniższe oszacowanie. Jeśli $\|f_n - f\|_* \to 0$, to „$\int f_n \to \int f$" (całki nad $\mathbb{Z}_p$).*

$$I = \left| \int_{\mathbb{Z}_p} f(x)\,dx \right| \le p\|f\|_1.$$

Dowód. $I = |(\mathfrak{2}\, f)'(0)| \le \|\,\mathfrak{2}\, f\|_* \le p\|f\|_*$ (patrz **??**). □

Przypomnijmy, że ∇f to dyskretny gradient funkcji f, to jest: $\nabla f(x) = f(x+1) - f(x)$.

Fakt 3.7.4. *Dla $f \in S^1(\mathbb{Z}_p)$ mamy $I := \int_{\mathbb{Z}_p} \nabla f(x)\,dx = f'(0)$.*

Dowód. $I = (\mathfrak{2}\,\nabla f)'(0) = (f - f(0))'(0) = f'(0)$. □

Znamy nieoznaczone sumy dla funkcji dwumianowych, a zatem scałkowanie szeregu Mahlera nie sprawi trudności.

Fakt 3.7.5. *Niech $\sum_{k\ge 0} c_k \binom{x}{k}$ będzie szeregiem Mahlera dla f, funkcji klasy S^1. Wtedy*

$$\int_{\mathbb{Z}_p} f(x)\,dx = \sum_{k=0}^{\infty} \frac{(-1)^k c_k}{k+1}.$$

Dowód. Skoro $f_n(x) = \sum_{k\le n} c_k \binom{x}{k}$ dążą do $f(x)$ w $\|\cdot\|_*$, to wolno nam całkować wyraz po wyrazie, by otrzymać kolejno: $\sum_{k\ge 0} c_k \int (x \text{ nad } k)\,\mathrm{d}x$, $\sum_{k\ge 0} c_k (x \text{ nad } k+1)'(0)$, a potem $\sum_{k\ge 0} c_k \lim_{x\to 0}(x-1 \text{ nad } k)/(k+1)$ i prawą stronę. □

Przykład 3.7.6. *Ustalmy $t \in \mathbb{C}_p$, że $0 < |t| < 1$. Wtedy*

$$\int_{\mathbb{Z}_p} (1+t)^x\,dx = \int_{\mathbb{Z}_p} \sum_{k=0}^{\infty} t^k \binom{x}{k}\,dx = \sum_{k=0}^{\infty} \frac{(-t)^k}{k+1},$$

a to jest po prostu $\frac{1}{t}\log(1+t)$.

Przyda nam się więcej wzorów z tą całką. Przypomnijmy, że $\mathfrak{D}$ komutuje z translacją, zatem także z $\nabla = \tau - \mathrm{id}$.

Fakt 3.7.7. *Niechaj $P_0\colon f \mapsto f(0)\cdot 1$ rzutuje $S^1(\mathbb{Z}_p)$ na stałe. Wtedy: $\mathfrak{2}\,\tau = \tau\,\mathfrak{2} - P_0$, $\mathfrak{2}\,\mathfrak{D} = \mathfrak{D}\,\mathfrak{2} - P_0\mathfrak{D}\,\mathfrak{2}$, zaś $\mathfrak{D}\,\mathfrak{2}$ komutuje z translacjami τ_x*

Dowód. Z definicji, dla $n \ge 1$ mamy

$$\ldots = \mathfrak{2}(\tau f)(n) = \sum_{j=0}^{n-1} \tau f(j) = \sum_{j=0}^{n-1} f(j+1)$$

$$= \sum_{j=1}^{n} f(j) = \mathfrak{2}\, f(n+1) - f(0) = \tau\,\mathfrak{2}\, f(n) - f(0),$$

co dowodzi pierwszego stwierdzenia (całkowite $n \ge 1$ w $\mathbb{Z}_p$ leżą gęsto, ciągłość funkcji). Z drugiej strony, różniczkowanie $\mathfrak{2}\,\tau f = \tau\,\mathfrak{2}\, f - f(0)$ prowadzi do $\mathfrak{D}\,\mathfrak{2}\,\tau f = \mathfrak{D}\tau\,\mathfrak{2}\, f = \tau\mathfrak{D}\,\mathfrak{2}\, f$. Do tego, ponieważ $\nabla\,\mathfrak{2}\, f = f$, ale $S\nabla f = f - f(0)$, to $\nabla\,\mathfrak{2} = \mathrm{id}$ oraz $\mathfrak{2}\,\nabla = \mathrm{id} - P_0$. Wnioskujemy, że $\mathfrak{2}\,\mathfrak{D}$ to $\mathfrak{2}\,\mathfrak{D}\nabla\,\mathfrak{2}$, czyli $\mathfrak{2}\,\nabla\mathfrak{D}\,\mathfrak{2} = \mathfrak{D}\,\mathfrak{2} - P_0\mathfrak{D}\,\mathfrak{2}$. □

Fakt 3.7.8. *Niech $f \in \mathcal{S}^1(\mathbb{Z}_p)$. Wtedy*

$$(\mathfrak{2}\, f)'(x) = \int_{\mathbb{Z}_p} \tau_x f(t)\,dt$$

$$\mathfrak{2}(f')(x) = \int_{\mathbb{Z}_p} f(x+t) - f(t)\,dt$$

Dowód. Całka z f to pochodna $(\mathfrak{2}\, f)'(0)$, więc

$$\ldots = \int_{\mathbb{Z}_p} f(t+1)\,\mathrm{d}t = \int_{\mathbb{Z}_p} \tau f(t)\,\mathrm{d}t = (\mathfrak{2}\,\tau f)'(0)$$
$$= \mathfrak{D}\,\mathfrak{2}\,\tau f(0) = \tau\mathfrak{D}\,\mathfrak{2}\, f(0) = \mathfrak{D}\,\mathfrak{2}\, f(1) = (Sf)'(1).$$

Ogólny wzór dla $x = n$ otrzymujemy przez iterację, natomiast dla dowolnego $x \in \mathbb{Z}_p$ z ciągłości i gęstości.

Skorzystamy teraz z 3.7.4: $\int_{\mathbb{Z}_p} \nabla f(x+t)\,\mathrm{d}t = f'(x)$. Stąd wynika, że $\mathfrak{2}(f')(n)$ jest sumą teleskopową:

$$\mathfrak{2}(f')(n) = \int_{\mathbb{Z}_p} f(t+n) - f(t)\,\mathrm{d}t$$

Ponownie odwołujemy się do ciągłości i gęstości, by powyższy wzór był prawdziwy nie tylko dla $n \in \mathbb{N}$, ale też $n \in \mathbb{Z}_p$. □

Fakt 3.7.9. *Jeżeli $f \in \mathcal{S}^2(\mathbb{Z}_p)$, to $F \in \mathcal{S}^1(\mathbb{Z}_p)$ i*

$$F'(x) := \left[\int_{\mathbb{Z}_p} f(x+t)\,dt\right]' = \int_{\mathbb{Z}_p} f'(x+t)\,dt.$$

Dowód. Skoro $f \in \mathcal{S}^2$, to $f' \in \mathcal{S}^1$, więc prawa strona równania z faktu definiuje funkcję $G(x)$ klasy $\mathcal{S}^1$ równą $(\mathfrak{2}\, f')'(x)$, czyli $(\mathfrak{D}\,\mathfrak{2}\,\mathfrak{D} f)(x)$, więc $G = \mathfrak{D}\,\mathfrak{2}\,\mathfrak{D} f$. Zauważmy przy tym, że $\mathfrak{2}\,\mathfrak{D}$ to $\mathfrak{D}\,\mathfrak{2} - P_0\mathfrak{D}\,\mathfrak{2}$, zatem $G = \mathfrak{D}\mathfrak{D}\,\mathfrak{2}\, f = (\mathfrak{2}\, f)'' = F'$. □

Fakt 3.7.10. *Jeśli σ jest inwolucją $x \mapsto -1 - x$ dla $\mathbb{Z}_p$, to*

$$\int_{\mathbb{Z}_p} (f\circ\sigma)\,dx = \int_{\mathbb{Z}_p} f\,dx.$$

Dzięki temu możemy podać wzór na całkę Volkenborna z dowolnej funkcji nieparzystej: to po prostu $-f'(0)/2$.

3.8 Antypochodna

Fakt 3.8.1. *Dla każdej ciągłej funkcji $f\colon X \to \mathcal{K}$ ($X \subseteq \mathcal{K}$) i $\varepsilon > 0$ istnieje lokalnie stała $g\colon X \to \mathcal{K}$, że $|f(x) - g(x)| < \varepsilon$.*

Dowód. Relacja $x \simeq y$, gdy $|f(x) - f(y)| < \varepsilon$, rozbija X na otwarnięte klasy abstrakcji U_i. Wybierzmy z każdej po jednym elemencie a_i. Niech $g(x) = f(a_i)$, jeśli $x \in U_i$. □

Wniosek 3.8.2. *Jeśli X nie ma izolatorów, to $g' = 0$.*

Twierdzenie 12 (Kaplansky)**.** *Jeżeli zbiór $X \subseteq \mathcal{K}$ jest zwarty, zaś $f\colon X \to \mathcal{K}$ ciągła, to istnieje wielomian $P\colon \mathcal{K} \to \mathcal{K}$, że dla każdego $x \in X$, $|P(x) - f(x)| < \varepsilon$.*

Twierdzenie Kaplansky'ego nie jest wybredne co do ciała $\mathcal{K}$, natomiast twierdzenie Weierstraßa (o jednostajnej granicy wielomianów) staje się fałszywe (!) dla $\mathbb{C}$ zamiast $\mathbb{R}$.

Dowód. Fakt połączony ze zwartością X pokazują, że można ograniczyć się do indykatorów kul.

Bez straty ogólności, niech $0 \in X$, $f(0) = 1$. Wybierzmy $c_1, \ldots, c_m \in X$, by $|c_1| \le \ldots \le |c_m|$ i $X \subseteq \bigsqcup_{k\le m} \mathcal{B}[c_k, \delta]$ ($c_0 = 0$). Wtedy $\delta < |c_1|$. Dla pewnego s mamy $(\delta/|c_1|)^s < \varepsilon$. Indukcyjnie wskażemy $n_1, \ldots, n_m$, by funkcja

$$P(x) = \prod_{j=1}^{m} \left[1 - \frac{x^s}{c_j^s}\right]^{n_j}$$

miała potrzebne własności: $|P(x) - 1| < \varepsilon$ dla x z $\mathcal{B}[0,\delta]$ i $|(x)| < \varepsilon$ dla x z kolejnych kul.

Niech $x \in \mathcal{B}[0,\delta]$. Wtedy $1-(x/c_j)^s \in \mathcal{B}[1,\varepsilon]$ dla każdego j. Skoro $\mathcal{B}[1,\varepsilon]$ jest grupą z mnożeniem (co najmniej dla $\varepsilon<1$), wnioskujemy, że $|P(x)-1|<\varepsilon$ niezależnie od $n_1,\ldots,n_m$.

Niech teraz $x \in \mathcal{B}[c_i,\delta]$ dla $i \geq 1$. Wtedy $|x-c_i| \leq \delta$ i $|x|=|c_i|$, zatem

$$|1-(x/c_j)^s| \leq \begin{cases} \max(1,|x/c_j|^s) \leq |c_i/c_j|^s & j<i \\ |1-x/c_j| \leq \delta/|c_1| & j=i \\ \max(1,|x/c_j|^s) \leq 1 & j>i \end{cases}$$

Chcemy, żeby $|P(x)|<\varepsilon$, czyli

$$\left|\frac{c_i}{c_1}\right|^{sn_1} \cdot \ldots \cdot \left|\frac{c_i}{c_{i-1}}\right|^{sn_{i-1}} \cdot \left(\frac{\delta}{|c_1|}\right)^{n_i} < \varepsilon$$

dla ustalonych $n_1,\ldots,n_{i-1}$. Dobre n_i zawsze znajdziemy. □

Rozpatrujemy funkcje $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$.

Fakt 3.8.3. *Zbiór antypochodnych f jest gęsty w zbiorze $\mathcal{C}(\mathbb{Z}_p,\mathbb{Q}_p)$.*

Dowód. Jeśli $g'=0$ (z wniosku) i $F'=f$, to $(F+g)'=f$. □

Funkcja $\sum_{n\geq 0} p^n x^{p^n-1}$ jest analityczna, ale dla $x=1$ jej antypochodna nie zbiega. Natomiast antypochodna dowolnej funkcji lokalnie analitycznej też jest taka.

Fakt 3.8.4. *Antypochodna funkcji lokalnie analitycznej jest lokalnie analityczna, rzędu o jeden wyższego.*

Funkcja $\sum_{n\geq 0} qx^{q-1}$, $q=p^n$, pokazuje, że słowa „lokalnie" nie można pominąć. Zastanowimy się teraz, czy każda ciągła funkcja $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ ma antypochodną.

Fakt 3.8.5. *Niech funkcje $f_1, f_2, \ldots$ będą ograniczone na $\mathbb{Z}_p$, tak by $f=\sum_{n\geq 1} f_n$ zbiegał jednostajnie. Jeśli F_n jest antypochodną f_n i $\|F_n\|_\triangle := \max(\|F_n\|, \|\Phi_1 F_n\|) \leq \|f_n\|$, to szereg $\sum_n F_n$ także zbiega jednostajnie, do antypochodnej f.*

Dowód. Z jednostajnej zbieżności $\|f_n\|$ dąży do zera, więc $\|F_n\|$ także (i F jest dobrze określoną funkcją ciągłą). Ustalmy $\varepsilon>0$ i N, takie że $\|f_n\|<\varepsilon$ dla $n>N$.

Wtedy $|\Phi_1 F_n(s,t)-f_n(t)|_p \leq \max(\|\Phi_1 F_n\|, \|f_n\|) < \varepsilon$ jednostajnie w $s \neq t \in \mathbb{Z}_p$. Dla x bliskich a, lewa strona jest mniejsza od ε również dla $n \leq N$ (x,a zamiast s,t), można zatem „zgubić" indeksy n. □

Jeżeli funkcje F_n są klasy $\mathcal{C}^1$, dowód daje się poprawić tak, by F też była.

Twierdzenie 13 (Dieudonné)**.** *Każda ciągła $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ posiada antypochodną.*

Dowód. Lemat ze spostrzeżeniem pokazują, iż wystarczy nam ograniczyć się do lokalnie stałych f i pokazać antypochodną F klasy $\mathcal{C}^1$, $\|F\|_\triangle \leq \|f\|$. Niech $f=\sum_{m=0}^{q} \lambda_m[x \in m+p^n\mathbb{Z}_p]$ dla $q=p^n-1$. Wtedy naturalnym kandydatem na funkcję F jest $\sum_m \lambda_m(x-m)[x \in m+p^n\mathbb{Z}_p]$. Jej pochodna to f, zaś $\|F\| \leq \|f\|$.

Pokażemy, że $|\Phi_1 F(x,y)|_p \leq \|f\|$ dla różnych $x,y \in \mathbb{Z}_p$. Niech $x \in m+p^n\mathbb{Z}_p$, $y \in m'+p^n\mathbb{Z}_p$. Jeśli liczby m i m' są równe, to $F(x)-F(y)=\lambda_m(x-y)$. Jeśli nie, to $|x-y|_p$ można szacować z dołu przez większą z $|x-m|_p$, $|y-m'|_p$, ale wtedy $|F(x)-F(y)|_p = |\lambda_m(x-m)+\lambda_{m'}(y-m')|_p \leq \|f\|\cdot|x-y|_p$, co kończy dowód. □

Fakt 3.8.6. *Funkcja $f\colon X \to \mathcal{K}$ jest pierwszej klasy Baire'a (jest punktową granicą f. ciągłych), wtedy i tylko wtedy gdy posiada ona antypochodną.*

Twierdzenie to nie ma rzeczywistego odpowiednika, ale wiadomo, że tylko implikacja w lewo jest prawdziwa. Dowód w lewo (ultrametryczny) również jest prosty. W prawo trzeba skorzystać z kilku lematów.

Lemat 3.8.7. *Jeśli $f\colon X \to \mathcal{K}$ jest pierwszej klasy Baire'a, to jest sumą przeliczalnie wielu lokalnie stałych $f_n\colon X \to \mathcal{K}$, takich że $\|f_n\| \leq \|f\|$ (dla ograniczonych f).*

Lemat 3.8.8. *Ustalmy $\varepsilon>0$ oraz domkniętą kulę $\mathcal{B} \subseteq X$. Istnieje wtedy liniowe odwzorowanie $F\colon X \to \mathcal{K}$, antypochodna indykatora $\mathcal{B}$, normy co najwyżej ε, takie że $|F(x-y)| \leq |x-y|$ (dla $x,y \in \mathcal{B}$) i lub „$\leq |x-y|$" (w pozostałych przypadkach), zerowe poza kulą $\mathcal{B}$.*

Lemat 3.8.9. *Jeśli $f\colon X \to \mathcal{K}$ jest lokalnie stała, zaś $\varepsilon>0$, to istnieje lokalnie liniowa antypochodna $F\colon X \to \mathcal{K}$, że $\|F\| \leq \varepsilon$ i $|F(x)-F(y)| \leq \max(|f(x)|,\varepsilon)|x-y|$.*

3.9 Dyfeomorfizmy

Definicja 3.9.1. *Dyfeomorfizmem otwarniętych zbiorów jest każdy dwustronnie różniczkowalny homeomorfizm.*

Fakt 3.9.2. *Niepuste otwarnięte podzbiory $\mathbb{C}_p$ są dyfeomorficzne.*

Dowód. Jako że $\mathbb{C}_p$ nie jest lokalnie zwarte, ale jest ośrodkowe, wystarczy zapisać obydwa jako unię przeliczalnie wielu dysków „domkniętych" i skleić liniowe mapy między nimi. □

Fakt 3.9.3. *Każde nieograniczone, otwarnięte i niepuste podzbiory p. lokalnie zwartej są dyfeomorficzne.*

Fakt 3.9.4 („Peano")**.** *$\mathbb{Q}_p$ i $\mathbb{Q}_p^2$, $\mathbb{Z}_p$ i $\mathbb{Z}_p^2$ są homeomorficzne.*

Fakt 3.9.5. *$\mathbb{Z}_p$ i $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ są dyfeomorficzne tylko dla $p=2$.*

Rozdział 4
Imperium topologii

4.1 Klasyfikacja lokalnie zwartych ciał

Podejmiemy się klasyfikacji czegoś więcej niż samych tylko ciał ultrametrycznych: lokalnie zwartych ciał charakterystyki zero.

Zakładamy po cichu, że do dyspozycji mamy miarę Haara: na każdej lokalnie zwartej grupie G istnieje dodatnia miara Radona μ, która jest niezmiennicza na lewe przesunięcia. Na taką miarę patrzymy jak na dodatni ciągły funkcjonał liniowy na przestrzeni zwarcie niesionych funkcji ciągłych $G \to \mathbb{R}$ (lub inaczej). Brzmi nieźle i pozwala na udowodnienie, że lokalnie zwarte ciała są metryzowalne. Ich klasyfikacja: $\mathbb{R}$, $\mathbb{C}$, skończone rozszerzenia $\mathbb{Q}_p$ (chyba?).

4.2 Zwarta przestrzeń $\mathbb{Z}_p$

Przez liczby p-adyczne rozumiemy szeregi formalne $\sum_{i=0}^{\infty} a_i p^i$, gdzie całkowite współczynniki a_i spełniają $0 \le a_i \le p-1$. Takie szeregi można utożsamiać z ciągiem a_i.

Kartezjański produkt $X_p = \{0, \dots, p-1\}^{\mathbb{N}}$ ma topologię produktową (czynniki są dyskretne), zatem jest zwarty. Jest też całkowicie rozłączny.

Jest całkiem sporo metryk zgodnych z topologią na X_p, dla $x = (x_0, x_1, \dots)$ i $y = (y_0, y_1, \dots) \in X_p$ możemy przyjąć

$$d(x,y) = \sup_{i \ge 0} \frac{\delta(x_i, y_i)}{p^i} = \frac{1}{p^{v_p(x-y)}} \text{ czy } \sum_{i=0}^{\infty} \frac{\delta(x_i,y_i)}{p^{i+1}},$$

ale nie tylko. Wszystkie metryki na zwartej metryzowalnej są jednostajnie równoważne. Te dające wierny obraz struktury warstw $\mathbb{Z}_p$: dla każdej $k \in \mathbb{N}$ warstwy $p^k\mathbb{Z}_p$ są izometryczne w $\mathbb{Z}_p$, lubimy. Z p-adyczą metryką mnożenie jest kontrakcją: $d(px, py) = d(x,y)/p$, zatem ciągłe.

4.3 Zbiór Cantora

Zbiór Cantora $C \subseteq [0,1]$ składa się z tych punktów, których rozwinięcia w systemie trójkowym nie zawierają cyfry jeden. Mamy ciągłą bijekcję $\psi\colon \mathbb{Z}_2 \to C$, $\sum_i a_i 2^i \mapsto \sum_i 2a_i/3^{i+1}$, która dzięki zwartości jest homeomorfizmem. Ciekawa jest też funkcja $\varphi\colon \mathbb{Z}_2 \to [0,1]$ zadana przez $\sum_i a_i 2^i \mapsto \sum_i a_i/2^{1+i}$. Diagram przemienny $\varphi = g \circ \psi$ (funkcja g zszywa krańcowe punkty zbioru Cantora) zachęca nas do rozważenia liniowych modeli $\mathbb{Z}_p$.

Fakt 4.3.1. *Funkcje $\psi_b\colon \mathbb{Z}_p \to [0,1]$ określone dla $b > 1$ są ciągłe. Gdy $b > p$, są różnowartościowym homeomorfizmem na obraz. Kiedy $b = p$, ψ_b jest tylko surjekcją.*

$$\psi_b\colon \sum_{i=0}^{\infty} a_i p^i \mapsto \frac{b-1}{p-1} \sum_{i=0}^{\infty} \frac{a_i}{b^{i+1}}$$

4.4 Grupy topologiczne

Grupa topologiczna to zwykła grupa $\mathcal{G}$ z topologią, przy której funkcja $\mathcal{G} \times \mathcal{G} \to \mathcal{G}$, $(x,y) \mapsto xy^{-1}$ jest ciągła.

Fakt 4.4.1. *Grupy $(\mathbb{Z}_p, +)$ oraz $(\mathbb{Z}_p^\times, \cdot)$ są topologiczne.*

Dowód. Istnieje fundamentalny układ otoczeń z podgrup dla 1 w $\mathbb{Z}_p^\times$: to $1+p^k\mathbb{Z}_p$. Jeżeli $\alpha, \beta \in \mathbb{Z}_p$, to $(1+p^n\beta)^{-1} = 1+p^n\beta'$ (tu $\beta' \in \mathbb{Z}_p$), a zatem (dla $a = 1+p^n\alpha$ i $b = 1+p^n\beta$) mamy $ab^{-1} = 1+p^n\gamma$ dla pewnego $\gamma \in \mathbb{Z}_p$. Konsekwencją tego faktu dla $a' \in a(1+p^n\mathbb{Z}_p)$ oraz $b' \in b(1+p^n\mathbb{Z}_p)$ jest

$$a'b'^{-1} \in ab^{-1}(1+p^n\mathbb{Z}_p) \qquad n \ge 1$$

i $(x,y) \mapsto xy^{-1}$ jest ciągłe. Indeks $1+p\mathbb{Z}_p$ w $\mathbb{Z}_p^\times$ to $p-1$; podgrupa ta jest otwarta (i topologiczna).

Jeżeli $a' \in a+p^n\mathbb{Z}_p$ i $b' \in b+p^n\mathbb{Z}_p$, to $a'-b'$ należy do $a-b+p^n\mathbb{Z}_p$ dla $n \ge 0$. Innymi słowy, gdy $|x-a|, |y-b| \le |p^n|$, to $|(x-y)-(a-b)| \le p^{-n}$, zatem odejmowanie $x-y$ jest ciągłe w każdym punkcie (a,b). □

Podamy teraz bez dowodu kilka najważniejszych faktów, które dotyczą grup topologicznych. Wszystko można znaleźć w dobrym podręczniku poświęconym tym obiektom.

Fakt 4.4.2. *Grupa topologiczna jest metryzowalna, wtedy i tylko wtedy gdy jest Hausdorffa i posiada przeliczalny fundamentalny układ otoczeń elementu neutralnego.*

Od metryki można wtedy wymagać, by była niezmiennicza na lewe przesunięcia.

Każdą grupę $\mathcal{G}$ można uzupełnić do $\widehat{\mathcal{G}}$: zupełnej, w którą $\mathcal{G}$ zanurza się gęsto, że morfizmy $\mathcal{G} \to \mathcal{G}'$ (w zupełną) pochodzą od złożeń $\mathcal{G} \to \widehat{\mathcal{G}}$ i $\widehat{\mathcal{G}} \to \mathcal{G}'$ (jednoznacznie).

Fakt 4.4.3. *Jeżeli $H \le \mathcal{G}$ jest podgrupą grupy topologicznej G oraz zawiera otoczenie elementu neutralnego, to jest otwarnięta w $\mathcal{G}$.*

Na przykład $p^n\mathbb{Z}_p$ ($n \ge 0$) w addytywnej $\mathbb{Z}_p$ lub $1+p^n\mathbb{Z}_p$ ($n \ge 1$) w multiplikatywnej $1+p\mathbb{Z}_p$ są otwarnięte.

Gdy przez $\pi\colon \mathcal{G} \to \mathcal{G}/H$ oznaczymy kanoniczny rzut (tutaj $H \triangleleft \mathcal{G}$), to dla otwartego $U \subseteq \mathcal{G}$ mamy $\pi^{-1}(\pi U) = \bigcup_{h \in H} Uh$ (również otwarty). Zatem rzut jest ciągły i otwarty, lecz nie musi być domknięty.

Fakt 4.4.4. *Iloraz $\mathcal{G}/H$ jest skończony, $T_2 \Leftrightarrow H$ jest domknięta oraz skończonego indeksu $\Rightarrow$ iloraz jest dyskretny $\Leftrightarrow$ H jest otwarta $\Rightarrow$ iloraz jest $T_2 \Leftrightarrow H$ domknięta.*

Dyskretne podgrupy $\mathbb{R}$ są postaci $a\mathbb{Z}$, więc iloraz $\mathbb{R}$ przez dyskretną (nietrywialną) jest zwarty. Niedyskretne podgrupy $\mathbb{R}$ leżą gęsto na prostej.

Fakt 4.4.5. *Domknięte podgrupy $\mathbb{Z}_p$ to ideały ($\{0\}$, $p^m\mathbb{Z}_p$).*

Dowód. Abelowa grupa to $\mathbb{Z}$-moduł. Jeśli grupa $H \le \mathbb{Z}_p$ jest domknięta, to dla $h \in H$ mamy implikację: gdy $\mathbb{Z}H \subseteq H$, to $\mathbb{Z}_p a \subseteq \operatorname{cl} \mathbb{Z}a \subseteq \operatorname{cl} H = H$. Czyli domknięta podgrupa to ideał $\mathbb{Z}_p$ (lub $\mathbb{Z}_p$-modułu). □

Uwaga! Jeżeli $\mathcal{R}$ jest pierścieniem topologicznym, to grupa $\mathcal{R}^*$ elementów odwracalnych nie musi być topologiczna. Ale można na niej zadać inną topologię, od włożenia $x \mapsto (x, x^{-1})$ dla $\mathcal{R}^*$ w $\mathcal{R}^2$. Wtedy $\mathcal{R}^* \hookrightarrow \mathcal{R}$ jest ciągłe, chociaż być może nie jest homeomorfizmem na obraz. Oto przykład.

Niech H będzie zespoloną p. Hilberta z ortonormalną bazą e_i. Rozpatrzmy ciąg ciągłych operatorów T_n przerzucających e_i na e_i (jeśli $i \ne n$) lub $\frac{1}{n}e_n$ (jeśli nie). Dla każdego $x \in H$, $\|T_n x - x\|^2 \to 0$, więc oraz $T_n \to I$ w silnej topologii na pierścieniu ograniczonych operatorów. Ale $T_n^{-1} \not\to I$, bo

$$x = \sum_{n=1}^{\infty} \frac{e_n}{n}.$$

Fakt 4.4.6. *Ciągły morfizm $\mathbb{Z}_p^\times \to \mathbb{Q}_p^\times$ jest postaci $\zeta u \mapsto \zeta^v u^x$ dla $\zeta \in \mu_{p-1}$, $u \in 1+p\mathbb{Z}_p$, $v \in \mathbb{Z}/(p-1)\mathbb{Z}$ i $x \in \mathbb{Z}_p$.*

4.5 Cewka

Ciała $\mathbb{R}$ i $\mathbb{Q}_p$ połączyć można w interesującą grupę topologiczną, solenoid. Przedstawimy jej konstrukcję i własności.

Kanoniczne homomorfizmy $\varphi_n\colon \mathbb{R}/p^{n+1}\mathbb{Z} \to \mathbb{R}/p^n\mathbb{Z}$, $x \bmod p^{n+1}\mathbb{Z} \mapsto x \bmod p^n\mathbb{Z}$ (dla $n \geq 0$) tworzą układ rzutowy $(\mathbb{R}/p^n\mathbb{Z}, \varphi_n)_{n\geq 0}$ grup topologicznych.

Definicja 4.5.1. ***Solenoid*** p***-adyczny*** $\mathbb{S}_p$ *to jego rzutowa granica.*

$\mathbb{S}_p$ jest zwartą grupą abelową. Mamy kanoniczne rzuty ψ_n, $\mathbb{S}_p \to \mathbb{R}/p^n\mathbb{Z}$, ciągłe homomorfizmy „na". W szczególności, $\psi = \psi_0$ jest ciągłą surjekcją, zaś solenoid: nakryciem okręgu.

To daje krótki ciąg dokładny $0 \to \mathbb{Z}_p \to \mathbb{S}_p \to \mathbb{R}/\mathbb{Z} \to 0$. Okrąg został przedstawiony jako iloraz solenoidu, zaś solenoid jako nakrycie okręgu o włóknie $\mathbb{Z}_p$.

Powszechnie wiadomo, że każdej liczbie całkowitej $m \geq 1$ odpowiada jedyna cykliczna podgrupa rzędu m w okręgu, czyli $m^{-1}\mathbb{Z}/\mathbb{Z} \subseteq \mathbb{R}/\mathbb{Z}$. Prawdą jest też następujące stwierdzenie:

Fakt 4.5.2. *Dla każdej całkowitej $m \geq 1$, względnie pierwszej z p, solenoid $\mathbb{S}_p$ zawiera jedyną cykliczną podgrupę C_m rzędu m.*

Dowód. Oznaczmy przez C_m^n cykliczną podgrupę rzędu m w okręgu $\mathbb{R}/p^n\mathbb{Z}$. Funkcje przejścia φ_n, $\mathbb{R}/p^{n+1}\mathbb{Z} \to \mathbb{R}/p^n\mathbb{Z}$, mają jądra rzędu p względnie pierwszego z m. Indukują więc izomorfizmy $C_m^{n+1} \to C_m^n$. Rzutową granicą tego stałego ciągu jest cykliczna podgrupa $C_m \subseteq \mathbb{S}_p$. Aby udowodnić jedyność, rozpatrzmy dowolny homomorfizm $\sigma\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{S}_p$. Złożenie $\psi_n \circ \sigma$, $\mathbb{Z}/m\mathbb{Z} \to \mathbb{S}_p \to \mathbb{R}/p^n\mathbb{Z}$, ma obraz w jedynej cyklicznej podgrupie C_m^n okręgu $\mathbb{R}/p^n\mathbb{Z}$. Zatem σ ma obraz w C_m, a to kończy dowód. □

Podgrupę można zrzutować na okrąg: $\psi(C_m) = m^{-1}\mathbb{Z}/\mathbb{Z}$ (oczywiście zawarty w $\mathbb{R}/\mathbb{Z}$). Skoro $\psi^{-1}(m^{-1}\mathbb{Z}/\mathbb{Z}) \cong C_m \times \mathbb{Z}_p$, C_m jest maksymalną skończoną podgrupą przeciwobrazu (ψ).

Fakt 4.5.3. *Solenoid p-adyczny $\mathbb{S}_p$ nie ma p-torsji.*

Dowód. Ustalmy morfizm $\sigma\colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{S}_p$. Wtedy poniższe złożenia są trywialne.

$$\varphi_n \circ \psi_{n+1} \circ \sigma\colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{S}_p \to \mathbb{R}/p^{n+1}\mathbb{Z} \to \mathbb{R}/p^n\mathbb{Z}$$

Obraz złożenia $\psi_{n+1} \circ \sigma$ leży w jedynej cyklicznej podgrupie okręgu $\mathbb{R}/p^{n+1}\mathbb{Z}$ rzędu p. Podgrupa ta jest jądrem morfizmu φ_n oraz $\psi_n \circ \sigma = \varphi_n(\psi_{n+1} \circ \sigma)$. Zatem nie istnieje element rzędu p^k, $k \geq 1$, w $\mathbb{S}_p$. □

Fakt 4.5.4. *Solenoid p-adyczny zawiera podgrupę izomorficzną z $\mathbb{R}$ (gęstą), podobnie dla $\mathbb{Q}_p$.*

Dowód. Projekcje $f_n\colon \mathbb{R} \to \mathbb{R}/p^n\mathbb{Z}$ są zgodne z funkcjami przejścia układu rzutowego, którym zdefiniowaliśmy solenoid ($f_n = \varphi_n \circ f_{n+1}$). Istnieje więc jedyna faktoryzacja $f\colon \mathbb{R} \to \mathbb{S}_p$. Jeśli $x \neq 0 \in \mathbb{R}$, to gdy $p^n > x$, mamy $f_n(x) \neq 0 \in \mathbb{R}/p^n\mathbb{Z}$, a zatem $f(x) \neq 0 \in \mathbb{S}_p$. To pokazuje, że homomorfizm f jest injekcją (poza tym, $\bigcap_n \ker f_n = \bigcap_n p^n\mathbb{Z} = \{0\}$). Obraz f jest gęsty: obrazy f_n (które są „na") też są. Rozpatrzmy podgrupy H_k, $\psi^{-1}(p^{-k}\mathbb{Z}/\mathbb{Z}) \subset \mathbb{S}_p$. Mamy $H_0 = \mathbb{Z}_p$, a to jest podgrupa indeksu p^k w H_k: $H_k = \varprojlim_n p^{-k}\mathbb{Z}/p^n\mathbb{Z} \cong p^{-k}\mathbb{Z}_p$. Zatem

$$\mathbb{Q}_p \cong \psi^{-1}(\mathbb{Z}[1/p]/\mathbb{Z}) = \bigcup \psi^{-1}(p^{-k}\mathbb{Z}/\mathbb{Z}) = \bigcup H_k,$$

a to jest podzbiór $\mathbb{S}_p$. Gęstość tej podgrupy wynika z gęstości wszystkich obrazów $\psi_n(\mathbb{Q}_p) = \mathbb{Z}[1/p]/p^n\mathbb{Z} \subset \mathbb{R}/p^n\mathbb{Z}$. □

Dzięki temu mamy prosty wniosek:

Fakt 4.5.5. *Solenoid jest continuum (zwarty i spójny).*

Dowód. Wiemy z topologii, że gdy $A \subseteq X$ jest spójny, to każdy $B \subseteq X$, że $A \subseteq B \subseteq \operatorname{cl} A$, też. Weźmy za A podprzestrzeń (spójną) $f(\mathbb{R}) \subseteq \mathbb{S}_p$, która jest gęsta w solenoidzie. □

Na zakończenie przedstawimy solenoid jako *linę, która jest bardzo skręcona*. Ciąg homomorfizmów ciągłych

$$f_n\colon \mathbb{R} \times \mathbb{Q}_p \to \mathbb{R}/p^n\mathbb{Z}\colon (t, x) \mapsto t + \sum_{i<n} a_i p^i \pmod{p^n\mathbb{Z}}$$

jest zgodny z układem rzutowym, więc możemy faktoryzować go do $f(t, x) = t + x\colon \mathbb{R} \times \mathbb{Q}_p \to \mathbb{S}_p$.

Lemat 4.5.6. *Jądrem morfizmu f jest dyskretna podgrupa $\mathbb{R} \times \mathbb{Q}_p$, $\Gamma = \{(a, -a) : a \in \mathbb{Z}[1/p]\} \subseteq \mathbb{R} \times \mathbb{Q}_p$.*

Dowód. Jeśli $f(t, x) = 0$, to $f_n(t, x) = \psi_n \circ f(t, x) = 0 \in \mathbb{R}/\mathbb{Z}$, a stąd wynika, że $t + \sum_{i<n} a_o p^i \in p^n\mathbb{Z}$ dla $n \geq 1$, czyli $t = -x$. Zawieranie $\Gamma \subseteq \ker f$ jest oczywiste.

Dla pokazania dyskretności wystarczy wskazać otoczenie zera w produkcie $\mathbb{R} \times \mathbb{Q}_p$, które kroiłoby trywialnie Γ. Jeśli para $(-a, a)$ leży w otwartym zbiorze $(-1, 1) \times \mathbb{Z}_p$ i Γ, to $a \in \mathbb{Z}[1/p]$ jest postaci $\sum_{i\geq 0} a_i p^i$.

Ale $\mathbb{Z}[1/p]$ kroi się z $\mathbb{Z}_p$ do $\mathbb{Z}$, więc $a \in \mathbb{Z} \cap (-1, 1) = \{0\}$ i dowód jest zakończony. □

Fakt 4.5.7. *$\mathbb{S}_p$ jest izomorficzny (algebraicznie jak i topologicznie) z ilorazem $\mathbb{R} \times \mathbb{Q}_p$ przez Γ (przez izomorfizm f').*

Dowód. Wszystkie funkcje f_n są surjekcjami, zaś obraz granicy f jest gęsty. Ponadto $f(t, x) = f(s, y)$, gdzie $s = t + \langle x \rangle \in \mathbb{R}$ i $y = [x] \in \mathbb{Z}_p$. Pójdźmy o krok dalej, $f(s, y) = f(u, z)$, gdzie $u = s - [s] \in [0, 1)$ i $z = y + [s] \in \mathbb{Z}_p$. To pokazuje, że obraz f, $f([0, 1] \times \mathbb{Z}_p)$, jest zwarty, domknięty.

Stąd wnioskujemy, że f jest „na", zaś f' to bijekcja. Ciągła bijekcja f' między p. zwartymi awansuje do homeomorfizmu: iloraz Hausdorffa (Γ jest dyskretna, domknięta) to także obraz zwartego $[0, 1] \times \mathbb{Z}_p$. □

Solenoid to także iloraz topologicznej przestrzeni $[0, 1] \times \mathbb{Z}_p$ przez relację równoważności $(1, x) \simeq (0, x + 1)$. Wyobraźmy sobie walec $[0, 1] \times \mathbb{Z}_p$ i zszyjmy końce skręcając je jednocześnie.

Fakt 4.5.8. *Domknięte podgrupy $\mathbb{S}_p$ to C_m, $C_m \times p^k\mathbb{Z}_p$ i $\mathbb{S}_p$, gdzie $p \nmid m$ i $k \in \mathbb{Z}$.*

Fakt 4.5.9. *Solenoid jest nierozkładalnym continuum.*

4.6 Topologia teoriomnogościowa

Fakt 4.6.1. *Całkowicie niespójna, zwarta p. metryczna bez izolatorów jest homeomorficzna z $\mathbb{Z}_2$. Zwarta p. metryczna jest obrazem $\mathbb{Z}_2$.*

Twierdzenie 14 (Sierpiński)**.** *Przeliczalna przestrzeń metryczna bez izolatorów jest homeomorficzna z $\mathbb{Q}$.*

Stąd bierze się zaskakująca własność $\mathbb{Q}$.

Wniosek 4.6.2. *Topologia na $\mathbb{Q}$ „nie zależy" od normy.*

Twierdzenie 15 (Vaughan, 1937)**.** *Przestrzeń metryczną X można zmetryzować tak, by zwarte były dokładnie domknięte i ograniczone podzbiory, wtedy i tylko wtedy gdy X jest ośrodkowa i lokalnie zwarta.*

Przykład 4.6.3. $X = \mathbb{Q}_p$.

Wymiar zupełnej przestrzeni metrycznej X to najmniejsza liczba całkowita n, że w każde pokrycia X można wpisać inne pokrycie krotności $n+1$ (krotność to największa całkowita m, dla której można wybrać m zbiorów o niepustym przekroju). Przykładowo $\dim \mathbb{R}^n = n$.

Fakt 4.6.4. *Przestrzeń $\mathbb{Q}_p$ jest zerowymiarowa.*

Dowód. Każdy otwarty podzbiór $X \subseteq \mathbb{Q}_p$ jest przeliczalną unią rozłącznych dysków. □

Rozdział 5
Kalifat algebry

5.1 Algebraiczne spojrzenie na $\|\cdot\|$

Niech $\mathcal{K}$ będzie ciałem, na którym mamy niearchimedesowską wartość bezwzględną $\|\cdot\|$.

Definicja 5.1.1. *Pierścień waluacji $\mathcal{K}$ to $\mathcal{O} = \mathcal{B}[0,1]$, ideałem zaś jest $\mathfrak{p} = \mathcal{B}(0,1)$.*

Fakt 5.1.2. *Ideał $\mathfrak{p} \lhd \mathcal{O}$ jest maksymalny, podpierścień $\mathcal{O} \leq \mathcal{K}$ też.*

Dowód. Pokażemy najpierw nie wprost, że $\mathcal{O}$ to maksymalny podpierścień. Jeżeli podpierścień $\mathcal{R}$ zawiera element x, taki że $|x| > 1$, to sam jest całym ciałem, gdyż $\mathcal{K} = \bigcup_{n\geq 1} x^n\mathcal{O}$.

Każdy ideał większy od $\mathfrak{p}$ musi zawierać jedność, a przez to pokrywać się z pierścieniem $\mathcal{O}$. □

Definicja 5.1.3. *Ciało $\mathfrak{K} = \mathcal{O}/\mathfrak{P}$ to ciało residuów.*

Pierścienie, w których ideał maksymalny jest tylko jeden, nazywamy lokalnymi.

Fakt 5.1.4. *Dla ciała $\mathcal{K} = \mathbb{Q}$ i p-adycznej wartości bezwzględnej, $\mathcal{O} = \mathbb{Z}_{(p)}$, $\mathfrak{p} = p\mathbb{Z}_{(p)}$, zaś $\mathfrak{K} = \mathbb{F}_p$ (ciało o p elementach).*

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\}$$

Fakt 5.1.5. *Niech $\mathcal{K}$ będzie zupełnym ciałem z ultrametryką. Ustalmy element $\xi \in \mathfrak{p}$ i reprezentantów $S \subseteq \mathcal{O}$ (z zerem) dla klas $\mathcal{O}/\xi\mathcal{O}$. Każdy $x \in \mathcal{K}^*$ jest sumą $\sum_{i\geq m} a_i\xi^i$, gdzie $a_m \neq 0$ oraz ($m \geq 0$ dla $x \in \mathcal{O}$), więc $\mathcal{O}$ jest izomorficzne z $\varprojlim \mathcal{O}/\xi^n\mathcal{O}$.*

Dowód. Możemy znaleźć dokładnie jeden $a_0 \in S$, taki że $x - a_0$ leży w $\xi\mathcal{O}$. Indukcja daje $x = a_0 + \ldots + a_{n-1}\xi^{n-1} + x_n\xi^n$, gdzie $a_i \in S$, $x_n \in \mathcal{O}$. Ciąg $x - x_n\xi^n$ jest Cauchy'ego, zaś dla $x \in \mathcal{K}$ mamy $|\xi^k x| \leq 1$ (k: jakieś). □

Kiedy $\mathcal{K}$ nie jest zupełne, izomorfizm z faktu staje się tylko zanurzeniem w uzupełnienie $\mathcal{O}$.

Fakt 5.1.6. *Dla niedyskretnego ciała $\mathcal{K}$ z ultrametryką albo $\mathfrak{p}$ jest główny, albo $\mathfrak{p} = \mathfrak{p}^2$ i $\mathcal{O}$ nie jest noetherowski.*

Dowód. Z założeń wiemy, że $\Gamma = |\mathcal{K}^\times| \neq \{1\}$ i albo $\Gamma \cap (0,1)$ zawiera element maksymalny θ, albo ciąg zbieżny do jedynki.

W pierwszym przypadku wybieramy taki $\pi \in \mathfrak{p}$, że $|\pi| = \theta$, wtedy ideał $\mathfrak{p} = \pi\mathcal{O}$ jest główny.

W drugim, dla każdego $x \in \mathfrak{p}$ znajdujemy element y, że $|x| < |y| < 1$, wtedy $x = y(x/y) \in \mathfrak{p}^2$ i $\mathfrak{p} = \mathfrak{p}^2$. Podgrupa Γ leży gęsto w $\mathbb{R}_+$, zaś ideały $B[0,r]$ dla $r \in \Gamma \cap (0,1)$ są parami różne, więc A nie jest noetherowski. □

5.2 Logarytm i eksponensa

Zajmijmy się grupą $\mathbb{Z}_p^\times$. Lemat Hensela pokazał, że zawiera $(p-1)$-sze pierwiastki z jedynki. Dla prostoty „$q_2 = 4$ i $q_p = p$". Podzbiory $U = 1 + p\mathbb{Z}_p$ i $U_1 = 1 + q\mathbb{Z}_p$ są podgrupami $\mathbb{Z}_p^\times$, $U_1 \subset U$. Jeśli $p = 2$, to $U = \mathbb{Z}_p^\times$, jeśli nie, to $U_1 = U$. Elementy U nazywa się **jeden-jednościami**. Niech $W = (q\mathbb{Z}_p, +)$.

Fakt 5.2.1. *Logarytm p-adyczny zadaje homomorfizm $U \to \mathbb{Z}_p^+$ oraz izomorfizm $U_1 \to W$ (funkcja odwrotna: eksponensa). Wtedy $U_1 \cong W \cong \mathbb{Z}_p^+$ są beztorsyjne, $\log_p(U) \subseteq p\mathbb{Z}_p$.*

Dowód. Oczywisty po ustępie 7. □

Wniosek 5.2.2. *Dla każdej pierwszej p mamy $\mathbb{Z}_p^\times \cong V \times U$, gdzie $U \cong \mathbb{Z}_p^+$ to beztorsyjna pro-p-grupa, zaś grupa $V \leq \mathbb{Z}_p^\times$ składa się z pierwiastków jedności w $\mathbb{Q}_p$ (część torsyjna). Jest cykliczna, rzędu $\varphi(q)$.*

Dowód. Łatwo widać, że istnieje poniższy ciąg dokładny (jest to definicja U). Chcemy pokazać, że się „rozdziela".

$$1 \to U_1 \to \mathbb{Z}_p^\times \xrightarrow{\pi} (\mathbb{Z}/q\mathbb{Z})^\times \to 0.$$

Lemat Hensela połączony z twierdzeniem Straßmana mówi, że $\mathbb{Z}_p^\times$ zawiera grupę V pierwiastków jedności, cykliczną i rzędu $\varphi(q)$. Elementy V są różne modulo q (lemat Hensela dla $p > 2$). Jeżeli $\pi(\zeta_1) = \pi(\zeta_2)$, to $\zeta_1\zeta_2^{-1} = 1 + qx \in U$ dla $x \in \mathbb{Z}_p$, czyli $\zeta_1 = \zeta_2 \bmod q$, a jedyny przypadek, kiedy to jest możliwe, to $\zeta_1 = \zeta_2$.

Strzałka π indukuje izomorfizm $V \cong (\mathbb{Z}/q\mathbb{Z})^\times$. Reszta jest prosta: dla $u \in \mathbb{Z}_p^\times$ istnieje $\zeta \in V$, takie że $\pi(\zeta) = \pi(u)$, wtedy $u \mapsto (\zeta, u\zeta^{-1})$ uzasadnia $\mathbb{Z}_p^\times \cong V \times U$. □

5.3 Charakter Teichmüllera

Z faktu 5.2.2 możemy wywnioskować, że dla pierwszej $p \neq 2$ mamy inkluzję $\omega : \mathbb{F}_p^\times \cong V \hookrightarrow \mathbb{Z}_p^\times$; określmy do tego $\omega(0) = 0$. Funkcję ω nazywa się **charakterem Teichmüllera**. Czasem tej nazwy używa się dla charakteru Dirichleta, to jest złożenia ω z redukcją mod p: $\mathbb{Z} \to \mathbb{F}_p \to \mathbb{Z}_p$.

Żeby nie było zbyt łatwo, często przez ω oznacza się rzut z $\mathbb{Z}_p^\times$ na V, by każdy $x \in \mathbb{Z}_p^\times$ zapisywał się jednoznacznie jako $x = \omega(x) \cdot x_1$ z $x_1 \in 1 + q\mathbb{Z}_p$. Taka definicja jest sensowna: rozszerzając rzut na $\mathbb{Z}_p$ (do zera na niejednościach) i obcinając do $\mathbb{Z}$, dostaniemy charakter Dirichleta. Niech „$(x) = x_1$".

Fakt 5.3.1. *Jeżeli $p \neq 2$ i $x \in \mathbb{Z}_p^\times$, to $\omega(x)$ dane jest wzorem*

$$\omega(x) = \lim_{n\to\infty} x^{p^n}.$$

Dowód. Skoro $\omega(x)^{p-1} = 1$, to $\omega(x)^{p^n} = \omega(x)$ dla każdego n. Z drugiej strony, $x_1 = 1 + qy$, więc

$$(1 + qy)^p = 1 + pqy + q^2 \cdot \text{reszta},$$

a stąd wynika $x_1^p \in 1 + p^2\mathbb{Z}_p$. Można to powtórzyć: indukcyjnie pokazuje się, że $x_1^r \in 1 + p^{n+1}\mathbb{Z}_p$ i $x_1^r \to 1$ ($r = p^n$). □

Jeżeli $p = 2$, to część odkryć trzeba poprawić: $\mathbb{F}_2^\times = \{1\}$.

5.4 Pierścień $\mathbb{Z}_p$

Fakt 5.4.1. *Pierścień $\mathbb{Z}_p$ nie ma dzielników zera.*

Dowód. Ustalmy liczby $a, b \in \mathbb{Z}_p$ różne od zera. Wtedy p nie dzieli iloczynu $a_v b_w$, gdzie $v = v_p(a)$, $w = v_p(b)$, ale to jest właśnie pierwszy niezerowy współczynnik w rozwinięciu ab, zatem $ab \neq 0$. □

Niech $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Odwzorowanie $\sum_i a_i p^i \mapsto a_0 \pmod p$ jest homomorfizmem pierścieni, **redukcją modulo** p. Iloraz jest ciałem, więc jądro $p\mathbb{Z}_p$ jest ideałem maksymalnym w $\mathbb{Z}_p$.

Fakt 5.4.2. *Grupa $\mathbb{Z}_p^\times$ składa się z p-adycznych liczb całkowitych rzędu zero ($a_0 \neq 0$).*

Dowód. Jeśli p-adyczna l. całkowita odwraca się, to jej redukcja w $\mathbb{F}_p$ również. Ustalmy więc $x \in \mathbb{Z}_p$ rzędu zero.

Skoro redukcja x w ciele $\mathbb{F}_p$ nie jest zerem, to odwraca się i możemy wskazać $0 < y_0 < p$, że $x_0 y_0 = 1 + kp$ dla pewnej liczby k. Przyjmijmy, że $x = x_0 + p\alpha$, wtedy $xy_0 = 1 + p\beta$ (gdzie $\beta \in \mathbb{Z}_p$), a taką liczbę łatwo odwrócić, co jakoś kończy rozumowanie.

$$(1 + p\beta)^{-1} = 1 - \beta p + \beta^2 p^2 - \dots \qquad \square$$

Pierścień $\mathbb{Z}_p$ ma jeden ideał maksymalny, $p\mathbb{Z}_p = \mathbb{Z}_p \setminus \mathbb{Z}_p^\times$. Dokładniej: $\mathbb{Z}_p \setminus \{0\}$ to $\coprod_{k\geq 0} p^k \mathbb{Z}_p^\times$. Ideały główne pierścienia $\mathbb{Z}_p$, $p^k\mathbb{Z}_p$, kroją się do $\{0\}$.

Fakt 5.4.3. *Pierścień $\mathbb{Z}_p$ jest dziedziną ideałów głównych (nie ma innych ideałów niż wyżej wymienione).*

Dowód. Ustalmy niezerowy ideał $I \leq \mathbb{Z}_p$ z elementem $x \in I$ o minimalnym rzędzie, k. Wtedy $x = p^k u$, gdzie u to jedność i $(p^k) \subseteq I$, gdyż $p^k = u^{-1}x$. Niechaj $y \in I$ będzie rzędu $l \geq k$. Wtedy druga inkluza wynika z $y = p^l u' = p^k p^{l-k} u'$. $\square$

5.5 Granice rzutowe

Homomorfizm $\varepsilon_n \colon \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ uogólnia redukcję. Skoro $\sum_{i<n} a_i p^i$ dąży do liczby p-adycznej $\sum_{i\geq 0} a_i p^i$, chcemy tego samego dla pierścieni $\mathbb{Z}/p^n\mathbb{Z}$ i $\mathbb{Z}_p$. Nic trudnego. Umożliwią nam to: kanoniczny homomorfizm $\varphi_n \colon \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ oraz przemienny diagram: „$\varepsilon_n = \varphi_n \circ \varepsilon_{n+1}$".

Definicja 5.5.1. *Układ rzutowy to ciąg funkcji $\varphi_n \colon E_{n+1} \to E_n$ (oraz samych zbiorów E_n). Jego granicą jest zbiór E z funkcjami $\psi_n \colon E \to E_n$, że $\psi_n = \varphi_n \circ \psi_{n+1}$, o ile spełniony jest warunek uniwersalny: dla drugiej „granicy" E' z funkcjami f_n mamy funkcję f, by $f_n = \psi_n \circ f \colon E' \to E \to E_n$ („faktoryzacja").*

$$E_0 \leftarrow E_1 \leftarrow \dots \leftarrow E_n \leftarrow \dots \leftarrow \varprojlim E_n = E$$

Możemy iterować $f_n = \psi_n \circ f_{n+1}$, by uzyskać $f_n = \psi_n \circ f$:

$$\begin{aligned} f_n &= \varphi_n \circ f_{n+1} = \varphi_n \circ \varphi_{n+1} \circ f_{n+2} \\ &= (\varphi_n \circ \varphi_{n+1} \circ \dots \circ \varphi_{n+k}) \circ f_{n+k+1} = \psi_n \circ f, \end{aligned}$$

f zachowuje się jak granica f_j, zaś ψ_n to granica złożeń funkcji przejścia. Łatwo zauważyć, że granica rzutowa nie zależy od początkowych wyrazów (w skończonej ilości), więc można je pominąć.

Fakt 5.5.2. *Każdy układ rzutowy $(E_n, \varphi_n)_{n\geq 0}$ ma granicę.*

Jeśli funkcje przejścia są „na", to rzuty ψ_n też i granica jest niepusta. Granice rzutowe istnieją dla wielu obiektów, nie tylko grup, ale także przestrzeni topologicznych.

Fakt 5.5.3. *Klasa niepustych, zwartych przestrzeni topologicznych jest zamknięta na branie granic odwrotnych.*

Fakt 5.5.4. *Jeśli A jest podzbiorem granicy E dla E_n, to ma miejsce równość* $\operatorname{cl} A = \bigcap_{n=0}^{\infty} \psi_n^{-1}(\operatorname{cl} \psi_n(A))$.

Dla grup mamy trochę inny wynik. Załóżmy, że $\mathcal{G}$ to granica rzutowa grup $\mathcal{G}_n$ z homomorfizmami $\psi_n \colon \mathcal{G} \to \mathcal{G}_n$.

Fakt 5.5.5. *Zachodzi $\bigcap \ker \psi_n = \{e\}$, zaś grupa G jest kanonicznie izomorficzna z $\varprojlim(G/\ker \psi_n)$.*

Pierścień szeregów formalnych $\mathbb{Z}_p$ można opisać w języku granic rzutowych.

Fakt 5.5.6. *Odwzorowanie, które wiąże liczbę p-adyczną z ciągiem jej częściowych sum modulo p^n, $\mathbb{Z}_p \to \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$, jest izomorfizmem topologicznych pierścieni.*

Dowód. Skoro homomorfizmy przejścia φ_n są dane przez

$$\sum_{i\leq n} a_i p^i \pmod{p^{n+1}} \mapsto \sum_{i<n} a_i p^i \pmod{p^n},$$

to konsekwentne ciągi w $\prod \mathbb{Z}/p^n\mathbb{Z}$ są dokładnie ciągami sum częściowych szeregu $\sum_{i\geq 0} a_i p^i$ ($0 \leq a_i \leq p-1$), czyli liczbami p-adycznymi.

Relacje $x_n = \sum_{i\leq n} a_i p^i$, $a_0 = x_1$, $a_n = (x_{n+1} - x_n)p^{-n}$ pokazują nam, że faktoryzacja $\mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ jest bijekcją, czyli izomorfizmem, a jednocześnie homeomorfizmem (jako ciągła bijekcja między p. zwartymi). $\square$

Homomorfizmy $\mathbb{Z} \to \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ wyznaczają coś jeszcze: graniczny homomorfizm $\mathbb{Z} \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, który można utożsamić z kanonicznym włożeniem $\mathbb{Z} \to \mathbb{Z}_p$. Funkcja

$$\sum_{i<n} a_i p^i \pmod{p^n} \mapsto \sum_{i<n} a_i p^i \pmod{p^n\mathbb{Z}_p}$$

definiuje izomorfizm $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$, a w szczególności $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Ogólniej $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$. Cóż, obcięcie homomorfizmu $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ (redukcji) do $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$ (podpierścień ułamków o mianowniku, który nie dzieli się przez p) jest (z drugiej strony) „na" i ma jądro $p^n\mathbb{Z}_{(p)}$. Zyskaliśmy w ten sposób izomorfizm $\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)} \cong \mathbb{Z}/p^n\mathbb{Z}$: $\mathbb{Z}_p$ to rzutowa granica $\varprojlim \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$; uzupełnienie $\mathbb{Z}_{(p)}$.

Jeszcze inna definicja p-adycznych liczb całkowitych bierze się z funkcji $\sum a_i X^i \mapsto \sum a_i p^i$, homomorfizmu pierścieni $\mathbb{Z}[[x]] \to \mathbb{Z}_p$. Zadaje ona izomorfizm $\mathbb{Z}[[x]]/(X - p) \to \mathbb{Z}_p$ (kanoniczny).

Granica rzutowa to konstrukcja z teorii kategorii, z powodu jej dużej ogólności nie będzie nam więcej potrzebna.

5.6 Ciało $\mathbb{Q}_p$

Pierścień $\mathbb{Z}_p$ jest dziedziną całkowitości, więc można określić na jego podstawie ciało ułamków: $\mathbb{Q}_p = \operatorname{Frac} \mathbb{Z}_p$. Gdy $x = p^m u$ (u: jedność w $\mathbb{Z}_p$), to $1/x = p^{-m}u^{-1}$. Ciało $\mathbb{Q}_p$ jest generowane (jako pierścień) przez $\mathbb{Z}_p$ i ujemne potęgi p, tzn. $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$. Reprezentacja $1/x = p^{-m}u^{-1}$ pokazuje coś jeszcze:

$$\mathbb{Q}_p = \bigcup_{m\geq 0} p^{-m}\mathbb{Z}_p \text{ oraz } \mathbb{Q}_p^\times = \coprod_{m\in\mathbb{Z}} p^m \mathbb{Z}_p^\times$$

Struktura ultramentryczna na $\mathbb{Q}_p$ jest na tyle ciekawa, że możemy poświęcić jej chwilę. Jeśli to zrobimy, możemy dojść na przykład do takiej obserwacji.

Fakt 5.6.1. *Ciało $\mathbb{Q}_p$ indukuje na $\mathbb{Z}_p$ topologię p-adyczną. Jest ono lokalnie zwarte, charakterystyki 0. Utożsamia się je z uzupełnieniem $\mathbb{Q}$ lub $\mathbb{Z}[1/p]$ względem metryki p-adycznej.*

Liczby wymierne pośród p-adycznych zlokalizować nie jest trudno, co trochę szokuje. Analogia z $\mathbb{R}$ jest oczywista.

Fakt 5.6.2. *Niech $x = \sum_i a_i p^i \in \mathbb{Q}_p$ ($0 \leq a_i \leq p-1$). Liczba x jest wymierna, wtedy i tylko wtedy gdy ciąg cyfr a_i jest od pewnego miejsca okresowy.*

Dowód. Przedstawimy samą ideę prostego, ale trochę nużącego dowodu. Mnożąc przez x przez $p^{v(x)}$ można założyć, że $x \in \mathbb{Z}_p$. Jeżeli ciąg cyfr jest od pewnego miejsca okresowy, to x jest sumą liczby całkowitej i kombinacji liniowej (nad $\mathbb{Z}$) szeregów postaci $\sum_{j\geq 0} p^{s+jt} = p^s/(1-p^t) \in \mathbb{Q}$, czyli sam x jest wymierny.

W drugą stronę można założyć, że $x = a/b$ jest dodatni, a, b są względnie pierwsze i p nie dzieli b. Rozwijając p-adycznie:

$$\sum_{j\le\beta} b_j p^j \cdot \sum_{i\ge 0} x_i p^i = \sum_{k\le\alpha} a_k p^k.$$

Zaczynając od $(x_{l-1}, \dots, x_{l-\beta}, r_l) \in (\mathbb{Z}/p\mathbb{Z})^{\beta+1}$ pewien bliżej nieokreślony algorytm znajduje krotkę $(x_l, \dots, x_{l-\beta+1}, r_{l+1})$. Zbiór $(\mathbb{Z}/p\mathbb{Z})^{\beta+1}$ jest skończony, więc kiedyś wpadniemy na cykl. Wiemy, że ten opis jest mętny, ale nic nie zrobimy. □

Definicja 5.6.3. *Liczby postaci $x = \sum_{i\ge m} x_i p^i \in \mathbb{Q}_p$ rozbijają się na część całkowitą $[x] \in \mathbb{Z}_p$ oraz ułamkową $\langle x\rangle \in \mathbb{Z}[1/p] \subseteq \mathbb{Q}$:*

$$x = [x] + \langle x\rangle = \sum_{i\ge 0} x_i p^i + \sum_{i<0} x_i p^i.$$

Fakt 5.6.4. *Ze zwykłymi cyframi mamy $0 \le \langle x\rangle < 1$.*

Dowód. $\langle x\rangle < (p-1)\sum_{i\ge 1} |p^j| = 1.$ □

Przyjrzyjmy się teraz reprezentantom mod 1, to znaczy w $\mathbb{Z}[1/p]/\mathbb{Z} \subset \mathbb{R}/\mathbb{Z}$. Okrąg $\mathbb{R}/\mathbb{Z}$ można zanurzyć w płaszczyźnie zespolonej:

$$\mathbb{R} \to \mathbb{R}/\mathbb{Z} \to \mathbb{C}^\times : t \mapsto \exp(2\pi i t).$$

John Tate (to jemu zawdzięczamy notację) badał kiedyś funkcję $\tau\colon \mathbb{Q}_p \to \mathbb{C}^\times$ określoną wzorem $\tau(x) = \exp(2\pi\mathrm{i}\langle x\rangle)$. Na przykład gdy $v(x) = -1$, czyli $x = k/p + y$, $0 < k \le p-1$, $y \in \mathbb{Z}_p$, to $\tau(x) = \zeta^k$, gdzie ζ to pierwotny p-ty pierwiastek jedności w $\mathbb{C}$. Obrazem $p^{-1}\mathbb{Z}_p$ przez τ jest $\mu_p \subseteq \mathbb{C}^\times$, przy czym użyliśmy tu notacji: $\mu_m = \{z \in \mathbb{C} : z^m = 1\}$. Niech

$$\mu = \bigcup_{m\ge 1} \mu_m = \{z \in \mathbb{C} : \exists_{m\ge 1} z^m = 1\}.$$

Po ustaleniu pierwszej p mamy rozkład $\mu = \mu_{(p)} \cdot \mu_{p^\infty}$, gdzie $\mu_{(p)}$ to grupa pierwiastków jedności rzędu względnie pierwszego z p, zaś μ_{p^∞} to grupa pierwiastków rzędu p^i; ta ostatnia jest p-podgrupą Sylowa w torsyjnej abelowej μ. Użyty tu produkt jest oczywiście prosty. Zauważmy jeszcze, że ciąg grup cyklicznych $\mu_p \subset \mu_{p^2} \subset \dots$ jest wstępujący i

$$\mu_{p^\infty} = \bigcup_{k\ge 0} \mu_{p^k} \subset \mathbb{C}^\times.$$

Fakt 5.6.5. *Funkcja τ jest homomorfizmem. Definiuje izomorfizm addytywnej grupy $\mathbb{Q}_p/\mathbb{Z}_p$ oraz multiplikatywnej μ_{p^∞}.*

Dowód. Różnica $\langle x+y\rangle - \langle x\rangle - \langle y\rangle$ jest równa $[x]+[y]-[x+y]$, zatem należy do $\mathbb{Z}[1/p] \cap \mathbb{Z}_p = \mathbb{Z}$. Wartość τ dla tejże różnicy to 1 i $\tau(x+y) = \tau(x)\tau(y)$. Funkcja τ to homomorfizm, którego jądro składa się z tych $x \in \mathbb{Q}_p$, że $\langle x\rangle \in \mathbb{Z}$: $\ker\tau = \mathbb{Z}_p$.

Do obrazu τ należą liczby postaci $\exp(2\pi\mathrm{i}k/p^m)$, równe po prostu $\exp(2\pi\mathrm{i}/p^m)^k$. Przyjmując $k = 1$ dostajemy p^m-te pierwiastki jedności, które generują grupę μ_{p^∞}. □

Rozłożymy teraz $\mathbb{Q}$ „niezależnie" od liczb p-adycznych.

Każda liczba wymierna jest postaci $x = p^v \frac{a}{b}$, gdzie $v \in \mathbb{Z}$, zaś a, b są względnie pierwsze z p. Kiedy $v = -m < 0$, możemy użyć twierdzenia Bézout: $1 = \alpha p^m + \beta b$. Zatem

$$x = \frac{\alpha a}{b} + \frac{\beta b}{p^m} \in \mathbb{Z}_{(p)} + \mathbb{Z}[1/p].$$

Wynika stąd, że $\mathbb{Q} = \mathbb{Z}_{(p)} + \mathbb{Z}[1/p]$ (rozkład indukowany przez $\mathbb{Q}_p = \mathbb{Z}_p + \mathbb{Z}[1/p]$).

Suma $\mathbb{Q}_p = \mathbb{Z}_p + \mathbb{Z}[1/p]$ nie jest prosta, ponieważ składniki kroją się do $\mathbb{Z}$. Jeżeli włożymy $\mathbb{Z}$ w $\mathbb{Z}_p \oplus \mathbb{Z}[1/p]$ poprzez funkcję $m \mapsto (m, -m)$ z obrazem Γ, to homomorfizmy dodawania

$$\mathbb{Z}_{(p)} \oplus \mathbb{Z}[1/p] \to \mathbb{Z}_{(p)} + \mathbb{Z}[1/p] = \mathbb{Q}$$
$$\mathbb{Z}_p \oplus \mathbb{Z}[1/p] \to \mathbb{Z}_p + \mathbb{Z}[1/p] = \mathbb{Q}_p$$

mają to samo jądro, Γ. Podzielenie sum prostych przez Γ daje nam odpowiednio $\mathbb{Q}$ i $\mathbb{Q}_p$.

Podgrupa $\mathbb{Z}_p \le \mathbb{Q}_p$ nie ma prostego dopełnienia. Istotnie, jeżeli $\Gamma \le \mathbb{Q}_p$ jest dowolną podgrupą, taką że $\Gamma \cap \mathbb{Z}_p = \{0\}$, to jest ona dyskretna w $\mathbb{Q}_p$, a co za tym idzie jest trywialna. W pewnym sensie $\mathbb{Z}[1/p]$ jest najlepszym, na co możemy liczyć; mamy jednoznaczny rozkład na $x \in \mathbb{Z}_p$ i $y \in [0,1) \cap \mathbb{Z}[1/p]$. Problem w tym, że drugi zbiór nie jest podgrupą.

Wskażemy wszystkie automorfizmy $\mathbb{Q}_p$ nad $\mathbb{Q}$.

Lemat 5.6.6. *Liczba $x \in \mathbb{Q}_p^\times$ jest jednością ($x \in \mathbb{Z}_p^\times$), wtedy i tylko wtedy gdy x^{p-1} ma n-te pierwiastki dla ∞ wielu n.*

Dowód. ($\Rightarrow$) $x \not\equiv 0 \bmod p\mathbb{Z}_p$ i $x^{p-1} \equiv 1 \bmod p\mathbb{Z}_p$. Rozważmy równanie $P(X) = X^n - x^{p-1} = 0$. Przybliżony pierwiastek to $1 \bmod p$, a kiedy n nie jest krotnością p, to $P'(1) = n$ nie znika mod p. Lemat Hensela daje dokładne rozwiązanie $\xi \in \mathbb{Z}_p$.

($\Leftarrow$) Jeśli $x^{p-1} = y_n^n$, to $(p-1)v(x) = nv(y_n)$, więc n dzieli lewą stronę nieskończenie często. Zatem $v(x) = 0$, gdyż x nie jest zerem. □

Fakt 5.6.7. *Ciało $\mathbb{Q}_p$ ma tylko jeden automorfizm, $\psi\colon x \mapsto x$.*

Dowód. Niech φ będzie automorfizmem ciała $\mathbb{Q}_p$. Trzyma on jedności w $\mathbb{Q}_p^\times$, co wynika z ich charakteryzacji.

Jeśli $x \in \mathbb{Q}_p^\times$ zapiszemy jako $x = p^n u$, gdzie $n = v(x)$ oraz $u \in \mathbb{Z}_p^\times$ jest jednością, to

$$\varphi(x) = \varphi(p^n u) = \varphi(p^n)\varphi(u) = p^n \varphi(u).$$

Oznacza to, że $v(\varphi(x)) = n = v(x)$, zaś sam automorfizm zachowuje p-adyczny rząd i jest ciągły. Ustalmy $y \in \mathbb{Q}_p$ i ciąg $y_n \in \mathbb{Q}$ zbieżny do y, na przykład ciąg obciętych rozwinięć p-adycznych dla y. Automorfizm φ jest trywialny na liczbach wymiernych, zatem

$$\varphi(y) = \varphi(\lim_n y_n) = \lim_n \varphi(y_n) = \lim y_n = y.$$ □

Jest to p-adyczny odpowiednik twierdzenia mówiącego, że jedynym automorfizmem algebraicznym $\mathbb{R}$ jest identyczność. W tych przypadkach algebraiczne automorfizmy nad $\mathbb{Q}$ okazują się być ciągłe i przez to trywialne. Istnieje jednak nieskończenie wiele automorfizmów $\mathbb{C}$, choć tylko dwa z nich są ciągłe. Skoro $\mathbb{Q}(\sqrt{2}) \subset \mathbb{C}$, to funkcję $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ można przedłużyć do całego $\mathbb{C}$.

5.7 Pierścień adeli

W rozdziale poświęconym mechanice kwantowej pojawiają się charaktery ciała $\mathbb{Q}_p$. Analogicznie można je określić na przykład dla $\mathbb{Q}$ i tym właśnie się zajmiemy – a dokładniej ich klasyfikacją. Do tego celu użyjemy pierścienia adelicznego.

Definicja 5.7.1. *Pierścień adeli $A_\mathbb{Q} \subsetneq \mathbb{R} \times \prod_p \mathbb{Q}_p$ składa się z tych ciągów, których wyrazy od pewnego miejsca leżą w (stosownych) $\mathbb{Z}_p$. Działania (dodawanie i mnożenie) określone są punktowo.*

Adele leżą między sumą $\bigoplus_p \mathbb{Q}_p$ i produktem $\prod_p \mathbb{Q}_p$. Ich elementy oznaczamy przez $(a_\infty, a_2, a_3, \dots)$. Ciało $\mathbb{Q}$ wkłada się w $A_\mathbb{Q}$ przez odwzorowanie przekątniowe, $r \mapsto (r, r, r, \dots)$.

Definicja 5.7.2. *Jeśli a jest adelem, to Ψ_a jest charakterem $\mathbb{Q}$:*

$$\Psi_a(r) = \chi_\infty(ra_\infty) \prod_p \chi_p(ra_p).$$

Fakt 5.7.3. *Odwzorowanie $a \mapsto \Psi_a$ jest surjekcją, którego jądro to wymierne adele.*

Dowód. „The character group of $\mathbb{Q}$", Keith Conrad. □

5.8 Wektory Witta

Ernst Witt pokazał w 1936 jak zadać strukturę pierścienia na zbiorze nieskończonych ciągów o wyrazach z przemiennego pierścienia $\mathcal{R}$, by z $\mathcal{R} = \mathbb{F}_p$ otrzymać liczby p-adyczne, $\mathbb{Z}_p$.

Dodawanie liczb p-adycznych jako szeregów potęgowych sprawia ból przez problemy podczas przenoszenia klasycznych cyfr $\{0, 1, \ldots, p-1\}$. Teichmüller proponował, by zastąpić je rozwiązaniami $x^p = x$ w $\mathbb{Z}_p$ (które można opuszczać do $\mathbb{F}_p$ i podnosić charakterem $\omega\colon \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$). To zmienia elementy $\mathbb{Z}_p$ w nieskończone ciągi o wyrazach z $\omega(\mathbb{F}_p^\times) \cup \{0\}$.

Chociaż z punktu widzenia teorii mnogości, $\mathbb{Z}_p$ to $\prod_{\mathbb{N}} \mathbb{F}_p$, zbiory te różnią się jako pierścienie. Przypomnijmy, że ω nie jest addytywny, ale pomimo to $\omega(k) = \omega(i) + \omega(j) \bmod p$ w $\mathbb{Z}_p$ pociąga $i + j = k$ w $\mathbb{F}_p$. Skrótowo zapisujemy to jako $m \circ \omega = \mathrm{id}_{\mathbb{F}_p}$, gdzie $m\colon \mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

Każdy element $\mathbb{Z}_p$ zapisuje się jako szereg potęgowy od p ze współczynnikami od Teichmüllera. Teraz $a_j^p = a_j$ i możemy po drętwych rachunkach (patrz: Wikipedia) dojść do

$$\sum_{j=0}^{m} c_j^{p^{m-j}} \cdot p^j \equiv \sum_{j=0}^{m} (a_j^{p^{m-j}} + b_j^{p^{m-j}}) \cdot p^j \mod p^{m+1}$$

To jakoś motywuje nasze postępowanie. Ustalmy pierwszą liczbę p.

Definicja 5.8.1. *Wektor Witta nad przemiennym pierścieniem $\mathcal{R}$ to ciąg z $\mathcal{R}^{\mathbb{N}}$.*

Definicja 5.8.2. *Wielomian Witta W_n to $\sum_j p^j x_j^{p^{n-j}}$.*

Definicja 5.8.3. *Ciąg $(W_0, W_1, \ldots)$ to składowa-duch wektora Witta, oznacza zazwyczaj przez $(x^{(0)}, x^{(1)}, x^{(2)}, \ldots)$*

Na zbiorze wektorów (Witta) jest dokładnie jedna struktura pierścienia, tak by suma i produkt były zadane wielomianami o całkowitych współczynnikach (niezależnych od $\mathcal{R}$), zaś każdy wielomian (Witta) był homomorfizmem w $\mathcal{R}$:

1. $X^{(i)} + Y^{(i)} = (X+Y)^{(i)}$,
2. $X^{(i)} Y^{(i)} = (XY)^{(i)}$.

Jeżeli p w $\mathcal{R}$ jest odwracalne, to dostajemy $\mathcal{R}^{\mathbb{N}}$, dla $\mathbb{F}_n$ – liczby p-adyczne, zaś dla $\mathbb{F}(p^n)$ – nierozgałęzione rozszerzenie stopnia n dla $\mathbb{Z}_p$.

Definicja 5.8.4. *Uniwersalny wielomian Witta to $W_n = \sum_{d|n} d x_d^{n:d}$.*

5.9 Problem Waringa

Dla $n > 1$ i przemiennego pierścienia z jedynką $\mathcal{R}$ określamy funkcję $g(n, \mathcal{R})$ jako najmniejszą liczbę s, że każdy element $\mathcal{R}$ jest sumą s n-tych potęg elementów $\mathcal{R}$ (jeśli istnieje) lub ∞ (jeśli nie). Problem Waringa polega na oszacowaniu wartości tej funkcji.

Definicja 5.9.1. *$W(\mathcal{K})$ to pierścień wektorów Witta nad $\mathcal{K}$, czyli (jedyne) zupełne i nierozgałęzione rozszerzenie $\mathbb{Z}_p$ o ciele residuów $\mathcal{K}$ algebraicznym nad $\mathbb{F}_p$.*

Mam nadzieję, że definicja ta nie jest na wojnie z sekcją poświęconą wektorom Witta w kalifacie algebry.

Niech $n = p^t d$, gdzie $(p, d) = 1$, $\varepsilon = 1$, $p \neq 2$ albo $\varepsilon, p = 2$. Lemat Hensela wystarcza do pokazania

Wniosek 5.9.2. *Jeśli $a \equiv x_1^n + \ldots + x_s^n \bmod p^{t+\varepsilon}$, zaś któryś z $x_i \in W(\mathcal{K})$ jest jednością, to a jest sumą pewnych s potęg n-tych elementów $W(\mathcal{K})$.*

Przyjmijmy $p \neq 2$. Jeśli a jest jednością, to w dowolnym przedstawieniu jako n-te potęgi jeden z x_i musi być jednością. Zatem jedności w $W(\mathcal{K})$ są sumą co najwyżej $g(n, W_{t+1}(\mathcal{K}))$ n-tych potęg, gdzie pierścień $W_{t+1}(\mathcal{K}) = W(\mathcal{K})/p^{t+1}$ składa się z przyciętych wektorów Witta.

Jeśli a nie jest jednością, to jest nią $a - 1$. Wtedy zachodzi nierówność $g(n, W(\mathcal{K})) \leq g(n, W_{t+1}(\mathcal{K})) + 1$. Oczywistym jest, że $g(n, W(\mathcal{K})) \geq g(n, W_{t+1}(\mathcal{K}))$, choć nie musi być tu równości ($\mathcal{K} = \mathbb{F}_p$, $p = 3$, $n = 2$).

Przez $g(n, r, W(\mathcal{K}))$ rozumiemy najmniejszą liczbę s, dla której istnieją $x_1, \ldots, x_s$ w $W(\mathcal{K})$, że $v(x_1^n + \ldots + x_s^n) = r$. Tutaj v była p-adyczną waluacją na $W(\mathcal{K})$. Oczywistym jest, że $g(n, 0, W(\mathcal{K})) = 1$. Jeżeli $n = p^t d$, $(p, d) = 1$ i $r \leq t$, a przy tym $v(x_1^n + \ldots + x_s^n) = r$, to któryś x_i jest odwracalny: gdyby tak nie było, mielibyśmy $v(\ldots) \geq n \geq p^t > t$. To spostrzeżenie jeszcze okaże się przydatne.

Bovey „udowodnił" fakt mocniejszy od poniższego dla $\mathbb{Z}_p$: niestety błędnie. My podamy ogólniejsze stwierdzenie.

Lemat 5.9.3. *Jeśli $n = p^t d$ i $(p, d) = 1$, to*

$$g(n, W_{t+1}(\mathcal{K})) \leq g(n, \mathcal{K}) \sum_{r=0}^{t} g(n, r, W(\mathcal{K}))$$

Dowód. Indukcja względem t. Przypadek $t = 0$, jest oczywisty, niech $t > 0$. Jeżeli $a \in W_{t+1}(\mathcal{K})$, to z założenia indukcyjnego wiemy, że istnieją $x_1, \ldots, x_s$ w $W_{t+1}(\mathcal{K})$, gdzie

$$s \leq g(n, \mathcal{K}) \sum_{r=0}^{t-1} g(n, r, W(\mathcal{K})),$$

że $x_1^{n/p} + \ldots + x_s^{n/p} = a$. Uwaga: $x^{n/p} \equiv (\sigma x)^n \bmod p^t$, gdzie σ jest odwrotnością automorfizmu Frobeniusa dla $W(\mathcal{K})$. Dostajemy $(\sigma x_1)^n + \ldots + (\sigma x_s)^n = a - bp^t$. Istnieją także $y_1, \ldots, y_u$, że $\sum y_i^n = cp^t$, $u \leq g(n, t, W(\mathcal{K}))$ i c nie dzieli się przez p. Wreszcie istnieją takie $z_1, \ldots, z_v$, że $\sum z_i^n \equiv b/c \bmod p$ (oraz $v \leq g(n, \mathcal{K})$). Wynika stąd, że

$$\begin{aligned} \sum (\sigma x_i)^n + \sum y_i^n \sum z_i^n &\equiv a - bp^t + cp^t b/c \\ &\equiv a \pmod{p^{t+1}}. \end{aligned}$$

Oznacza to, że a jest sumą co najwyżej $s + uv$ n-tych potęg w pierścieniu W_{t+1}. □

Wniosek 5.9.4. *Jeżeli $\mathcal{K}$ jest algebraicznie domknięte, to zachodzi nawet $g(n, r, W(\mathcal{K})) \leq 2r + 1$ dla $1 \leq r \leq t$. Przy tych samych założeniach, $g(n, W(\mathcal{K})) \leq (t+1)^2 + 1$.*

Dowód. Rozmaitości algebraiczne i Teichmüller :/. □

Fakt 5.9.5. *Jeśli $n = pd$, $(p, q) = 1$ i $q = p \geq 27d^6, 13$ albo też $p \neq q \geq 4d^4$, to $g(n, 1, W(\mathbb{F}_q)) \leq 3$ i $g(n, W(\mathbb{F}_q)) \leq 9$.*

Ostrzejsze oszacowania można znaleźć w pracy Volocha [**?**], naprawia ona usterki ze wcześniejszej pracy Boveya [**?**]. W pewnych przypadkach znamy dokładne wartości $g(\cdot, \mathbb{Z}_p)$ dla $p \neq 2$: $g((p-1)p^t) = p^{t+1}$, $g(\frac{1}{2}(p-1)p^t) = \frac{1}{2}(p^{t+1} - 1)$.

Fakt 5.9.6. *$g(p, \mathbb{Z}_p) \leq 4$, dla $p \leq 211$ różnych od $3, 7, 11, 17, 59$ nawet $g = 3$.*

Fakt 5.9.7. *$g(p^2, 2, W(\mathbb{F}_q)) \leq 5$ dla $q = p^a \geq p^7$ i dużych p.*

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, $\mathbb{Q}_p(\sqrt{\varepsilon}) = \{x + y\sqrt{\varepsilon} : x, y \in \mathbb{Q}_p\}$, jest ciałem.

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

Jeśli $z = x + \sqrt{\varepsilon}y$, $x, y \in \mathbb{Q}_p$, to parę (x, y) dla z nazwiemy współrzędnymi kartezjańskimi. Zbiór punktów, które spełniają równanie $z\overline{z} = c$, będzie dla nas „okręgiem”. Niech $\mathbb{Q}_p^\varepsilon \leq \mathbb{Q}_p^\times$ składa się z liczb c tej postaci: $c = r^2$ lub $c = \kappa r^2$, gdzie $r \in \mathbb{Q}_p^\times$, $\kappa \in \mathbb{Q}_p^\varepsilon$ nie jest kwadratem. Para (ρ, σ), gdzie $\rho = r$ lub $\rho = \nu r$ ($\nu \in \mathbb{Q}_p^\times(\sqrt{\varepsilon})$), $z = \rho\sigma$ i $\sigma\overline{\sigma} = 1$ to współrzędne biegunowe. „Okrąg” $z\overline{z} = 1$ to $\{(1 + \varepsilon t^2, 2t)/(1 - \varepsilon t^2) : t \in \mathbb{Q}_p\}$, jest on zbiorem zwartym.

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.

Przestrzeń $\mathbb{Q}_p^n$ z iloczynem skalarnym $\langle x \mid y \rangle$ danym przez $\sum_{i=1}^n x_i y_i$ zachowuje nierówność Cauchy'ego Schwarza. Kula $B_\gamma(a)$ jest produktem kul $B_\gamma(a_i)$ (rozpatrujemy tu metrykę od normy $|x|_p = \max_i |x_i|_p$).

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 $\|\cdot\| : \mathcal{V} \to \mathbb{R}_+$ 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:

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

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 $m_1 < m_2 < \dots$ „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 $v_1, \dots, v_{n-1}$, $\mathcal{W}$. 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 $c_1, \dots, c_N$, 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 $x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathcal{F}[x]$ 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 $[\mathcal{K} : \mathbb{Q}_p] = [\mathcal{K} : \mathcal{L}][\mathcal{L} : \mathbb{Q}_p]$. □

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 $f(x) = x^n + \ldots + a_1 x + a_0$ 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 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 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 16 (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 $f = \sum_{i \leq n} a_i x^i$ (wielomianu) kładziemy $\|f\| := \max\{|a_j| : 0 \leq j \leq n\}$. Oczywiście przedłuża to naszą wartość bezwzględną. Pokażemy multiplikatywność. Jasnym jest to, że $\|fg\| \leq \|f\| \cdot \|g\|$.

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 $x \in L$: $\|\sum_{k=1}^n \xi_k e_k\|_1 = \max\{|\xi_k| : k \leq n\}$. Funkcja ta ma własności normy, ale nie wiemy jeszcze, czy jest multiplikatywna. Weźmy zatem dwa elementy $x = \sum_{i \leq n} \xi_i e_i$, $y = \sum_{i \leq n} \eta_i e_i$ ($\xi, \eta \in \mathcal{K}$), wtedy $\|xy\|_1$, „norma" ich iloczynu, to $\|\sum_{i,j \leq n} \xi_i \eta_j e_i e_j\|_1 \leq \max_{i,j} |\xi_i||\eta_j| \|e_i e_j\|_1$, 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 $\|x^n\|_2 \leq \|x\|_2^n$, ma to ręce i nogi. Twierdzimy przy tym, że funkcja ν ma pewne własności dla $\lambda \in \mathcal{K}$ oraz $x, y \in L$: $\nu(1) = 1$, $\nu(x^k) = \nu(x)^k$, $\nu(xy) \leq \nu(x)\nu(y)$, $0 \leq \nu(x) \leq \|x\|_2$, $\nu(\lambda x) = |\lambda|\nu(x)$ oraz $0 \leq \nu(x) \leq \|x\|_2$. 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: $\nu_1 \leq \nu_2$, gdy $\nu_1(x) \leq \nu_2(x)$ 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.

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

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. □

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

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

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 $g_0(x) = (bc)^{-1}g_1(x)$, $h_0(x) = h_1(x)$. □

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 $n \ge 1$ 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 17 (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 $0 \le i < n$ 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 $|b_rc_s| = |a_n| = 1$.

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 $|a_0| \le 1/p^2$, 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 wciąż 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 $\frac{1}{e}\mathbb{Z}$. □

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 $\mathbb{Q}_p$. □

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 $X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$, który spełnia założenia dla kryterium Eisensteina (17).*

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 18 (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: $(1+\pi x)^{-1} = 1 - \pi x + (\pi x)^2 - (\pi x)^3 + \ldots$ 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 $0 \le l < e$ oraz $1 \le i \le f$, 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. $\sum_{n\ge1}(1-\zeta)^n : n = 0$.

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 19 (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 $i = 1, 2, \ldots, n$, 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

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

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 $\lambda_1 = \lambda, \lambda_2, \ldots, \lambda_n$ 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 $\mu_1, \ldots, \mu_m$) 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 $\zeta_2, \zeta_3, \ldots$, 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 $\sigma : \mathbb{Q}_p^a \to \mathbb{Q}_p^a$, 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 $\sigma_1, \ldots, \sigma_{d+1}$, które obcięte do $\mathbb{Q}_p(\zeta_{d-1})$ są identycznością (więc trzymają $\zeta_1, \ldots, \zeta_{d-1}$), 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:

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

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 $y_ix_i=1$ 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 $1-x_iy_i=0$ 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 $\mathcal{I}\lhd\mathcal{R}$ 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 $\lim_{\mathcal{U}}|x_i|=\lim_{\mathcal{U}}|x_i-y_i|\leq\sup|x_i-y_i|$ 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 $\mathbb{R}_{\geq0}$. □

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 $\mathcal{B}_{(i_1,i_2,\ldots)}=\bigcap_{n\geq1}\mathcal{B}_{i_1\ldots i_n}$ (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.*

Rozdział 7
Funkcje specjalne

W analizie nad $\mathbb{R}$ funkcje specjalne można definiować na wiele sposobów, przez rozwinięcia w szereg, równania różniczkowe, całki parametryczne, równania funkcyjne i tak dalej.

Inną metodą jest wzięcie zwykłej funkcji f określonej na $[a,\infty)\subset\mathbb{R}$ o wymiernych wartościach dla całkowitych $n\geq a$ i patrzenie na ciągłą funkcję $\mathbb{Z}_p\to\mathbb{C}_p$ przedłużającą $n\mapsto f(n)$. $\mathbb{Z}\cap[a,\infty)$ jest gęste w $\mathbb{Z}_p$, więc nie może być dwóch przedłużeń.

Poszukiwanie p-adycznych wariantów funkcji określanych normalnie na podzbiorach $\mathbb{C}$ zaczniemy właśnie od logarytmu i eksponensa.

7.1 Logarytm ($\mathbb{Q}_p$)

Definicja 7.1.1. *Logarytm to formalny szereg*

$$f(x)=\log(1+x)=\sum_{n=1}^{\infty}-\frac{(-x)^n}{n}.$$

Logarytm zbiega „gorzej” niż funkcja $\log\colon\mathbb{R}_+\to\mathbb{R}$.

Wypadałoby znać jego promień zbieżności: współczynniki tutaj nie maleją w normie.

Fakt 7.1.2. *Logarytm ma sens dla $x\in 1+p\mathbb{Z}_p=\mathcal{B}(1,1)$.*

Dowód. Skoro $0\leq\frac{1}{n}v_p(n)\leq\frac{1}{n}\log_p n\to 0$ i $|a_n|=p^{v_p(n)}$, to $p^{-0}=1$ jest szukanym promieniem. Łatwo widać, że nie ma dla $|x|=1$ zbieżności. □

Mamy nadzieję, że logarytm p-adyczny nie zostanie nigdy pomylony ze zwykłym (rzeczywistym) przy podstawie p.

By funkcja $\log_p\colon\mathcal{B}\to\mathbb{Q}_p$ zasługiwała na bycie logarytmem, musi mieć jego własności. Tak rzeczywiście jest.

Fakt 7.1.3. *Dla $a,b\in 1+p\mathbb{Z}_p$ jest $\log_p ab=\log_p a+\log_p b$.*

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

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

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

$$g'(x)=(1+y)f'(y+(1+y)x)=\frac{(1+y)}{1+y+(1+y)x}$$

$$=\frac{1}{1+x}=f'(x)\Rightarrow g(x)=f(x)+C.$$

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

Jeśli $p=2$, to $-1\in\mathcal{B}$, a to umożliwia obliczenie $\log_p(-1)$, 0, co nie powinno szokować.

Lemat Hensela pozwalał określić, dla jakich m istnieją m-te pierwiastki jedności w $\mathbb{Q}_p$ pod warunkiem, że $p\nmid m$. W $\mathbb{Q}_p$ nie ma takich dla $m=p^n$, co można pokazać w trzech krokach (poza patologicznym przypadkiem $p=2$ i $n=1$).

Fakt 7.1.4. *Logarytm p-adyczny ma dokładnie jedno ($x=1$ jeśli $p>2$) lub dwa ($x=\pm 1$ dla $p=2$) miejsca zerowe.*

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

Wniosek 7.1.5. *Dla $x\in 1+p\mathbb{Z}_p$ oraz $p\neq 2$ ($p=2$), które spełnia $x^p=1$ ($x^4=1$), mamy $x=1$ ($x=\pm 1$) – zatem p-te (czwarte) pierwiastki jedności w $\mathbb{Q}_p$ nie istnieją.*

Wniosek 7.1.6. *W $\mathbb{Q}_p$ żyje $\max\{2,p-1\}$ pierwiastków jedności.*

7.2 Eksponens (klasyczny)

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

Lemat 7.2.1. *Zachodzi $(p-1)v_p(n!)<n$.*

Dowód. Prawdziwość nierówności wynika z

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

Lemat 7.2.2. *Szereg $\sum_{n=0}^{\infty}x^n:n!$, protoplasta eksponensa, zbiega wtedy i tylko wtedy gdy $v_p(x)>1/(p-1)$.*

Dowód. Promieniem zbieżności „protoplasty” jest co najmniej $p^{-1/(p-1)}$, gdyż $|1/n!|=p^{v_p(n!)}<p^{n/(p-1)}$.

Z drugiej stony, gdy $n=p^m$, to $v_p(n!)=(n-1)/(p-1)$. Jeśli ustalimy x o waluacji równej $1/(p-1)$, to $x^n/n!$ nie dąży do zera (a sam szereg nie jest zbieżny), gdyż poniższe wyrażenie nie zależy od m.

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

Nierówność z lematu jest trochę dziwna, przecież dla $p\neq 2$ i $x\in\mathbb{Z}_p$ wartość bezwzględna, $|x|$, może być albo większa lub równa 1 (więc większa niż $p^{-1/(p-1)}$) lub mniejsza lub równa $1/p$ (ta zaś liczba jest mniejsza), nie ma wartości „pomiędzy”. A zatem dysk z lematu jest po prostu otwartym o promieniu jeden: lemat nie jest jednak bezsensowny, w szczególności dla ciał, które zawierają $\mathbb{Q}_p$ (np. $\mathbb{C}_p$).

Definicja 7.2.3. *Eksponens $\exp_p\colon\mathcal{B}\to\mathbb{Q}_p$ jest określona na $p\mathbb{Z}_p$ (dla $p\neq 2$) lub $4\mathbb{Z}_2$ przez podany wcześniej szereg.*

Fakt 7.2.4. *Jeżeli $x,y,x+y\in\mathcal{B}(0,p^{-1/(p+1)})$, to $\exp(x+y)$ jest równe $\exp x\exp y$.*

Dowód. Dowód to po prostu formalna manipulacja szeregów.

$$L=\exp_p(x+y)=\sum_{n\geq 0}\frac{(x+y)^n}{n!}=$$

$$=\sum_{n\geq 0}\sum_{k\leq n}\frac{1}{n!}\frac{n!}{k!(n-k)!}x^{n-k}y^k$$

$$=\sum_{n\geq 0}\sum_{k\leq n}\frac{x^{n-k}}{(n-k)!}\frac{y^k}{k!}=\sum_{m\geq 0}\frac{x^m}{m!}\cdot\sum_{k\geq 0}\frac{y^k}{k!}$$

$$=\exp_p(x)\exp_p(y)=R$$ □

Zwykła eksponensa i logarytm są do siebie odwrotne, czy $\exp_p(\log_p(1+x))=1+x$ tam, gdzie jest zbieżność? Fakt 2.3.3 ma założenia, które trzeba sprawdzić.

Fakt 7.2.5. *Załóżmy, że jest $|x|<p^{-1/(p-1)}$ ($x\in\mathbb{Z}_p$). Zachodzi wtedy $\log_p(\exp_p x)=x$ oraz $\exp_p(\log_p(1+x))=1+x$.*

Dowód. Bez straty ogólności niech $x \neq 0$. Podczas składania $\log_p(\exp_p x)$, wstawiamy $\exp_p x - 1$ do wzoru na $\log_p(1+x)$. Skoro tak, korzystamy z założenia i piszemy:

$$|\exp_p x - 1| = \left|\sum_{n=1}^{\infty} \frac{x^n}{n!}\right| < \frac{|x|^n}{p^{n/(p-1)}} < 1$$

Można jeszcze lepiej oszacować waluację $v = v_p(x^{n-1}/n!)$:

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

gdzie s to suma cyfr n w rozwinięciu p-adycznym i $n \geq 2$. Stąd wynika, że $v_p(x) < v_p(x^n/n!)$ i wreszcie korzystamy z lematu 2.3.3 dla $\log_p \circ \exp_p$, gdyż

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

Złożymy teraz szeregi w drugą stronę. Niech $n > 1$ oraz $a_n = -(-x)^n/n$. Wtedy (dla $v = v_p(a_n) - v_p(x)$) mamy

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

Wykażemy nieujemność tego, co pozostało w nawiasach. Niech $n = p^v n'$ z $n' \nmid p$, czyli

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

A zatem $|(-1)^{n+1}x^n/n| < |x|$ i do akcji wkracza fakt 2.1.2: $|\log_p(x)| = |x| < p^{-1/(p-1)}$ daje żądaną równość. □

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

W ciałach charakterystyki p dzieje się coś niedobrego.

Fakt 7.2.6. *Analityczna f z wypukłego otoczenia zera spełniająca jeden z warunków: $f' = f$ lub $f(x+y) = f(x)f(y)$ jest zerem.*

Szereg z definicji eksponensa wcale nie ma sensu, jako że $n!$ nie odwraca się dla $n \geq p$.

7.3 Szereg dwumianowy

Zajmiemy się wreszcie szeregami dwumianowymi (warto się zapoznać z treścią sekcji 5.2 i 5.3). W $\mathbb{R}$ funkcję $(1+x)^\alpha$ można rozwinąć w szereg potęgowy zbieżny dla $|x| < 1$:

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

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

Fakt 7.3.1. *Jeśli $\alpha \in \mathbb{Z}_p$ i $n \geq 0$, to $(\alpha \text{ nad } n) \in \mathbb{Z}_p$. Jeżeli do tego $|x| < 1$, to szereg $B(\alpha, x)$ jest zbieżny.*

Dowód. Dla każdego n rozpatrzmy wielomian

$$P_n(x) = \prod_{k=0}^{n-1} \frac{x-k}{k+1} \in \mathbb{Q}[x].$$

Wielomiany określają ciągłe funkcje $\mathbb{Q}_p \to \mathbb{Q}_p$. Wiemy, że dla $\alpha \in \mathbb{Z}_+$ mamy $P_n(\alpha) \in \mathbb{Z}$. Obraz $\mathbb{Z}_+$ przez P_n leży w $\mathbb{Z}$, więc po domknięciu uzyskujemy upragnione $P_n[\mathbb{Z}_p] \subseteq \mathbb{Z}_p$. □

Z równości formalnych szeregów potęgowych wynika, że dla $\alpha = a/b \in \mathbb{Z}_{(p)}$ i $|x| < 1$ prawdziwa jest równość między $(1+x)^a$ oraz $(B(a/b, x))^b$, co nadaje sensu definicji:

Definicja 7.3.2. $(1+x)^{a/b} := B(a/b, x)$.

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

Przykład 7.3.3 (Koblitz). *Jeśli $p = 7$, $\alpha = 1/2$, $x = 7/9$, to w $\mathbb{R}$ pierwiastek z $1+x$ jest równy $4/3$, ale w $\mathbb{Q}_7$ nie: $|x| = 1/7$, więc dla $n \geq 1$ jest $|(1/2 \text{ nad } n)x^n| \leq |x|^n = 7^{-n} < 1$. To pociąga za sobą $(1+x)^{1/2} \in 1 + 7\mathbb{Z}_7$, a także $|(1+x)^{1/2} - 1| < 1$, lecz $|4/3 - 1| = 1$, więc to $-4/3$ jest pierwiastkiem z $1+x$.*

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

Interesujący wynik dotyczący szeregów p-adycznych i ich zbieżności przedstawiony jest w sekcji 2.4 na podstawie pracy Burgera i Struppecka z 1996 roku.

Fakt 7.3.4. *Niech $1+x$ będzie kwadratem $\frac{a}{b}$, gdzie $a, b > 0$ są względnie pierwsze, zaś S to zbiór tych pierwszych liczb, dla których szereg $B(1/2, x)$ zbiega w $\mathbb{Q}_p$ (lub $\mathbb{Q}_\infty = \mathbb{R}$).*

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

Dowód. Szczególny przypadek twierdzenia Bombieriego. □

Wygląda na to, że dwa poniższe stwierdzenia pochodzą od samego Koblitza, jednak brakuje im dowodu.

Fakt 7.3.5. *Szeregu dwumianowy $B(\alpha, x)$ ma tę samą wartość w ciałach $\mathbb{Q}_p$ i $\mathbb{R}$ (między innymi) dla:*

- *$\alpha = -n \in -\mathbb{N}$ oraz $x = -p/(p+1)$.*
- *$\alpha = 1/2$ oraz $xm^2 = p^2 + 2mp$, $m > (\sqrt{2}+1)p$, $p \nmid m$.*

Fakt 7.3.6. *Szereg dwumianowy $B(1/2, p/n^2)$ zbiega do różnych, ale wymiernych liczb w $\mathbb{Q}_p$ i $\mathbb{R}$ dla (na przykład) $p = 2n+1 \geq 7$.*

7.4 Logarytm (japoński)

Pracujemy w $\mathcal{K} = \mathbb{C}_p$.

Fakt 7.4.1. $\log \exp x = x$, $\exp \log(1+x) = 1+x$, *o ile* $|x| < r_p$.

(To było tylko przypomnienie).

Wniosek 7.4.2. *Morfizm $\log\colon 1 + \mathfrak{p} \to \mathcal{K}$ jest „na". Jego jądro to $\mu(p^\infty)$. Obcięty do $1 + \mathcal{B}(0, r_p)$ jest (injektywną) izometrią.*

Fakt 7.4.3. *Dokładnie jeden morfizm $f\colon \mathcal{K}^\times \to \mathcal{K}$ ma poniższe własności (logarytm Iwasawy Log): $f(p) = 0$ (normalizacja), zaś obcięcie f do $\mathcal{B}(1,1)$ pokrywa się ze zwykłym logarytmem (to znaczy szeregiem potęgowym).*

Dowód. (Jednoznaczność) Podgrupy $p^{\mathbb{Q}}\mu_{(p)}$ i $1+\mathfrak{p}$ generują całe $\mathcal{K}^\times$. Jest to oczywiste dla μ, gdyż ciało $\mathcal{K}$ (charakterystyki 0) nie ma addytywnej torsji. Z drugiej strony, jeśli $x^a = p^b$, to $af(x) = bf(p) = 0$, co daje $f(x) = 0$.

(Istnienie) Niech f będzie zerem na $p^{\mathbb{Q}}\mu$, gdyż zgadza się to z logarytmem na przekroju $p^{\mathbb{Q}}\mu$ z $1+\mathfrak{p}$, $\mu(p^\infty)$. Ale podgrupa $\mu(p^\infty)$ to dokładnie jądro logarytmu. □

Fakt 7.4.4. *Logarytm Iwasawy jest lokalnie analityczny: dla $a \neq 0$ i $|x-a| < |a|$ mamy $\operatorname{Log} x = \operatorname{Log} a - \sum_{k\geq 1}^{\infty}[1-x/a]^k/k$.*

Fakt 7.4.5. *Dla $x \in \mathbb{Z}_p^\times$, $(1-p)\operatorname{Log} x = \sum_{k\geq 1}(1-x^{p-1})^k/k$.*

Fakt 7.4.6. *Dla zupełnych podciał $K \subseteq \mathbb{C}_p$, $\operatorname{Log}[K^\times] \subseteq K$.*

Fakt 7.4.7. *Dla każdego ciągłego automorfizmu σ ciała $\mathbb{C}_p$ prawdą jest $\operatorname{Log}(x^\sigma) = (\operatorname{Log} x)^\sigma$.*

W swojej pracy doktorskiej („Prolongement de la fonction exponentielle en dehors de son cercle de convergence") M. C. Sarmant-Durix pokazała, że funkcja wykładnicza przedłuża się na całe $\mathbb{C}_p$. Robert zaś postanowił podążać za Schikhofem (ale nie widać tego tutaj).

Fakt 7.4.8. *Ustalmy $a \in \mathbb{C}_p$, że $|1-a|_p < 1$. Wtedy*

$$\operatorname{Log} a = \lim_{n\to\infty} \frac{a^{p^n}-1}{p^n}.$$

Jeżeli $b \in \mathbb{C}_p$, $|b|_p = 1$ i ω jest charakterem Teichmüllera, to

$$\operatorname{Log} b = \lim_{n\to\infty} \frac{b^{p^{n!}} - \omega_p(b)}{\omega_p(b)p^{n!}}.$$

7.5 Trygonometria van Hamme'a

Poniższe konstrukcje mogą działać w wielu ciałach, my jednak ograniczymy się do $\mathbb{Q}_p$ (charakterystyki zero, ciało residuów charakterystyki p).

Szeregami potęgowymi można określić funkcje $\sin_p$, $\cos_p$, ale nie będą okresowe (ze względu na fakt 2.3.11).

Fakt 7.5.1. $\sin_p^2 x + \cos_p^2 x = 1$.

Fakt 7.5.2. $\cosh_p^2 x - \sinh_p^2 x = 1$.

Fakt 7.5.3. *Sinus jest izometrią z $E = \mathcal{B}(0, p^{1/(1-p)})$ w $1+E$.*

Fakt 7.5.4. *Kosinus nie jest lokalnie injektywny w 0.*

Fakt 7.5.5. *Jeśli p jest postaci $4k+1$, to w $\mathbb{Q}_p$ równanie $x^2+1=0$ ma rozwiązanie $x = i$ spełniające $\exp_p(ix) = \cos_p(x) + i\sin_p(x)$.*

Wniosek 7.5.6. *Okrąg $\{(x,y) \in \mathbb{Q}_p^2 : x^2+y^2 = 1\}$ jest zwarty dokładnie dla $p = 2$ lub $p = 4k+3$.*

Fakt 7.5.7. *Tangens (iloraz sinusa i kosinusa) jest analityczną funkcją $E \to \mathbb{C}_p$.*

Dowód. Funkcja $\log_p \cos$ jest dobrze określona i analityczna, a razem z nią jej pochodna. □

Definicja 7.5.8. *Arkus tangens dla $x \in \mathbb{C}_p \setminus \{i, -i\}$ to*

$$\arctan x = \frac{1}{2i}\log_p \frac{1+ix}{1-ix}.$$

Jest to oczywiście funkcja odwrotna do tangensa, bowiem w przeciwnym przypadku nie nazywałaby się tak. Znika (między innymi) w zerze i nieskończoności.

Fakt 7.5.9. *Dla $|x|_p < 1$ mamy*

$$\arctan x = \sum_{k=0}^{\infty}(-1)^k \frac{x^{2k+1}}{2k+1}.$$

Fakt 7.5.10. *Dla $x \neq i, -i$ mamy*

$$\arctan' x = \frac{1}{1+x^2}.$$

Fakt 7.5.11. *Jeśli $xy \neq 1$ oraz $x, y \neq i, -i$, to*

$$\arctan \frac{x+y}{1-xy} = \arctan x + \arctan y.$$

Fakt 7.5.12. *Jeśli $z \neq 0, i, -i$, to $0 = \arctan z + \arctan 1/z$.*

Fakt 7.5.13. *Jeśli $x \neq 0$, $x^2+y^2 \neq 0$, to*

$$\log_p(x+iy) = \frac{1}{2}\log_p(x^2+y^2) + i\arctan\frac{y}{x}.$$

Fakt 7.5.14. *Największym dyskiem zbieżności $\arctan$, który zawiera $a \in \mathbb{C}_p$, jest $\{x \in \mathbb{C}_p : |x-a|_p < \min(|a-i|_p, |a+i|_p)$.*

Definicja 7.5.15. *Dla $|x|_p < 1$ i $x \in \mathbb{C}_p$ mamy*

$$\arcsin x = \frac{1}{i}\log_p(ix + \sqrt{1-x^2}).$$

Fakt 7.5.16. *Dla $|x|_p < 1$ mamy*

$$\arcsin' x = \sqrt{1-x^2}^{-1}.$$

Fakt 7.5.17. *Arkus sinus jest analityczną surjekcją na $\mathbb{C}_p$.*

Definicja 7.5.18. *Ustalmy $x \in \mathcal{B}(\sqrt{1-a^2}, |a^2|_p)$, niezerowe $a \in E$.*

$$\arccos_a(x) = \frac{1}{i}\log_p(x + ia\sqrt{(1-x^2)/a^2}).$$

Fakt 7.5.19. *Dla $|x - \cos a|_p < |a|_p^2$ mamy*

$$\arccos' x = -\frac{1}{a}\sqrt{a^2/(1-x^2)}.$$

7.6 Logarytm (diamentowy)

Poznamy zaraz funkcję, która choć nie jest równa $\log_p \Gamma_p$, i tak zasługuje na swoją nazwę: log gamma Diamonda.

Definicja 7.6.1. *Dla $x \in \mathbb{C}_p \setminus \mathbb{Z}_p$ niech*

$$G_p(x) = \int_{\mathbb{Z}_p} (x+u)(\log_p(x+u) - 1)\, du.$$

Fakt 7.6.2. $G_p(x+1) - G_p(x) = \log_p x$.

Dowód. Niech $f(x,u) = (x+u)(\log p(x+u) - 1)$. Wtedy to $f(x+1,u) - f(x,u) = f(x,u+1) - f(x,u)$, zatem prawdą jest też $G_p(x+1) - G_p(x) = \partial_u f(x,0) = \log_p(x)$. □

Fakt 7.6.3. $G_p(1-x) = -G_p(x)$.

Dowód. Skoro $\log_p(-1) = 0$, to $f(-x,u) = -f(x,-u)$.

$$\begin{aligned} -G_p(-x) &= \int_{\mathbb{Z}_p} f(x,-u)\,\mathrm{d}u = \int_{\mathbb{Z}_p} -f(x,u+1)\,\mathrm{d}u \\ &= \int_{\mathbb{Z}_p} -f(x+1,u)\,\mathrm{d}u = G_p(1+x). \end{aligned}$$ □

Fakt 7.6.4. *Dla $m \in \mathbb{N}$,*

$$G_p(x) = \frac{2x-1}{2}\cdot\log_p m + \sum_{j=0}^{m-1} G_p\frac{x+j}{m}.$$

Dowód. Mamy $f(y,mu) = (y+mu)\log_p m + mf(y/m,u)$, a do tego równość

$$G_p(x) = \int_{\mathbb{Z}_p} f(x,u)\,\mathrm{d}u = \frac{1}{m}\sum_{j=0}^{m-1} f(x,j+mu)\,\mathrm{d}u.$$

Podkładając $y = x+j$ dostajemy

$$\int_{\mathbb{Z}_p} f(x,j+mu)\,\mathrm{d}u = (y-\frac{m}{2})\log_p m + mG_p\frac{y}{m}.$$

Ale

$$\frac{1}{m}\sum_{j=0}^{m-1}(x+j-\frac{m}{2})\log_p m = (x-\frac{1}{2})\log_p m. \qquad \square$$

Fakt 7.6.5. *Funkcja G_p jest lokalnie analityczny.*

Fakt 7.6.6. *Związek z Γ_p Mority:*

$$\log_p \Gamma_p(x) = \sum_{j=0}^{p-1} G_p\frac{x+j}{p},$$

ale sumujemy jedynie po tych j, że $|x+j|_p = 1$.

7.7 Gamma Mority

Załóżmy najpierw, że $p \geq 3$. Funkcja $n \mapsto n!$ nie przedłuża się w ciągły sposób na $\mathbb{Z}_p$. Gdybyśmy mieli ciągłą $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$, taką że $f(n) = nf(n-1)$ dla całkowitych $n \geq 1$, to taka sama relacja zachodziłaby dla $n \in \mathbb{Z}_p$. Zatem

$$f(n) = n(n-1)(n-2)\cdot\ldots\cdot p^m f(p^m-1)$$

dla całkowitych $n > p^m$, gdzie p^m jest ustaloną potęgą p. Skoro f jest ciągła na zwartej $\mathbb{Z}_p$, to jest ograniczona, czyli istnieje $C > 0$, że $|f(x)| \leq C$ tamże. Napisany wyżej rozkład pokazuje, że $|f(n)| \leq |p^m|\cdot C$ dla całkowitych $n > p^m$, ale one leżą gęsto w $\mathbb{Z}_p$, zatem $\|f\|_\infty \leq |p|^m \cdot C$. Liczba m była dowolna, więc musimy mieć $\|f\|_\infty = 0$.

To smutne. Problemy wzięły się stąd, że duże silnie są zbyt podzielne przez potęgi p. Zdefiniujmy więc **obciętą silnię**, $n!^*$. Kluczem do sukcesu jest uogólnienie przystawania Wilsona.

$$n!^* = \prod_{j=1}^{n}{}^{\!\!\prime}\; j \qquad \text{(produkt po } p\nmid j\text{)}$$

Fakt 7.7.1. *Niech a i $v \geq 1$ będą całkowite, wtedy*

$$\prod_{j=a}^{a+p^v-1}{}^{\!\!\prime}\; j \equiv -1 \pmod{p^v}.$$

Dowód. Reprezentantów ilorazu $\mathbb{Z}/p^v\mathbb{Z}$ wyczerpują całkowite $a \leq j < a+p^v$. Liczby niepodzielne przez p odpowiadają za odwracalne elementy, tzn. elementy grupy $G = (\mathbb{Z}/p^v\mathbb{Z})^\times$. Łącząc dowolny element $g \in G$ z odwrotnym, g^{-1}, znosimy je wszystkie poza sytuacją, gdy $g^2 = 1$. W pierścieniu $\mathbb{Z}/p^v\mathbb{Z}$ jest tak wtedy i tylko wtedy, gdy $g = \pm 1$ lub $g \pm 1$ są jednocześnie dzielnikami zera. Tak jednak może być tylko wtedy, gdy p dzieli różnicę, 2, co nie zachodzi nigdy. $\square$

Fakt ten pociąga dla funkcji $f(n) = (-1)^n \prod_{j=1}^{n-1}{}'\; j$ (gdy $n \geq 2$) relację $f(a) \equiv f(a+mp^v)$ modulo p^v. Odwzorowanie $a \mapsto f(a)\colon \mathbb{N}\setminus\{0,1\} \to \mathbb{Z}$ jest jednostajnie ciągłe w topologii p-adycznej, zatem przedłuża się jednoznacznie do $\mathbb{Z}_p \to \mathbb{Z}_p$.

Definicja 7.7.2. *Przedłużenie to Γ_p, funkcja gamma Mority.*

Lemat 7.7.3. $\Gamma_p(\mathbb{Z}_p) \subseteq \mathbb{Z}_p^\times \subset \mathbb{Z}_p$

Jakie własności ma ta funkcja? Przede wszystkim $\Gamma_p(2) = 1$ i $\Gamma_p(3) = -2$. Jeśli $n \leq p-1$ jest nieparzyste, to $\Gamma_p(n+1) = n!$, jeśli jest parzyste, to $-n!$. Z definicji widać, że $\Gamma_p(n) \in \mathbb{Z}_p^\times$ jest dana przez

$$\Gamma_p(n+1) = \frac{(-1)^{n+1}n!}{\prod_{1\leq kp\leq n} kp} = \frac{(-1)^{n+1}n!}{[n/p]!p^{[n/p]}}$$

gdy całkowita n jest większa lub równa 2. Z definicji mamy też, że $\Gamma_p(n+1)$ to $-n\Gamma_p(n)$ (jeśli $p\nmid n$) lub $-\Gamma_p(n)$ (jeśli nie) i (z ciągłości) ogólniej

$$\Gamma_p(x+1) = \begin{cases} -x\Gamma_p(x) & \text{dla } x \in \mathbb{Z}_p^\times \\ -\Gamma_p(x) & \text{dla } x \in p\mathbb{Z}_p \end{cases}$$

Dla wygody wprowadzamy pomocniczą $h_p(x)$ równą $-x$ dla $x \in \mathbb{Z}_p^\times$ ($|x| = 1$) lub -1 (dla $x \in p\mathbb{Z}_p$, $|x| < 1$).

Fakt 7.7.4. *Jeśli $p > 2$, to funkcja Γ_p jest ciągła. Poza tym,*

1. $\Gamma_p(0) = 1$ *i* $\Gamma_p(n+1) = (-1)^{n+1}n!$ *dla* $1 \leq n < p$.
2. $|\Gamma_p(x)| = 1$
3. $|\Gamma_p(x) - \Gamma_p(y)| \leq |x-y|$
4. $\Gamma_p(x+1) = h_p(x)\Gamma_p(x)$
5. $\Gamma_p(x)\Gamma_p(1-x) = (-1)^{R(x)}$, *gdzie* $1 \leq R(x) \leq p$ *oraz* $R(x) \equiv x \pmod p$.

Dowód. Punkt trzeci wynika z przystawania $\Gamma(a+mp^v)$ do $\Gamma(a)$ modulo p^v oraz ciągłości. Dla dowodu piątego połóżmy $f(x) = \Gamma_p(x)\cdot\Gamma_p(1-x)$ …szczegóły zna Robert. $\square$

Zwykła funkcja Γ spełnia dla $m \geq 2$ tożsamość:

$$\prod_{j=0}^{m-1}\Gamma\left(z+\frac{j}{m}\right) = (2\pi)^{(m-1)/2}m^{1/2-mz}\cdot\Gamma(mz).$$

Fakt 7.7.5 (mnożnikowy wzór Gaußa)**.** *Niech funkcja f_m będzie określona dla $m \geq 1$ niepodzielnych przez p:*

$$f_m\colon x \mapsto \prod_{j=0}^{m-1}\Gamma_p\left(x+\frac{j}{m}\right).$$

Niech $s(y) = \frac{1}{p}(R(y)-y)$, przy czym $1 \leq R(y) \leq p$ przystaje do y mod p. Wtedy

$$f_m(x) = \frac{m^{1+(p-1)s(mx)}}{m^{R(mx)}}\cdot\Gamma_p(mx)\underbrace{\prod_{j=0}^{m-1}\Gamma_p\left(\frac{j}{m}\right)}_{\varepsilon_m}.$$

Dowód. Policzmy czynnik Gaussa $G_m(x) = f(x)/\Gamma_p(mx)$.

$$\begin{aligned} ? = G(x+1/m) &= \frac{\prod_{j=1}^{m}\Gamma_p(x+j/m)}{\Gamma_p(mx+1)} \\ &= \frac{1}{h_p(mx)\Gamma_p(mx)}\cdot\frac{\Gamma_p(x+1)}{\Gamma_p(x)}\prod_{j=0}^{m-1}\Gamma(x+j/m) \\ &= \frac{h_p(x)}{h_p(mx)}G(x) = \lambda(x)G(x) \end{aligned}$$

Lokalnie stały mnożnik λ wyznacza kolejne wartości, gdyż $G(1/m)$ to $\lambda(0)G(0)$, $G(2/m)$ to $\lambda(0)\lambda(1/m)G(0)$, i tak dalej. Skoro m, p są względnie pierwsze, to $\prod_{i=0}^{j-1}\lambda(i/m) = (1/m)^u$, gdzie u to ilość względnie pierwszych z p tych i, że $0 < i < j$, czyli $j-1-[(j-1)/p]$. Rozwijając p-adycznie $j-1$:

$$j = \underbrace{(j-1)_0+1}_{R(j)} + p\left[\frac{j-1}{p}\right],$$

gdzie $R(j) \equiv j \pmod p$ jest dobre. To dowodzi

$$j-1-\left[\frac{j-1}{p}\right] = R(j)-1+(p-1)\left[\frac{j-1}{p}\right],$$

więc $\prod_{i=0}^{j-1}\lambda(i/m) = m^{1-R(j)}(m^{p-1})^{s(j)}$ z $s(j) = \frac{1}{p}(R(j)-j)$, które ciągle przedłuża się do $\mathbb{Z}_p$. Pokazaliśmy, że

$$G(j/m) = \prod_{j=0}^{j-1}\lambda(i/m)G(0)$$
$$= m^{1-R(j)}(m^{p-1})^{s(j)}\cdot G(0),$$

ale tylko dla całkowitych $x = j/m$. Z ciągłości wzór prawdziwy jest dla wszystkich $x \in \mathbb{Z}_p$. (Khm: $\varepsilon_m = G(0)$). □

Lemat 7.7.6. *Mamy równość $\varepsilon_m^4 = 1$, a nawet $\varepsilon_m^2 = 1$, chyba że m jest parzyste, zaś p postaci $4k+1$ (wtedy -1).*

Dowód. Gdy $2 \nmid m$, to ε_m wynosi $\Gamma_p(1/m)\cdot\ldots\cdot\Gamma_p((m-1)/m)$, bo $\Gamma_p(0) = 1$. Pogrupujmy czynniki z „j" i „$m-j$" do ±1; okaże się, że $\varepsilon_m = \pm1$. Dla parzystego m pozostanie jeden czynnik: $\varepsilon_m = \pm\Gamma_p(1/2)$, więc $\varepsilon_m^2 = \Gamma_p(1/2)^2$. Tę liczbę znamy: jest równa -1, wtedy i tylko wtedy gdy $p = 4k+1$. □

Ciągła funkcja na $\mathbb{Z}_p$ to szereg Mahlera: dla $a_k = (\nabla^k f)(0)$ mamy $f(x) = \sum_{k=0}^{\infty} a_k(x \text{ nad } k)$. Współczynniki a_k można związać z wartościami f (jak wcześniej!):

$$\sum_{k=0}^{\infty} a_k\frac{x^k}{k!} = \exp(-x)\sum_{n=0}^{\infty} f(n)\frac{x^n}{n!}.$$

Fakt 7.7.7. *Niech $\Gamma_p(x+1) = \sum_{k=0}^{\infty} a_k\binom{x}{k}$ jako szereg Mahlera. Wtedy jego współczynniki spełniają zależność:*

$$\sum_{k=0}^{\infty}(-1)^{k+1}a_k\frac{x^k}{k!} = \frac{1-x^p}{1-x}\exp\left(x+\frac{x^p}{p}\right).$$

Dowód. Obliczymy $\varphi(x)/e^x$, gdzie $\varphi(x)$ jest zadana szeregiem $\sum_{n=0}^{\infty}\Gamma_p(n+1)x^n/n!$. Sumujemy po warstwach mod p:

$$\varphi(x) = \sum_{j=0}^{p-1}\sum_{m=0}^{\infty}\Gamma_p(mp+j+1)\frac{x^{mp+j}}{(mp+j)!}.$$

Tutaj możemy zaś (dla $n = mp+j$, $m = [n/p]$) użyć równości $\Gamma_p(n+1) = (-1)^{n+1}n!/([n/p]!p^{[n/p]})$. Otrzymujemy w ten sposób $\Gamma_p(mp+j+1) = (-1)^{mp+j+1}\cdot(mp+j)!/(m!p^m)$ oraz $-\varphi(x) = \ldots$

$$= \sum_{m=0}^{\infty}\frac{(-x)^{mp}}{p^m m!}\sum_{j=0}^{p-1}(-x)^j = \frac{1-(-x)^p}{1-(-x)}\exp\frac{(-x)^p}{p}$$ □

Chcemy rozwinąć $\log\Gamma_p$ w szereg potęgowy. Skorzystamy z poniższego wzoru dla całki Volkenborna:

$$\mathfrak{d}(f')(x) = \int_{\mathbb{Z}_p}[f(x+y)-f(y)]\,\mathrm{d}y$$

i funkcji $f(x) = x\operatorname{Log}x - x$ dla $|x| = 1$ (wtedy $f'(x) = \operatorname{Log}x$) i 0 dla $|x| < 1$ (wtedy $f'(x) = 0$), więc $f'(x) = \operatorname{Log}h_p(x)$. Tutaj Log jest logarytmem Iwasawy: znika na pierwiastkach jedności, więc $\operatorname{Log}(-x) = \operatorname{Log}x$. Zatem f jest nieparzysta i całka z niej jest zerem (to ważne).

$\nabla\operatorname{Log}\Gamma_p(x) = \operatorname{Log}\Gamma_p(x+1) - \operatorname{Log}\Gamma_p(x) = \operatorname{Log}h_p(x)$. Ponieważ $\mathfrak{d}\nabla f = f - f(0)$ oraz $\operatorname{Log}\Gamma_p(0) = \operatorname{Log}1 = 0$, wnioskujemy stąd $\operatorname{Log}\Gamma_p(x) = \mathfrak{d}\operatorname{Log}h_p(x)$. Powyższy wzór dla całki Volkenborna z $f' = \operatorname{Log}h_p$ daje

$$\operatorname{Log}\Gamma_p(x) = \int_{\mathbb{Z}_p^\times}[(x+y)\operatorname{Log}(x+y) - (x+y)]\,\mathrm{d}y.$$

Jak zachowuje się $\operatorname{Log}\Gamma_p$?

Fakt 7.7.8. *Dla $x \in p\mathbb{Z}_p$ mamy*

$$\operatorname{Log}\Gamma_p(x) = \lambda_0 x - \sum_{m=1}^{\infty}\frac{\lambda_m x^{2m+1}}{2m(2m+1)},$$
$$\lambda_0 = \int_{\mathbb{Z}_p^\times}\operatorname{Log}t\,dt \quad \lambda_m = \int_{\mathbb{Z}_p^\times}\frac{dt}{t^{2m}}.$$

Wniosek 7.7.9. *Zachodzi*

$$\frac{\Gamma_p'}{\Gamma_p}(x) = \int_{\mathbb{Z}_p^\times}\operatorname{Log}(x+t)\,dt$$
$$(\operatorname{Log}\Gamma_p)''(x) = \int_{\mathbb{Z}_p^\times}\frac{dt}{x+t}.$$

Z Kazandzidisem jeszcze lepiej poznamy $\log\Gamma_p$.

Twierdzenie 20 (Kazandzidis)**.** *Wzór niżej zachodzi dla pierwszych $p \geq 3$, ale jeśli $p = 3$, to zamiast p^3 należy wpisać p^2.*

$$\binom{pn}{pk} \equiv \binom{n}{k} \pmod{p^3nk(n-k)\binom{n}{k}\mathbb{Z}_p}$$

Fakt 7.7.10. *Funkcja $x \mapsto \log\Gamma_p(px)$ ($\mathbb{Z}_p \to ?$) zadana jest przez obcięty szereg o współczynnikach z $p\mathbb{Z}_p$ i*

$$|f(x+y) - f(x) - f(y)| \leq |p^3xy(x+y)|.$$

Pokażemy, że funkcję Γ Mority można określić dla $p = 2$.

Fakt 7.7.11. *Dla $v \geq 3$, jądro homomorfizmu „redukcja modulo 4" $(\mathbb{Z}/2^v\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$ jest cykliczne, generowane przez 5.*

Określmy ciąg: $f(1) = 1$, $f(n) = \coprod_{j=1}^{n-1} j$ (tutaj $p = 2$). Spełnia on między innymi nierówność $|f(m)-f(n)| \leq |m-n|$ dla $m, n \geq 1$ i $|m-n| \leq 1/8$. Dzięki jednostajnej ciągłości f przedłuża się jednoznacznie do $\mathbb{Z}_2 \to 1+2\mathbb{Z}_2$.

Funkcję tę nadal oznaczamy przez f.

Definicja 7.7.12. *$\Gamma_2(n) = (-1)^n f(n)$ (to zachowa własności Γ_p).*

Poniższe stwierdzenie pochodzi z książki Koblitza.

Fakt 7.7.13. *Niech $a = 2+\Gamma_5(1/4)^2$, zaś $3b = 1-2\Gamma_7(1/3)^2$. Wtedy $a^2 = -1$ oraz $b^2 = -3$ (choć $\Gamma(1/3)$ jest przestępna!).*

Dowód. Kohomologia p-adyczna. □

7.8 Eksponens (Artina-Hassego)

Zwykła eksponensa ma promień zbieżności mniejszy niż jeden, ponieważ jej współczynnikom $a_n = 1/n!$ zbyt szybko rosną mianowniki. Zanim to naprawimy, powtórka z teorii liczb.

Lemat 7.8.1. *Niech n ma k różnych dzielników pierwszych. Wtedy $\sum_{d|n}|\mu(d)| = 2^k$ i $\sum_{d|n}\mu(d) = 0$.*

Fakt 7.8.2. *Dla dowolnej liczby pierwszej p zachodzi*

$$\sum_{n=1}^{\infty} -\frac{\mu(n)}{n}\log(1-x^n) = x$$
$$\sum_{n\geq1}^{p\nmid n} -\frac{\mu(n)}{n}\log(1-x^n) = x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \ldots$$

Dowód. Ponieważ $\sum_{m=1}^{\infty} t^m : m = -\log(1-t)$, to

$$x = \sum_{m=1}^{\infty}\frac{x^m}{m}\sum_{n|m}\mu(n) = \sum_{n=1}^{\infty}\mu(n)\sum_{m=1}^{\infty}\frac{x^{nm}}{nm}$$
$$= \sum_{n=1}^{\infty} -\frac{\mu(n)}{n}\log(1-x^n)$$

Podobnie,

$$\sum_{m=1}^{\infty}\frac{x^m}{m}\sum_{n|m}^{p\nmid n}\mu(n)=\sum_{n\geq 1}^{p\nmid n}\mu(n)\sum_{m=1}^{\infty}\frac{x^{nm}}{nm}$$
$$=\sum_{n\geq 1}^{p\nmid n}-\frac{\mu(n)}{n}\log(1-x^n).$$

Warunki $n\mid m$ i $p\nmid n$ prowadzą do $n\mid mp^{-v}$, gdzie $v=v_pm$. Pierwsza część lematu sprawia, że stosowna suma znika zawsze z wyjątkiem sytuacji, gdy $m=p^v$. □

Nałożenie eksponensa na obie strony drugiej równości jest tak ważne, że otrzymany szereg dostał własną nazwę.

Definicja 7.8.3. *Eksponens Artina-Hassego to*

$$E_p(x):=\exp\Big(\sum_{k=0}^{\infty}\frac{1}{p^k}\cdot x^{p^k}\Big).$$

Fakt 7.8.4. *Eksponens E_p leży w $1+x\mathbb{Z}_p[[x]]$, zbiega na $\mathcal{B}(0,1)$ i spełnia tam $|E_p(x)|=1$, $|E_p(x)-1|=|x|$.*

Dowód. Dowód lepiej podać później, po twierdzeniu 21. □

Fakt 7.8.5. *Promień zbieżności $\exp(x+x^p:p)$ to $r_p^\alpha=r_f<1$, $\alpha=(2p-1):p^2$, więc $r_p<r_f$ (r_p: promień zbieżności $\exp x$).*

Podamy teraz inny dowód faktu, że współczynniki szeregu potęgowego Artina-Hassego leżą w $\mathbb{Z}_p$.

To, jak bardzo podniesienie $f(x^p)$ przypomina $f(x)^p$ jest miarą całkowitości współczynników f. Dokładniej:

Twierdzenie 21 (Dieudonné, Dwork)**.** *Formalny szereg potęgowy $f(x)\in 1+x\mathbb{Q}_p[[x]]$ ma współczynniki w $\mathbb{Z}_p$, wtedy i tylko wtedy gdy spełniony jest warunek*

$$\frac{f(x)^p}{f(x^p)}\in 1+px\mathbb{Z}_p[[x]].$$

Dowód. Dowód implikacji $\Rightarrow$: jeżeli $f(x)\in 1+x\mathbb{Z}_p[[x]]$, to mamy $f(x)^p\equiv f(x^p)\bmod p$. Oba szeregi leżą w $1+x\mathbb{Z}_p[[x]]$, $f(x^p)$ jest odwracalny.

W drugą stronę: napiszmy $f(x)=\sum_{i=0}^{\infty}a_ix^i$ (gdzie a_0 to 1, $a_i\in\mathbb{Q}_p$) i załóżmy, że

$$f(x)^p=f(x^p)\big[1+p\sum_{i=1}^{\infty}b_ix^i\big]\qquad b_j\in\mathbb{Z}_p.$$

Widać, że $b_1=a_1\in\mathbb{Z}_p$. Załóżmy (dla kroku indukcyjnego), że $a_i\in\mathbb{Z}_p$ dla $i<n$ i porównajmy współczynniki przy x^n po obu stronach. Po lewej stronie stoi

$$\Big[\sum_{i\leq n}a_ix^i\Big]^p=\sum_{i\leq n}a_i^px^{ip}+p(\dots).$$

Niezapisane jednomiany to iloczyny $a_{i_1}\dots a_{i_p}x^{\sum i_k}$. Mają dwa różne indeksy i_k (przynajmniej). Wyznaczymy je mod $\mathbb{Z}_p$, a zatem wszystkie jednomiany bez a_n nie będą grały wielkiej roli: z założenia indukcyjnego mają współczynniki w $\mathbb{Z}_p$. Jedyne interesujące wielomiany z a_n mają pojedynczy czynnik a_nx^n i pozostałe $a_0=1$. Zatem po lewej stronie przy x^n stoi a_i^p (jeśli $ip=n$) $+pa_n+$ rzeczy z $p\mathbb{Z}_p$. Umówmy się, że $a_{n/p}=0$ dla $p\nmid n$. Po prawej stronie,

$$\sum_{i\leq n/p}a_ix^{pi}\cdot\Big(1+p\sum_{i\leq n}b_ix^i\Big),$$

współczynnik przy x^n to $a_{n/p}$ + gruz z $p\mathbb{Z}_p$. Ale mamy $n/p<n$, więc założenie indukcyjne daje $a_{n/p}\in\mathbb{Z}_p$, zatem $a_{n:p}^p\equiv a_{n:p}$ modulo $p\mathbb{Z}_p$, $pa_n\in p\mathbb{Z}_p$ i $a_n\in\mathbb{Z}_p$. □

Przykład 7.8.6. *Eksponens E_p spełnia równość formalnych szeregów $E_p(x)^p=\exp(px)E_p(x^p)$. Spójrz niżej.*

Fakt 7.8.7. *Mamy $e^{px}\in 1+px\mathbb{Z}_p[[x]]$, a dla nieparzystego p nawet $e^{px}\in 1+px\mathbb{Z}_p\{x\}$.*

Dowód. Mamy $v_p(n!)=(n-S_p(n)):(p-1)$, zatem dla $n\geq 1$ jest $v_p(p^n:n!)\geq n-(n-1):(p-1)\geq 1$. Dla $p=2$ można określić, kiedy mamy równość: $S_2(n)=1$, czyli $n=2^v$. Jeśli $p\geq 3$, to $v_p(p^n:n!)\geq(p-2)(p-1)\cdot n\to\infty$. □

7.9 Eksponens (Dworka)

Pierwiastkami równania $x+x^p:p=0$ są zero i pierwiastki $x^{p-1}+p=0$, „π" Problem w tym, że nie możemy dokonać tu podstawienia: $\exp(\pi+\pi^p:p)\neq\exp(0)=1!$

W klasycznym $\mathbb{C}$-przypadku pierwiastki jedności dają się określić jako specjalne wartości eksponensy. Okazuje się, że tutaj również, poniższa obserwacja pochodzi od Dworka.

Fakt 7.9.1. *Niech $\pi^{p-1}+p=0$ oraz $\zeta_\pi:=\exp(\pi+\pi^p:p)$. Wtedy ζ_π jest p-tym pierwiastkiem jedności równym $1+\pi$ mod π^2.*

Zauważmy, że zazwyczaj takie π żyje w $\mathbb{Q}_p^a$.

Definicja 7.9.2. *Szereg Dworka to $E_\pi(x):=\exp(\pi(x-x^p))$, jest elementem $\mathbb{Q}_p(\pi)[[x]]$.*

Twierdzenie 22 (Dwork)**.** *Rozszerzenie $\mathbb{Q}_p(\pi)$ jest całkowicie oraz poskromienie rozgałęzione, stopnia $p-1$, Galois: to $\mathbb{Q}_p(\mu_p)$.*

Dokładniej:

1. dokłanie jeden element $\zeta_\pi\in\mathbb{Q}_p(\pi)$ jest x pierwiastkiem jedności (p-tym), że $\zeta_\pi\equiv 1+\pi\bmod\pi^2$
2. promień zbieżności $E_\pi(x)$ to $p^\beta>1$, $\beta=1/p-1/p^2$.
3. jeśli $a\in\mathbb{Q}_p$ i $a^p=a$, to $E_\pi(a)^p=1$, $E_\pi(a)\equiv 1+a\pi$ mod π^2.

Nastał czas sum Gaußa.

Definicja 7.9.3. *Morfizm $\psi\colon\mathbb{F}_q\to\mathcal{K}^\times$ to addytywny charakter $\mathbb{F}_q$. Morfizm $\chi\colon\mathbb{F}_q^\times\to\mathcal{K}^\times$, $\chi(0)=0$ to multiplikatywny charakter $\mathbb{F}_q$, gdzie q jest potęgą p. Nazewnictwo jest tradycyjne.*

Fakt 7.9.4. *Każda rodzina homomorfizmów $\mathcal{G}\to\mathcal{K}^\times$ jest liniowo niezależna w $\mathcal{K}$-liniowej p. funkcji $\mathcal{G}\to\mathcal{K}$ (grupa, ciało).*

Fakt 7.9.5. *Jeśli $\tau\colon\mathbb{F}\to\mathcal{K}^\times$ to nietrywialny charakter (addytywny) skończonego ciała, nie ma innych charakterów niż $\psi(x)=\tau(ax)$ dla różnych $a\in\mathbb{F}$.*

Przejdźmy do tw. Grossa-Koblitza.

Wybierzmy pierwotny p-ty pierwiastek jedności $\zeta_p\in\mathbb{C}_p$, niech $\mathcal{K}=\mathbb{Q}_p(\zeta_p)$. Jak widzieliśmy, ideał $\mathfrak{p}$ jest maksymalny w $\mathcal{O}_p$. Istnieje generator (jedyny!) π dla $\mathfrak{p}$, że $\pi^{p-1}=-p$ oraz $\pi\equiv\zeta_p-1\bmod(\zeta_p-1)^2$. Odwrotnie, wybór π, pierwiastka $\pi^{p-1}=-p$ w $\mathbb{C}_p$, daje ciało $\mathcal{K}=\mathbb{Q}_p(\pi)$, czyli rozszerzenie Galois dla $\mathbb{Q}_p$, ze wszystkimi pierwiastkami jedności rzędu p. Tylko jeden z nich spełnia $\zeta_p\equiv 1+\pi\bmod\pi^2$ (szereg Dworka $E_\pi(1)=\zeta_p$).

Addytywny charakter $\mathbb{F}_p$ jest określony przez $\psi(1)\in\mu_p$. Wybierzmy $\psi(1)=\zeta_\pi$, wtedy $\psi(v)=\zeta_\pi^v$ dla $v\in\mathbb{F}_p$. Od tej chwili rozpatrywać możemy sumy Gaußa postaci

$$G(\chi,\psi)=\sum_{x\in\mathbb{F}_p}\chi(x)\zeta_\pi^x,\qquad\chi(0)=0,$$

χ jest multiplikatywnym charakterem $\mathbb{F}_p$ z wartościami w $\mathcal{K}$. Dokładniej, wartości χ to pierwiastki jedności rzędu dzielącego

$p-1$ (i 0): $G(\chi,\psi)\in\mathbb{Q}(\mu_p,\mu_{p-1})=\mathbb{Q}(\mu_{p(p-1)})$. Interesujące są sumy Gaußa postaci

$$\sum_{x\in\mathbb{F}_p^\times}\omega(x)^{-a}\psi(x)=\sum_{x\in\mathbb{F}_p}\omega(x)^{-a}\zeta_\pi^x,\qquad \omega(0)=0$$

gdzie $\omega(x)\in\mu_{p-1}$ to jedyny pierwiastek jedności w $\mathcal{K}$ mający redukcję x w ciele residuów $\mathcal{O}/\mathfrak{p}$ dla $\mathcal{K}$. Tutaj, całkowita a liczy się tylko mod $p-1$: lepiej wziąć $\alpha\in\frac{1}{p-1}\mathbb{Z}/\mathbb{Z}$ i położyć

$$G_\alpha=-\sum_{x\in\mathbb{F}_p}\omega(x)^{-(p-1)a}\zeta_\pi^x,\qquad \omega(0)=0$$

Wybieramy taki znak, by G_0 było równe 1. Warto nadmienić, że te sumy Gaußa związane są z p-adyczną funkcją Γ Mority: kiedy $\alpha=a/(p-1)$ dla $0\le a<p-1$, możemy napisać wprost: $G_\alpha=\pi^a\Gamma_p(\alpha)$ (szczególny przypadek tw. Grossa-Koblitza).

Wartości Γ_p są jednościami w $\mathbb{Z}_p$, poprzedni wzór daje więc dokładny rząd $|G_\alpha|=|\pi|^a=r_p^a=|p|^{a/(p-1)}$. Przytoczone wyżej twierdzenie pokazuje, że $\Gamma_p(a/(p-1))\in\mathbb{Q}(\pi,\mu_{p^2-p})$, a ta wartość jest algebraiczna, bo $\pi^{p-1}=-p$.

Spróbujemy uogólnić to wszystko. Niech $\alpha\in\mathbb{Z}_{(p)}$, $\mathbb{Q}\cap\mathbb{Z}_p$, będzie wymierną o mianowniku N względnie pierwszym z p. Dla wysokiej potęgi $q=p^f$ rozszerzenie $\mathbb{F}_q$ stopnia f swego prostego ciała zawiera N-ty pierwiastek jedności. Będziemy więc pracować w poskromionym rozszerzeniu rozgałęzionym $\mathcal{K}=\mathbb{Q}_p(\pi,\mu_{q-1})\subset\mathbb{C}_p$ o indeksie rozgałęzienia $e=p-1$, stopniu residuum f, zatem stopnia $n=ef$ nad $\mathbb{Q}_p$.

Dla $\alpha\in\frac{1}{N}\mathbb{Z}/\mathbb{Z}\subset\frac{1}{q-1}\mathbb{Z}/\mathbb{Z}$ wybieramy reprezentację:

$$0\le\langle\alpha\rangle=a/(q-1)<1$$

i piszemy p-adyczne rozwinięcie licznika:

$$a=a_0+a_1p+\ldots+a_{f-1}p^{f-1}<q-1<q=p^f$$

Niech $S_p(a)=a_0+a_1+\ldots+a_{f-1}$ oznacza sumę cyfr a. Niech całkowite $a^{(i)}$ za rozwinięcie mają cykliczną permutację $a=a^{(0)}$. Przykładowo $a^{(1)}=a_{f-1}+a_0p+\cdots+a_{f-2}p^{f-1}$.

Z drugiej strony, jeśli nietrywialny addytywny charakter ψ ciała prostego $\mathbb{F}_p$ jest nadal taki sam, to złożenie ψ ze śladem $\mathrm{Tr}\colon\mathbb{F}_q\to\mathbb{F}_p$, $x\mapsto x+x^p+\cdots+x^*$, (gdzie $*=p^{f-1}$) jest nietrywialnym addytywnym charakterem $\mathbb{F}_q$.

Nietrywialność śladu wynika z tego, że rozszerzenie $\mathbb{F}_q/\mathbb{F}_p$ jest rozdzielcze ($\mathbb{F}_q$ jest skończone).

Czas na niespodziankę.

Twierdzenie 23 (Gross-Koblitz, 1979)**.** *Wartość sumy Gaußa G_α dla $0\le\alpha=a/(q-1)<1$ to*

$$-\sum_{x\in\mathbb{F}_p}^{x\neq0}\omega(x)^{-a}\psi(\mathrm{Tr}(x))=\pi^{S_p(a)}\prod_{j=0}^{f-1}\Gamma_p\left(\frac{a^{(j)}}{q-1}\right).$$

7.10 Funkcja ζ Riemanna

Rozpatrzmy zbiór liczb

$$f(2k)=2\cdot\frac{\zeta(2k)}{\pi^{2k}}\cdot(1-p^{2k-1})\cdot\frac{(2k-1)!}{(-4)^k},$$

gdy $2k$ przebiega wszystkie dodatnie liczby parzyste w tej samej klasie abstrakcji modulo $p-1$. Okazuje się, że $f(2k)$ zawsze jest wymierna. Co więcej, jeśli dwie wartości $2k$ są p-adycznie bliskie, to $f(2k)$ też są bliskie sobie (zakładając, że $2k$ nie dzieli się przez $p-1$). Oznacza to, że funkcję f można jednoznacznie przedłużyć do $\mathbb{Z}_p\to\mathbb{Q}_p$.

Lemat 7.10.1. *Niech $n=2k+1>0$ będzie liczbą nieparzystą. Wtedy możemy napisać*

$$\sin(nx)=P_n(\sin x)\ \bullet\ \cos(nx)=Q_{n-1}(\sin x)\cdot\cos x,$$

gdzie wielomian P_n (Q_{n-1}) ma całkowite współczynniki oraz stopień co najwyżej n ($n-1$).

Dowód. Będziemy dowodzić indukcyjnie względem k. Lemat trywializuje się dla $k=0$ ($n=1$). Załóżmy, że zachodzi dla $k-1$. Wtedy

$$\begin{aligned}\ldots&=\sin[(2k+1)x]=\sin[(2k-1)x+2x]\\&=\sin(2k-1)x\cos2x+\cos(2k-1)x\sin2x\\&=P_{2k-1}(\sin x)(1-2\sin^2x)\\&+\cos xQ_{2k-2}(\sin x)2\sin x\cos x.\end{aligned}$$

Dowód dla kosinusa jest bardzo podobny. □

Fakt 7.10.2. *Mamy $\pi x\prod_{n\ge1}(1+x^2/n^2)=\sinh(\pi x)$, $x\in\mathbb{R}$.*

Dowód. Podręcznik rzeczywistego analityka. □

Fakt 7.10.3. *Zachodzi równość*

$$\zeta(2k)=(-1)^k\pi^{2k}\frac{2^{2k-1}}{(2k-1)!}\left(-\frac{B_{2k}}{2k}\right).$$

Dowód. Zlogarytmujmy „fakt" 7.10.2. Po prawej stronie mamy $\log\sinh(\pi x)=\log(1-\exp(-2\pi x))+\pi x-\log2$, natomiast po lewej $\log\pi+\log x-\sum_{k\ge1}(-1)^kx^{2k}\zeta(2k)/k$, dla $x\in(0,1)$.

Różniczkujemy wyraz po wyrazie względem x, mnożymy przez x i zamieniamy x na $x/2$:

$$\frac{\pi x}{e^{\pi x}-1}+\frac{\pi x}{2}=1+\sum_{k=1}^{\infty}\frac{(-1)^{k+1}\zeta(2k)}{2^{2k-1}}x^{2k}$$

Wystarczy przyrównać współczynniki parzystych potęg x. □

7.10.1 Interpolacja funkcji $s\mapsto a^s$

Zajmiemy się teraz interpolacją funkcji wykładniczej, aby móc później podać dobrą motywację dla osobliwych kroków, które inaczej mogłyby wydać się dziwaczne.

Niech $a=n$ będzie ustaloną liczbą naturalną zanurzoną w $\mathbb{Q}_p$. Dla każdej naturalnej s, n^s należy do $\mathbb{Z}_p$. Liczby naturalne tworzą gęsty zbiór w $\mathbb{Z}_p$, więc można próbować przedłużyć $f(s)=n^s$ (w oparciu o ciągłość), ale napotkamy na problemy.

Niech m będzie dużą potęgą p.

Czy n^s i n^t są sobie bliskie dla bliskich s i t, przykładowo: $t=s+m$ dla dużego m? Niekoniecznie. Jeżeli $n=p$, $s=0$, to $|n^s-n^t|_p=|1-p^{t-s}|_p=1$, niezależnie od wyboru m.

Małe twierdzenie Fermata orzeka, że $n\equiv n^p \bmod p$ dla $1<n<p$, co pociąga $n\equiv n^p\equiv\ldots\equiv n^m \bmod p$, a to z kolei implikuje $n^s-n^{s+m}=n^s(1-n^m)\equiv n^s(1-n) \bmod p$ i znowu $|n^s-n^t|_p=1$ niezależnie od m.

Na szczęście nie jest aż tak tragicznie. Wybierzmy n takie, by przystawało do 1 modulo p, na przykład $n=1+kp$. Niech $|t-s|_p\le m^{-1}$, czyli $t=s+qm$ dla $q\in\mathbb{Z}$. Załóżmy, że $t>s$. Zachodzi $|n^s-n^t|_p=|1-n^{t-s}|_p=|1-(1+kp)^{qm}|_p$. Ale rozwinięcie $(1+kp)^{qm}$ w

$$1+(qm)kp+\frac{qm(qm-1)}{2}(kp)^2+\ldots+(kp)^{qm}$$

pokazuje, że wartość bezwzględną n^s-n^t można szacować z góry przez małą wielkość $|m|/p$.

Okazuje się, że p wcale nie musi dzielić $n-1$, by $s\mapsto a^s$ była ciągłą funkcją $\mathbb{Z}_p\to\mathbb{Z}_p$. Zażądajmy mianowicie, by s i t przystawały modulo $p-1$ oraz modulo wysoka potęga p, zaś n niech nie będzie krotnością p.

Dokładniej, ustalmy $s_0\in\{0,1,\ldots,p-2\}$. Zamiast brać n^s dla naturalnych s, ograniczmy się do tych (s), które przystają do s_0 modulo $p-1$. Teraz $s=s_0+(p-1)s_1$ dla nieujemnej s_1 i badamy $n^{s_0+(p-1)s_1}$. Możemy, gdyż $n^s=n^{s_0}(n^{p-1})^{s_1}$, a przy

tym $n^{p-1} \equiv 1 \bmod p$. Wracamy do początku z n^{p-1} zamiast n, s_1 zamiast s (z dodatkowym czynnikiem n^{s_0}).

Przejdźmy do funkcji zeta Riemanna dla $s > 1$:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Naiwna interpolacja sumy przez interpolację składników nie zadziała, gdyż nawet wyrazy, które można interpolować ($p \nmid n$) tworzą rozbieżny szereg w $\mathbb{Z}_p$. Zapomnijmy jednak o tym na chwilę.

Pozbądźmy się wyrazów, którym odpowiadają n podzielne przez p.

$$\zeta(s) = \sum_{n\geq 1}^{p\nmid n} \frac{1}{n^s} + \sum_{n\geq 1}^{p|n} \frac{1}{n^s} = \sum_{n\geq 1}^{p\nmid n} \frac{1}{n^s} + \sum_{n\geq 1}^{\infty} \frac{1}{p^s n^s}$$
$$= \sum_{n\geq 1}^{p\nmid n} \frac{1}{n^s} + \frac{\zeta(s)}{p^s} = \frac{1}{1-p^{-s}} \sum_{n\geq 1}^{p\nmid n} \frac{1}{n^s}.$$

Później zajmiemy się ostatnim członem,

$$\zeta^*(s) := \sum_{n\geq 1}^{p\nmid n} \frac{1}{n^s} = \left(1-p^{-s}\right)\zeta(s).$$

Proces ten zwie się „wyjmowaniem p-czynnikiem Eulera", gdyż funkcja ζ ma słynne przedstawienie jako produkt:

$$\zeta(s) = \prod_{q\in\mathbb{P}} \frac{1}{1-q^{-s}}.$$

Na zakończenie zapowiadamy przystawanie

$$(1-p^{2k-1})(-B_{2k}/2k) \equiv (1-p^{2l-1})(-B_{2l}/2l)$$

modulo p^{N+1} i dobrych k, l, które zostało odkryte jeszcze przez Kummera, ale jego ważność dla p-adycznego odpowiednika funkcji ζ Riemanna została dostrzeżona dopiero przez Kubotę i Leopoldta w 1964.

7.10.2 Dystrybucje

Dystrybucje zdefiniowane niżej mają mało wspólnego z analizą funkcjonalną, ale ta nazwa nie jest w ostateczności taka zła. Otwarty podzbiór $\mathbb{Q}_p$ jest zwarty, wtedy i tylko wtedy gdy jest skończoną unią przedziałów. To wiele tłumaczy.

Zbiory $x + p^n\mathbb{Z}_p$ ($x \in \mathbb{Q}_p$, $n \in \mathbb{Z}$) nazwiemy *przedziałami* lub *dyskami* i oznaczymy $\langle x \rangle_n$.

Definicja 7.10.4. *Dystrybucja na zwarto-otwartym $X \subseteq \mathbb{Q}_p$ jest $\mathbb{Q}_p$-liniowym morfizmem μ z „p. lokalnie stałych $X \to \mathbb{Q}_p$" w $\mathbb{Q}_p$.*

Będziemy pisać skrótowo $\oint f\,\mu := \mu(f)$. Okazuje się, że można podać inną, równoważną definicję dystrybucji:

Definicja 7.10.5. *Addytywna funkcja z rodziny zwarto-otwartych $Y \subseteq X$ w $\mathbb{Q}_p$.*

Przejście między nimi zapewniają indykatory.

Fakt 7.10.6. *Każda funkcja μ ze zbioru „przedziałów" z X w $\mathbb{Q}_p$, dla której prawdziwa jest poniższa równość, przedłuża się jednoznacznie do dystrybucji na X: $\sum_{k=0}^{p-1} \mu(\langle x + kp^n \rangle_{n+1}) = \mu(\langle x \rangle_n)$.*

Dowód. Jeśli zwarto-otwarty zbiór $U \subseteq X$ jest unią U_s, trzeba zdefiniować $\mu(U)$ jako $\sum_s \mu(U_s)$.

Mając dwie partycje, $\bigcup_s I_s = \bigcup'_s I_s$, możemy znaleźć nową, drobniejszą: $I_s = \bigcup_t I_{st}$. Zbiory I_{st} przebiegają przez dyski $\langle y \rangle_m$ dla ustalonego $m > n$ i zmiennej $y \equiv x \bmod p^n$, gdy I_s jest postaci $\langle x \rangle_n$.

Wykorzystamy wielokrotnie wzór z założenia do pokazania, że dystrybucja nie zależy od partycji: $\mu(I_s)$, czyli $\mu(\langle x \rangle_n)$, to $\sum_k \mu(\langle x + kp^n \rangle_m)$ (suma od $k = 0$ do $p^{m-n} - 1$), jednak to jest po prostu $\sum_t \mu(I_{st})$.

Addytywność jest oczywista. □

Podamy teraz kilka przykładów dystrybucji dla $\alpha \in \mathbb{Z}_p$.

1. Haara: $\mu(\langle a \rangle_n) := |p^n|$. Przedłuża się do $\mathbb{Z}_p$ i jest jedyną niezmienniczą na przesunięcia.
2. Diraca: $\mu_\alpha(U) = 1$, wtedy i tylko wtedy gdy $\alpha \in U$.
3. Mazura: $\mu_{\text{Mazur}}(\langle a \rangle_n) = a|p^n| - 1/2$, jeśli a leży między między 0, $p^n - 1$ i jest wymierną całkowitą.

Pisząc (teraz) $\langle a \rangle_n$ zakładamy, że $0 \leq a \leq p^n - 1$.

Fakt 7.10.7. *Funkcja μ_B^i przedłuża się do dystrybucji na $\mathbb{Z}_p$, „i-tej Bernoulliego" (dla $i \in \mathbb{N}$): $\mu_B^i(\langle x \rangle_n) = p^{n(i-1)} B_i(x|p^n|)$.*

Dowód. Sprawdzimy założenia faktu 7.10.6. Tamtejsza strona lewa ma wartość $p^{(n+1)(i-1)} \sum_{k=0}^{p-1} B_i(x|p^{n+1}| + k|p|)$, więc po przemnożeniu przez $|p^{n(i-1)}|$ i położeniu $\lambda = x|p^{n+1}|$ okazuje się, że pokazujemy $B_i(\lambda p) = p^{i-1} \sum_{k=0}^{p-1} B_i(\lambda + k|p|)$.

Wyrażenie po prawej stronie to, z definicji, $i!$-krotność dla współczynnika przy z^i w

$$p^{i-1} \sum_{k=0}^{p-1} \frac{z\exp((x+k|p|)z)}{\exp z - 1} = \frac{p^{i-1} i \exp(\lambda i)}{\exp(i|p|) - 1},$$

przy czym jest to równe dokładnie

$$\frac{p^i(|p|z)\exp[(\lambda p)|p|z]}{\exp(|p|z) - 1} = p^i \sum_{k=0}^{\infty} B_k(\lambda p) \frac{(|p|z)^k}{k!}.$$

W ten sposób doszliśmy do równości kończącej dowód:

$$p^i B_i(\lambda p) p^{-i} = B_i(\lambda p).$$ □

Warto zauważyć, że w ten sposób „nie można" zdefiniować dystrybucji z innymi wielomianami – przyjmiemy to jednak bez dowodu.

7.10.3 Miary i całki

Definicja 7.10.8. *Dystrybucja p-adyczna μ na X, której wartości są ograniczone przez stałą na zwarto-otwartych $U \subseteq X$, to miara.*

Dystrybucja Diraca μ_α dla ustalonego $\alpha \in \mathbb{Z}_p$ jest miarą, ale dystrybucje Bernoulliego nie. Dzięki „regularyzacji" można to naprawić.

Dla $x \in \mathbb{Z}_p$ niech $\{x\}_n$ będzie wymierną całkowitą między 0, $p^n - 1$, która przystaje do x mod p^n.

Niech $\lambda \neq 1$ będzie wymierną całkowitą niepodzielną przez p; $\mu_{k,\lambda}$ będzie zregularyzowaną dystrybucją Bernoulliego na $\mathbb{Z}_p$: $\mu_{k,\lambda}(U) = \mu_B^k(U) - \lambda^{-k}\mu_B^k(\lambda U)$.

Fakt 7.10.9. *$|\mu_{1,\lambda}(U)|_p \leq 1$ dla zwarto-otwartych $U \subseteq \mathbb{Z}_p$.*

Dowód. Zauważmy, że $(1/\lambda - 1) \in 2\mathbb{Z}_p$, jeżeli $p \neq 2$. Kiedy $p = 2$, to $1/\lambda - 1 \equiv 0 \bmod 2$ i wszystko jest w porządku. Skoro $[\lambda x|p^n|] \in \mathbb{Z}$, to ze wzoru $2\lambda\mu_{1,\lambda}(\langle x \rangle_n) = 2[\lambda x|p^n|] + 1 - \lambda$ wynika $\mu_{1,\lambda}(\langle x \rangle_n) \in \mathbb{Z}_p$, co kończy dowód. □

Zatem $\mu_{1,\lambda}$ jest miarą i gra pierwsze skrzypce w p-adycznej teorii całki, jest niemalże tak ważna, jak $\mathrm{d}x$ w $\mathbb{R}$-analizie.

Udowodnimy teraz kluczową kongruencję wiążącą $\mu_{k,\lambda}$ z $\mu_{1,\lambda}$. Wydaje się, że dowód ten jest nieprzyjemnie obliczeniowy, ale staje się zrozumiały, kiedy pomyśli się o podobnej sytuacji w zwykłej analizie.

Jeśli walczymy z całką $\int f(x^{1:k})\,\mathrm{d}x$ i podstawimy $x \mapsto x^k$, to (skoro $d(x^k) : dx = kx^{k-1}$) $d(x^k)$ udaje miarę μ_k wzorem $\mu_k[a,b] = b^k - a^k$.

Nasza relacja przyjmuje postać

$$\lim_{b\to a} \frac{\mu_k([a,b])}{\mu_1([a,b])} = ka^{k-1}.$$

Fakt 7.10.10. *Niech d_k oznacza najmniejszy wspólny mianownik dla współczynników $B_k(x)$. Wtedy*

$$d_k\mu_{k,\lambda}(\langle a\rangle_n) \equiv d_k k a^{k-1}\mu_{1,\lambda}(\langle a\rangle_n) \mod p^n.$$

Dowód. Wiemy z ogólnej teorii, że wielomian $B_k(x)$ zaczyna się od $B_0x^k + kB_1x^{k-1} + \ldots = x^k - \frac{k}{2}x^{k-1} + \ldots$, więc teraz $d_k\mu_{k,\lambda}(\langle a\rangle_n) = d_k p^{n(k-1)}(B_k(a|p^n|) - \lambda^{-k}B_k(\{\lambda a\}_n|p^n|))$.

Wielomian $d_kB_k(x)$ ma całkowite współczynniki i stopień k. Wystarczy więc, że zajmiemy dwoma wiodącymi członami, to jest $d_kx^k - d_k\frac{k}{2}x^{k-1}$, ponieważ nasz x ma mianownik p^n (tu niższe człony zostają zjedzone przez $p^{n(k-1)}$).

Skorzystamy teraz z tego, że $\lambda a \equiv \{\lambda a\}_n \mod p^n$, a także $\{\lambda a\}_N|p^n| = \lambda a|p^n| - \lfloor \lambda a|p^n|\rfloor$ (podłoga). Niech $\beta = \lambda a$ i $I = d_k\mu_k(\langle a\rangle_n)$.

$$\begin{aligned}
I &\equiv d_k p^{n(k-1)}((a|p^n|)^k - (\{\beta\}_n|p^n|/\lambda)^k \\
&\quad - k((a|p^n|)^{k-1} - (\{\beta\}_n|p^n|)^{k-1}\lambda^{-k})/2) \\
&= d_k(a^k|p^n| - p^{n(k-1)}(\beta|p^n| - \lfloor\beta|p^n|\rfloor)^k\lambda^{-k} \\
&\quad - k(a^{k-1} - p^{n(k-1)}(\beta|p^n| - \lfloor\beta|p^n|\rfloor)^{k-1}\lambda^{-k})/2) \\
&\equiv d_k(a^k|p^n| - \lambda^{-k}(\beta^k p^n - k\beta^{k-1}\lfloor\beta|p^n|\rfloor) \\
&\quad - k(a^{k-1} - \lambda^{-k}\beta^{k-1})/2) \\
&= d_k k a^{k-1}(2\lfloor\beta|p^n|\rfloor + 1 - \lambda)(2\lambda)^{-1} \\
&= d_k k a^{k-1}\mu_{1,\lambda}(\langle a\rangle_n),
\end{aligned}$$

przy czym wszystkie przystawania są mod p^n. □

Wniosek 7.10.11. *$\mu_{k,\lambda}$ jest miarą dla $k \geq 1$ i $\lambda \in \mathbb{Z}\setminus(p\mathbb{Z}\cup\{1\})$.*

Dowód. Pokażemy ograniczoność dla $Y = \langle a\rangle_n$:

$$\begin{aligned}
|\mu_{k,\lambda}(Y)|_p &\leq \max(|p^n d_k^{-1}|_p, |ka^{k-1}\mu_{1,\lambda}(Y)|_p) \\
&\leq \max(|d_k^{-1}|_p, |\mu_{1,\lambda}(Y)|_p) \leq 1 + |d_k|_p^{-1}
\end{aligned}$$ □

Po co w ogóle zmieniać dystrybucje Bernoulliego na miary? Dla nieograniczonych dystrybucji μ, $\oint f\mu$ jest zdefiniowana tylko dla lokalnie stałych f, zaś już ciągłe f stanowią problem. „Miara" μ jest do niczego, jeśli nie można całkować względem niej ciągłych.

Problemy pojawiają się na przykład dla dystrybucji Haara i $\mathrm{id}\colon \mathbb{Z}_p \to \mathbb{Z}_p$: sumy Riemanna nie są niezależne od partycji pierścienia $\mathbb{Z}_p$.

Pokażemy, że dla ograniczonych dystrybucji nic się jednak nie psuje. X jest zwarto-otwartym podzbiorem $\mathbb{Z}_p$.

Fakt 7.10.12. *Niech μ będzie p-adyczną miarą na X, zaś f ciągłą funkcją $X \to \mathbb{Q}_p$. Wtedy sumy Riemanna zbiegają do granicy w $\mathbb{Q}_p$ gdy $n \to \infty$, niezależnie od wyboru $x_{a,n} \in \langle a\rangle_n$ (ale sumujemy tylko po tych a, że $\langle a\rangle_n \subseteq X$):*

$$S_{n,\{x_{a,n}\}} = \sum_{a=0}^{p^n-1} f(x_{a,n})\mu(\langle a\rangle_n).$$

Dowód. Niech $\mu(U) \leq B$ dla zwarto-otwartych $U \subseteq X$. Krok pierwszy polega na oszacowaniu $|S_{n,\{x(a,n)\}} - S_{m,\{x(a,m)\}}|_p$ dla $m > n$. Rozpiszmy X jako skończoną unię dysków i weźmy tak duże n, że zbiory $\langle a\rangle_n$ leżą w X lub są z nim rozłączne.

Bez straty ogólności przyjmujemy, że $|f(x) - f(y)|_p < \varepsilon$ dla $x \equiv y \mod p^n$. Wtedy (druga suma po $\langle a\rangle_m \subseteq X$):

$$\begin{aligned}
\ldots &= |S_{n,\{x(a,n)\}} - S_{m,\{x(a,m)\}}|_p \\
&= \left|\sum_{a=0}^{p^m-1}(f(x_{\overline{a},n}) - f(x_{a,m}))\mu(\langle a\rangle_m)\right|_p \\
&\leq \max(|f(x_{\overline{a},n}) - f(x_{a,m})|_p \cdot |\mu(\langle a\rangle_m)|_p) \leq \varepsilon B,
\end{aligned}$$

bo $x_{\overline{a},n} \equiv x_{a,m} \mod p^n$ (lewa strona jest bowiem z definicji najmniejszą nieujemną klasą abstrakcji). Sumy Riemanna mają jakąś granicę.

Bardzo podobnie pokazuje się to, że jest niezależna ona od wyboru ciągu $x_{a,n}$. □

Definicja 7.10.13. *Całką (Koblitza) z ciągłej funkcji $f\colon X \to \mathbb{Q}_p$ względem miary μ jest granica sum Riemanna, o ile istnieje.*

Definicja zgadza się z poprzednią dla lokalnie stałych f.

Fakt 7.10.14. *Jeśli ciągła funkcja $f\colon X \to \mathbb{Q}_p$ spełnia $|f(x)|_p \leq A$ dla $x \in X$ i $\mu(U) \leq B$ dla zwarto-otwartych $U \subseteq X$, to*

$$\left|\oint f\mu\right|_p \leq AB.$$

Wniosek 7.10.15. *Jeżeli $f, g\colon X \to \mathbb{Q}_p$ są ciągłymi funkcjami, dla których $|f(x) - g(x)|_p \leq \varepsilon$ dla wszystkich $x \in X$ i $\mu(U) \leq B$ dla zwarto-otwartych $U \subseteq X$, to*

$$\left|\oint f\mu - \oint g\mu\right|_p \leq \varepsilon B.$$

7.10.4 Transformacja Mellina-Mazura

Jeśli $X \subseteq \mathbb{Z}_p$ jest zwarty i otwarty, to można do niego obciąć miarę μ z $\mathbb{Z}_p$: wtedy całka z f nad X to całka nad $\mathbb{Z}_p$ funkcji $f\cdot\chi_X$. Chcieliśmy interpolować $-B_k/k$. Mamy prosty związek

$$\oint 1\cdot\mu_B^k = \mu_B^k(\mathbb{Z}_p) = B_k.$$

Dla różnych k dystrybucje μ_B^k nie są ze sobą związane, ale ich regularne odpowiedniki tak!

Wniosek 7.10.16. *Niech funkcja $X \subseteq \mathbb{Z}_p$ będzie zwarto-otwarty. Określmy funkcję $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ wzorem $f(x) = x^{k-1}$. Wtedy*

$$\oint_X 1\cdot\mu_{k,\lambda} = k\oint_X f\mu_{1,\lambda}$$

Dowód. Z faktu 7.10.10 wynika, że dla $m = n - v_p(d_k)$ mamy kongruencję $\mu_{k,\alpha}(\langle a\rangle_n) \equiv ka^{k-1}\mu_{1,\alpha}(\langle a\rangle_n) \mod p^m$. Biorąc n tak duże, by X było unią dysków postaci $\langle a\rangle_n$, mamy

$$\begin{aligned}
\oint_X 1\mu_{k,\lambda} &= \sum_{a=0}^{p^n-1}\mu_{k,\lambda}(\langle a\rangle_n) \equiv \sum_{a=0}^{p^n-1} ka^{k-1}\mu_{1,\lambda}(\langle a\rangle_n) \\
&= k\sum_{a=0}^{p^n-1} f(a)\mu_{1,\lambda}(\langle a\rangle_n).
\end{aligned}$$

Idziemy z n do nieskończoności. □

Prawa strona wygląda dużo lepiej, ponieważ k nie pojawia się magicznie w indeksie μ, ale wykładniku (f). Wiemy już, jak wygląda interpolacja x^{k-1} dla ustalonego x: wystarczy nam, by $x \not\equiv 0 \mod p$. Aby wszystkie argumenty miały tę własność, weźmy $X = \mathbb{Z}_p^\times$.

Twierdzimy, że całkę z x^{k-1} nad $\mathbb{Z}_p^\times$ względem $\mu_{1,\lambda}$ można interpolować. Połączymy teraz odkrycia ustępu o przedłużaniu

$s \mapsto a^s$ z wnioskami poprzedniej podsekcji. Wnioski te mówią nam, że jeśli $|f(x) - x^{k-1}|_p \le \varepsilon$ dla $x \in \mathbb{Z}_p^\times$, to

$$\left| \oint_{\mathbb{Z}_p^\times} f\mu_{1,\lambda} - \oint_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\lambda} \right|_p \le \varepsilon.$$

Wybierzmy za f funkcję x^{l-1}, gdzie $l \equiv k \bmod p-1$ oraz p^n. Zachodzi: $|x^{l-1} - x^{k-1}|_p \le p^{-n-1}$, a to implikuje

$$\left| \oint_{\mathbb{Z}_p^\times} x^{l-1}\mu_{1,\lambda} - \oint_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\lambda} \right|_p \le p^{-n-1}$$

Dochodzimy do wniosku, że dla ustalonego $0 \le s_0 \le p-2$ i k biegnącego przez $S(s_0) := [s_0 + (p-1)\mathbb{Z}] \cap \mathbb{N}_+$ możemy przedłużyć naszą funkcję do p-adycznych całkowitych:

$$\oint_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\lambda} \text{ do } \oint_{\mathbb{Z}_p^\times} x^{s_0+s(p-1)-1}\mu_{1,\lambda}$$

Trochę zabłądziliśmy! Interpolowaliśmy

$$\oint_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\lambda} = \frac{1}{k}\oint_{\mathbb{Z}_p^\times} 1\mu_{k,\lambda}.$$

Związemy teraz te dwie liczby.

$$\begin{aligned}\frac{1}{k}\oint_{\mathbb{Z}_p^\times} 1\mu_{k,\lambda} &= \frac{\mu_{k,\lambda}(\mathbb{Z}_p^\times)}{k} = \frac{B_k}{k}(1-\lambda^{-k})(1-p^{k-1}) \\ &= (\lambda^{-k}-1)(1-p^{k-1}) \cdot \oint_{\mathbb{Z}_p} \frac{-1}{k}\mu_B^k.\end{aligned}$$

Wyraz $1-p^{k-1}$ pojawił się, ponieważ obcięliśmy całkę z $\mathbb{Z}_p$ do $\mathbb{Z}_p^\times$. Ten fenomen został przewidziany wcześniej: nie można przedłużyć n^s, gdy $p \mid n$ – konieczne jest pozbycie się p-czynnika Eulera. Zajmiemy się więc

$$(1-p^{k-1})(-B_k/k) = \frac{1}{\lambda^{-k}-1}\oint_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\lambda}$$

Wystąpienie $k-1$ zamiast $-k$ zaskakuje tylko początkowo, za sprawą funkcyjnego równania wiążącego coś z czymś innym.

Definicja 7.10.17. *Jeżeli k jest dodatnia i całkowita, to*

$$\zeta_p(1-k) := (1-p^{k-1}) \cdot \frac{-B_k}{k}.$$

Powinno się w tym miejscu wyprowadzić klasyczne fakty teorii liczb o liczbach Bernoulliego. Uznawano je za eleganckie, ale i tajemnicze niezwykłości, zanim związano je z ζ_p Kuboty i Leopoldta oraz miarą Mazura $\mu_{1,\alpha}$. Clausen z van Staudtem też maczali w tym palce.

Fakt 7.10.18. $k\zeta(1-k) + B_k = 0$.

Dowód. Skorzystamy z definicji $\zeta(1-k) = \sum n^{k-1}$. Niech $\mathfrak{D}$ oznacza (lokalnie) $(\mathrm{d}/\mathrm{d}t)^{k-1} \ldots|_{t=0}$.

$$\begin{aligned}\zeta(1-k) &= \sum_{n\ge1} n^{k-1} = \sum_{n\ge1} \mathfrak{D}\exp nt = \mathfrak{D}\sum_{n\ge1}\exp nt \\ &= \mathfrak{D}\left[\frac{1}{1-\exp t} - 1\right] = -\mathfrak{D}\frac{1}{t}\sum_{n=1}^{\infty} B_n\frac{t_n}{n!} \\ &= \mathfrak{D}\sum_{n=0}^{\infty} -\frac{B_n}{n}\frac{t^{n-1}}{(n-1)!} = -\frac{B_k}{k}.\end{aligned}$$

□

Głębsze przemyślenia sprawiają, że dla $s \in \mathbb{Z}_p$ i ustalonego $s_0 \in \{0,1,\ldots,p-2\}$ ($s \ne 0$, gdy $s_0 = 0$) określamy:

$$\zeta_{p,s_0}(s) := \frac{\oint_{\mathbb{Z}_p^\times} x^{s_0+(p-1)s-1}\mu_{1,\lambda}}{\lambda^{-(s_0+(p-1)s)}-1}.$$

Jeżeli k jest postaci $s_0+(p-1)k_0$, to $\zeta_p(1-k)$ i $\zeta_{p,s_0}(k_0)$ są tym samym, więc myślimy o ζ_{p,s_0} jak o p-adycznych „gałęziach" dla ζ_p (interesują nas parzyste s_0!). Uwaga: prawa strona nie zależy (!) od λ.

Pominęliśmy przypadek $s = s_0 = 0$, bo wtedy mianownik znika, co odpowiada $\zeta_p(1)$. Tak więc p-adyczna funkcja ζ też ma „biegun" w 1.

Fakt 7.10.19. *Dla ustalonych p i s_0 funkcja $\zeta_{p,s_0}(s)$ jest ciągła.*

Pozostaje wytłumaczyć, skąd wzięła się nazwa podsekcji. Otóż transformatą Mellina funkcji f jest

$$(\mathcal{M}f)(s) = \int_0^\infty x^{s-1}f(x)\,\mathrm{d}x.$$

W $\mathbb{R}$-analizie transformatą $(\exp x - 1)^{-1}$ jest $\Gamma(s)\zeta(s)$, zaś ζ_p możemy traktować jako transformatę Mellina-Mazura dla zregularyzowanej miary $\mu_{1,\lambda}$.

Fakt 7.10.20. *Funkcje $\exp x$, $\cos x$, $\frac{1}{x}\sin x$, $\frac{1}{x}\log 1+x$ są tam, gdzie $\exp x$ jest określona, kwadratami funkcji p-adycznych.*

7.11 Stałe matemagiczne

Fakt 7.11.1. *W żadnym z ciał $\mathbb{Q}_p$ nie ma stałej Nepera.*

Dowód. Szereg dla $\exp_p(1)$ jest rozbieżny w $\mathbb{Q}_p$, zaś znalezienie pierwiastka dla $\exp_2(4)$ lub $\exp_p(p)$ ($p \ge 3$) wymaga wyboru (niestety, niekanonicznego). □

Fakt 7.11.2. *Kosinus nie ma zera, sinus ma tylko jedno (0), w dodatku nie istnieje takie $t \in \mathcal{K}$, że $\sin(x) = \cos(x+t)$.*

Nie określimy więc tak odpowiednika $\pi \approx 3,1415926535$. Warto zwrócić uwagę na punkt piąty faktu 7.7.4 dla $x = 1/2$.

Fakt 7.11.3. *Zwykła funkcja Γ spełnia $\Gamma(z)\Gamma(1-z) = \pi : \sin \pi z$, a stąd $\Gamma(1/2) = \sqrt{\pi}$.*

Zatem odpowiednikiem π w $\mathbb{Q}_p$ powinna być $\Gamma_p(1/2)^2$, -1 (w $\mathbb{Q}_{4k+1}$) lub 1 (w $\mathbb{Q}_{4k+3}$).

Różniczkując $\Gamma_p(x+1) = \Gamma_p(x)h_p(x)$ dostaniemy

$$\frac{\Gamma_p'(x+1)}{\Gamma_p(x+1)} - \frac{\Gamma_p'(x)}{\Gamma_p(x)} = \frac{h_p'(x)}{h_p(x)}.$$

Istnieje stała c, że dla każdego $x \in \mathbb{Z}_p$ jest

$$\frac{\Gamma_p'(x)}{\Gamma_p(x)} = c + L_p(x),$$

gdzie $L_p(x)$ to nieoznaczona suma poprzedniej prawej strony. Po wstawieniu do wzoru $x = 1$ mamy (dla $m \in \mathbb{N}$):

$$\frac{\Gamma_p'(m)}{\Gamma_p(m)} = \frac{\Gamma_p'(1)}{\Gamma_p(1)} + \sum_{j<m}{}' \frac{1}{j}.$$

To przypomina wzór, który jest prawdziwy też dla zwykłej funkcji Γ i zachęca do zdefiniowania nowej stałej.

Definicja 7.11.4. *Stała (p-adyczna) Eulera to $\gamma_p := -\Gamma_p'(0)$.*

Schikhof nie wie nic na temat jej (nie)wymierności.

Fakt 7.11.5. $|\gamma_p|_p \le 1$, *a w* $\mathbb{Q}_p$

$$\gamma_p = \lim_{n\to\infty} \frac{1}{p^n}\left[1 - \frac{(-1)^p p^n!}{p^{n-1}!p^{p^n-1}}\right].$$

Rozdział 8
Analiza funkcjonalna

Ktoś kiedyś powiedział, że teoria przestrzeni unormowanych nad ciałami innymi niż $\mathbb{R}$ (p. Banacha) czy $\mathbb{C}$ (algebry Banacha, operatory) jest ekscentryczna. Wprawdzie istnieje, ale nigdy nawet nie otarła się o główny nurt matematyki. Nie szkodzi.

Sferyczna zupełność (zdefiniowana na końcu rozdziału 6.) służy zaspokojeniu potrzeb analizy funkcjonalnej i nie jest poza nią przesadnie ważnym pojęciem.

Fakt 8.0.1. *Niech X będzie przestrzenią ultrametryczną. Połóżmy $\rho(x,y) = \exp[\log d(x,y)]$ dla $x \neq y$, $\rho(x,x) = 0$. Funkcja ρ jest dyskretną metryką na X, która spełnia nierówności $\rho \leq d \leq e\rho$.*

Wniosek 8.0.2. *Sferyczna zupełność zależy od metryki, a nie samej topologii.*

Definicja 8.0.3. *Niech $Y \subseteq X$. Punkt $b \in Y$ jest najlepszą aproksymacją $a \in X$ w Y, gdy $d(a,b) = d(a,Y)$.*

Fakt 8.0.4. *Jeśli $Y \subseteq X$ nie jest pusty i jest sferycznie zupełny, to każdy punkt $a \in X$ ma najlepszą aproksymację w Y.*

Dowód. Niech $\mathcal{B}_n = \{y \in Y : d(y,a) \leq d(a,Y) + 1/n\}$ dla $n \in \mathbb{N}$. Zbiory $\mathcal{B}_n$ tworzą malejący ciąg niepustych kul w Y, za najlepszą aproksymację służą elementy przekroju $\bigcap_n \mathcal{B}_n$. □

Jeśli Y nie jest sferycznie zupełna, można wskazać taką przestrzeń $Y \cup \{a\}$, że a nie ma najlepszej aproksymacji w Y. Punkty przestrzeni Hilberta mają dokładnie jedną najlepszą aproksymację w domkniętym i wypukłym zbiorze, ale (prawie zawsze) nie tutaj. Niestety, piękne twierdzenia się psują.

Fakt 8.0.5. *Jeżeli $Y \subseteq X$ nie jest pusty i brak mu izolatorów, zaś $a \in X \setminus Y$ ma najlepszą aproksymację $b \in Y$, to ma ich ∞ wiele (też w Y).*

Dowód. Każdy punkt $\mathcal{B}[b, d(a,Y)] \cap Y$ dobrze przybliża. □

Nie ma też średniej Banacha dla ograniczonych ciągów w przestrzeni ultrametrycznej:

Fakt 8.0.6. *Nie można określić odwzorowania $\lim\colon \ell^\infty \to \mathcal{K}$, które byłoby $\mathcal{K}$-liniowe, pokrywałoby się z granicą ciągu (jeśli ta istnieje) i $\lim(\xi_1, \xi_2, \ldots) = \lim(0, \xi_1, \xi_2, \ldots)$.*

Dowód. Wskazówka: ciąg $a_n = n$ jest ograniczony. □

8.1 Grupa Pontriagina

Niech $\mathcal{K}$ będzie skończonym rozszerzeniem $\mathbb{Q}_p$, co implikuje jego lokalną zwartość.

Definicja 8.1.1. *Charakter to ciągły morfizm $\mathcal{K} \to \mathbb{C}^\times$, którego wartości leżą na okręgu jednostkowym.*

Fakt 8.1.2. *Wartości charakteru leżą w μ_{p^∞}, jest on lokalnie stały.*

Ustalmy nietrywialny charakter ψ. Funkcja $\psi_a(x) = \psi(ax)$ również jest charakterem dla dowolnego $a \in \mathcal{K}$.

Fakt 8.1.3. *Morfizm $f\colon \mathcal{K} \to \mathcal{K}^\#$, $a \mapsto \psi_a$, jest różnowartościowy.*

Przykładem nietrywialnego elementu z multiplikatywnej grupy $\mathcal{K}^\#$ (wszystkich charakterów) jest złożenie śladu $\mathcal{K}$ nad $\mathbb{Q}_p$ z morfizmem Tate'a τ. Na $\mathcal{K}^\#$ zadaje się topologię od układu otoczeń:

Definicja 8.1.4. *Otoczeniem charakteru χ dla $\varepsilon > 0$ i zwartego $A \subseteq \mathcal{K}$ jest $V_{\varepsilon,A} = \{\chi' \in \mathcal{K}^\# : |\chi'(x) - \chi(x)| \leq \varepsilon\}$.*

Fakt 8.1.5. *Zarówno morfizm f, jak i morfizm do niego odwrotny, są ciągłe. Zatem obraz $f(\mathcal{K})$ jest lokalnie zwarty i domknięty w $\mathcal{K}^\#$.*

Przedstawiony wyżej obiekt istnieje dla każdej lokalnie zwartej grupy abelowej $\mathcal{G}$:

Definicja 8.1.6. *Dual Pontriagina to $\mathcal{G}^\#$, zbiór ciągłych morfizmów $\mathcal{G} \to \{z \in \mathbb{C} : |z| = 1\}$.*

Fakt 8.1.7. *Grupy $(\mathcal{G}^\#)^\#$ oraz $\mathcal{G}$ są kanonicznie izomorficzne: ma to sens, gdyż każdy dual Pontriagina jest lokalnie zwartą grupą abelową.*

Fakt 8.1.8. *Addytywna grupa lokalnie zwartego ciała $\mathcal{K} = \mathcal{G}$ jest izomorficzna ze swoim dualem (co stanowi uogólnienie przypadku $\mathbb{R}$).*

Fakt 8.1.9. *Dual ośrodkowej grupy jest metryzowalny.*

Fakt 8.1.10. *Dla lokalnie zwartych grup abelowych $\mathcal{G}$, dyskretność (zwartość) jest równoważna zwartości (dyskretności) dualu $G^\#$.*

Historia 7. *Lew Pontriagin.*

Mając do dyspozycji dual Pontriagina, możemy już podać abstrakcyjny wariant transformaty Fouriera.

Definicja 8.1.11. *Jeśli f leży w $L^1(\mathcal{G})$, to jej transformata jest ciągła, ograniczona i znika w nieskończoności: $\int_\mathcal{G} f(x)\overline{\chi(x)}\, d\mu(x)$.*

Każdej mierze Haara μ na $\mathcal{G}$ odpowiada dokładnie jedna miara Haara ν na $\mathcal{G}^\#$, że gdy $g \in L^1(\mathcal{G})$, $\widehat{g} \in L^1(\mathcal{G}^\#)$, to

$$g(x) = \int_{\mathcal{G}^\#} \widehat{g}(\chi)\chi(x)\, \mathrm{d}\nu(\chi),$$

przy czym równość zachodzi μ-prawie wszędzie (a jeśli g jest ciągła, to dosłownie wszędzie). Prowadzi to do transformaty odwrotnej.

Definicja 8.1.12. *Odwrotna transformata całkowalnej funkcji f na $\mathcal{G}^\#$ zadana jest wzorem $\int_{\mathcal{G}^\#} f(\chi)\chi(x)\, d\nu(\chi)$.*

Fakt 8.1.13. *Przestrzeń Banacha $L^1(\mathcal{G})$ jest łączną oraz przemienną algebrą ze splotem $(f * g)(x) = \int_\mathcal{G} f(x-y)g(y)\, d\mu(y)$.*

Fakt 8.1.14. *Transformata splotu $f * g$ jest produktem transformat funkcji f oraz g.*

Twierdzenie 24 (Plancherel)**.** *Transformata zwarcie niesionej oraz ciągłej funkcji $f\colon \mathcal{G} \to \mathbb{C}$ leży w $L^2(\mathcal{G}^\#)$ oraz*

$$\int_G |f(x)|^2\, d\mu(x) = \int_{\widehat{G}} \left|\widehat{f}(\chi)\right|^2\, d\nu(\chi).$$

Ostrzeżenie: jeżeli lokalnie zwarta grupa $\mathcal{G}$ nie jest zwarta, to przestrzeń $L^1(\mathcal{G})$ nie zawiera w sobie $L^2(\mathcal{G})$, sic.

8.2 Inne?

Cały czas przez $\mathcal{K}$ będziemy oznaczać zupełne rozszerzenie ultrametryczne dla $\mathbb{Q}_p$. Rozumiemy już p. wektorowe nad $\mathcal{K}$ skończonego wymiaru. Nadszedł wreszcie czas na przypadek $\dim_\mathcal{K} = \infty$. Od teraz prawie wszystko jest ultrametryczne nawet, kiedy nie jest to zaznaczone.

8.3 Sumy proste

Definicja 8.3.1. *Suma prosta rodziny p. unormowanych E_i to suma (algebraiczna) z normą supremum: $\|x\| = \sup_i \|x_i\|$.*

$$\bigoplus_{i\in I} E_i = \{(x_i) : \textit{skończenie wiele } x_i \neq 0\} \subseteq \prod_{i\in I} E_i$$

Kiedy wszystkie E_i są przestrzeniami Banacha, rozpatruje się zwyczajowo uzupełnienie tejże sumy prostej.

Oto konstrukcja. Nośnikiem $x = (x_i) \in \prod_i E_i$ jest zbiór $I_x = \{i \in I : x_i \neq 0\}$. Przez $\|x_i\| \to 0$ rozumiemy zaś, że dla każdego $\varepsilon > 0$ i skończenie wielu i, $\|x_i\| > \varepsilon$. W takiej sytuacji sam nośnik jest co najwyżej przeliczalny jako unia $I_x(1/n)$.

Fakt 8.3.2. *Uzupełnieniem sumy prostej p. Banacha jest dokładnie*

$$\widehat{\bigoplus}_{i\in I} E_i = \{x : \|x_i\| \to 0\}.$$

Dowód. Dowód jest naprawdę porywający, jak na funkcjonalną analizę przystało. Zbiór x, że $\|x_i\| \to 0$, jest podprzestrzenią wektorową w $\prod_i E_i$, zaś suma prosta leży w nim gęsto. Teraz pokażemy zupełność sumy prostej Banacha, gdyż tak nazywa się zbiór z faktu.

Niech $n \mapsto (x_i^n)_i$ będzie ciągiem Cauchy'ego. Dla każdego i, $n \mapsto x_i^n$ ma granicę x_i w E_i. Dla ustalonej $\varepsilon > 0$ istnieje N_ε, że $m, n \geq N_\varepsilon$ pociąga $\|x^n - x^{(m)}\| \leq \varepsilon$. Nierówność po prawej stronie nie staje się zakłamana po tym, jak dopiszemy indeksy x_i, po przejściu z m do granicy w ∞ uzyskujemy z kolei $n \geq N_\varepsilon$ pociąga $\|x_i^n - x_i\| \leq \varepsilon$. Ale $\|x_i^n\| \leq \varepsilon$ poza zbiorem skończonym, więc $\|x_i\| \leq \max(\|x_i^n\|, \|x_i^n - x_i\|) \leq \varepsilon$. Tak uzasadniamy, że x gdzieś leży. Zauważmy, że $x^n \to x$, gdyż $\|x^n - x\| = \sup_i \|x_i^n - x_i\| \leq \varepsilon$. □

Jeżeli wszystkie przestrzenie Banacha $E_i = E$ są sobie równe, to algebraiczną sumę prostą oznaczamy też przez $E^{(I)}$. Jej uzupełnienie oznacza się przez $c_0(I; E)$, udaje się w ten sposób notację Stefana Banacha dla $\mathcal{K} = \mathbb{C}$.

Nic nie ryzykujemy, jeżeli przyjmiemy: $c_0(I) = c_0(I; \mathcal{K})$, $c_0(E) = c_0(\mathbb{N}, E)$, $c_0 = c_0(\mathbb{N}) = c_0(\mathbb{N}, \mathcal{K})$.

Wniosek 8.3.3. *Funkcja-suma $E^{(I)} \to E$ ma jednoznaczne ciągłe przedłużenie $\Sigma\colon c_0(I; E) \to E$, gdzie E jest p. Banacha.*

Abstrakcyjny bełkot tłumaczy uniwesalność sum prostych.

8.4 Bazy normalne

Kiedy E, F są przestrzeniami nad $\mathcal{K}$ z normą, przez $L(E, F)$ rozumiemy przestrzeń ciągłych liniowych funkcji $E \to F$. Ale liniowa funkcja jest ciągła dokładnie wtedy, gdy jest ciągła w zerze, lub, równoważnie, jest ograniczona:

$$\|T\| := \sup_{x\neq 0} \frac{\|Tx\|}{\|x\|} < \infty$$

Z definicji tej wynika, że $\|Tx\| \leq \|T\| \cdot \|x\|$, a zatem T jest kontrakcją dokładnie dla $\|T\| \leq 1$. Nierówność ta pokazuje też, że $\|Tx\| \leq \|T\|$ dla $\|x\| \leq 1$, zatem $\sup_{\|x\|\leq 1} \|Tx\| \leq \|T\|$. Wbrew temu, co dzieje się w klasycznej analizie funkcjonalnej, nierówność może być ostra. Jeśli $1 \notin \|E\|$, to jednostkowa sfera jest pusta, a otwarte kule jednostkowe są domknięte. Niechaj $T(x) = x$. Wtedy $\sup_{\|x\|\leq 1} \|x\| < 1 = \|T\|$.

Fakt 8.4.1. *Jeżeli F jest zupełna, to $L(E, F)$ też.*

Wniosek 8.4.2. *Jeżeli E jest unormowana, to jej dual $L(E, \mathcal{K})$, E', jest przestrzenią Banacha.*

Niech I będzie jakimś zbiorem indeksów, zaś E p. Banacha. Przestrzeń ograniczonych ciągów $(a_i)_{i\in I}$ w E razem z normą $\sup_i \|a_i\|$ jest przestrzenią Banacha, oznaczaną $l^\infty(I; E)$.

Fakt 8.4.3. *Topologiczny dual do $c_0(I, E)$ oraz $l^\infty(I, E')$ są (jako p. unormowane) kanonicznie izomorficzne.*

Dowód. Jeśli φ jest funkcjonałem na $c_0(I; E)$, przez $\varphi_i = \varphi \circ \varepsilon_i$ oznaczymy obcięcie do i-tego czynnika E w $c_0(I; E)$. Skoro $\|\varphi_i\| \leq \|\varphi\|$, mamy ograniczoną rodzinę $(\varphi_i) \in l^\infty(I; E')$.

Odwrotnie, jeśli $(\varphi_i) \in l^\infty(I; E')$, definiujemy funkcjonał wzorem $\varphi(x) = \sum_i \varphi_i(x)$ na $c_0(I; E)$ przez $(a_i) \mapsto \sum_i \varphi_i(a_i)$ (szereg jest sumowalny, gdyż ciąg φ_i jest ograniczony, zaś $\|a_i\|$ dąży do zera).

Obie funkcje, $\varphi \mapsto (\varphi \circ \varepsilon_i)$ oraz $(\varphi) \mapsto \sum_i \varphi$, są liniowe i zmniejszają normę: to wzajemnie odwrotne izometrie. □

Innymi słowy, dwuliniowa $c_0(I; E) \times l^\infty(I, E') \to \mathcal{K}$

$$((a_i), (\varphi_i)) \mapsto \sum_i \varphi_i(a_i)$$

jest dualnym parowaniem, które dowodzi faktu.

Wniosek 8.4.4. *Przestrzeń $l^\infty(I) = l^\infty(I, \mathcal{K})$ jest Banacha.*

W przestrzeni c_0 elementy $e_i = (\delta_{ij})$ (kroneckerowskie symbole) mają następującą własność. Każdy ciąg $(a_n) \in c_0$ jest sumą dokładnie jednego zbieżnego szeregu $a = \sum_{n\geq 0} a_n e_n$. Wtedy $\|a\| = \sup_{n\geq 0} |a_n| = \max_{n\geq 0} |a_n|$. Rodzina $\{e_i\}_{i=0}^\infty$ jest kanoniczną bazą (chociaż nie jest bazą, bo algebra liniowa dopuszcza tylko skończone kombinacje liniowe!).

To motywuje następującą definicję.

Definicja 8.4.5. *Rodzina $(e_i)_{i\in I}$ elementów p. Banacha E to baza normalna, jeśli każdy $x \in E$ można zapisać jako $\sum_I x_i e_i$, gdzie $|x_i| \to 0$, zaś $\|x\| = \sup_{i\in I} |x_i|$ (szereg ma zbiegać).*

Fakt 8.4.6. *Jeśli E to ultrametryczna p. Banacha z normalna bazą $(e_i)_{i\in I}$, to $(x_i) \mapsto \sum_{i\in I} x_i e_i$ zadaje liniową bijekcję z $c_0(I; \mathcal{K})$ do E, a nawet izometrię. Liniowa izometria bijektywna zadaje bazę normalną (obraz bazy kanonicznej w $c_0(I; \mathcal{K})$).*

Przykład 8.4.7. *Każda p. Banacha $c_0(I)$ ma bazę (orto)normalną.*

Przykład 8.4.8. *W szczególności: $c_0(\{1, \ldots, n\}) \cong \mathcal{K}^n$.*

Przykład 8.4.9. *Przestrzeń $C(\mathbb{Z}_p, \mathcal{K})$ z dwumianami Newtona (tw. Mahlera) albo ψ_i (van der Puta).*

8.5 Klasyczne twierdzenia

Istnieje odpowiednik faktu 5.1.5 dla przestrzeni Banacha, ale nie będziemy się tym czymś dla świętego spokoju zajmować. Zamiast tego skaczemy do nieznanego nikomu twierdzenia.

Twierdzenie 25 (Monna, Fleischer)**.** *Każda ultrap. Banacha E nad zupełnym ciałem $\mathcal{K}$, że $|\mathcal{K}^\times|$ jest dyskretne w $\mathbb{R}_{>0}$, ma normalną bazę dokładnie wtedy, gdy $\|E\| = |\mathcal{K}|$.*

Efektem ubocznym badania przestrzeni funkcji liniowych jest natomiast coś innego.

Wniosek 8.5.1. *Istnieje kanoniczny izomorfizm $(c_0(J))' \cong l^\infty(J)$.*

Na koniec czeka na nas wisienka na torcie z 1952 roku.

Twierdzenie 26 (Ingleton)**.** *Jeżeli $V \leq E$ jest podprzestrzenią p. unormowanej nad ciałem $\mathcal{K}$ (sferycznie zupełnym), operator obcięcia do V ($\psi \mapsto \psi\mid_V$, $E' \to V'$) jest surjekcją, a funkcjonały z V' można przedłużać do E' bez zmiany normy („tw. Hahna-Banacha").*

Rozdział 9
Równania różniczkowe

9.1 Liczby Liouville'a

Fakt 9.1.1. *Jeśli operator A z przestrzeni ciągłych funkcji $\mathbb{Z}_p \to \mathcal{K}$ w siebie spełnia warunek Lipschitza, to istnieje $\|\cdot\|$-izometria p. funkcji $\mathbb{Z}_p \to \mathcal{K}$ o zerowej pochodnej na zbiór rozwiązań $f' = Af$.*

Definicja 9.1.2. *Dla $\lambda \in \mathbb{Z}_p$, $\nu(\lambda) = \liminf_n |n-\lambda|_p^{1:n}$.*

Definicja 9.1.3. *Mówimy, że λ jest liczbą Liouville'a, gdy $\nu(\lambda) = 0$.*

Van der Put postawił w 1980 problem, który rozwiążemy (z „Meromorphic differential equations over valued fields", Indag. Math. 42, Fasc. 3).

Fakt 9.1.4. *Niech funkcja $g\colon \mathbb{Z}_p \to \mathcal{K}$ będzie ciągła, a w zerze też różniczkowalna, $\lambda \in \mathbb{Z}_p$. Niech $\lambda \in \mathbb{Z}_p$. Jeśli $\lambda = 0$, $g(0) = 0$. Jeśli $\lambda = 1$, $g'(0) = 0$. Istnieje $\mathcal{C}^1$-rozwiązanie (?) dla $xy' - \lambda y = g$.*

Uwaga. Zbiór rozwiązań stanowi warstwę w przestrzeni $\mathcal{C}^1$ podgrupy $\{f\colon \mathbb{Z}_p \to \mathcal{K} : xf'(x) - \lambda f(x) = 0\}$, której wymiar jest nieskończony.

Dowód. Niech $g(0) = g'(0) = 0$, przez P oznaczmy obcięcie antyderywatu do p. ciągłych $\mathbb{Z}_p \to \mathcal{K}$, które zerują się w zerze, C_0. Wskażemy takie u, że $y = Pu$ będzie rozwiązaniem.

Łatwo sprawdzić, że $Qu(x) := (\lambda Pu(x) + g(x))/x$ (dla $x \neq 0$) i $Qu(0) := 0$ określa funkcję z C_0 w C_0. Oszacowanie $|Pu(x)| \leq |x|_p \cdot \|u\|/p$ daje $\|Qu - Qv\| \leq \|u-v\|/p$. Funkcja Q jest kontrakcją, więc ma punkt stały u.

W ogólnym przypadku stosujemy pierwszą część do funkcji $g(x) - g'(0)x - g(0)$ i dostajemy funkcję f_1, potrzebną do

$$y(x) := f_1(x) + \begin{cases} g'(0)x & \lambda = 0 \\ -g(0) & \lambda = 1 \\ \frac{g'(0)x}{1-\lambda} - \frac{g(0)}{\lambda} & \lambda \neq 0,1 \end{cases},$$

rozwiązania ogólnego równania. □

Pytanie, czy równanie $xy' - \lambda y = g$ ma $\mathcal{C}^\infty$-rozwiązania dla każdej $\mathcal{C}^\infty$-funkcji g z $g(0)$ i $g'(0) = 0$, chyba wciąż pozostaje otwarte.

Definicja 9.1.5. *Luka w $x = \sum_{j \geq 0} a_j p^j$ długości $[tp^{-s}]$ to para liczb $s < t$, taka że $a_s \neq 0$, $a_t \neq 0$, ale $a_k = 0$ dla $s < k < t$.*

Fakt 9.1.6. *Liczba $\lambda \in \mathbb{Z}_p$ jest Liouville'a, wtedy i tylko wtedy gdy w jej rozwinięciu są dowolnie duże luki.*

Fakt 9.1.7. *Liczby Liouville'a są przestępne („nad $\mathbb{Q}$").*

Dowód. Niech liczba $a \in \mathbb{Z}_p$ będzie algebraiczna nad ciałem $\mathbb{Q}$ z wielomianem minimalnym $f(x) = a_0 + \ldots + a_d x^d$, $a_d \neq 0$. Skoro funkcja f spełnia warunek Lipschitza ze stałą c, to dla $n \in \mathbb{N}$ jest $|f(n)|_p \leq c|n-a|_p$. Dla dużych n, $f(n) \neq 0$, gdyż f ma co najwyżej d zer, a jednocześnie $|f(n)|_p \geq 1/|f(n)|_\infty$. Skoro tak, $1/|f(n)|_p \leq (|a_0|_\infty + \ldots + |a_d|_\infty)n^d$. Istnieje pewna stała $c' > 0$, że $|n-a|_p \geq c'/n^d$, skąd $\nu(a) = 1$. □

Fakt 9.1.8. *Liczby Liouville'a tworzą gęsty G_δ podzbiór $\mathbb{Z}_p$.*

Warto tu wspomnieć o twierdzeniu Baire'a: niepusta oraz zupełna przestrzeń metryczna nie jest przeliczalną unią nigdzie gęstych i domkniętych zbiorów.

Dowód. Niech $n \in \mathbb{N}$. Dobry wybór $n_1 < n_2 < \ldots$ sprawia, że liczba $n + p^{n_1} + p^{n_2} + \ldots$ jest blisko n i ma dowolnie długie luki. Domknięcie zbioru liczb Liouville'a zawiera $\mathbb{N}$, zatem całe $\mathbb{Z}_p$. Niech $U_{mk} = \{x \in \mathbb{Z}_p : |m-x|_p < k^{-m}\}$. Liczby Liouville'a to dokładnie $\bigcap_{k\in\mathbb{N}} \bigcap_{n\in\mathbb{N}} \bigcup_{m\geq n} U_{mk}$. □

Fakt 9.1.9. *Liczby Liouville'a tworzą zbiór zerowy (można je pokryć kulami, których suma średnic jest dowolnie mała).*

Dowód. Zbiór liczb Liouville'a leży w $\bigcup_{m\geq n} U_{mk}$ dla każdych $k, n \in \mathbb{N}$ przy zachowaniu notacji z poprzedniego dowodu. Średnica zbioru U_{mk} nie przekracza k^{-m}, zatem dla $k \geq 2$ mamy $\sum_{m\geq n} d(U_{mk}) \leq k^{1-n}$. Bierzemy duże k, n. □

Fakt 9.1.10. *Niech $\lambda \in \mathbb{Z}_p$ będzie liczbą Liouville'a. Wtedy równanie różniczkowe $(1-x)(xf'(x) - \lambda f(x)) = 1$ nie posiada rozwiązań analitycznych na żadnym otoczeniu 0*

Dowód. Zapiszmy $f(x) = \sum_{n=0}^\infty b_n x^n$. Podstawienie tego do naszego równania daje $b_n(n-\lambda) = 1$. Jeśli $\lambda \notin \mathbb{Z}$ (jeśli λ jest całkowita, rozumowanie niepotrzebnie się komplikuje), szereg f ma zerowy promień zbieżności, $\nu(\lambda)$. □

Zajmiemy się polami wektorowymi.

Fakt 9.1.11. *Niech $f, g\colon \mathcal{K}^2 \to \mathcal{K}$ będą ciągłymi funkcjami. Istnieje $\mathcal{C}^1$-funkcja $F\colon \mathcal{K}^2 \to \mathcal{K}$, że $\partial_x F = f$, $\partial_y F = g$.*

Dowód. Niech $x \mapsto x_n$ będzie przybliżeniem identyczności (to jest ciągiem odwzorowań $\sigma_0, \sigma_1, \ldots : \mathcal{K} \to \mathcal{K}$, że σ_0 jest stała, $\sigma_m \circ \sigma_n = \sigma_n \circ \sigma_m = \sigma_n$ jeśli $m \geq n$, $|x-y| < \sigma^n$ implikuje $\sigma_n(x) = \sigma_n(y)$ oraz $|\sigma_n(x) - x| < \rho^n$, $0 < \rho < 1$ ustalone), $x'_n = x_{n+1} - x_n$, $y'_n = y_{n+1} - y_n$. Wtedy $F(x,y)$:

$$\sum_{n\geq 0} f(x_n, y_n)x'_n + g(x_n, y_n)y'_n$$

jest w porządku. □

Twierdzenie Schwarza o mieszaniu (dobrych) pochodnych czosnkowych nie jest prawdziwe.

Wniosek 9.1.12. *Istnieje funkcja $f\colon \mathcal{K}^2 \to \mathcal{K}$ o ciągłych drugich pochodnych czosnkowych, że*

$$\frac{\partial^2 f}{\partial x \partial y} = 1, \text{ jednak } \frac{\partial^2 f}{\partial y \partial x} = 0.$$

Dowód. Weźmy $\partial_y f = x$, $\partial_x f = 0$ i zróżniczkujmy. □

Fakt 9.1.13. *Jeśli $f\colon \mathcal{K}^2 \to \mathcal{K}$ jest $\mathcal{C}^2$, to drugie (mieszane) pochodne są równe.*

Rozdział 10
Teoria funkcji

Rozdział 11
Mechanika kwantowa

Ten rozdział miał być poświęcony mechanice kwantowej, ale wygląda na to, że jednak nie do końca tak będzie.

11.1 Analityczny wstęp

Aby zachować zgodność z książką, na której się bazujemy, do końca rozdziału tymczasowo przyjmiemy oznaczenia:

$$B_n(a) = \{x \in \mathbb{Q}_p : |x-a|_p \le p^n\}$$
$$S_n(a) = \{x \in \mathbb{Q}_p : |x-a|_p = p^n\}.$$

Definicja 11.1.1. *Ciągły morfizm $\chi\colon \mathbb{Q}_p^+ \to \mathbb{C}$ o obrazie zawartym w jednostkowym okręgu to charakter addytywny.*

Łatwo sprawdzić, że funkcja $\exp(2\pi i\langle \xi x\rangle)$ spełnia warunki tej definicji dla ustalonego ξ. Swoją drogą, Rosjanie używają $\{\,\}$ zamiast $\langle\,\rangle$, ale my trzymamy się konwencji Roberta z definicji 5.6.3. Okazuje się, że innych charakterów nie ma!

Fakt 11.1.2. *Każdy charakter jest postaci $\chi(x) = \exp(2\pi i\langle \xi x\rangle_p)$, „$\chi_p(\xi x)$" dla pewnego $\chi \in \mathbb{Q}_p$.*

Dowód. Niech χ będzie dowolnym (addytywnym) charakterem. Wtedy $\chi(0) = 1$, $\chi(nx) = \chi(x)^n$, $n \in \mathbb{Z}$. Zanim zajmiemy się całym ciałem $\mathbb{Q}_p$, przeprowadzimy dochodzenie w sprawie charakterów dla B_n.

Jeżeli $\chi \not\equiv 1$, to istnieje $k \in \mathbb{Z}$, że $\chi(x) \equiv 1$ dla $x \in B_k$. Istotnie, warunki $\chi(0) = 1$, $|\chi(x)| = 1$ i ciągłość χ na kuli B_n pozwalają wybrać taką gałąź funkcji $\log \chi(x) = i \arg \chi(x)$, która jest ciągła w zerze i $\arg \chi(0) = 0$ oraz $k \in \mathbb{Z}$, takie że $|\arg \chi(x)| < 1$ dla $x \in B_k$. Skoro $nx \in B_k$ dla $x \in B_k$, $n \in \mathbb{N}$, wnioskujemy $|\arg \chi(x)| = |\arg \chi(nx)|/n < 1/n$, mamy więc $\arg \chi(x) = 0$ i stąd już $\chi(x) \equiv 1$ dla $x \in B_k$.

Zakładamy, że dysk B_k jest maksymalny.

Pokażemy teraz, że dla każdej całkowitej $r \in (k, n]$ prawdą jest $\chi(p^{-r}) = \exp(2\pi i m p^{k-r})$, gdzie liczba m nie zależy od r i spełnia $1 \le m < p^{n-k}$.

Mamy $1 = \chi(p^{-k}) = \chi(p^{-r})^q$, $q = p^{n-k}$, dla $r = n$. Jeżeli $k < r < n$, to $\chi(p^{-r}) = \chi(p^{-n})^s = [\exp(2\pi i m p^{k-n})]^s$, przy czym $s = p^{n-r}$. Niech $\xi = p^k m$, gdzie $p^{-k} \ge |\xi|_p > p^{-n}$. To oznacza, że $\chi(p^{-r}) = \chi_p(p^{-r}\xi)$.

Niech $x \in B_n \setminus B_k$. Wtedy $\chi(x) = \chi_p(\xi x)$ dla pewnego ξ, że $|\xi|_p > p^{-n}$: niech $x = x_0 p^{-r} + \ldots + x_{r-k+1}p^{1-k} + x'$, gdzie $x_0 \ne 0$, $x' \in B_k$ dla pewnego r, że $k < r \le n$.

Już udowodnione własności pozwalają nam na

$$\begin{aligned}\chi(x) &= \chi(p^{-r})^{x_0}\chi(p^{1-r})^{x_1}\cdot\ldots\cdot\chi(p^{1-k})^{x_{r-k+1}}\chi(x')\\ &= \chi_p(x'\xi)\prod_{i=0}^{r-k+1}\chi_p(p^{i-r}\xi)^{x_i}\\ &= \chi_p(x_0p^{-r}\xi + \ldots + x_{r-k+1}p^{1-k}\chi + x'\xi)\\ &= \chi_p(\xi x).\end{aligned}$$

Przypadek $\xi = 0$ jest niemożliwy: wtedy $\chi(x) = \chi_p(0) = 1$ w B_n, co przeczy wyborowi liczby k. Pokazaliśmy, iż charakter dla dysku B_n jest taki jak trzeba: z $\xi = 0$ lub $|\xi|_p \ge p^{1-n}$.

Niech $\chi(\xi) \not\equiv 1$ będzie charakterem $\mathbb{Q}_p$. Wtedy w dysku B_0 ma przedstawienie $\chi(x) = \chi_p(\xi_0' x)$, gdzie $\xi_0' \in \mathbb{Q}_p$, $|\xi_0'|_p > 1$. Pokażemy, że w dysku B_1 mamy coś bardzo podobnego, tzn. $\chi(x) = \chi_p(\xi_1' x)$, gdzie $\xi_1' = \xi_0' + \xi_0$, $\xi_0 \in \{0, \ldots, p-1\}$.

Wiemy już, że $B_1 = B_0 \sqcup S_1$. Każdy element S_1 ma postać $x = x_0 p^{-1} + x'$, $x_0 \in \{1, \ldots, p-1\}$, $x' \in B_0$. Zatem w S_1:

$$\begin{aligned}\chi(x) &= \chi(1/p)^{x_0}\chi_p(\xi_0' x') = \chi(1)^{x_0\cdot p}\chi_p(\xi_0' x')\\ &= \chi_p(\xi_0')^{x_0\cdot p}\chi_p(\xi_0' x') = \chi_p(\xi_0' x_0/p)\chi_p(\xi_0 x_0/p)\\ &\cdot \chi_p(\xi_0' x' + \xi_0 x') = \chi_p((\xi_0' + \xi_0)(x_0/p + x'))\\ &= \chi_p(\xi_1' x)\end{aligned}$$

dla pewnego $\xi_0 = 0, 1, \ldots, p-1$.

Powtarzamy proces w dysku B_2 i dostajemy jeszcze lepsze przedstawienie $\chi(x) = \chi_p(\xi_2' x)$, $\xi_2' = \xi_0' + \xi_0 + \xi_1 p$.

Indukcyjne rozumowanie zapewnia nam istnienie jakiegoś $\xi = \xi_0' + \xi_0 + \xi_1 p + \xi_2 p^2 + \ldots \in \mathbb{Q}_p$. □

Wniosek 11.1.3. *Grupa (addytywna) $\mathbb{Q}_p$ jest izomorficzna z własną grupą charakterów za sprawą odwzorowania $\xi \mapsto \chi_p(\xi x)$.*

Niech $\chi_\infty(x) = \exp(-2\pi i x)$.

Fakt 11.1.4 („adelizm"). *Dla $x \in \mathbb{Q}$, $\prod_{p=2}^{\infty}\chi_p(x) = 1$.*

Dowód. Niech $x = c(p_1^{\alpha_1}\cdot\ldots\cdot p_n^{\alpha_n})^{-1}$, gdzie p_i są pierwsze i nie dzielą c. Wtedy mamy $x = m + \sum_{i=1}^n c_i p^{-\alpha_i}$ dla pewnej całkowitej m. Wynika stąd, że

$$\prod_{p<\infty}\chi_p(x) = \prod_{i\le n}\exp\Big(2\pi i\frac{c_i}{p_i^{\alpha_i}}\Big) = \exp(2\pi i x).$$ □

Definicja 11.1.5. *Multiplikatywny charakter ciała $\mathbb{Q}_p$ jest to ciągły homomorfizm $\mathbb{Q}_p^\times \to \mathbb{C}$.*

Fakt 11.1.6. *Multiplikatywny charakter $\mathbb{Q}_p$ jest postaci*

$$\pi(x) = |x|_p^{\alpha-1}\pi_0(|x|_p x),$$

gdzie π_0 jest charakterem S_0, $|\pi_0(x')|_p = 1$ dla $x' \in S_0$, $\alpha \in \mathbb{C}$.

Dowód jest na tyle podobny do tego, który uzasadniał już klasyfikację addytywnych charakterów, że pominiemy go.

Każdy element x ciała $\mathbb{Q}_p(\sqrt{\varepsilon})$ ma postać $z = r\sigma$ lub $\nu r\sigma$, gdzie $r \in \mathbb{Q}_p$, $\nu\overline{\nu}$ nie jest kwadratem w $\mathbb{Q}_p$ i $\sigma\overline{\sigma} = 1$.

Fakt 11.1.7. *Niech π_1 będzie multiplikatywnym charakterem ciała $\mathbb{Q}_p$, zaś π_2: „okręgu" C. Wtedy $\pi^2(\nu) = \pi_1(\nu\overline{\nu})\pi_2(\nu/\overline{\nu})$, a także $\pi(r\sigma) = \pi_1(r)\pi_2(\sigma)$ ($\pi(\nu r\sigma) = \pi(\nu)\pi(r\sigma)$) wyznaczają nam w jednoznaczny sposób charaktery dla $\mathbb{Q}_p(\sqrt{\varepsilon})$.*

Nie do końca wiadomo, czy niżej opisana całka jest istotnie czymś nowym.

Ciało $\mathbb{Q}_p$ jest lokalnie zwartą grupą abelową, więc istnieje na jego addytywnej grupie miara Haara, dodatnia miara $\mathrm{d}x$, która jest niezmiennicza na przesunięcia. Staje się jedyna po unormowaniu przez $\int\chi(B_0)\,\mathrm{d}x = 1$, przy czym χ oznacza tu indykator, a nie charakter!

Jeżeli $K \subseteq \mathbb{Q}_p$ jest zwarty, to miara $\mathrm{d}x$ definiuje dodatni funkcjonał ciągły na $\mathcal{C}(K)$ (z normą maksimum), całkę nad tym zbiorem.

Definicja 11.1.8. *Funkcję $f \in L^1_{loc}$ nazywamy całkowalną na $\mathbb{Q}_p$, jeśli istnieje granica*

$$\lim_{N\to\infty}\int_{B_N} f(x)\,dx = \sum_{n\in\mathbb{Z}}\int_{S(n)} f(x)\,dx.$$

Granicę tę nazywamy całką (niewłaściwą).

Fakt 11.1.9 (zamiana zmiennych I). *$d(xa) = |a|_p dx$ dla $a \in \mathbb{Q}_p^\times$.*

Dowód. Miara $d(xa)$ jest niezmiennicza na przesunięcia, więc różni się od $d(x)$ tylko czynnikiem $C(a) > 0$. Widać, że jest on charakterem grupy $\mathbb{Q}_p^\times$, przy czym $\pi_0(a') = 1$ i $C(a) = |a|_p^{\alpha-1}$. Dysk B_0 jest unią $B_{-1}(k)$ dla $k = 0, 1, \ldots, p-1$, zbiorów równej miary. Zatem $d(xp) = (dx)/p$ i $C(p) = |p|_p$, $\alpha = 2$. □

Policzymy teraz kilka całek.

Przykład 11.1.10. $\int_X 1\,dx = p^n$ ($n \in \mathbb{Z}$, $X = B_n$).

Dowód. $\int_X dx = \int_{|y|_p \le 1} d(p^{-n}y) = |p^{-n}|_p = p^n$. □

Wynika stąd, że „okrąg" (S_n) w $\mathbb{Q}_p$ ma dodatnie pole, gdyż jest różnicą dwóch dysków, wbrew temu, czego spodziewać się można po okręgu na prostej rzeczywistej: $\int_{S_n} dx = p^n - p^{n-1}$.

Uogólnieniem powyższej całki jest:

Fakt 11.1.11. *Dla odpowiednio regularnych f zachodzi*

$$\int_{\mathbb{Q}_p} f(|x|_p)\,dx = \frac{p-1}{p}\sum_{n\in\mathbb{Z}} f(p^n)p^n.$$

Wniosek 11.1.12. *Jeżeli $f(x) = x^{\alpha-1}$ i $\Re\,\alpha > 0$, to*

$$\int_{B_0} |x|_p^{\alpha-1}\,dx = \frac{p-1}{p}\cdot\frac{p^\alpha}{p^\alpha-1}.$$

Wniosek 11.1.13. *Jeżeli $f = \ln$ (logarytm naturalny), to*

$$\int_{B_0} \ln|x|_p\,dx = \frac{\ln p}{1-p}.$$

Dowód. $-(1-1/p)\ln p\sum_{n=0}^\infty np^{-n} = (1-p)^{-1}\ln p$. □

Fakt 11.1.14 (zamiana zmiennych II)**.** *Jeżeli $\sigma(y)$ to analityczny homeomorfizm między otwarniętymi K_1 i $K_2 \subseteq \mathbb{Q}_p$ o niezerowej pochodnej, to dla $f \in \mathcal{C}(K)$ prawdziwa jest równość*

$$\int_{K_2} f(x)\,dx = \int_{K_1} |\sigma'(y)|_p \cdot f(\sigma(y))\,dy.$$

Dowód. Wystarczy sprawdzić poprawność stwierdzenia dla f, indykatora zbioru K_2, przez pokrycie go małymi i rozłącznymi dyskami w skończonej ilości. □

Przykład 11.1.15. *Jeżeli $n \in \mathbb{Z}$, to*

$$\int_{B(n)} \chi_p(\xi x)\,dx = p^n\cdot[|\xi|_p \le p^{-n}].$$

Dowód. Dla $|\xi|_p \le p^{-n}$ jest $|\xi x|_p \le 1$ i $\chi_p(\xi x) = 1$, stąd

$$\int_{B(n)} \chi_p(\xi x)\,\mathrm{d}x = \int_{B(n)} 1\,\mathrm{d}x = p^n.$$

Jeśli $|\xi|_p \ge p^{1-n}$, to dla pewnego $y \in S_n$ jest $|\xi y|_p \ge p$, a więc $\chi_p(\xi y) \not\equiv 1$. Zmiana zmiennych $x = t - y$ przekształca lewą całkę do

$$\int_{B_n(y)} \chi_p(\xi t - \xi y)\,\mathrm{d}t = \chi_p(-\xi y)\int_{B(n)} \chi_p(\xi t)\,\mathrm{d}t.$$ □

Przykład 11.1.16. *Jeżeli szereg $\sum_{\gamma\ge 0}|f(p^{-\gamma})|p^{-\gamma}$ jest zbieżny, to całka z $f(|x|_p)\chi_p(\xi x)$ nad $\mathbb{Q}_p$ wynosi*

$$\frac{p-1}{p|\xi|_p}\sum_{\gamma=0}^\infty \frac{f(p^{-\gamma}|\xi|_p^{-1})}{p^\gamma} - \frac{f(p|\xi|_p^{-1})}{|\xi|_p}.$$

Dowód. Wynika to z poprzedniego przykładu i definicji całki (niewłaściwej) po użyciu sztuczki pozwalającej wyznaczyć pole okręgu. □

Wniosek 11.1.17. *Jeśli $f(x) = \ln|x|_p$, to*

$$\int_{\mathbb{Q}_p} \ln|x|_p\chi_p(\xi x)\,dx = \frac{p\ln p}{|\xi|_p(1-p)}.$$

Wniosek 11.1.18. *Jeśli $f(x) = |x|_p^{\alpha-1}$, $\Re\alpha > 0$, to*

$$\int_{\mathbb{Q}_p} |x|_p^{\alpha-1}\chi_p(\xi x)\,dx = \frac{1-p^{\alpha-1}}{1-p^{-\alpha}}|\xi|_p^{-\alpha}.$$

Wniosek 11.1.19. *Poprzedni wniosek z $\alpha = 1$, jeśli $\xi \ne 0$.*

Przykład 11.1.20. *Jeśli $f(x) = (|x|_p^2 + m^2)^{-1}$, to*

$$\begin{aligned} I &= \int_{\mathbb{Q}_p} \frac{\chi_p(\xi x)}{|x|_p^2+m^2}\,dx \\ &= \frac{p-1}{p|\xi|_p}\sum_{n=0}^\infty \frac{p^{-n}}{p^{-2n}|\xi|_p^{-2}+m^2} - \frac{|\xi|_p^{-1}}{p^2|\xi|_p^{-2}+m^2} \\ &= \frac{p-1}{p|\xi|_p^{-1}}\sum_{n\ge 0}\frac{1}{p^n}\Big(\frac{1}{p^{-2n}+m^2|\xi|_p^2} - \frac{1}{p^2+m^2|\xi|_p^2}\Big) \end{aligned}$$

Wniosek 11.1.21. *Przy $|\xi|_p$ dążącym do ∞ mamy asymptotykę*

$$\int_{\mathbb{Q}_p} \frac{\chi_p(\xi x)}{|x|_p^2+m^2}\,dx \approx \frac{p^4+p^3}{p^2+p+1}\frac{1}{m^4|\xi|_p^3}.$$

Dowód. Mniej uciążliwy rachunkowo niż pozornie:

$$\begin{aligned} \ldots &= \lim_{|\xi|_p\to\infty}|\xi|_p^3\int_{\mathbb{Q}_p}\frac{\chi_p(\xi x)}{|x|_p^2+m^2}\,\mathrm{d}x = \frac{p-1}{pm^4} \\ &\quad\cdot\lim_{|\xi|_p\to\infty}\sum_{n=0}^\infty\frac{p^2-p^{-2n}}{p^n}\Big(1-\frac{p^{-2n}}{p^{-2n}+m^2|\xi|_p^2}\Big) \\ &= \frac{p-1}{pm^4}\sum_{n=0}^\infty(p^{2-n}-p^{-3n}) \\ &= \frac{p-1}{pm^4}\Big(\frac{p^2}{1-p^{-1}} - \frac{1}{1-p^{-3}}\Big). \end{aligned}$$ □

Całka rzeczywista maleje wykładniczo:

$$\int_{-\infty}^\infty \frac{\exp(-2\pi i\xi x)}{x^2+m^2}\,\mathrm{d}x = \frac{\pi}{m\exp(2\pi m|\xi|)}.$$

Miara $\mathrm{d}x$ z $\mathbb{Q}_p$ przenosi się na przestrzeń produktową $\mathbb{Q}_p^n$. Aby zredukować całki wielowymiarowe do duż prostszych w jednym wymiarze, należy użyć twierdzenia Fubiniego.

Twierdzenie 27 (Fubini)**.** *Niech dana będzie taka funkcja $f(x,y)$ dla $x \in \mathbb{Q}_p^n$ i $y \in \mathbb{Q}_p^m$, że całka iterowana*

$$\int_{\mathbb{Q}_p^n}\int_{\mathbb{Q}_p^m}|f(x,y)|\,dy\,dx$$

istnieje. Wtedy funkcja f jest całkowalna na $\mathbb{Q}_p^{n+m}$, zaś iterowane całki są sobie równe:

$$\int_{\mathbb{Q}_p^n}\int_{\mathbb{Q}_p^m} f(x,y)\,dy\,dx = \int_{\mathbb{Q}_p^m}\int_{\mathbb{Q}_p^n} f(x,y)\,dx\,dy$$

i pokrywają się wartością z całką $f(x,y)$ nad $\mathbb{Q}_p^{n+m}$.

Fakt 11.1.22 (zamiana zmiennych III)**.** *Jeśli $x_i(y_1,\ldots,y_n)$ jest homeomorfizmem między otwarto-zwartymi K_1 i $K_2 \subseteq \mathbb{Q}_p^n$, którego współrzędne są analityczne i $\det\|\partial x_i/\partial y_k\| \ne 0$, to*

$$\int_{K_2} f(x)\,dx = \int_{K_1}\left|\det\frac{\partial x_i}{\partial y_k}\right|_p f(x(y))\,dy.$$

Fakt 11.1.23 (całka Gaußa)**.** *Jeśli $a \ne 0$, to*

$$\int_{\mathbb{Q}_p}\chi_p(ax^2+bx)\,dx = \lambda_p(a)|a|_p^{-1/2}\chi_p(-b^2/4a),$$

gdzie $\sqrt{2}\lambda_2(a) = (1+i)i^{a_1}(-1)^{a_2}$, jeśli $2 \mid v_2(a)$, natomiast $\sqrt{2}\lambda_2(a) = 1+(-1)^{a_1}i$ w przeciwnym razie.

Dla $p > 2$, $\lambda_p(a) = 1$ (jeśli $2 \mid v_p(a)$), (a_0/p), jeśli $4 \mid p-1$ oraz $i(a_0/p)$ w przeciwnym razie.

Sowieci liczą teraz śmieszne całki, gaussowskie oraz różne warianty $\int_X \chi_p(t(x-y)^2)\,\mathrm{d}y$.

Fakt 11.1.24. $\lambda_p(a)\lambda_p(b) = \lambda_p(a+b)\lambda_p(1/a+1/b)$.

Rozdział 12
Teoria reprezentacji

12.1 Teoria reprezentacji Blondela

Teoria reprezentacji w tym rozdziale wyłożona jest w naprawdę telegraficznym skrócie. Tak długo, jak to możliwe, będziemy pracować z przestrzenią wektorową nad ciałem, zakładając, że nie ma charakterystyki p. Naszym „węgielnym kamieniem" będzie następujące stwierdzenie: gładkie oraz nierozkładalne reprezentacje p-adycznej grupy reduktywnej nad ciałem, które ma charakterystykę różną od p, są osiągalne.

Definicja 12.1.1. *Grupa topologiczna $\mathcal{G}$ jest proskończona, gdy jest zwarta i całkowicie niespójna.*

Fakt 12.1.2. *Proskończone grupy topologiczne $\mathcal{G}$ są izomorficzne z $\varprojlim \mathcal{G}/U$, gdzie U przebiega otwarte podgrupy normalne.*

Fakt 12.1.3. *Jeśli ilorazy $\mathcal{G}/U$ są p-grupami, to granica odwrotna również nią jest.*

Przykład 12.1.4. $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

Definicja 12.1.5. *Grupa topologiczna $\mathcal{G}$ jest lokalnie proskończona, gdy każde otoczenie $e \in G$ zawiera otwartą i zwartą podgrupę*

Fakt 12.1.6. *Lokalna proskończoność $\mathcal{G}$ jest równoważna lokalnej zwartości i całkowitej niespójności.*

Przykład 12.1.7. $(\mathbb{Q}_p, +)$.

Definicja 12.1.8. *Reprezentacja $(\pi, \mathcal{V})$ grupy $\mathcal{G}$ w przestrzeni $\mathcal{V}$ nad ciałem $\mathcal{K}$ to homomorfizm $\pi\colon G \to Aut_{\mathcal{K}}(\mathcal{V})$.*

Definicja 12.1.9. *Niezerowa reprezentacja jest nieredukowalna, gdy właściwe podprzestrzenie $\mathcal{V}$ są niestabilne względem automorfizmów $\pi(G)$.*

Definicja 12.1.10. *Reprezentacja jest nierozkładalna, jeśli $\mathcal{V}$ nie da się rozłożyć jako sumę prostą właściwych podprzestrzeni, które same są stabilne względem tych samych automorfizmów $\pi(G)$.*

Definicja 12.1.11. *Reprezentacja $(\pi, \mathcal{V})$ dla $\mathcal{G}$ jest gładka, jeżeli wszystkie zbiory postaci $G_v = \{g \in \mathcal{G} : \pi(g)(v) = v\} \subseteq \mathcal{G}$ dla v, stabilizatory w $\mathcal{G}$, są otwartymi podzbiorami $\mathcal{G}$.*

Definicja 12.1.12. *Gładka reprezentacja $(\pi, \mathcal{V})$ dla $\mathcal{G}$ jest osiągalna, o ile $\mathcal{V}^K$ ma skończony wymiar dla każdej zwartej podgrupy otwartej $K \leq \mathcal{G}$.*

1. Miara Haara.
2. Algebra Heckego.
3. Koniezmienniki.
4. Charaktery.
5. Lemat Schura, charakter centralny.
6. Reprezentacje Z-zwarte.
7. Paraboliczna indukcja, restrykcja, para.
8. Rozkład Iwahoriego.
9. Reprezentacje szpiczaste.

Twierdzenie 28. *Każda gładka reprezentacja nieredukowalna dla $\mathcal{G}$ nad $\mathcal{K}$ o charakterystyce różnej od p jest osiągalna.*

Rozdział 13
Trupiogłowe królestwo

Rozdział 14
Uwagi historyczne

14.1 Preludium (arytmetyka)

Pojęcie (oraz sama nazwa) *waluacji* pochodzi z pracy Kürschaka z 1913, stanowi ono uogólnienie *wartości bezwzględnej*. Przy ich użyciu pokazał, że każde ciało z waluacją można rozszerzyć do ciała zupełnego oraz algebraicznie domkniętego; zainspirowała go książka Hensela z 1908 (przykład: $\mathbb{Q}_p$ i $\mathbb{C}_p$). Świat dowiedział się o twierdzeniu Ostrowskiego w roku 1918, chociaż Ostrowski potrafił je uzasadnić kwietniem dwa lata wcześniej. My przedstawiliśmy dowód Artina (1932). Lemat Hensela (przedstawiony później w dużo większej ogólności) jest wnioskiem z lematu Hensela-Rychlika, o którym nikt nie pamięta. Reguła lokalno-globalna (dla form kwadratowych) pojawia się w rozprawie doktorskiej Hassego z 1921 roku. Hasse rok wcześniej przeniósł się do Marburga z Göttingen po tym, jak odkrył w antykwariacie książkę „Zahlentheorie" Hensela z 1913 roku. Minkowski zmarł w 1909 r., jednak podstawy geometrii liczb wyłożył trzynaście lat wcześniej.

14.2 Analiza

Większość z uzyskanych w tym rozdziale wyników jest klasyczna i nie wymaga dodatkowego komentarza. Zrozumienie przykładu wymaga poznania eksponensy Artina-Hassego. Problem, czy liczba $\sum_n n!$ jest wymierna, czy nie, pochodzi jeszcze od Schikhofa, zatem pozostaje otwarty od ponad trzech dekad. Twierdzenie Straßmanna pojawia się w jego pracy z 1928 roku, „Über den Wertevorrat von Potenzreihen im Gebiet der p-adischen Zahlen". Formułę pozwalającą na wyznaczenie waluacji p-adycznej silnii znał już A. Legendre w 1830 („Théorie des Nombres"). Dyskusja szeregów dwumiennych podąża za Koblitzem. Konstrukcja dziwnie zbieżnego szeregu różni się od pracy Bürgera i Struppecka jedynie notacją.

Sztywne przestrzenie analityczne są odpowiednikiem zespolonych, ale nad niearchimedesowym ciałem. Wprowadził je J. Tate w roku 1962 jako efekt uboczny prac nad ujednoliceniem p-adycznych krzywych eliptycznych o złej redukcji. Ich zaletą jest to, że sens mają dla nich analityczne przedłużanie i spójność, ale ceną za to jest pojęciowa złożoność.