Geometria z Algebrą Liniową II*

Arkadiusz Męcel

WYKŁAD 16, 4.05.2021 r.

Definicja

Parę (X, d), gdzie X to niepusty zbiór, zaś $d : X \times X \to [0, \infty)$ jest funkcją nazywamy **przestrzenią metryczną**, jeśli spełnione są następujące założenia:

- $d(x, y) = 0 \Leftrightarrow x = y$, dla każdych $x, y \in X$,
- $d(x, y) = d(y, x)$, dla każdych $x, y \in X$,
- $d(x, z) \leq d(x, y) + d(y, z)$, dla każdych $x, y, z \in X$.

Funkcję d nazywamy **metryką** lub **odległością** na zbiorze X.

Definicja

Parę (X, d), gdzie X to niepusty zbiór, zaś $d : X \times X \to [0, \infty)$ jest funkcją nazywamy **przestrzenią metryczną**, jeśli spełnione są następujące założenia:

- $d(x, y) = 0 \Leftrightarrow x = y$, dla każdych $x, y \in X$,
- $d(x, y) = d(y, x)$, dla każdych $x, y \in X$,
- $d(x, z) \leq d(x, y) + d(y, z)$, dla każdych $x, y, z \in X$.

Funkcję d nazywamy **metryką** lub **odległością** na zbiorze X.

Przykłady (zachęcam do wyszukania w Sieci: „Okręgi w różnych przestrzeniach metrycznych").

- metryka euklidesowa na $X = \mathbb{R}^2$:

$$d((x_1, x_2), (y_1, y_2)) = \sqrt{(y_1 - x_1)^2 + (y_2 - x_2)^2}.$$

- metryka taksówkowa na $X = \mathbb{R}^2$:

$$d((x_1, x_2), (y_1, y_2)) = |x_1 - y_1| + |x_2 - y_2|.$$

Definicja

Parę (X, d), gdzie X to niepusty zbiór, zaś $d : X \times X \to [0, \infty)$ jest funkcją nazywamy **przestrzenią metryczną**, jeśli spełnione są następujące założenia:

- $d(x, y) = 0 \Leftrightarrow x = y$, dla każdych $x, y \in X$,
- $d(x, y) = d(y, x)$, dla każdych $x, y \in X$,
- $d(x, z) \leq d(x, y) + d(y, z)$, dla każdych $x, y, z \in X$.

Funkcję d nazywamy **metryką** lub **odległością** na zbiorze X.

Definicja

Niech (X, d) będzie przestrzenią metryczną. Ciąg (x_n) elementów z (X, d) nazywamy **zbieżnym** do punktu $x \in X$, ozn. $\lim_{n\to\infty} x_n = x$, jeśli dla każdego $\epsilon > 0$ istnieje $N \in \mathbb{N}$ takie, że dla każdego $n \geq N$ zachodzi

$$d(x_n, x) < \epsilon.$$

Definicja

Niech (X, d) będzie przestrzenią metryczną.

- **Ciągiem Cauchy'ego** w przestrzeni metrycznej X nazywamy ciąg (x_n) taki, że dla każdego $\epsilon > 0$ istnieje $N \in \mathbb{N}$ takie, że dla każdych $n_1, n_2 > N$:

$$d(x_{n_1}, x_{n_2}) < \epsilon.$$

- Ciągi Cauchy'ego (x_n), (y_n) w przestrzeni metrycznej (X, d) nazywamy **równoważnymi**, ozn. $(x_n) \sim (y_n)$, jeśli

$$\lim_{n\to\infty} d(x_n, y_n) = 0.$$

- Przestrzeń metryczną nazywamy **zupełną**, jeśli każdy ciąg Cauchy'ego ma w niej granicę.[a]

[a] Wiadomo, że $\mathbb{Q}$ z metryką $d(x, y) = |x - y|$ nie jest zupełna.

Definicja

Normą na ciele K nazywamy odwzorowanie $\|,\| : K \to [0, \infty)$ spełniające:

- $\|x\| = 0 \Leftrightarrow x = 0$, dla każdego $x \in K$,
- $\|xy\| = \|x\| \cdot \|y\|$, dla każdych $x, y \in K$,
- $\|x + y\| \leq \|x\| + \|y\|$, dla każdych $x, y \in K$.

Definicja

Normą na ciele K nazywamy odwzorowanie $\|,\| : K \to [0, \infty)$ spełniające:

- $\|x\| = 0 \Leftrightarrow x = 0$, dla każdego $x \in K$,
- $\|xy\| = \|x\| \cdot \|y\|$, dla każdych $x, y \in K$,
- $\|x + y\| \leq \|x\| + \|y\|$, dla każdych $x, y \in K$.

Przykłady:

- **Norma trywialna** $\|,\|$ na ciele K, czyli: $\|0\| = 0$ oraz $\|x\| = 1$, dla $x \neq 0$.
- Na ciałach skończonych jest tylko trywialna norma (dlaczego?).
- Na $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ mamy normy $\|x\| = |x|$, gdzie $|x|$ jest modułem.
- Na ciele funkcji wymiernych $\mathbb{R}(x)$ dla każdego wielomianu nierozkładalnego p stopnia ≥ 1 mamy normę $\|f\| = 2^{-n}$, gdzie n jest takie, że:

$$f(x) = p(x)^n \cdot \frac{g(x)}{h(x)}, \quad \mathrm{NWD}(g(x), p(x)) = \mathrm{NWD}(h(x), p(x)) = 1.$$

Definicja

Normą na ciele K nazywamy odwzorowanie $\|,\| : K \to [0,\infty)$ spełniające:

- $\|x\| = 0 \Leftrightarrow x = 0$, dla każdego $x \in K$,
- $\|xy\| = \|x\| \cdot \|y\|$, dla każdych $x, y \in K$,
- $\|x + y\| \leq \|x\| + \|y\|$, dla każdych $x, y \in K$.

Proste obserwacje wynikające z definicji normy: dla każdych $x, y \in K$ mamy:

$$\|1\| = 1, \quad \|x\| = \|-x\|, \quad \|x/y\| = \|x\|/\|y\| \ \text{(gdy } y \neq 0\text{)},$$

$$\|x \pm y\| \geq |\,\|x\| - \|y\|\,|, \quad \|x - y\| \leq \|x\| + \|y\|,$$

Definicja

Normą na ciele K nazywamy odwzorowanie $\|,\| : K \to [0, \infty)$ spełniające:

- $\|x\| = 0 \Leftrightarrow x = 0$, dla każdego $x \in K$,
- $\|xy\| = \|x\| \cdot \|y\|$, dla każdych $x, y \in K$,
- $\|x + y\| \leq \|x\| + \|y\|$, dla każdych $x, y \in K$.

Proste obserwacje wynikające z definicji normy: dla każdych $x, y \in K$ mamy:

$$\|1\| = 1, \quad \|x\| = \|-x\|, \quad \|x/y\| = \|x\|/\|y\| \ \text{(gdy } y \neq 0),$$
$$\|x \pm y\| \geq |\,\|x\| - \|y\|\,|, \quad \|x - y\| \leq \|x\| + \|y\|,$$

Niech K będzie ciałem z normą $\|.\|$. Funkcja $d : K \times K \to [0, \infty)$ dana wzorem

$$d(x, y) = \|x - y\|$$

jest metryką na K. Mówimy, że jest to **metryka indukowana** przez normę $\|.\|$.

Definicja

Niech p będzie dowolną liczbą pierwszą, zaś z – liczbą całkowitą.

- Przez $v_p(z)$ oznaczamy największe n całkowite takie, że
$$p^n \mid z,$$
zwane **wykładnikiem** p**-adycznym liczby** z.
- Jeśli $x = \frac{a}{b}$, gdzie $a, b \in \mathbb{Z}$, $b \neq 0$, to określamy:
$$v_p(x) = v_p(a) - v_p(b).$$
- **Normą** p**-adyczną** nazywamy funkcję $|.|_p : \mathbb{Q} \to [0, \infty)$ określoną wzorem:
$$|x|_p = \begin{cases} p^{-v_p(x)} & , x \neq 0 \\ 0 & , x = 0. \end{cases}.$$

Przykłady obliczeń:

- $|2|_2 = 2^{-v_2(2)} = \frac{1}{2}$,
- $|3|_2 = 2^{-v_2(3)} = 1$,
- $|4|_2 = 2^{-v_2(4)} = \frac{1}{4}$,
- $|-\frac{128}{7}|_2 = |\frac{2^7}{-7}|_2 = 2^{-v_2(2^7)+v_2(-7)} = 2^{-7} = 1/128$.
- $|13,23|_3 = 1/27$, bo $13 + \frac{23}{100} = \frac{1323}{100} = \frac{3^3 \cdot 49}{100}$.

Przykłady obliczeń:

- $|2|_2 = 2^{-v_2(2)} = \frac{1}{2}$,
- $|3|_2 = 2^{-v_2(3)} = 1$,
- $|4|_2 = 2^{-v_2(4)} = \frac{1}{4}$,
- $|-\frac{128}{7}|_2 = |\frac{2^7}{-7}|_2 = 2^{-v_2(2^7)+v_2(-7)} = 2^{-7} = 1/128.$
- $|13,23|_3 = 1/27$, bo $13 + \frac{23}{100} = \frac{1323}{100} = \frac{3^3 \cdot 49}{100}$.

Ćwiczenie dla (samodzielnego) upewnienia się, że wszystko jest jasne.

Uwaga

Niech $0 \neq x \in \mathbb{Q}$, wówczas jeśli przez $\mathbb{P}$ oznaczymy zbiór wszystkich (dodatnich) liczb pierwszych, to

$$|x| \cdot \prod_{p \in \mathbb{P}} |x|_p = 1.$$

Fakt

Norma p-adyczna jest normą na $\mathbb{Q}$.

Fakt

Norma p-adyczna jest normą na $\mathbb{Q}$.

Dowód. Jest jasne, że $|x|_p \geq 0$ przy czym równość zachodzi tylko dla $x = 0$.

Fakt

Norma p-adyczna jest normą na $\mathbb{Q}$.

Dowód. Jest jasne, że $|x|_p \geq 0$ przy czym równość zachodzi tylko dla $x = 0$.

- Niech: $x = \frac{p^a m}{n}, y = \frac{p^b r}{s}$, gdzie p jest pierwsza oraz $p \nmid r, s, m, n \in \mathbb{Z}$. Wówczas $xy = \frac{p^{a+b} mr}{ns}$ oraz $p \nmid mr, ns$, czyli $|xy|_p = p^{-(a+b)} = |x|_p |y|_p$.

Fakt

Norma p-adyczna jest normą na $\mathbb{Q}$.

Dowód. Jest jasne, że $|x|_p \geq 0$ przy czym równość zachodzi tylko dla $x = 0$.

- Niech: $x = \frac{p^a m}{n}, y = \frac{p^b r}{s}$, gdzie p jest pierwsza oraz $p \nmid r, s, m, n \in \mathbb{Z}$. Wówczas $xy = \frac{p^{a+b} mr}{ns}$ oraz $p \nmid mr, ns$, czyli $|xy|_p = p^{-(a+b)} = |x|_p |y|_p$.
- Bez straty ogólności możemy założyć, że $a \leq b$ i wtedy:

$$|x+y|_p = \left| \frac{p^a (sm + p^{b-a} nr)}{ns} \right|_p \leq p^{-a} = |x|_p.$$

Innymi słowy otrzymujemy, że: $|x+y|_p \leq \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$.

Fakt

Norma p-adyczna jest normą na $\mathbb{Q}$.

Dowód. Jest jasne, że $|x|_p \geq 0$ przy czym równość zachodzi tylko dla $x = 0$.

- Niech: $x = \frac{p^a m}{n}, y = \frac{p^b r}{s}$, gdzie p jest pierwsza oraz $p \nmid r, s, m, n \in \mathbb{Z}$.
  Wówczas $xy = \frac{p^{a+b} mr}{ns}$ oraz $p \nmid mr, ns$, czyli $|xy|_p = p^{-(a+b)} = |x|_p |y|_p$.
- Bez straty ogólności możemy założyć, że $a \leq b$ i wtedy:

$$|x + y|_p = \left| \frac{p^a(sm + p^{b-a} nr)}{ns} \right|_p \leq p^{-a} = |x|_p.$$

  Innymi słowy otrzymujemy, że: $|x + y|_p \leq \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$.

Definicja

Normę $\|.\|$ na ciele K nazywamy **niearchimedesowską**, jeśli spełnia $\|x + y\| \leq \max(\|x\|, \|y\|)$, dla dowolnych $x, y \in K$.

Definicja

Powiemy, że **metryki** d_1, d_2 **są równoważne** na zbiorze X, jeśli ciąg (x_n) elementów z X jest Cauchy'ego względem d_1 wtedy i tylko wtedy, gdy jest ciągiem Cauchy'ego względem d_2. Mówimy, że **normy** $\|.\|_1$ i $\|.\|_2$ **są równoważne** na w ciele K, jeśli indukują równoważne metryki.

Definicja

Powiemy, że **metryki** d_1, d_2 **są równoważne** na zbiorze X, jeśli ciąg (x_n) elementów z X jest Cauchy'ego względem d_1 wtedy i tylko wtedy, gdy jest ciągiem Cauchy'ego względem d_2. Mówimy, że **normy** $\|.\|_1$ i $\|.\|_2$ **są równoważne** na w ciele K, jeśli indukują równoważne metryki.

Przykład. Na ciele $\mathbb{Q}$ żadna z norm $|.|_p$ jest równoważna formie $|.|$, bo ciąg $x_n = p^n$ jest ciągiem Cauchy'ego względem $|.|_p$, ale nie względem $|.|$. Także jeśli $p_1 \neq p_2$ są liczbami pierwszymi, to ciąg $x_n = (p_1/p_2)^n$ spełnia:

$$|x_n|_{p_1} \to 0, \quad |x_n|_{p_2} \to \infty.$$

Definicja

Powiemy, że **metryki** d_1, d_2 **są równoważne** na zbiorze X, jeśli ciąg (x_n) elementów z X jest Cauchy'ego względem d_1 wtedy i tylko wtedy, gdy jest ciągiem Cauchy'ego względem d_2. Mówimy, że **normy** $\|.\|_1$ i $\|.\|_2$ **są równoważne** na w ciele K, jeśli indukują równoważne metryki.

Przykład. Na ciele $\mathbb{Q}$ żadna z norm $|.|_p$ jest równoważna formie $|.|$, bo ciąg $x_n = p^n$ jest ciągiem Cauchy'ego względem $|.|_p$, ale nie względem $|.|$. Także jeśli $p_1 \neq p_2$ są liczbami pierwszymi, to ciąg $x_n = (p_1/p_2)^n$ spełnia:

$$|x_n|_{p_1} \to 0, \quad |x_n|_{p_2} \to \infty.$$

Twierdzenie Ostrowskiego

Każda nietrywialna norma na $\mathbb{Q}$ jest równoważna jednej z norm $|.|_p$ lub $|.|$.

Dowód można znaleźć w Lekturze nieobowiązkowej 10.

Twierdzenie

Niech K będzie ciałem z normą $\|.\|$. Przez $\widehat{K}$ oznaczamy zbiór klas równoważnych ciągów Cauchy'ego na K postaci $[(x_n)]$, gdzie

$$[(a_n)] = [(b_n)] \Leftrightarrow (a_n) \sim (b_n) \Leftrightarrow \lim_{n\to\infty} \|a_n - b_n\| = 0.$$

Dla $k \in K$ niech $\widehat{k}$ będzie ciągiem stale równym k. Wówczas na $\widehat{K}$ określona jest struktura ciała z działaniami:

$$[(a_n)] + [(b_n)] = [(a_n + b_n)], \quad [(a_n)] \cdot [(b_n)] = [(a_n b_n)],$$

gdzie elementem zerowym jest $[\widehat{0}]$, zaś jedynką jest $[\widehat{1}]$.

Twierdzenie

Niech K będzie ciałem z normą $\|.\|$. Przez $\widehat{K}$ oznaczamy zbiór klas równoważnych ciągów Cauchy'ego na K postaci $[(x_n)]$, gdzie

$$[(a_n)] = [(b_n)] \Leftrightarrow (a_n) \sim (b_n) \Leftrightarrow \lim_{n\to\infty} \|a_n - b_n\| = 0.$$

Dla $k \in K$ niech $\widehat{k}$ będzie ciągiem stale równym k. Wówczas na $\widehat{K}$ określona jest struktura ciała z działaniami:

$$[(a_n)] + [(b_n)] = [(a_n + b_n)], \quad [(a_n)] \cdot [(b_n)] = [(a_n b_n)],$$

gdzie elementem zerowym jest $[\widehat{0}]$, zaś jedynką jest $[\widehat{1}]$.

Dowód. Prostym (choć nieco żmudnym) ćwiczeniem jest sprawdzenie, że działania $+, \cdot$ są dobrze określone na $\widehat{K}$, tzn. jeśli $(a_n) \sim (c_n)$, $(b_n) \sim (d_n)$, to:

$$[(a_n + c_n)] = [(b_n + d_n)], \quad [(a_n c_n)] = [(b_n d_n)].$$

Dowód istnienia odwrotności niezerowego elementu w $\widehat{K}$ (na K jest norma $\|.\|$).

Dowód istnienia odwrotności niezerowego elementu w $\widehat{K}$ (na K jest norma $\|.\|$).

- Weźmy taki ciąg Cauchy'ego (a_n), że $\|a_n\| \not\to 0$. Wówczas istnieje liczba dodatnia c oraz liczba całkowita dodatnia N, że dla $n > N$ mamy $\|a_n\| > c$.

Dowód istnienia odwrotności niezerowego elementu w $\widehat{K}$ (na K jest norma $\|.\|$).

- Weźmy taki ciąg Cauchy'ego (a_n), że $\|a_n\| \not\to 0$. Wówczas istnieje liczba dodatnia c oraz liczba całkowita dodatnia N, że dla $n > N$ mamy $\|a_n\| > c$.
- Określamy ciąg
$$b_n = \begin{cases} 0, & 1 \leq n \leq N-1 \\ a_n^{-1}, & n \geq N \end{cases}.$$

Dowód istnienia odwrotności niezerowego elementu w $\widehat{K}$ (na K jest norma $\|.\|$).

- Weźmy taki ciąg Cauchy'ego (a_n), że $\|a_n\| \not\to 0$. Wówczas istnieje liczba dodatnia c oraz liczba całkowita dodatnia N, że dla $n > N$ mamy $\|a_n\| > c$.
- Określamy ciąg
$$b_n = \begin{cases} 0, & 1 \leq n \leq N-1 \\ a_n^{-1}, & n \geq N \end{cases}.$$
- Ciąg (a_n) jest Cauchy'ego oraz dla $n, m \geq N$ mamy:
$$0 \leq \|b_m - b_n\| = \|a_m^{-1} - a_n^{-1}\| = \frac{\|a_m - a_n\|}{\|a_m\| \cdot \|a_n\|} \leq \frac{\|a_m - a_n\|}{c^2},$$
czyli ciąg (b_n) też jest Cauchy'ego.

Dowód istnienia odwrotności niezerowego elementu w $\widehat{K}$ (na K jest norma $\|.\|$).

- Weźmy taki ciąg Cauchy'ego (a_n), że $\|a_n\| \not\to 0$. Wówczas istnieje liczba dodatnia c oraz liczba całkowita dodatnia N, że dla $n > N$ mamy $\|a_n\| > c$.
- Określamy ciąg
$$b_n = \begin{cases} 0, & 1 \leq n \leq N-1 \\ a_n^{-1}, & n \geq N \end{cases} .$$
- Ciąg (a_n) jest Cauchy'ego oraz dla $n, m \geq N$ mamy:
$$0 \leq \|b_m - b_n\| = \|a_m^{-1} - a_n^{-1}\| = \frac{\|a_m - a_n\|}{\|a_m\| \cdot \|a_n\|} \leq \frac{\|a_m - a_n\|}{c^2},$$
czyli ciąg (b_n) też jest Cauchy'ego.
- Oczywiście mamy
$$[(a_n)] \cdot [(c_n)] = [(a_n c_n)] = [(\underbrace{0, \ldots, 0}_{N-1}, 1, 1, \ldots)],$$
co znaczy, że $[(a_n)] \cdot [(c_n)] = [\widehat{1}]$.

Uwaga

Niech K będzie ciałem z normą $\|,\|$ i niech (a_n) będzie ciągiem Cauchy'ego w K. Wówczas:

- Ciąg $\|a_n\|$ jest zbieżny.
- Jeśli $(b_n) \sim (a_n)$, to $\lim\limits_{n\to\infty} \|a_n\| = \lim\limits_{n\to\infty} \|b_n\|$.

Uwaga

Niech K będzie ciałem z normą $\|,\|$ i niech (a_n) będzie ciągiem Cauchy'ego w K. Wówczas:

- Ciąg $\|a_n\|$ jest zbieżny.
- Jeśli $(b_n) \sim (a_n)$, to $\lim\limits_{n\to\infty} \|a_n\| = \lim\limits_{n\to\infty} \|b_n\|$.

Dowód.

- Mamy:
$$|\,\|a_n\| - \|a_m\|\,| \leq \|a_n - a_m\|.$$
co oznacza, że ciąg $\|a_n\|$ jest ciągiem Cauchy'ego w $\mathbb{R}$, czyli ciągiem zbieżnym.

- Jeśli $(b_n) \sim (a_n)$, to:
$$0 \leq \lim_{n\to\infty} |\,\|a_n\| - \|b_n\|\,| \leq \lim_{n\to\infty} \|a_n - b_n\| = 0.$$

Twierdzenie - ćwiczenie (argumenty są te same co na AM I)

Niech K będzie ciałem i $\|.\|$ – normą na K. Wówczas:

- na ciele $\widehat{K}$ określona jest norma $\|.\|$ dana wzorem:

$$\|[(a_n)]\| = \lim_{n\to\infty} \|a_n\|,$$

Twierdzenie - ćwiczenie (argumenty są te same co na AM I)

Niech K będzie ciałem i $\|.\|$ – normą na K. Wówczas:

- na ciele $\widehat{K}$ określona jest norma $\|.\|$ dana wzorem:

$$\|[(a_n)]\| = \lim_{n\to\infty} \|a_n\|,$$

- przy utożsamieniu $k \in K \mapsto [\widehat{k}]$ ciało K traktować można jako gęsty podzbiór w $\widehat{K}$, tzn. dla każdego $[(a_n)] \in \widehat{K}$ i dla każdego $\epsilon > 0$ istnieje $k \in K$ takie, że

$$\|[a_n] - [\widehat{k}]\| < \epsilon,$$

Twierdzenie - ćwiczenie (argumenty są te same co na AM I)

Niech K będzie ciałem i $\|.\|$ – normą na K. Wówczas:

- na ciele $\widehat{K}$ określona jest norma $\|.\|$ dana wzorem:
$$\|[(a_n)]\| = \lim_{n\to\infty} \|a_n\|,$$
- przy utożsamieniu $k \in K \mapsto [\widehat{k}]$ ciało K traktować można jako gęsty podzbiór w $\widehat{K}$, tzn. dla każdego $[(a_n)] \in \widehat{K}$ i dla każdego $\epsilon > 0$ istnieje $k \in K$ takie, że
$$\|[a_n] - [\widehat{k}]\| < \epsilon,$$
- przestrzeń $\widehat{K}$ z metryką wyznaczoną przez normę $\|.\|$ jest zupełna,

Twierdzenie - ćwiczenie (argumenty są te same co na AM I)

Niech K będzie ciałem i $\|.\|$ – normą na K. Wówczas:

- na ciele $\widehat{K}$ określona jest norma $\|.\|$ dana wzorem:

$$\|[(a_n)]\| = \lim_{n\to\infty} \|a_n\|,$$

- przy utożsamieniu $k \in K \mapsto [\widehat{k}]$ ciało K traktować można jako gęsty podzbiór w $\widehat{K}$, tzn. dla każdego $[(a_n)] \in \widehat{K}$ i dla każdego $\epsilon > 0$ istnieje $k \in K$ takie, że

$$\|[a_n] - [\widehat{k}]\| < \epsilon,$$

- przestrzeń $\widehat{K}$ z metryką wyznaczoną przez normę $\|.\|$ jest zupełna,
- jeśli $\lim\limits_{n\to\infty} A_n = [(a_n)]$, $\lim\limits_{n\to\infty} B_n = [(b_n)]$, dla pewnych $A_n, B_n, [(a_n)], [(b_n)] \in \widehat{K}$, to

$$[(a_n)] + [(b_n)] = \lim_{n\to\infty} A_n + B_n, \quad [(a_n)] \cdot [(b_n)] = \lim_{n\to\infty} A_n \cdot B_n.$$

Definicja

Niech $\mathbb{Q}$ będzie ciałem z metryką wyznaczoną przez normę p-adyczną. Wówczas ciało $\widehat{\mathbb{Q}}$ nazywamy **ciałem liczb *p*-adycznych**, ozn. $\mathbb{Q}_p$.

Definicja

Niech $\mathbb{Q}$ będzie ciałem z metryką wyznaczoną przez normę p-adyczną. Wówczas ciało $\widehat{\mathbb{Q}}$ nazywamy **ciałem liczb p-adycznych**, ozn. $\mathbb{Q}_p$.

Podstawowe twierdzenie

Dla $0 < m \in \mathbb{Z}$ niech $d_{-m}, \ldots, d_0, d_1, \ldots$ będą nieujemnymi liczbami całkowitymi mniejszymi niż p, przy czym $d_{-m} > 0$. Rozważmy szereg:

$$d_{-m}p^{-m} + d_{-m+1}p^{-m+1} + \ldots + d_0 + d_1 p + d_2 p^2 \ldots \qquad (*).$$

Wówczas:

- sumy częściowe szeregu $(*)$ tworzą ciąg Cauchy'ego w $\mathbb{Q}$ (względem $|.|_p$),
- dla każdego elementu $A \in \mathbb{Q}_p$ istnieje dokładnie jeden reprezentujący go ciąg Cauchy'ego (A_i), którego wyrazami są sumy cześciowe szeregu typu $(*)$.

Dowód.

Sumy częściowe $(*)$ tworzą ciąg Cauchy'ego względem normy $|.|_p$, bo dla każdego $\epsilon > 0$ można wskazać N takie, że $p^{-N} < \epsilon$, i dla $k > n > N$ mamy:

$$\left|\sum_{i=-m}^{k} d_i p^i - \sum_{i=-m}^{n} d_i p_i\right|_p = \left|\sum_{i=n+1}^{k} d_i p^i\right|_p \leq \max_{n<i\leq k} |d_i p^i|_p \leq p^{-N} < \epsilon.$$

Dowód.

Sumy częściowe $(*)$ tworzą ciąg Cauchy'ego względem normy $|.|_p$, bo dla każdego $\epsilon > 0$ można wskazać N takie, że $p^{-N} < \epsilon$, i dla $k > n > N$ mamy:

$$\left|\sum_{i=-m}^{k} d_i p^i - \sum_{i=-m}^{n} d_i p_i\right|_p = \left|\sum_{i=n+1}^{k} d_i p^i\right|_p \leq \max_{n<i\leq k} |d_i p^i|_p \leq p^{-N} < \epsilon.$$

Dowód jednoznaczności rozwinięcia w szereg $(*)$ rozpoczniemy od $\mathbb{Q}$.

Lemat podstawowy

Jeśli $x \in \mathbb{Q}$ oraz $|x|_p \leq 1$, to dla każdego całkowitego $i \geq 1$ istnieje dokładnie jedna liczba liczba całkowita $x_i \in \{0, 1, 2, \ldots, p^i - 1\}$ taka, że $|x_i - x|_p \leq p^{-i}$.

Idea: liczba x oraz x_i mają te same i cyfr (od prawej) postaci $d_i = x_{i+1} - x_i \in \{0, 1, \ldots, p - 1\}$ (gdzie $d_0 = x_1$) w tym, co nazwiemy za kilka slajdów rozwinięciem p-adycznym x (jak już wykażemy zbieżność $(*)$).

Dowód Lematu Podstawowego. Niech $x \in \mathbb{Q}$ oraz $|x|_p \leq 1$, to dla każdego i istnieje dokładnie jedna liczba liczba całkowita $x_i \in \{0, 1, 2, \ldots, p^i - 1\}$ taka, że $|x_i - x|_p \leq p^{-i}$.

Dowód Lematu Podstawowego. Niech $x \in \mathbb{Q}$ oraz $|x|_p \leq 1$, to dla każdego i istnieje dokładnie jedna liczba liczba całkowita $x_i \in \{0, 1, 2, \ldots, p^i - 1\}$ taka, że $|x_i - x|_p \leq p^{-i}$.

- Niech $x = a/b$, gdzie $\mathrm{NWD}(a, b) = 1$. Skoro $|a/b|_p \leq 1$, to

$$\mathrm{NWD}(b, p^i) = 1.$$

Dowód Lematu Podstawowego. Niech $x \in \mathbb{Q}$ oraz $|x|_p \leq 1$, to dla każdego i istnieje dokładnie jedna liczba liczba całkowita $x_i \in \{0, 1, 2, \ldots, p^i - 1\}$ taka, że $|x_i - x|_p \leq p^{-i}$.

- Niech $x = a/b$, gdzie $\mathrm{NWD}(a, b) = 1$. Skoro $|a/b|_p \leq 1$, to
$$\mathrm{NWD}(b, p^i) = 1.$$
- Z lematu Bezout istnieją $m, n \in \mathbb{Z}$, że $mb + np^i = 1$.

Dowód Lematu Podstawowego. Niech $x \in \mathbb{Q}$ oraz $|x|_p \leq 1$, to dla każdego i istnieje dokładnie jedna liczba liczba całkowita $x_i \in \{0, 1, 2, \ldots, p^i - 1\}$ taka, że $|x_i - x|_p \leq p^{-i}$.

- Niech $x = a/b$, gdzie $\mathrm{NWD}(a, b) = 1$. Skoro $|a/b|_p \leq 1$, to
$$\mathrm{NWD}(b, p^i) = 1.$$
- Z lematu Bezout istnieją $m, n \in \mathbb{Z}$, że $mb + np^i = 1$.
- Niech $y_i = am$. Wówczas:
$$\begin{aligned} |y_i - x|_p = |am - a/b|_p &= |a/b|_p \cdot |mb - 1|_p \\ &\leq |mb - 1|_p = |np^i|_p = |n|_p \cdot p^{-i} \leq p^{-i}. \end{aligned}$$

Dowód Lematu Podstawowego. Niech $x \in \mathbb{Q}$ oraz $|x|_p \leq 1$, to dla każdego i istnieje dokładnie jedna liczba liczba całkowita $x_i \in \{0, 1, 2, \dots, p^i - 1\}$ taka, że $|x_i - x|_p \leq p^{-i}$.

- Niech $x = a/b$, gdzie $\mathrm{NWD}(a, b) = 1$. Skoro $|a/b|_p \leq 1$, to
$$\mathrm{NWD}(b, p^i) = 1.$$
- Z lematu Bezout istnieją $m, n \in \mathbb{Z}$, że $mb + np^i = 1$.
- Niech $y_i = am$. Wówczas:
$$\begin{aligned} |y_i - x|_p &= |am - a/b|_p = |a/b|_p \cdot |mb - 1|_p \\ &\leq |mb - 1|_p = |np^i|_p = |n|_p \cdot p^{-i} \leq p^{-i}. \end{aligned}$$
- Korzystając z nierówności $|x + y|_p \leq \max\{|x|_p, |y|_p\}$, prawdziwej dla każdych $x, y \in \mathbb{Q}$ możemy dodać do y_i całkowitą wielokrotność p^i i dzięki szacowaniu
$$|y_i + sp^i - x|_p \leq \max\{|y_i - x|_p, |sp^i|_p\} \leq p^{-i}.$$
dostać jedyną liczbę całkowitą x_i pomiędzy 0 a p^i, dla której $|x_i - x|_p \leq p^{-i}$.

Przechodzimy do dowodu jednoznaczności rozwinięcia w szereg $(*)$ dla $\mathbb{Q}_p$..

Twierdzenie

Każdy element $A \in \mathbb{Q}_p$ o własności $|A|_p \leq 1$ reprezentowany jest przez dokładnie jeden ciąg Cauchy'ego (A_i) o wyrazach całkowitych spełniający $A = [(A_i)]$ oraz:

(i) $0 \leq A_i < p^i$, dla $i = 1, 2, \ldots$

(ii) $A_i \equiv A_{i+1} \bmod p^i$, dla $i = 1, 2, \ldots$.

Przechodzimy do dowodu jednoznaczności rozwinięcia w szereg $(*)$ dla $\mathbb{Q}_p$..

Twierdzenie

Każdy element $A \in \mathbb{Q}_p$ o własności $|A|_p \leq 1$ reprezentowany jest przez dokładnie jeden ciąg Cauchy'ego (A_i) o wyrazach całkowitych spełniający $A = [(A_i)]$ oraz:

(i) $0 \leq A_i < p^i$, dla $i = 1, 2, \ldots$

(ii) $A_i \equiv A_{i+1} \mod p^i$, dla $i = 1, 2, \ldots$.

Gdy $A \in \mathbb{Q}_p$ spełnia $|A|_p \leq 1$, wówczas wygodnie jest przedstawiać wyrazy ciągu (A_i) określonego w sformułowaniu twierdzenia formułami $A_i = d_0 + \ldots + d_{i-1}p^{i-1}$, gdzie wszystkie $d_i \in \{0, 1, \ldots, p-1\}$. Własność $A_{i+1} \equiv A_i \mod p^i$ daje nam:

$$A_{i+1} = d_0 + d_1 p + \ldots + d_{i-1}p^{i-1} + d_i p^i,$$

Jest więc sens przedstawiać A w postaci szeregu zbieżnego w $|.|_p$ postaci:

$$A = \sum_{n=0}^{\infty} d_n p^n, \qquad (\dagger).$$

Przechodzimy do dowodu jednoznaczności rozwinięcia w szereg $(*)$ dla $\mathbb{Q}_p$..

Twierdzenie

Każdy element $A \in \mathbb{Q}_p$ o własności $|A|_p \leq 1$ reprezentowany jest przez dokładnie jeden ciąg Cauchy'ego (A_i) o wyrazach całkowitych spełniający $A = [(A_i)]$ oraz:

(i) $0 \leq A_i < p^i$, dla $i = 1, 2, \ldots$

(ii) $A_i \equiv A_{i+1} \bmod p^i$, dla $i = 1, 2, \ldots$.

Jeśli $|A|_p > 1$, wtedy mnożymy A przez potęgę p równą $|A|_p$ i dostając liczbę p-adyczną postaci $A' = Ap^m$, gdzie $|A'|_p = 1$. Możemy więc napisać:

$$A = \sum_{n=-m}^{\infty} d_n p^n, \qquad (\dagger\dagger)$$

gdzie $d_{-m} \neq 0$.

Definicja

Niech $A \in \mathbb{Q}_p$. Wówczas:

- jeśli $|A|_p \leq 1$ oraz A jest opisana jednoznacznie szeregiem (†), to przedstawienie
$$A = \ldots d_n \ldots d_2 d_1 d_0$$
nazywamy (kanonicznym) **rozwinięciem** p-adycznym liczby A.

- jeśli $|A|_p > 1$ oraz A jest opisana jednoznacznie szeregiem (††), to przedstawienie:
$$A = \ldots d_n \ldots d_2 d_1 d_0, d_{-1} \ldots d_{-m}$$
nazywamy (kanonicznym) **rozwinięciem** p-adycznym liczby A.

Uwaga. Rozwinięcie p-adyczne jest jednoznaczne. Jest to oczywiście kontrast do sytuacji z rozwinięciami nad $\mathbb{R}$.

Dowód tego, że każdy element $A \in \mathbb{Q}_p$ o własności $|A|_p \leq 1$ reprezentowany jest przez dokładnie jeden ciąg Cauchy'ego (A_i) w $(\mathbb{Q}, |.|_p)$ spełniający: $A_i \in \mathbb{Z}, 0 \leq A_i < p^i$, dla $i = 1, 2, \ldots$ oraz $A_i \equiv A_{i+1} \mod p^i$, dla $i = 1, 2, \ldots$.

Dowód tego, że każdy element $A \in \mathbb{Q}_p$ o własności $|A|_p \leq 1$ reprezentowany jest przez dokładnie jeden ciąg Cauchy'ego (A_i) w $(\mathbb{Q}, |.|_p)$ spełniający: $A_i \in \mathbb{Z}, 0 \leq A_i < p^i$, dla $i = 1, 2, \ldots$ oraz $A_i \equiv A_{i+1} \mod p^i$, dla $i = 1, 2, \ldots$.

- Niech ciąg Cauchy'ego (b_i) reprezentuje element $A \in \mathbb{Q}_p$, gdzie $|A|_p \leq 1$. Oczywiście $\lim_{n \to \infty} |b_i|_p = |A|_p \leq 1$, więc można zakładać, że $|b_i|_p \leq 1$.

Dowód tego, że każdy element $A \in \mathbb{Q}_p$ o własności $|A|_p \leq 1$ reprezentowany jest przez dokładnie jeden ciąg Cauchy'ego (A_i) w $(\mathbb{Q}, |.|_p)$ spełniający: $A_i \in \mathbb{Z}, 0 \leq A_i < p^i$, dla $i = 1, 2, \ldots$ oraz $A_i \equiv A_{i+1} \mod p^i$, dla $i = 1, 2, \ldots$.

- Niech ciąg Cauchy'ego (b_i) reprezentuje element $A \in \mathbb{Q}_p$, gdzie $|A|_p \leq 1$. Oczywiście $\lim_{n \to \infty} |b_i|_p = |A|_p \leq 1$, więc można zakładać, że $|b_i|_p \leq 1$.
- Korzystamy najpierw z faktu, że (b_n) jest Cauchy'ego i dla każdego $j = 1, \ldots,$ dobieramy dodatnią liczbę całkowitą $N(j)$ taką, że dla każdych $i, i' \geq N(j)$:

$$|b_i - b_{i'}|_p \leq p^{-j}.$$

  Można założyć, że $N(j)$ jest ściśle rosnący, więc $N(j) \geq j$.

Dowód tego, że każdy element $A \in \mathbb{Q}_p$ o własności $|A|_p \leq 1$ reprezentowany jest przez dokładnie jeden ciąg Cauchy'ego (A_i) w $(\mathbb{Q}, |.|_p)$ spełniający: $A_i \in \mathbb{Z}, 0 \leq A_i < p^i$, dla $i = 1, 2, \ldots$ oraz $A_i \equiv A_{i+1} \bmod p^i$, dla $i = 1, 2, \ldots$.

- Niech ciąg Cauchy'ego (b_i) reprezentuje element $A \in \mathbb{Q}_p$, gdzie $|A|_p \leq 1$. Oczywiście $\lim\limits_{n\to\infty} |b_i|_p = |A|_p \leq 1$, więc można zakładać, że $|b_i|_p \leq 1$.
- Korzystamy najpierw z faktu, że (b_n) jest Cauchy'ego i dla każdego $j = 1, \ldots,$ dobieramy dodatnią liczbę całkowitą $N(j)$ taką, że dla każdych $i, i' \geq N(j)$:

  $$|b_i - b_{i'}|_p \leq p^{-j}.$$

  Można założyć, że $N(j)$ jest ściśle rosnący, więc $N(j) \geq j$.
- Na podstawie Lematu Podstawowego dla każdego j znajdujemy liczby całkowite A_j, gdzie $0 \leq A_j < p^j$ oraz:

  $$|A_j - b_{N(j)}|_p \leq p^{-j}.$$

Dowód tego, że każdy element $A \in \mathbb{Q}_p$ o własności $|A|_p \leq 1$ reprezentowany jest przez dokładnie jeden ciąg Cauchy'ego (A_i) w $(\mathbb{Q}, |.|_p)$ spełniający: $A_i \in \mathbb{Z}, 0 \leq A_i < p^i$, dla $i = 1, 2, \ldots$ oraz $A_i \equiv A_{i+1} \bmod p^i$, dla $i = 1, 2, \ldots$.

- Niech ciąg Cauchy'ego (b_i) reprezentuje element $A \in \mathbb{Q}_p$, gdzie $|A|_p \leq 1$. Oczywiście $\lim\limits_{n\to\infty} |b_i|_p = |A|_p \leq 1$, więc można zakładać, że $|b_i|_p \leq 1$.
- Korzystamy najpierw z faktu, że (b_n) jest Cauchy'ego i dla każdego $j = 1, \ldots,$ dobieramy dodatnią liczbę całkowitą $N(j)$ taką, że dla każdych $i, i' \geq N(j)$:
$$|b_i - b_{i'}|_p \leq p^{-j}.$$
Można założyć, że $N(j)$ jest ściśle rosnący, więc $N(j) \geq j$.
- Na podstawie Lematu Podstawowego dla każdego j znajdujemy liczby całkowite A_j, gdzie $0 \leq A_j < p^j$ oraz:
$$|A_j - b_{N(j)}|_p \leq p^{-j}.$$
- Wykażemy teraz, że ciąg (A_n) jest równoważny do (b_n) oraz spełnia (i), (ii).

Dowód tego, że każdy element $A \in \mathbb{Q}_p$ o własności $|A|_p \leq 1$ reprezentowany jest przez dokładnie jeden ciąg Cauchy'ego (A_i) w $(\mathbb{Q}, |.|_p)$ spełniający: $A_i \in \mathbb{Z}, 0 \leq A_i < p^i$, dla $i = 1, 2, \ldots$ oraz $A_i \equiv A_{i+1} \mod p^i$, dla $i = 1, 2, \ldots$.

Dowód tego, że każdy element $A \in \mathbb{Q}_p$ o własności $|A|_p \leq 1$ reprezentowany jest przez dokładnie jeden ciąg Cauchy'ego (A_i) w $(\mathbb{Q}, |.|_p)$ spełniający: $A_i \in \mathbb{Z}, 0 \leq A_i < p^i$, dla $i = 1, 2, \ldots$ oraz $A_i \equiv A_{i+1} \mod p^i$, dla $i = 1, 2, \ldots$.

- Pokażmy, że $A_j \equiv A_{j+1} \mod p^j$. Mamy:

$$\begin{aligned} |A_{j+1} - A_j|_p &= |A_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (A_j - b_{N(j)})|_p \\ &\leq \max(|A_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p, |A_j - b_{N(j)}|_p) \\ &\leq \max(p^{-(j+1)}, p^{-j}, p^{-j}) = p^{-j}. \end{aligned}$$

Przy okazji dostaliśmy, że dla $i \geq N(j)$ mamy $|A_i - A_j|_p \leq p^{-j}$.

Dowód tego, że każdy element $A \in \mathbb{Q}_p$ o własności $|A|_p \leq 1$ reprezentowany jest przez dokładnie jeden ciąg Cauchy'ego (A_i) w $(\mathbb{Q}, |.|_p)$ spełniający: $A_i \in \mathbb{Z}, 0 \leq A_i < p^i$, dla $i = 1, 2, \ldots$ oraz $A_i \equiv A_{i+1} \bmod p^i$, dla $i = 1, 2, \ldots$.

- Pokażmy, że $A_j \equiv A_{j+1} \bmod p^j$. Mamy:

$$\begin{aligned} |A_{j+1} - A_j|_p &= |{\color{red}A_{j+1} - b_{N(j+1)}} + {\color{blue}b_{N(j+1)} - b_{N(j)}} - (A_j - b_{N(j)})|_p \\ &\leq \max(|{\color{red}A_{j+1} - b_{N(j+1)}}|_p, |{\color{blue}b_{N(j+1)} - b_{N(j)}}|_p, |A_j - b_{N(j)}|_p) \\ &\leq \max(p^{-(j+1)}, p^{-j}, p^{-j}) = p^{-j}. \end{aligned}$$

  Przy okazji dostaliśmy, że dla $i \geq N(j)$ mamy $|A_i - A_j|_p \leq p^{-j}$.

- Weźmy dowolny j. Wtedy dla każdego $i \geq N(j)$ mamy:

$$\begin{aligned} |A_i - b_i|_p &= |A_i - A_j + A_j - b_{N(j)} - (b_i - b_{N(j)})|_p \\ &\leq \max(|A_i - A_j|_p, |A_j - b_{N(j)}|_p, |b - b_{N(j)}|_p) \\ &\leq \max(p^{-j}, p^{-j}, p^{-j}) = p^{-j}. \end{aligned}$$

  Stąd $\lim_{n\to\infty} |A_n - b_n|_p = 0$.

Dowód tego, że każdy element $A \in \mathbb{Q}_p$ o własności $|A|_p \leq 1$ reprezentowany jest przez dokładnie jeden ciąg Cauchy'ego (A_i) w $(\mathbb{Q}, |.|_p)$ spełniający: $A_i \in \mathbb{Z}, 0 \leq A_i < p^i$, dla $i = 1, 2, \ldots$ oraz $A_i \equiv A_{i+1} \bmod p^i$, dla $i = 1, 2, \ldots$.

- Dowodzimy jednoznaczność (A_i). Jeśli ciąg (A'_i) ma własności (i) i (ii) oraz $A_{i_0} \neq A'_{i_0}$ dla pewnego i_0, to mamy

  $$A_{i_0} \not\equiv A'_{i_0} \bmod p^{i_0}$$

  bo obydwie te liczby są pomiędzy 0 a p^{i_0}.

Dowód tego, że każdy element $A \in \mathbb{Q}_p$ o własności $|A|_p \leq 1$ reprezentowany jest przez dokładnie jeden ciąg Cauchy'ego (A_i) w $(\mathbb{Q}, |.|_p)$ spełniający: $A_i \in \mathbb{Z}, 0 \leq A_i < p^i$, dla $i = 1, 2, \ldots$ oraz $A_i \equiv A_{i+1} \mod p^i$, dla $i = 1, 2, \ldots$.

- Dowodzimy jednoznaczność (A_i). Jeśli ciąg (A'_i) ma własności (i) i (ii) oraz $A_{i_0} \neq A'_{i_0}$ dla pewnego i_0, to mamy

$$A_{i_0} \not\equiv A'_{i_0} \mod p^{i_0}$$

  bo obydwie te liczby są pomiędzy 0 a p^{i_0}.

- Z drugiej strony dla $i > i_0$ mamy

$$A_i \equiv A_{i_0} \mod p^{i_0}, \text{ oraz } A'_{i_0} \equiv A'_i \mod p^{i_0},$$

  czyli $A_i \not\equiv A'_i \mod p^{i_0}$.

Dowód tego, że każdy element $A \in \mathbb{Q}_p$ o własności $|A|_p \leq 1$ reprezentowany jest przez dokładnie jeden ciąg Cauchy'ego (A_i) w $(\mathbb{Q}, |.|_p)$ spełniający: $A_i \in \mathbb{Z}, 0 \leq A_i < p^i$, dla $i = 1, 2, \ldots$ oraz $A_i \equiv A_{i+1} \bmod p^i$, dla $i = 1, 2, \ldots$.

- Dowodzimy jednoznaczność (A_i). Jeśli ciąg (A'_i) ma własności (i) i (ii) oraz $A_{i_0} \neq A'_{i_0}$ dla pewnego i_0, to mamy

$$A_{i_0} \not\equiv A'_{i_0} \bmod p^{i_0}$$

  bo obydwie te liczby są pomiędzy 0 a p^{i_0}.

- Z drugiej strony dla $i > i_0$ mamy

$$A_i \equiv A_{i_0} \bmod p^{i_0}, \text{ oraz } A'_{i_0} \equiv A'_i \bmod p^{i_0},$$

  czyli $A_i \not\equiv A'_i \bmod p^{i_0}$.

- Stąd dla każdego $i \geq i_0$ mamy:

$$|A_i - A'_i|_p > p^{-i_0},$$

  co oznacza, że $(A_i) \not\sim (A'_i)$, co kończy dowód.

Ilustracje rozwinięć p-adycznych dla liczb wymiernych (zawartych w $\mathbb{Q}_p$).

Ilustracje rozwinięć *p*-adycznych dla liczb wymiernych (zawartych w $\mathbb{Q}_p$).

- Liczba 320 ma rozwinięcie $5 + 3 \cdot 7 + 6 \cdot 7^2 = 635$.

Ilustracje rozwinięć p-adycznych dla liczb wymiernych (zawartych w $\mathbb{Q}_p$).

- Liczba 320 ma rozwinięcie $5 + 3 \cdot 7 + 6 \cdot 7^2 = 635$.
- Liczba -1 ma przedstawienie $-1 = 6 + 6 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 = \ldots 6666$.

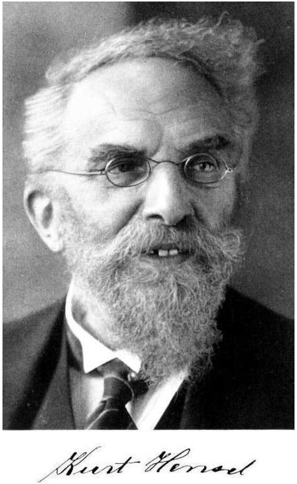
Ilustracje rozwinięć p-adycznych dla liczb wymiernych (zawartych w $\mathbb{Q}_p$).

- Liczba 320 ma rozwinięcie $5 + 3 \cdot 7 + 6 \cdot 7^2 = 635$.
- Liczba -1 ma przedstawienie $-1 = 6 + 6 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 = \ldots 6666$.
- Liczba $\frac{1}{2}$ ma przedstawienie $3 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + \ldots = \ldots 2223$.

  Powód? $1 = 2(d_0 + d_1 p + d_2 p^2 + \ldots)$, więc mamy układ kongruencji:

$$\begin{cases} 1 = 2d_0 & \bmod 5 \\ 1 = 2d_0 + 2d_1 \cdot 5 & \bmod 5^2 \\ 1 = 2d_0 + 2d_1 \cdot 5 + 2d_2 \cdot 5^2 & \bmod 5^3 \\ & \vdots \end{cases} \Rightarrow \begin{cases} d_0 & = 3 \\ d_1 & = 2 \\ d_2 & = 2 \\ & \vdots \end{cases}.$$

- A jak jest dla liczb, które nie są wymierne? Można postępować podobnie, ale nie zawsze znajdziemy rozwiązania (na przykład niektórych pierwiastków kwadratowych nie ma w niektórych $\mathbb{Q}_p$). O tym na następnym wykładzie.



Kurt Hensel (1861-1941). Odkrywca liczb *p*-adycznych.