TWIERDZENIE OSTROWSKIEGO
WITOLD TOMASZEWSKI

Definicja 1. Normą w ciele $\mathbb{F}$ nazywamy odwzorowanie $||.||$ z $\mathbb{F}$ w liczby rzeczywiste nieujemne, takie że:
1. $||x|| = 0$ wtedy i tylko wtedy gdy $x = 0$,
2. $||x \cdot y|| = ||x|| \cdot ||y||$,
3. $||x + y|| \leq ||x|| + ||y||$ (*nierówność trójkąta*).

Uwaga 1. Z warunków 2. i 1. wynika, że $||1|| = 1$, $||-a|| = ||a||$ i $||a^k|| = ||a||^k$ dla $a \neq 0$ i dowolnej liczby całkowitej k.

Norma $||.||$ indukuje metrykę na $\mathbb{F}$:
$$d(x, y) = ||x - y||.$$

Definicja 2. Ciąg liczb wymiernych $(a_n)_{n\in\mathbb{N}}$ nazywamy ciągiem Cauchy'ego względem metryki d jeśli spełnia warunek:
$$\forall_{\varepsilon>0}\ \exists_{N\in\mathbb{N}}\ \forall_{n,m>N}\ \ d(a_n, a_m) < \varepsilon.$$

Definicja 3. Mówimy, że metryki d_1 i d_2 określone na tym samym zbiorze X są równoważne jeżeli każdy ciąg Cauchy'ego względem pierwszej metryki jest ciągiem Cauchy'ego względem drugiej metryki i odwrotnie każdy ciąg Cauchy'ego względem drugiej metryki jest ciągiem Cauchy'ego względem pierwszej metryki.

Mówimy, że dwie normy sa równoważne, jeżeli odpowiadające im metryki sa równoważne.

Stwierdzenie 1. *Jeśli $||.||_1$ i $||.||_2$ są normami na ciele $\mathbb{F}$ oraz istnieje $\alpha > 0$ taka, że $||x||_1 = ||x||_2^\alpha$ dla każdego $x \in \mathbb{F}$ to normy $||.||_1$ i $||.||_2$ są równoważne.*

Normy w ciele liczb wymiernych $\mathbb{Q}$

1. $||x|| = |x|^\alpha$ dla pewnego $0 < \alpha \leq 1$. Każda taka norma jest równoważna normie $|.|$.
2. Norma trywialna tj. norma taka, że $||x|| = 0$ jeśli $x = 0$ i $||x|| = 1$ jeśli $x \neq 0$.
3. Normy p-adyczne. Niech p będzie liczbą pierwszą. Dla każdej niezerowej liczby całkowitej a określamy wartość $\mathrm{ord}_p(a)$ (zwaną *p-adic-ordinal*), jako najwyższą potęgę liczby p dzielącą a. Na przykład: $\mathrm{ord}_2(7) = 0$; $\mathrm{ord}_3(9) = 2$; $\mathrm{ord}_3(18) = 2$. Dodatkowo przyjmujemy $\mathrm{ord}_p(0) = 1$. Funkcja ord_p ma własność logarytmu:

$$\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b). \tag{1}$$

Jeśli $x = \frac{a}{b}$ jest liczbą wymierną to definiujemy
$$\mathrm{ord}_p(x) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b).$$

Zauważmy, że wartość $\operatorname{ord}_p(x)$ zależy tylko od x a nie od zapisu w postaci $x = \frac{a}{b}$. Niech zatem $x = \frac{ca}{cb}$ dla pewnego $c \in \mathbb{Z}, c \neq 0$. Mamy wtedy:

$$\operatorname{ord}_p\left(\frac{ca}{cb}\right) = \operatorname{ord}_p(ca) - \operatorname{ord}_p(cb) \overset{(1)}{=}$$
$$\operatorname{ord}_p(c) + \operatorname{ord}_p(a) - \operatorname{ord}_p(c) - \operatorname{ord}_p(b) =$$
$$\operatorname{ord}_p(a) - \operatorname{ord}_p(b) = \operatorname{ord}_p(\tfrac{a}{b}).$$

Teraz definiujemy normę na $\mathbb{Q}$ następująco:

$$|x|_p = \begin{cases} p^{-\operatorname{ord}_p(x)} & \text{jeśli} \quad x \neq 0, \\ 0 & \text{jeśli} \quad x = 0. \end{cases}$$

Stwierdzenie 2. *$|.|_p$ jest normą na $\mathbb{Q}$.*

Dowód. Warunki 1. i 2. definicji 1 są łatwe do sprawdzenia. Sprawdzimy warunek 3. Dosyć łatwo można sprawdzić ten warunek gdy $x = 0$ lub $y = 0$ lub $x + y = 0$. Załóżmy więc, że $x, y, x + y$ są różne od zera. Niech $x = a/b$, $y = c/d$. Wtedy $x+y = (ad+bc)/bd$, a stąd mamy $\operatorname{ord}_p(x+y) = \operatorname{ord}_p(ad+bc) - \operatorname{ord}_p(b) - \operatorname{ord}_p(d)$. Zauważmy ze najwyższa potęga p dzieląca sumę dwóch liczb całkowitych jest większa bądź równa minimum z najwyższych potęg liczby p dzielących pierwszą i drugą liczbę. Mamy więc:

$$\operatorname{ord}_p(x + y) \geq \min(\operatorname{ord}_p(ad); \operatorname{ord}_p(bc)) - \operatorname{ord}_p(b) - \operatorname{ord}_p(d) =$$
$$\min(\operatorname{ord}_p(a) + \operatorname{ord}_p(d), \operatorname{ord}_p(b) + \operatorname{ord}_p(c)) - \operatorname{ord}_p(b) - \operatorname{ord}_p(d) =$$
$$\min(\operatorname{ord}_p(a) - \operatorname{ord}_p(b), \operatorname{ord}_p(c) - \operatorname{ord}_p(d)) = \min(\operatorname{ord}_p(x), \operatorname{ord}_p(y)) =$$
$$-\max(-\operatorname{ord}_p x, -\operatorname{ord}_p y).$$

Przejście między drugą, a trzecią linijką nie powinno sprawiać problemu. Stąd mamy

$$|x + y|_p = p^{-\operatorname{ord}_p(x+y)} \leq p^{max(-\operatorname{ord}_p(x), -\operatorname{ord}_p y)} =$$
$$\max(p^{-\operatorname{ord}_p(x)}, p^{-\operatorname{ord}_p(y)}) = \max(|x|_p, |y|_p) \leq |x|_p + |y|_p.$$

□

Stwierdzenie 3. *Jeżeli $0 < \lambda < 1$ to funkcja*

$$||x|| = \begin{cases} \lambda^{\operatorname{ord}_p(x)} & \textit{jeśli} \quad x \neq 0, \\ 0 & \textit{jeśli} \quad x = 0. \end{cases}$$

jest normą w ciele $\mathbb{Q}$, równoważną z normą $|.|_p$.

Dowód. Fakt ze $||.||$ jest normą na $\mathbb{Q}$ można udowodnić analogicznie jak w dowodzie Stwierdzenia 2. Równoważność norm wynika ze Stwierdzenia 1. □

Twierdzenie 1 (Ostrowski)**.** *Każda nietrywialna norma na $\mathbb{Q}$ jest równoważna normie $|.|_p$ lub normie $|.|$.*

Dowód. **1.** Załóżmy ze istnieje $n \in \mathbb{N}$ takie, że $||n|| > 1$. Niech n_0 będzie najmniejszą taką liczbą naturalną, że $||n_0|| > 1$. Z Uwagi 1 wynika, że $n_0 > 1$. Ponieważ $n_0 > 1$ i $||n_0|| > 1$ to istnieje $\alpha > 0$ taka, że $||n_0|| = n_0^\alpha$. Weźmy dowolne n i zapiszmy je w systemie pozycyjnym przy podstawie n_0:

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \ldots + a_{s(n)} n_0^{s(n)} \tag{2}$$

gdzie $0 \leq a_i < n_0$ i $a_{s(n)} \neq 0$. Ponieważ n_0 jest najmniejszą liczbą naturalną o własności $||n_0|| > 1$ to $||a_i|| \leq 1$ dla $i = 0, \ldots, s(n)$. Zachodzi też $n_0^{s(n)} \leq n$. Stąd mamy:

$$\begin{aligned}
&||n|| \leq ||a_0|| + ||a_1 n_0|| + ||a_2 n_0^2|| + \ldots + ||a_{s(n)} n_0^{s(n)}|| = \\
&||a_0|| + ||a_1|| \cdot ||n_0|| + ||a_2|| \cdot ||n_0^2|| + \ldots + ||a_{s(n)}|| \cdot ||n_0^{s(n)}|| = \\
&||a_0|| + ||a_1|| \cdot n_0^\alpha + ||a_2|| \cdot n_0^{2\alpha} + \ldots + ||a_{s(n)}|| \cdot n_0^{s(n)\alpha} \leq \\
&1 + n_0^\alpha + n_0^{2\alpha} + \ldots + n_0^{s(n)\alpha} \leq \\
&n_0^{s(n)\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \ldots + n_0^{-s(n)\alpha}) \leq n^\alpha \sum_{i=0}^{s(n)} \left(\frac{1}{n_0^\alpha}\right)^i \leq n^\alpha \sum_{i=0}^{\infty} \left(\frac{1}{n_0^\alpha}\right)^i.
\end{aligned}$$

Zatem istnieje stała $C = \sum_{i=0}^{\infty} \left(\frac{1}{n_0^\alpha}\right)^i$ taka, że

$$||n|| \leq C n^\alpha,$$

dla każdej liczby naturalnej n (chyba jest jasne, że szereg $\sum_{i=0}^{\infty} \left(\frac{1}{n_0^\alpha}\right)^i$ jest zbieżny).

Weźmy teraz dowolne $n, k \in \mathbb{N}$. Wtedy $||n^k|| = ||n||^k \leq C n^{k\alpha}$, więc:

$$||n|| \leq \sqrt[k]{C} n^\alpha.$$

Możemy zastosować przejście graniczne $k \to \infty$. Ponieważ $\lim_{k\to\infty} \sqrt[k]{C} = 1$ to otrzymujemy $||n|| \leq n^\alpha$, dla każdej liczby naturalnej n.

Liczba n zapisana w postaci (1) spełnia nierówności

$$n_0^{s(n)} \leq n \leq n_0^{s(n)+1},$$

a stąd otrzymujemy

$$||n_0^{s(n)+1}|| = ||n_0^{s(n)+1} - n + n|| \leq ||n_0^{s(n)+1} - n|| + ||n||.$$

Zatem

$$\begin{aligned}
&||n|| \geq ||n_0^{s(n)+1}|| - ||n_0^{s(n)+1} - n|| \\
&\geq n_0^{(s(n)+1)\alpha} - (n_0^{s(n)+1} - n)^\alpha \quad (\text{bo } ||m|| \leq m^\alpha \text{ dla każdego } m \in \mathbb{N}) \\
&\geq n_0^{(s(n)+1)\alpha} - \left(n_0^{s(n)+1} - n_0^{s(n)}\right)^\alpha \quad (\text{bo } n \geq n_0^{s(n)}) \\
&\geq n_0^{(s(n)+1)\alpha} - n_0^{(s(n)+1)\alpha}\left(1 - \frac{1}{n_0}\right)^\alpha \\
&= n_0^{(s(n)+1)\alpha}\left(1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right) \\
&\geq C' n^\alpha.
\end{aligned}$$

A teraz rozumując jak poprzednio otrzymujemy $||n|| \geq n^\alpha$ dla każdego $n \in \mathbb{N}$. Zatem mamy $||n|| = n^\alpha$ dla wszystkich $n \in \mathbb{N}$. Z Uwagi 1 wynika, że

$$||x|| = |x|^\alpha,$$

dla wszystkich $x \in \mathbb{Q}$. Zatem ze Stwierdzenia 1 wynika, że norma $||.||$ jest równoważna normie $|.|$.

2. Załóżmy teraz, że $||n|| \leq 1$ dla wszystkich $n \in \mathbb{N}$. Muszą też istnieć liczby naturalne, których norma jest mniejsza od 1, bo w przeciwnym wypadku norma będzie trywialna. Niech n_0 będzie najmniejszym takim n. Liczba n_0 musi być pierwsza, ponieważ jeżeli $n_0 = n_1 n_2$, gdzie $n_1, n_2 < n_0$ to na podstawie definicji liczby n_0 mamy $||n_1|| = ||n_2|| = 1$, a wtedy $||n_0|| = ||n_1|| \cdot ||n_2|| = 1$ wbrew określeniu liczby n_0. Oznaczmy liczbę n_0 przez p, oraz $||p|| = \rho$. Pokażemy, że jeżeli q jest liczbą pierwszą różną od p to $||q|| = 1$. Załóżmy, że $||q|| < 1$. Ponieważ $||p|| < 1$ i $||q|| < 1$ to istnieją $N, M \in \mathbb{N}$, takie że $||q^N|| = ||q||^N < \frac{1}{2}$ i $||p^M|| = ||p||^M < \frac{1}{2}$. Liczby q^N i p^M sa względnie pierwsze, więc istnieją liczby całkowite m, n takie, że $mp^M + nq^N = 1$. Wtedy:

$$\begin{aligned} &1 = ||1|| = ||mp^M + nq^N|| \leq ||mp^M|| + ||nq^N|| = \\ &||m|| \cdot ||p^M|| + ||n|| \cdot ||q^N|| \leq ||p^M|| + ||q^N|| < \tfrac{1}{2} + \tfrac{1}{2} = 1. \end{aligned}$$

Co jest niemożliwe. Zatem $||q|| = 1$. Weźmy teraz dowolną liczbę naturalną a. Można ja zapisać jako iloczyn pewnych potęg różnych liczb pierwszych: $a = p_1^{d_1} p_2^{d_2} \ldots p_s^{d_s}$, przy czym $p_1 = p$ (wtedy wykładnik d_1 jest równy $\mathrm{ord}_p(a)$ i może być równy 0). Obliczamy normę a:

$$||a|| = ||p_1^{d_1} p_2^{d_2} \ldots p_s^{d_s}|| = ||p_1||^{d_1} ||p_2||^{d_2} \ldots ||p_s||^{d_s} = ||p_1||^{d_1} = \rho^{\mathrm{ord}_p(a)}.$$

Na podstawie Uwagi 1 otrzymujemy $||x|| = \rho^{\mathrm{ord}_p(x)}$, dla każdej liczby wymiernej x. Zatem na podstawie Stwierdzenia 3 norma $||.||$ jest równoważna normie $|.|_p$, to kończy dowód. □

Twierdzenie Ostrowskiego zostało udowodnione. To jeszcze nie wszytko. Ale to już inna historia...