Uroki zupełności

Jędrzej Garnek

Definicja 1. Waluacją na ciele K nazywamy funkcję $v : K \to \mathbb{Z} \cup \{\infty\}$ spełniającą:

- $v(x) = \infty \quad \Leftrightarrow \quad x = 0$,
- $v(x \cdot y) = v(x) + v(y)$,
- $v(x + y) \geqslant \min\{v(x), v(y)\}$,
- istnieje $\pi \in K$ takie, że $v(\pi) = 1$ (tzw. **uniformizator**), tzn. v jest surjekcją.

Zauważmy, że:

$$R := \{x \in K^* : v(x) \geqslant 0\}.$$

jest pierścieniem lokalnym o ideale maksymalnym:

$$\mathfrak{m} := \{x \in R : v(x) > 0\}$$

generowanym przez dowolny uniformizator (mówimy, że R jest **pierścieniem dyskretnej waluacji**).

Przykład 1. *Ustalmy liczbę pierwszą p. Wtedy na ciele $\mathbb{Q}$ można określić waluację:*

$$v_p\left(p^n \cdot \frac{a}{b}\right) = n, \qquad \text{jeżeli } p \nmid a, b$$

– zauważmy od razu, że uniformizatorem jest p. Pierścień waluacji dany jest jako:

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

Przykład 2. *Ustalmy $a \in \mathbb{C}$. Wtedy na ciele $\mathbb{C}(z)$ można określić waluację:*

$$v_a\left((z-a)^n \cdot g(z)\right) = n, \qquad \text{dla } g(a) \in \mathbb{C}^*$$

(rząd zera/bieguna w a). Uniformizatorem jest wtedy $(z - a)$. Pierścień waluacji dany jest jako:

$$\mathbb{C}(z)_{(z-a)} = \text{funkcje wymierne dobrze określone w } a$$

Przykład 3. *Uogólnimy poprzedni przykład. Niech $C : f(x, y) = 0$ będzie dowolną krzywą algebraiczną w $\mathbb{A}^2_{\mathbb{C}}$. Okazuje się, że punkt $P \in C(\mathbb{C})$ jest gładki wtw. gdy na pierścieniu*

$$\mathcal{O}_P := \text{ funkcje regularne dobrze określone w } P \ = A(C)_{\mathfrak{m}_P}$$

(gdzie $A(C) := \mathbb{C}[x, y]/(f(x, y))$ jest pierścieniem współrzędnych na C, tzn. pierścieniem funkcji regularnych na C, zaś $\mathfrak{m}_P = (x - x_0, y - y_0)$ – ideałem maksymalnym odpowiadającym punktowi $P = (x_0, y_0)$) można określić dyskretną waluację. Dowolna prosta przechodząca przez P i nie styczna do C jest wówczas uniformizatorem.

Zauważmy, że na ciele K wraz z waluacją v można wprowadzić wartość bezwzględną wzorem:

$$\|x\|_v = e^{-v(x)}$$

co pozwala z kolei na wprowadzenie metryki na podanych powyżej pierścieniach. Metryka ta jest dość „zabawna" (przykładowo wszystkie trójkąty są w niej równoramienne), jednak problem sprawia nam co innego. Przypomnijmy definicję znaną wszystkim dobrze z analizy i topologii:

Definicja 2. Przestrzeń metryczną nazwiemy **zupełną**, jeżeli dowolny ciąg Cauchy'ego jest w niej zbieżny.

Zauważmy, że podane powyżej ciała nie są zupełne – przyjmując w przykładzie 2 $a = 0$ mamy: $\sum_n \frac{x^n}{n!} \notin \mathbb{Q}(x)$. „Uzupełniając" pierścienie i ciała z poprzednich przykładów otrzymujemy następujące ciała/pierścienie:

Przykład 4. *Podstawiając w przykładzie 2 $a = 0$ oraz uzupełniając $\mathbb{C}(z)$ względem waluacji v_a dostajemy ciało szeregów Laurenta o współczynnikach wymiernych:*

$$\mathbb{C}((z)) = \left\{ \sum_{n \geqslant N} a_n z^n : N \in \mathbb{Z}, a_n \in \mathbb{Q} \right\}$$

Zauważmy, że wtedy pierścieniem waluacji jest $\mathbb{C}[[z]]$ – pierścień szeregów formalnych. Uniformizator i ciało reszt pozostają takie same.

Przykład 5. *Uzupełniając $\mathbb{Q}$ względem waluacji v_p dostajemy tzw. ciało liczb p-adycznych:*

$$\mathbb{Q}_p = \left\{ \sum_{n \geqslant N} a_n p^n : a_n \in \{0, 1, \ldots, p-1\}, N \in \mathbb{Z} \right\}$$

*(dodawanie następuje „z przenoszeniem" – tak jak w systemie dziesiętnym) wraz z pierścieniem waluacji (tzw. **liczby całkowite p-adyczne**):*

$$\mathbb{Z}_p = \left\{ \sum_{n \geqslant 0} a_n p^n : a_n \in \{0, 1, \ldots, p-1\} \right\}$$

Zauważmy, że każdy element $a = \sum_{n \geqslant 0} a_n p^n \in \mathbb{Z}_p$ jest wyznaczony przez zgodny ciąg elementów $\mathbb{Z}/p^n$:

$$a_0 \in \mathbb{Z}/p, \quad a_0 + pa_1 \in \mathbb{Z}/p^2, \quad a_0 + pa_1 + p^2 a_2 \in \mathbb{Z}/p^3, \ldots$$

– można więc równoważnie zdefniować $\mathbb{Z}_p$ jako granicę odwrotną:

$$\varprojlim \mathbb{Z}/p^n.$$

W dalszym ciągu przyda nam się redukcja do R/π^n dana jako:

$$a_0 + a_1 \cdot \pi + \ldots \mapsto a_0 + a_1 \cdot \pi + \ldots + a_{n-1} \cdot \pi^{n-1} \pmod{\pi^n}$$

W szczególności będziemy redukowali elementy do **ciała reszt** $k := R/\mathfrak{m}$ – zauważmy, że w poprzednich przykładach:

$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$$
$$\mathbb{C}[[x]]/x \cdot \mathbb{C}[[x]] \cong \mathbb{C}$$

Zastanówmy się, jak wyglądają nam znane liczby zapisane w postaci p-adycznej.

- Załóżmy, że $\frac{1}{2}$ jest postaci:
$$\frac{1}{2} = \sum_{n \geqslant 0} a_n 5^n.$$
Redukując $\pmod 5$ dostajemy: $2a_0 \equiv 1 \pmod 5$, czyli $a_0 = 3$. Redukując $\pmod{5^2}$ mamy $2 \cdot (3 + a_1 \cdot 5) \equiv 1 \pmod{5^2}$, co daje $a_1 = 4$. Okazuje się, że rozumowanie to możemy iterować, dostając liczbę $a \in \mathbb{Z}_5$, spełniającą:
$$\forall_n \qquad \frac{1}{2} \equiv a \pmod{5^n},$$
czyli $a = \frac{1}{2}$ (waluacja $v(a - \frac{1}{2})$ musi być nieskończona).

- W $\mathbb{Q}_5$ zachodzi równość:
$$-1 = \sum_{n \geqslant 0} 4 \cdot 5^n$$
wynikająca ze wzoru na sumę szeregu geometrycznego.

- zastanówmy się, czy $\sqrt{-1} \in \mathbb{Q}_5$, tzn. czy równanie $x^2 + 1 = 0$ ma rozwiązanie w $\mathbb{Q}_5$:
$$\sqrt{-1} = \sum_{n \geqslant 0} a_n 5^n \quad \Rightarrow \quad -1 \equiv a_0^2 \pmod 5 \quad \Rightarrow (\text{bez straty ogólności}) \quad a_0 = 2$$
$$\Rightarrow -1 \equiv (2 + a_1 \cdot 5)^2 \pmod{5^2} \quad \Rightarrow \quad a_1 = 2 \Rightarrow \quad \ldots$$
Za chwilę udowodnimy, że procedurę tą można zawsze kontynuować w nieskończoność.

Głównym powodem, dla którego ciała zupełne są tak ważne, jest to, że można w nich w prosty sposób konstruować elementy – zadając po prostu ciąg Cauchy'ego. Fakt ten wykorzystamy w następującym twierdzeniu, uogólniającym nasze poprzednie zmagania:

Lemat 3 (lemat Hensla)**.** *Załóżmy, że $(K, \|\cdot\|_v)$ jest przestrzenią zupełną. Niech $f \in R[x]$ i załóżmy, że $\widetilde{f} \in k[x]$ ma pierwiastek pojedynczy $a_0 \in k$ (tzn. $\widetilde{f}'(a_0) \neq 0$). Wtedy istnieje dokładnie jeden element $a \in R$ taki, że:*
$$a \equiv a_0 \pmod{\mathfrak{m}}, \qquad f(a) = 0$$

Dowód. Wystarczy pokazać indukcyjnie, że istnieje ciąg $a_n \in R$ taki, że element:
$$A_n := \sum_{0 \leqslant i \leqslant n} a_i \pi^i$$
spełnia $f(A_n) \equiv 0 \pmod{\pi^{n+1}}$ dla każdego n. Skonstruowany w ten sposób szereg jest zbieżny do pewnego elementu $a \in R$ (z zupełności R), który musi spełniać $f(a) = 0$.

Dla $n = 0$ wystarczy w dowolny sposób podnieść a_0 do R. Załóżmy, że mamy $a_0, \ldots, a_n$ takie, że zachodzi: $f(A_n) = \pi^{n+1} \cdot c$. Z rozwinięcia Taylora:
$$f(x + A_n) = f(A_n) + x \cdot f'(A_n) + x^2 \cdot g(x)$$
Podstawmy $x = \pi^{n+1} \cdot y$ i zredukujmy $\pmod{\pi^{n+2}}$:
$$f(\pi^{n+1} \cdot y + A_n) \equiv \pi^{n+1} \cdot c + \pi^{n+1} \cdot y \cdot f'(A_n) + 0 \pmod{\pi^{n+2}}$$

więc $f(\pi^{n+1} \cdot y + A_n) \equiv 0 \pmod{\pi^{n+2}}$ wtw. gdy:

$$c + y \cdot f'(A_n) \equiv 0 \pmod{\pi}$$

Zauważmy, że $f'(A_n) \equiv f'(a_0) \not\equiv 0 \pmod{\pi}$, więc powyższe równanie ma dokładnie jedno rozwiązanie $y \equiv (f'(A_n))^{-1} \cdot c \pmod{\pi}$. Wystarczy więc przyjąć $a_{n+1} := y$.

□

Lemat Hensla ma wiele uogólnień, przytoczmy niektóre z nich:

- jeżeli istnieje $a_0 \in R$ takie, że $v(f(a_0)) > 2 \cdot v(f'(a_0))$, to istnieje $a \in R$ spełniające $v(a - a_0) > v(f'(a_0)^2/f(a_0))$,
- jeżeli $\widetilde{f}(x) = g_0(x) \cdot h_0(x)$ dla pewnych $g_0, h_0 \in R[x]$, $NWD(g_0, h_0) = 1$, to istnieją wielomiany $g, h \in R[x]$, spełniające $\widetilde{g} = g_0$, $\widetilde{h} = h_0$, $f = g \cdot h$,
- wersja dla układu n równań z n niewiadomymi (zastępujemy pochodną przez jakobian).

Jako przykładowe zastosowania zauważmy jeszcze, że $\mu_{p-1} \subset \mathbb{Q}_p$ oraz $\sqrt{1+x} \in \mathbb{Q}((x))$.
Z teorioliczbowego punktu widzenia, powyższa procedura pozwala nam na podnoszenie rozwiązań z charakterystyki p do charakterystyki 0. Ciałem, które nas interesuje jest jednak $\mathbb{Q}$, a nie $\mathbb{Q}_p$. Czy można powiedzieć coś rozwiązaniach w $\mathbb{Q}$, wiedząc coś o rozwiązaniach p-adycznych? Jeżeli równanie nie ma rozwiązań p-adycznych, to nie ma też rozwiązań wymiernych – z zasady tej korzystamy często na elementarnej teorii liczb, stwierdzając, że równanie nie ma rozwiązań całkowitych/wymiernych, bo nie ma ich modulo np. 8, bądź też nie ma rozwiązań rzeczywistych. Czy jest możliwe odwrotne rozumowanie? Okazuje się, że w pewnych szczególnych przypadkach tak:

Twierdzenie 4 (zasada lokalno-globalna Hassego)**.** *Niech $q \in \mathbb{Q}[x_1, \ldots, x_n]$ będzie formą kwadratową n-zmiennych. Równanie $q(\boldsymbol{x}) = 0$ ma rozwiązanie w $\mathbb{Q}$ wtw. gdy ma rozwiązanie w dowolnym uzupełnieniu $\mathbb{Q}$, tzn. w $\mathbb{Q}_p$ dla każdego p oraz w $\mathbb{R}$.*

Zasada ta pozwala na uzyskanie efektywnych sposobów rozstrzygania, czy dana forma kwadratowa ma wymierne miejsca zerowe, mamy przykładowo:

Twierdzenie 5 (Legendre'a)**.** *Niech $a, b, c \in \mathbb{Z}$, $(a, b, c) \neq (0, 0, 0)$, $NWD(a, b) = NWD(b, c) = NWD(c, a) = 1$. Wtedy równanie:*

$$ax^2 + by^2 + cz^2 = 0$$

ma rozwiązanie $(x, y, z) \in \mathbb{Z}^3$, $(x, y, z) \neq (0, 0, 0)$, wtedy i tylko wtedy gdy a, b, c nie są tego samego znaku oraz jeżeli powyższe równanie ma rozwiązanie dla dowolnego $p|2abc$.

Dowód. Dla $p \nmid 2abc$ powyższe równanie ma rozwiązanie w $\mathbb{F}_p$ – wystaczy wykazać następujące fakty:

- istnieją niereszty kwadratowe $\pmod{p}$, które sumują się do reszty kwadratowej,
- istnieją reszty kwadratowe $\pmod{p}$, które sumują się do niereszty kwadratowej,

(wynika to z przeliczenia reszt i niereszt). Zauważmy, że jeżeli a jest resztą kwadratową, to $\{ax^2 : x \in \mathbb{F}_p\}$ jest zbiorem wszystkich reszt kwadratowych, podobnie jeżeli a jest niereszą, to $\{ax^2 : x \in \mathbb{F}_p\}$ jest zbiorem wszystkich niereszt. To pozwala na skostruowanie rozwiązania w $\mathbb{F}_p$. Korzystając z lematu Hensla dostajemy rozwiązanie w $\mathbb{Q}_p$. □

Okazuje się, że zasada Hassego nie zachodzi dla form wyższych stopni. Przykład stanowi równanie:

$$3x^3 + 4y^3 + 5z^3 = 0$$

które ma rozwiązanie w $\mathbb{R}$ oraz w dowolnym $\mathbb{Q}_p$, ale nie w $\mathbb{Q}$. Krzywe podobnej postaci są szczególnie przydatne przy obliczaniu rangi krzywej eliptycznej, tzn. rangi grupy $E(\mathbb{Q})$. Mamy ciąg dokładny:

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to Sel^2(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[2] \to 0$$

gdzie $Sel^{(2)}(E/\mathbb{Q})$ jest grupą 2-nakryć krzywej, zaś

$$Ш(E/\mathbb{Q}) = \ker\left(H^1(G_{\mathbb{Q}}, E) \to \prod_v H^1(G_{\mathbb{Q}_v}, E)\right)$$

jest grupą lokalnie trywialnych (mających punkt w dowolnym uzupełnieniu $\mathbb{Q}$) przestrzeni jednorodnych dla $E/\mathbb{Q}$. Grupa $Ш(E/\mathbb{Q})$ stanowi więc „przeszkodę do zachodzenia zasady Hassego". Jedyna nadzieja teorioliczbowców leży w tym, że jest ona skończona - pozwoliłoby to na sprytne ominięcie jej. Ale to już zupełnie inna historia...