Möbiusove transformacije in periodični verižni ulomki

Seminar

Nejc Zajc
Fakulteta za matematiko in fiziko
Oddelek za matematiko

17. marec 2020

1 Uvod

Z verižnimi ulomki oblike

$$b_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \ddots}},$$

se večinoma prvič srečamo pri teoriji števil, kjer so njihovi členi naravna števila. A ko to ne velja več in so členi poljubna kompleksna števila hitro opazimo potrebo po novih pristopih. Z verižnimi ulomki se lahko ukvarjamo s pomočjo Möbiusovih transformacij. To so funkcije oblike

$$g(z) = \frac{az + b}{cz + d}, \tag{1}$$

kjer so a, b, c in d kompleksna števila, za katera velja $ad - bc \neq 0$.

Njihov pomen za opazimo, če si definiramo $s_1(z) = \frac{az+1}{z} = a + \frac{1}{z}$ in $s_2(z) = \frac{bz+1}{z} = b + \frac{1}{z}$; tedaj je namreč

$$s(z) = s_1(s_2(z)) = a + \cfrac{1}{b + \cfrac{1}{z}}$$

končen verižni ulomek in hkrati Möbiusova transformacija. Transformacije bomo natančno definirali v poglavju 3 in jih uporabili v dokazu glavnega izreka tega članka, za začetek pa si natančneje oglejmo verižne ulomke.

2 Verižni ulomki

V članku se bomo ukvarjali z enostavnimi verižni ulomki. Enostaven verižni ulomek ima vse $a_i = 1$, zanj vpeljemo tudi krajši zapis, ki je v končni obliki enak

$$[b_0, b_1, \ldots, b_n] = b_0 + \cfrac{1}{b_1 + \cfrac{1}{\cdots + \cfrac{1}{b_n}}},$$

kjer je b_0 celo število, $b_1, b_2, \ldots$ pa naravna števila; enostaven verižni ulomek pa je nato enak

$$[b_0, b_1, b_2, \ldots] = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \ddots}} = \lim_{n\to\infty} [b_0, b_1, \ldots, b_n]. \tag{2}$$

Limita v (2) vedno obstaja, saj njegovi približki $[b_0, b_1, \ldots, b_n]$ strogo naraščajo za sode n in so navzgor omejeni s $[b_0, b_1]$ ter posledično konvergirajo. Za lihe n pa ti približki strogo padajo in so omejeni z $[b_0]$ ter tako tudi konvergirajo. Ker je razlika med zaporednima približkoma obratno sorazmerna z n^2, sta limiti enaki, posledično pa limita (2) obstaja.

Za verižni ulomek $[b_0, b_1, b_2, \ldots]$ rečemo, da je *periodičen* s periodo k, če je $b_n = b_{n+k}$ za vsa naravna števila n, in da je *sčasoma periodičen*, če je $b_n = b_{n+k}$ za vse dovolj velike n. Opazimo, da v primeru, ko je $[b_0, b_1, b_2, \ldots]$ periodičen s periodo k, kar označimo $\overline{[b_0, \ldots, b_{k-1}]}$ velja $b_0 = b_k \geq 1$. Člen b_0 je torej naravno število, vrednost periodičnega verižnega ulomka pa tako vedno večja od 1.

2.1 Kvadratna iracionalna števila

Definicija 1. *Realno število x je **kvadratno iracionalno število** (kvadratni iracional), če je iracionalno število, ki je ničla kvadratnega polinoma P s celoštevilskimi koeficienti.*

Naj bo x kvadratni iracional. Tedaj je ničla celoštevilskega kvadratnega polinoma in je zato oblike $x = \frac{a+b\sqrt{c}}{d}$, kjer so a, b, c in d cela števila, izmed katerih b, c in d ne smejo biti enaki nič, $c > 0$ pa ni popolni kvadrat. Ko vstavimo x v kvadratni celoštevilski polinom P, za katerega je ničla, vidimo da je polinom do množenja s skalarjem enolično določen Če je poljubno število take oblike ničla kvadratnega celoštevilskega polinoma vidimo, da je

polinom do množenja s skalarjem enolično določen. Druga ničla polinoma P je algebraična konjugirana vrednost x, t.j. $\frac{a-b\sqrt{c}}{d}$, ki jo označimo z x^*.

Za zapis realnih števil z enostavnimi verižnimi ulomki velja, da lahko vsako racionalno število zapišemo kot končen verižni ulomek, vsakemu iracionalnemu številu pa pripada enolično določen verižni ulomek oblike (2). O verižnih ulomkih kvadratnih iracionalov lahko povemo še več, za iracionalno število $x = [b_0, b_1, b_2, \ldots]$ veljata naslednji lastnosti. *Verižni ulomek* $[b_0, b_1, b_2, \ldots]$ *je sčasoma periodičen natanko tedaj, ko je* x *kvadratni iracional,* in $[b_0, b_1, b_2, \ldots]$ *je periodičen natanko tedaj, ko je* x *kvadratni iracional, katerega algebraična konjugirana vrednost* x^* *leži na intervalu* $(-1, 0)$. Prvo ekvivalenco sta dokazala Euler, ki je pokazal, da sčasoma periodičen ulomek predstavlja kvadratni iracional, in Lagrange, ki je dokazal obrat. Drugo lastnost pa je pokazal Galois.

Osrednji namen tega članka je pokazati kako lahko s pomočjo Möbiusovih transformacij na verižnih ulomkih dokažemo naslednji Galois-ev izrek.

Izrek 1 (Galois-ev izrek)**.** *Za* $x = \overline{[b_0, \ldots, b_{k-1}]}$ *velja* $\overline{[b_{k-1}, \ldots, b_0]} = -\frac{1}{x^*}$.

Oglejmo si primer uporabe transformacij, na posebnem primeru Galois-evega izreka.

Zgled 1. *Naj* $a, b \in \mathbb{N}$ *in* $\alpha = \overline{[a, b]}$. *S substitucijo dobimo* $\alpha = a+1/(b+1/\alpha)$. *Torej je* α *negibna točka* $s(z) = a + 1/(b + 1/z)$. *Za negibni točki s velja, da sta rešitvi enačbe* $bz^2 - abz - a = 0$. *To sta torej* α *in* α^*. *Ker iz Vietovih formul sledi* $\alpha\alpha^* = -\frac{a}{b} < 0$, *velja* $\alpha > 0 > \alpha^*$.
Definirajmo še $\beta = \overline{[b, a]}$. *Enak premislek nas pripelje do ugotovitve, da sta* β *in* β^* *rešitvi* $az^2 - abz - b = 0$ *ter da velja* $\beta > 0 > \beta^*$. *Če na zadnji enačbi uporabimo transformacijo* $w = -1/z$, *dobimo* $\{\alpha, \alpha^*\} = \{-1/\beta, -1/\beta^*\}$ *in zato* $\beta = -1/\alpha^*$, *kar bi nam povedal tudi Galois-ev izrek.*

3 Širši pogled

Pred dokazom izreka, si oglejmo delovanje in lastnosti kompleksnih funkcij, ravnine in v posebnem Möbiusovih transformacij.

3.1 Kompleksna ravnina

Kompleksni ravnini $\mathbb{C}$ dodajmo novo točko ∞ in tako tvorimo *razširjeno kompleksno ravnino,* ki jo označimo $\mathbb{C}_\infty = \mathbb{C} \cup \{\infty\}$.

Definicija 2. *Funkcija* g *z domeno* $\mathbb{C}_\infty$ *je* ***Möbiusova transformacija****, če jo lahko zapišemo v obliki* (1)*, kjer so* a, b, c *in* d *kompleksna števila za*

katera velja $ad - bc \neq 0$.
Če je $c \neq 0$, *potem v* (1) *velja* $g(\infty) = \frac{a}{c}$ *in* $g(-\frac{d}{c}) = \infty$, *sicer je* $g(\infty) = \infty$.

Vsaka Möbiusova transformacija g je bijekcija $\mathbb{C}_\infty$, saj je inverz funkcije oblike (1) enak $g^{-1}(z) = \frac{-dz+b}{cz-a}$. Vidimo da je g^{-1} Möbiusova transformacija, kratek račun pa nam utemelji, da to velja tudi za kompozitum dveh transformacij. Množica vseh Möbiusovih transformacij je torej grupa.

Označimo še *razširjeno realno os* kot $\mathbb{R}_\infty = \mathbb{R} \cup \infty$. Möbiusova transformacija ohranja $\mathbb{R}_\infty$ natanko tedaj, ko so vsi koeficienti v (1) realna števila. Iz predpostavke, da g ohranja $\mathbb{R}_\infty$ sledi željeno zaradi ..... PREMISLI!! Obrat pa je viden brez težav. Opazimo lahko še več, saj

$$\mathrm{Im}[g(z)] = \frac{(ad - bc)\mathrm{Im[z]}}{|cz + d|^2}$$

velja da g ohranja zgornjo kompleksno polravnino $\mathbb{H} = \{x + iy\,; x, y \in \mathbb{R}, y > 0\}$ natanko tedaj ko velja $ad - bc > 0$. V primeru ko je zadnja vrednost enaka -1 se kompleksni polravnini ravno zamenjata, kot je to pri $h(z) = \frac{1}{z}$; v primeru $k(z) = -\frac{1}{z}$ pa se polravnini ohranita.

Omenimo še, kako $\mathbb{C}_\infty$ opremimo z metriko. Stereografska projekcija je znan homeomorfizem med $\mathbb{C}$ in enotsko sfero $\mathbb{S}$ brez ene točke v $\mathbb{R}^3$. To projekcijo lahko razširimo do homeomorfizma med $\mathbb{C}_\infty$ in celotno sfero $\mathbb{S}$ ter nato prenesemo Evklidsko metriko iz $\mathbb{S}$ v metriko χ na $\mathbb{C}_\infty$. Za metrični prostor $(\mathbb{C}_\infty, \chi)$ je nato vsaka Möbiusova transformacija g homeomorfizem prostora $\mathbb{C}_\infty$ samega vase.

V primeru same zgornje polravnine $\mathbb{H}$ pa ob vpeljavi norme $||z|| = |z|/y$, kjer je $|z|$ absolutna vrednost kompleksnega števila z in $y = \mathrm{Im}[z]$, dobimo Poincaré-jev model polravnine, ki je eden izmed standardnih modelov hiperbolične ravnine. Tu so Möbiusove transformacije, ki ohranjajo $\mathbb{H}$ ($ad - bc > 0$), ravno vse izometrije $\mathbb{H}$. Meja prostora ustreza $\mathbb{R}_\infty$.

3.2 Modularna grupa

Definicija 3. ***Modularna grupa*** Γ *je grupa vseh Möbiusovih transformacij oblike* (1) *s celoštevilskimi koeficienti* a, b, c *in* d, *za katere velja* $ad - bc = 1$.

Kot smo že omenili, elementi Γ na $\mathbb{H}$ delujejo kot izometrije hiperbolične metrike, njihovo delovanje na $\mathbb{R}_\infty$ pa je tesno povezano s teorijo verižnih ulomkov. V grupi namreč med drugim leži tudi funkcija $s(z) = a+1/(b+1/z)$.

Posebno zanimive so ***loksodromične izometrije*** $\mathbb{H}$. To so Möbiusove transformacije, ki ohranjajo $\mathbb{H}$ in imajo dve različni negibni točki. Primer takšne funkcije je $z \mapsto 2z$, katere negibni točki sta 0 in ∞. Ob njihovi obravnavi pridemo do pomembne ugotovitve glede kvadratnih iracionalov.

Trditev 1. *Realno število x je kvadratno iracionalno število natanko tedaj ko je negibna točka nekega loksodromičnega elementa g modularne grupe Γ. Tedaj je algebraična konjugirana vrednost x^* druga negibna točka g.*

Tudi te trditve ne bomo dokazovali, bomo jo pa uporabili pri dokazovanju izreka. V ta namen si ogledjo še eno pomembno lastnost. Če je g loksodromična funckija z negibnima točkama u in v, potem je ena izmed njih, recimo u, *privlačna negibna točka*, druga (v tem primeru v) pa je *odbojna negibna točka*. To pomeni da ob večkratni aplikaciji funkcije g na elementu $z \neq v$ v limiti velja $g^n(z) = g(g(\cdots(g(z)))) \to u$. V že omenjenem primeru $z \mapsto 2z$ je ∞ privlačna negibna točka, 0 pa je odbojna. Praviloma velja, da je negibna točka w poljubne funkcije f privlačna oziroma odbojna, če velja zaporedoma $|f'(w)| < 1$ oziroma $|f'(w)| > 1$.

4 Dokaz izreka

S pridobljenim znanjem bomo v tem poglavju dokazali Galois-ev izrek. Dokaz temelji na naslednji lemi, ki posploši pomen algebraične konjugirane vrednosti števila, saj b_i v lemi niso nujno cela števila. Za lažji zapis bomo v lemi pri komponiranju uporabljali okrajšave kot na primer $s_1 s_2(z) = s_1(s_2(z))$.

Lema 1. *Za funkcije s_i, $i \in \{1, \ldots, k\}$ oblike $s : z \mapsto b + 1/z$, kjer je $b \geq 1$, ima končni kompozitum $S = s_1 \cdots s_k$ privlačno negibno točko $\zeta \in (1, \infty)$ in odbojno negibno točko $\tilde{\zeta} \in (-1, 0)$.*

Dokaz. Naj bo $S = s_1 \cdots s_2$, za $s_i(z) = b_i + 1/z$ in $b_i \geq 1$. Vsak s_i slika interval $(1, \infty)$ samega vase, torej naredi kompozitum S enako. Prav tako je vsak s_i skrčitev, kar posledično velja tudi za kompozitum S. Na podlagi Banachovega skrčitvenega načela lahko zato sklepamo, da ima S negibno točko $\zeta \in (1, \infty)$. Za določitev vrste negibne točke si pomagamo z velikostjo odvoda. Ker velja $|s_i'(z)| < 1$ na celem $(1, \infty)$, lahko preko verižnega pravila za odvajanje kompozituma sklepamo $|S'(\zeta)| < 1$. To pomeni, da je ζ privlačna negibna točka kompozituma S.
Definirajmo še $\tilde{S} = s_k \cdots s_1$. Analogni postopek nas pripelje do ugotovitve, da ima $\tilde{S}$ privlačno negibno točko $\tilde{\zeta} \in (1, \infty)$. Naj bo $\sigma(z) = -1/z$. Tedaj velja

$$\delta s_i(z) = -\frac{1}{b + \dfrac{1}{z}} = \frac{1}{-\dfrac{1}{z} - b} = s_i^{-1}\delta(z),$$

za vse z in zato tudi $\delta S = \tilde{S}^{-1}\delta$. Ko v zadnjo enačbo vstavimo $\delta(\tilde{\zeta})$ vidimo, da je tudi to negibna točka kompozituma S. Ker $\delta(\tilde{\zeta}) \in (-1, 0)$ je to od ζ različna negibna točka in je zato odbojna. □

Definicija 4. *aaabbbbbb*

Zgled 2. *bbb*

n	$\{1, 2, \ldots, n\}$	$\varphi(n)$
1	$\{\mathbf{1}\}$	1
2	$\{\mathbf{1}, 2\}$	1
3	$\{\mathbf{1}, \mathbf{2}, 3\}$	2
4	$\{\mathbf{1}, 2, \mathbf{3}, 4\}$	2
5	$\{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, 5\}$	4
6	$\{\mathbf{1}, 2, 3, 4, \mathbf{5}, 6\}$	2

Tabela 1: Vrednosti funkcije $\varphi(n)$ za $n = 1, 2, \ldots, 6$

Trditev 2. *fipp*

Dokaz: ccc □

Zgled 3. *aaa*

$$\begin{aligned}\varphi(n) &= \prod_{i=1}^{r} \varphi\left(p_i^{k_i}\right) = \prod_{i=1}^{r} \left(p_i^{k_i} - p_i^{k_i-1}\right) \\ &= \left(\prod_{i=1}^{r} p_i^{k_i}\right) \times \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = n \times \prod_{p \mid n} \left(1 - \frac{1}{p}\right). \qquad \square\end{aligned}$$

Izrek 2 (Eulerjev izrek)**.** *Euler*

Dokaz: ddd □

$$\begin{aligned}(f * (g + h))(n) &= \sum_{de=n} f(d)(g + h)(e) = \sum_{de=n} f(d)(g(e) + h(e)) \\ &= \sum_{de=n} f(d)g(e) + \sum_{de=n} f(d)h(e) \\ &= (f * g + f * h)(n). \qquad \square\end{aligned}$$

Angleško-slovenski slovar strokovnih izrazov

arithmetic function aritmetična funkcija
coprime tuj

Dirichlet convolution Dirichletova konvolucija
Dirichlet ring Dirichletov kolobar, kolobar aritmetičnih funkcij
divisor delitelj
Euler's phi function, Euler's totient function Eulerjeva funkcija φ
Euler's theorem Eulerjev izrek
Fermat's little theorem mali Fermatov izrek
fundamental theorem of arithmetic osnovni izrek aritmetike
greatest common divisor največji skupni delitelj, največja skupna mera
least common multiple najmanjši skupni večkratnik
Möbius function Möbiusova funkcija μ
Möbius inversion Möbiusov obrat, Möbiusova inverzija
multiple večkratnik
prime praštevilo; praštevilski
prime factor prafaktor
prime number praštevilo
relatively prime tuj

Literatura

[1] M. Aigner in G. M. Ziegler, *Proofs from THE BOOK*, 2. izdaja, Springer, Berlin–Heidelberg–New York, 2001.

[2] N. Calkin in H. S. Wilf, Recounting the rationals, *Amer. Math. Monthly* **107** (2000), 360–363.

[3] J. Grasselli, *Elementarna teorija števil*, DMFA – založništvo, Ljubljana, 2009.