Rotacije opisane s kvaternioni

Seminar

Timotej Mlakar
Fakulteta za matematiko in fiziko
Oddelek za matematiko

14. marec 2023

1 Uvod

Rotacije $\mathbb{R}^3$ navadno opisujemo z linearnimi preslikavami oziroma njim pripadajočimi matrikami. Zaradi narave matričnega množenja so lahko take operacije precej računsko časovno in prostorsko zahtevne. Tako lahko rotacije $\mathbb{R}^3$ predstavimo kot stranske učinke transformacij $\mathbb{E}^4 \simeq \mathbb{H}$.

Najprej se spomnimo rotacij na $\mathbb{R}^2 \simeq \mathbb{C}$. Naj bo $w = \frac{v}{|v|}$ za poljuben $v \in \mathbb{C}$. Preslikava $\varphi : \mathbb{C} \to \mathbb{C} : \varphi(z) = wz$ je bijektivna preslikava, ki zavrti celotno kompleksno ravnino za kot $arg(z)$ okoli izhodišča.

Če v zapišemo v polarnem zapisu kot $|z|e^{i\theta}$, je tedaj preslikava

$$\varphi : [0, 2\pi] \times \mathbb{C} \to \mathbb{C} :$$
$$\varphi(\theta, z) = ze^{i\theta}$$

zvezno odvedljiva na $[0, 2\pi] \times \mathbb{C}$. Za fiksen $z \in \mathbb{C}$ preslikava φ opiše krožnico z radijem $|z|$, za fiksen θ pa preslikava opiše rotacijo ravnine za kot θ.

Vemo torej, da se vsak $z \in \mathbb{C}$ da zapisati v polarnih koordinatah. Spomnemo se zapisa

$$z = |z|e^{i\theta} = |z|\cos\theta + |z|i\sin\theta,$$

kjer je $\theta \in \mathbb{R}$. Zapis ni enoličen, saj nam vsaka $\theta' = \theta + 2k\pi; k \in \mathbb{Z}$ opiše isto kompleksno število. Tak zapis bomo v podobnem smislu uporabili kasneje.

Definiramo $\Phi : \mathbb{R}^2 \to \mathbb{C} : (x, y) \mapsto \mathrm{x} + iy$. S preprostim računom pokažemo, da je Φ izomorfizem.

Vidimo, da namesto množenja vektorja z matriko lahko rotacijo realne ravnine predstavimo s preprostim množenjem dveh kompleksnih števil. To motivira podobni razmislek za rotacije v $\mathbb{R}^3$.

2 Kvaternionska algebra

2.1 Definicije in oznake

Definicija 1 *Naj bo V 4-razsežen vektorski prostor nad R. Izberemo bazo $\{\mathbf{1}, i, j, k\}$. Elementi V so oblike $\boldsymbol{q} = q_0\mathbf{1} + q_1 i + q_2 j + q_3 k = q_0 + \vec{q}$. Vektorski prostor V opremimo z operacijo množenja tako, da definiramo množenje njegovih baznih elementov, in sicer*

$$\begin{gathered}\mathbf{1}\mathbf{1} = \mathbf{1}, \quad \mathbf{1}i = i, \quad \mathbf{1}j = j, \quad \mathbf{1}k = k,\\ ij = k, \quad jk = i, \quad ki = j,\\ i^2 = j^2 = k^2 = ijk = -1\mathbf{1}.\end{gathered}$$

Naj bosta $p, q \in \mathbb{H}$. Definiramo seštevanje in množenje s skalarjem kot običajno

$$\begin{aligned}p + q &= (p_0 + q_0) + (\vec{p} + \vec{q}),\\ \lambda q &= \lambda\,(q_0 + \vec{q}) = \lambda q_0 + (\lambda\vec{q}).\end{aligned}$$

Prav tako definiramo običajno množenje v skladu z definicijo množenja baznih elementov. Tedaj lahko produkt pq napišemo kot

$$pq = (p_0 + q_0 - \vec{p}\vec{q}) + (p_0\vec{q} + q_0\vec{p} + \vec{p} \times \vec{q}),$$

kjer je $\vec{p}\vec{q}$ običajni skalarni produkt v $\mathbb{R}^3$. Tedaj V postane 4-razsežna algebra nad $\mathbb{R}$. Označimo $\mathbb{H}$ in jo imenujemo Kvaternionska algebra.

Opomba 1 *Za $p, q \in \mathbb{H}, \lambda \in \mathbb{R}$ velja*

$$(\lambda p)q = p(\lambda q) = \lambda(pq).$$

Definicija 2 *Naj bo $q = q_0 + \vec{q} \in \mathbb{H}$. S $\overline{q} = q_0 - \vec{q}$ označimo* konjugirani kvaternion *q.*

Velja, da je $q\overline{q} \in \mathbb{R}$. Tako lahko definiramo še

$$q^{-1} = \frac{1}{q\overline{q}}\overline{q}.$$

Prav tako lahko vidimo da je $\overline{p \cdot q} = \overline{q} \cdot \overline{p}$. Ker množenje kvaternionov ni komutativno, v splošnem $\overline{pq} \neq \overline{qp}$. Ker je $\mathbb{H}$ algebra, je na njej smiselno definirati skalarni produkt.

Definicija 3 *Naj bosta $p, q \in \mathbb{H}$. Definiramo skalarni produkt kvaternionov*

$$\langle p, q\rangle = \tfrac{1}{2}(\overline{p}q + \overline{q}p).$$

Norma porojena s skalarnim produktom je tedaj

$$|q| = ||q|| = \sqrt{\langle q, q\rangle}.$$

Opomba 2 *Iz definicije norme takoj sledi* $\langle q, q\rangle = q\overline{q} = \overline{q}q$. *Podobno kot absolutna vrednost na* $\mathbb{R}$ *in* $\mathbb{C}$ *je norma na kvaternionih multiplikativna.*

Za poljubna $p, q \in \mathbb{H}$ torej velja $|pq| = |p||q|$. Oglejmo si $|pq|^2$

$$|pq|^2 = \langle pq, pq\rangle = pq\overline{pq}.$$

Spomnimo se, da $\overline{p \cdot q} = \overline{q} \cdot \overline{p}$. Torej je

$$pq\overline{pq} = p \cdot q \cdot \overline{q} \cdot \overline{p} = p|q|^2\overline{p}.$$

Ker je $|q|^2$ skalar, pri množenju komutira s kvaternioni. Torej

$$p|q|^2\overline{p} = |q|^2 p\overline{p} = |q|^2|p|^2 = |p|^2|q|^2.$$

Sledi torej $|pq| = |p||q|$.

Podobno kot pri rotaciji kompleksne ravnine, kjer množimo s števili iz enotske krožnice, tukaj potrebujemo enotske kvaternione.

Definicija 4 *Naj bo* $q \in \mathbb{H}$. *Kvaternion q imenujemo* versor *oziroma* enotski kvaternion*, če velja* $|q| = 1$. *Če je* $q \in \mathbb{H}$ *poljuben* $|q| \neq 1$ *versor kvaterniona q dobimo z normiranjem. Označimo ga z* $U_q = \dfrac{q}{|q|}$. *Množico versorjev označimo s* $\boldsymbol{Q}_e$

Če velja $u \in \mathbb{H}, u = \vec{u}$ *in* $|u| = 1$*, kvaternion u imenujemo* čisti *oziroma* pravi *versor. Množico pravih versorjev označimo z* $\boldsymbol{U}_e$.

Kvaternione oblike $q = q_0\mathbf{1}, q_0 \in \mathbb{R}$ *imenujemo* skalarni kvaternioni.

Opomba 3 *Za čista versorja* $u, v \in \boldsymbol{U}_e$ *velja da* $\langle u, v\rangle = 0 \iff uv + vu = 0$.

Naj bosta $u, v \in \mathbf{U}_e$. Za poljuben versor iz $\mathbf{U}_e$ velja $\overline{u} = -u$. Pogledamo $\langle u, v\rangle$:

$$\langle u, v\rangle = \tfrac{1}{2}(\overline{u}v + \overline{v}u) = \tfrac{1}{2}(-uv - vu) = -\tfrac{1}{2}(uv + vu).$$

Od tu sledi da $\langle u, v\rangle = 0 \iff uv + vu = 0$.

Pomembna opazka tu je še naslednja: naj bo $u \in \mathbf{U}_e$. Ker $|u| = 1$ sledi, da je u neničeln kvaternion. Ker je $\mathbf{U}_e \subset \mathbb{H}$ in je $\mathbb{H}$ algebra, je vsak neničenli kvaternion obrnljiv. Vemo torej, da obstaja tak u^{-1} da je

$$uu^{-1} = 1.$$

Ker je za poljuben $q \in \mathbb{H}, q^{-1} = \frac{1}{\overline{q}q}\overline{q}$, za $u \in \mathbf{U}_e$ pa velja $u\overline{u} = |u|^2$, je

$$u^{-1} = \frac{\overline{u}}{|u|^2} = \frac{-u}{1} = -u.$$

Če združimo te dve dejstvi sledi, da

$$uu^{-1} = -uu = -u^2 = 1 \Rightarrow u^2 = -1.$$

3 Eulerjeva funkcija

Definicija 5 *Za vse $n \in \mathbb{N}$ s $\varphi(n)$ označimo število celih števil iz množice $\{1, 2, \ldots, n\}$, ki so tuja številu n. Preslikavo $\varphi : \mathbb{N} \to \mathbb{N}$ imenujemo* Eulerjeva funkcija.

Zgled 1 *Tabela 1 prikazuje izračun prvih šest vrednosti funkcije $\varphi(n)$. V n-ti vrstici so krepko natisnjena števila med 1 in n, ki so tuja številu n. Slika 1 pa grafično prikazuje prvih 100 vrednosti funkcije $\varphi(n)$.*

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 $n = 1, 2, \ldots, 6$

Slika 1: Vrednosti funkcije $\varphi(n)$ za $n = 1, 2, \ldots, 100$

Računanje $\varphi(n)$ po definiciji je pri velikem n zelo zamudno. Vendar ima Eulerjeva funkcija lepe lastnosti, zaradi katerih lahko njeno vrednost izračunamo tudi pri velikem argumentu, če ga le znamo razcepiti na prafaktorje.

Če je p praštevilo, med števili $1, 2, \ldots, p$ edinole število p ni tuje številu p, torej je $\varphi(p) = p - 1$. Skoraj prav tako preprosto lahko poiščemo vrednost $\varphi(n)$, če je n potenca nekega praštevila.

Trditev 1 *Naj bo p praštevilo in $k \in \mathbb{N}$. Potem je $\varphi(p^k) = p^k - p^{k-1}$.*

Dokaz: Število a je tuje številu p^k natanko tedaj, ko ni večkratnik praštevila p. Med števili $1, 2, \ldots, p^k$ je natanko $p^k/p = p^{k-1}$ večkratnikov števila p, torej je $\varphi(p^k) = p^k - p^{k-1}$. □

Izrek 1 *Eulerjeva funkcija je multiplikativna.*

Dokaz: Vzemimo tuji naravni števili a in b. Zapišimo vsa števila med 1 in ab v obliki tabele z a vrsticami in b stolpci:

$$\begin{array}{cccc} 1 & 2 & \cdots & b \\ b+1 & b+2 & \cdots & 2b \\ 2b+1 & 2b+2 & \cdots & 3b \\ \vdots & \vdots & \cdots & \vdots \\ (a-1)b+1 & (a-1)b+2 & \cdots & ab \end{array}$$

Za vsako število velja, da je tuje številu ab natanko tedaj, ko je tuje številu a in tuje številu b. Vrednost $\varphi(ab)$ lahko torej dobimo tako, da preštejemo, koliko je v gornji tabeli števil, ki so tuja tako številu a kot tudi številu b.

Števila v posameznem stolpcu dajejo vsa isti ostanek pri deljenju z b. Torej so bodisi vsa tuja številu b bodisi mu ni tuje nobeno od njih. Stolpcev, katerih elementi so tuji številu b, je toliko, kot je takih števil v prvi vrstici tabele, teh pa je ravno $\varphi(b)$.

Različna števila v posameznem stolpcu dajo različne ostanke pri deljenju z a. Če namreč števili $k_1 b + r$ in $k_2 b + r$, kjer je $0 \leq k_1, k_2 \leq a - 1$, dasta isti ostanek pri deljenju z a, je njuna razlika $(k_1 - k_2)b$ deljiva z a. Ker sta števili a in b tuji, sledi, da je z a deljiva razlika $k_1 - k_2$. To pa je možno le, če je $k_1 = k_2$, saj je $-(a-1) \leq k_1 - k_2 \leq a - 1$. Ker je dolžina stolpca enaka a, dobimo pri deljenju elementov stolpca z a ravno vse možne ostanke $0, 1, \ldots, a - 1$. Torej je v vsakem stolpcu $\varphi(a)$ števil tujih a.

To velja tudi za $\varphi(b)$ stolpcev, katerih elementi so tuji številu b. Potemtakem je v gornji tabeli $\varphi(b)\varphi(a)$ števil, ki so tuja tako številu b kot tudi številu a. Torej je $\varphi(ab) = \varphi(a)\varphi(b)$, kar pomeni, da je Eulerjeva funkcija multiplikativna. □

Zgled 2 *Izračunajmo $\varphi(10^k)$. Ker je $10^k = 2^k 5^k$, je po izreku 1 in trditvi 1*

$$\varphi(10^k) \;=\; \varphi(2^k)\varphi(5^k) \;=\; (2^k - 2^{k-1})(5^k - 5^{k-1}) \;=\; 4 \times 10^{k-1}.$$

Posledica 1

$$\varphi(n) \;=\; n \times \prod_{p \,|\, n} \left(1 - \frac{1}{p}\right),$$

kjer p preteče vse različne prafaktorje števila n.
Dokaz: Naj bo $n = \prod_{i=1}^{r} p_i^{k_i}$, kjer so $p_1, p_2, \ldots, p_r$ različna praštevila in $k_1, k_2, \ldots, k_r \in \mathbb{N}$. Po izreku 1 in trditvi 1 je potem

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

Trditev 2 *Za vse $n \in \mathbb{N}$ velja enačba*

$$\sum_{d \,|\, n} \varphi(d) = n, \tag{1}$$

kjer d preteče vse pozitivne delitelje števila n.

Dokaz: Za vse delitelje d števila n označimo

$$A_d = \left\{ \frac{kn}{d};\ k \in \mathbb{Z},\ 0 \le k < d,\ D(k,d) = 1 \right\}.$$

Recimo, da je $k_1 n/d_1 = k_2 n/d_2$, kjer je $D(k_1, d_1) = D(k_2, d_2) = 1$. Potem je $k_1 d_2 = k_2 d_1$, od koder sledi, da d_1 deli d_2 in obratno, kar pomeni, da je $d_1 = d_2$. Od tod zaključimo, da so si množice A_d paroma tuje, torej je

$$\left| \bigcup_{d \,|\, n} A_d \right| = \sum_{d \,|\, n} |A_d| = \sum_{d \,|\, n} \varphi(d).$$

Po drugi strani pa je

$$\bigcup_{d \,|\, n} A_d = \{0, 1, \ldots, n-1\}.$$

Res, naj bo $kn/d \in A_d$. Ker d deli n, je število kn/d celo, iz $0 \le k < d$ pa sledi $0 \le kn/d < n$, torej $kn/d \in \{0, 1, \ldots, n-1\}$. Vzemimo zdaj še poljuben $j \in \{0, 1, \ldots, n-1\}$ in označimo: $k = j/D(n,j)$, $d = n/D(n,j)$. Potem je $j = kD(n,j) = kn/d \in A_d$.

To pa pomeni, da je $\left|\bigcup_{d \,|\, n} A_d\right| = n$ in izrek je dokazan. $\square$

Izrek 2 (Eulerjev izrek) *Naj bosta $n \in \mathbb{N}$ in $a \in \mathbb{Z}$ tuji števili. Potem je*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dokaz: Naj bodo $k_1, k_2, \ldots, k_{\varphi(n)}$ vsa števila med 1 in n, ki so tuja n. Če za indeksa $i, j \in \{1, 2, \ldots, \varphi(n)\}$ velja $k_i a \equiv k_j a (\text{mod } n)$, sledi $n|(k_i a - k_j a)$ in zato $n|(k_i - k_j)$, saj sta števili n in a tuji. To pa je mogoče le, če je $i = j$. Števila $k_1 a, k_2 a, \ldots, k_{\varphi(n)} a$ so torej med seboj paroma nekongruentna po modulu n. Ker so tuja številu n, je množica njihovih ostankov pri deljenju z n enaka množici $\{k_1, k_2, \ldots, k_{\varphi(n)}\}$. Zato je $k_1 a \cdot k_2 a \cdots k_{\varphi(n)} a \equiv k_1 \cdot k_2 \cdots k_{\varphi(n)} (\text{mod } n)$, od tod pa po krajšanju s produktom $k_1 \cdot k_2 \cdots k_{\varphi(n)}$, ki je tuj številu n, dobimo $a^{\varphi(n)} \equiv 1 (\text{mod } n)$. □

Posledica 2 (mali Fermatov izrek) *Naj bo p praštevilo in $a \in \mathbb{Z}$ celo število, ki ni deljivo s p. Potem je*

$$a^{p-1} \equiv 1 \pmod{p}.$$

4 Möbiusova funkcija

Definicija 6 *Za vse $n \in \mathbb{N}$ naj bo*

$$\mu(n) = \begin{cases} 0, & \text{če } n \text{ deljiv s kvadratom praštevila,} \\ (-1)^r, & \text{sicer,} \end{cases}$$

kjer je r število različnih prafaktorjev števila n. Preslikavo $\mu : \mathbb{N} \to \mathbb{Z}$ imenujemo Möbiusova funkcija.

Zgled 3 *Tabela 2 prikazuje prvih nekaj vrednosti funkcije $\mu(n)$.*

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	−1	−1	0	−1	1	−1	0	0	1

Tabela 2: Vrednosti funkcije $\mu(n)$

Izrek 3 *Möbiusova funkcija je multiplikativna.*

Dokaz: Vzemimo tuji naravni števili a in b. Če je število ab deljivo s kvadratom praštevila, velja to tudi za a ali za b. V tem primeru je torej $\mu(ab) = 0 = \mu(a)\mu(b)$. Če pa število ab ni deljivo s kvadratom praštevila, velja to tudi za a in za b. Naj bo r število različnih prafaktorjev števila a, s pa število različnih prafaktorjev števila b. Potem je število različnih prafaktorjev števila ab enako $r + s$, torej je v tem primeru $\mu(ab) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(a)\mu(b)$. □

Trditev 3 *Za vse $n \in \mathbb{N}$ velja enačba*

$$\sum_{d\,|\,n} \mu(d) \;=\; \begin{cases} 1, & n = 1, \\ 0, & n > 1, \end{cases} \tag{2}$$

kjer d preteče vse pozitivne delitelje števila n.

Dokaz: Zadošča seštevati po tistih deliteljih d števila n, ki imajo same različne prafaktorje (sicer je $\mu(d) = 0$). Imenujmo takšne delitelje *enostavni*. Naj bo r število različnih prafaktorjev števila n. Število enostavnih deliteljev števila n, ki imajo natanko k prafaktorjev, je potem $\binom{r}{k}$, prispevek takega delitelja h gornji vsoti pa znaša $\mu(d) = (-1)^k$. Torej je

$$\sum_{d\,|\,n} \mu(d) \;=\; \sum_{k=0}^{r} (-1)^k \binom{r}{k} \;=\; \begin{cases} 1, & r = 0, \\ 0, & r > 0 \end{cases} \;=\; \begin{cases} 1, & n = 1, \\ 0, & n > 1. \end{cases} \qquad \square$$

Opomba 4 *Enačbo (2) bi lahko uporabili tudi za (rekurzivno) definicijo funkcije $\mu(n)$:*

$$\mu(n) \;=\; \begin{cases} 1, & n = 1, \\ -\displaystyle\sum_{d\,|\,n,\, d<n} \mu(d), & n > 1. \end{cases}$$

Möbiusova funkcija igra pomembno vlogo pri *Möbiusovem obratu*, ki nam omogoča izraziti aritmetično funkcijo $f(n)$, če poznamo funkcijo $g(n) = \sum_{d\,|\,n} f(d)$, kjer d preteče vse pozitivne delitelje števila n.

Izrek 4 (Möbiusov obrat) Za aritmetični funkciji f, g velja:

$$g(n) \;=\; \sum_{d\,|\,n} f(d) \quad\Longleftrightarrow\quad f(n) \;=\; \sum_{d\,|\,n} \mu\left(\frac{n}{d}\right) g(d)$$

Dokaz: Najprej vzemimo, da je $g(n) = \sum_{d\,|\,n} f(d)$ za vse $n \in \mathbb{N}$. Potem je

$$\begin{aligned} \sum_{d\,|\,n} \mu\left(\frac{n}{d}\right) g(d) \;&=\; \sum_{d\,|\,n} \mu\left(\frac{n}{d}\right) \sum_{k\,|\,d} f(k) \;=\; \sum_{k\,|\,n} f(k) \sum_{k\,|\,d\,|\,n} \mu\left(\frac{n}{d}\right) \\ &=\; \sum_{k\,|\,n} f(k) \sum_{a\,|\,(n/k)} \mu\,(a) \;=\; f(n). \end{aligned}$$

Drugo enakost smo dobili z zamenjavo vrstnega reda seštevanja, tretjo z uvedbo nove spremenljivke $a = n/d$, četrta pa sledi iz (2).

Vzemimo zdaj, da je $f(n) = \sum_{d\,|\,n} \mu\left(\frac{n}{d}\right) g(d)$ za vse $n \in \mathbb{N}$. Potem je

$$\begin{aligned}\sum_{d\,|\,n} f(d) &= \sum_{d\,|\,n} \sum_{k\,|\,d} \mu\left(\frac{d}{k}\right) g(k) = \sum_{k\,|\,n} g(k) \sum_{k\,|\,d\,|\,n} \mu\left(\frac{d}{k}\right) \\ &= \sum_{k\,|\,n} g(k) \sum_{b\,|\,(n/k)} \mu(b) = g(n).\end{aligned}$$

Drugo enakost smo dobili z zamenjavo vrstnega reda seštevanja, tretjo z uvedbo nove spremenljivke $b = d/k$, četrta pa sledi iz (2). □

Zgled 4

- *Iz enačbe (1) sledi z Möbiusovim obratom, da je*

$$\varphi(n) = \sum_{d\,|\,n} \mu\left(\frac{n}{d}\right) d.$$

- *Za vse $n \in \mathbb{N}$ s $\tau(n)$ označimo število vseh pozitivnih deliteljev števila n. Torej je $\tau(n) = \sum_{d\,|\,n} 1$, od koder sledi z Möbiusovim obratom, da je*

$$\sum_{d\,|\,n} \mu\left(\frac{n}{d}\right) \tau(d) = 1.$$

- *Za vse $n \in \mathbb{N}$ s $\sigma(n)$ označimo vsoto vseh pozitivnih deliteljev števila n. Torej je $\sigma(n) = \sum_{d\,|\,n} d$, od koder sledi z Möbiusovim obratom, da je*

$$\sum_{d\,|\,n} \mu\left(\frac{n}{d}\right) \sigma(d) = n.$$

5 Kolobar aritmetičnih funkcij

Definicija 7 *Za aritmetični funkciji $f, g : \mathbb{N} \to \mathbb{C}$ in za vse $n \in \mathbb{N}$ naj bo*

$$(f * g)(n) = \sum_{d\,|\,n} f(d) g\left(\frac{n}{d}\right).$$

Aritmetična funkcija $f * g$ je Dirichletova konvolucija *funkcij f in g.*

Trditev 4 *Naj bodo f, g, h aritmetične funkcije. Potem velja:*

(i) $f * g = g * f$,

(ii) $(f * g) * h = f * (g * h)$,

(iii) $f * (g + h) = f * g + f * h$.

Dokaz:

(i) Trditev sledi iz zapisa Dirichletove konvolucije v simetrični obliki

$$(f * g)(n) = \sum_{de=n} f(d)g(e), \tag{3}$$

kjer seštevamo po vseh urejenih parih naravnih števil (d, e), katerih produkt je enak n.

(ii) Z uporabo enačbe (3) izračunamo

$$\begin{aligned}((f * g) * h)(n) &= \sum_{de=n} (f * g)(d)h(e) = \sum_{de=n} \left(\sum_{ab=d} f(a)g(b) \right) h(e) \\ &= \sum_{abe=n} f(a)g(b)h(e) = \sum_{ac=n} f(a) \sum_{be=c} g(b)h(e) \\ &= \sum_{ac=n} f(a)(g * h)(c) = (f * (g * h))(n).\end{aligned}$$

Četrto enakost smo dobili z uvedbo nove spremenljivke $c = be$.

(iii) Z uporabo enačbe (3) izračunamo

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

Iz trditve 4 sledi, da je množica vseh aritmetičnih funkcij $f : \mathbb{N} \to \mathbb{C}$ z operacijama $+$ in $*$ komutativen kolobar. Imenujemo ga *Dirichletov kolobar* in označimo z $\mathcal{D}$.

Funkcija $\varepsilon \in \mathcal{D}$, ki za vse $n \in \mathbb{N}$ zadošča enačbi

$$\varepsilon(n) = \begin{cases} 1, & n = 1, \\ 0, & n > 1, \end{cases}$$

je enica kolobarja $\mathcal{D}$, saj za vse $f \in \mathcal{D}$ in $n \in \mathbb{N}$ velja

$$(f * \varepsilon)(n) = \sum_{de=n} f(d)\varepsilon(e) = f(n)\varepsilon(1) = f(n).$$

Brez težav se lahko prepričamo tudi, da je $\mathcal{D}$ cel kolobar in da je funkcija $f \in \mathcal{D}$ obrnljiva natanko tedaj, ko $f(1) \neq 0$.

Zdaj lahko enačbo (2) prepišemo v obliki

$$\mu * \mathbf{1} \;=\; \varepsilon,$$

kjer $\mathbf{1}$ označuje konstantno funkcijo z vrednostjo 1. Z drugimi besedami, Möbiusova funkcija je inverz konstantne funkcije $\mathbf{1}$ glede na Dirichletovo konvolucijo:

$$\mu \;=\; \mathbf{1}^{-1}.$$

Möbiusov obrat lahko torej zapišemo v obliki

$$g \;=\; f * \mathbf{1} \quad\Longleftrightarrow\quad f \;=\; g * \mu,$$

kjer njegova veljavnost postane očitna. Zgled 4 pa lahko prepišemo v obliki

$$\begin{aligned} \varphi * \mathbf{1} \;=\; \mathrm{id}_{\mathbb{N}} \;&\Longrightarrow\; \varphi \;=\; \mu * \mathrm{id}_{\mathbb{N}}, \\ \tau \;=\; \mathbf{1} * \mathbf{1} \;&\Longrightarrow\; \mu * \tau \;=\; \mathbf{1}, \\ \sigma \;=\; \mathrm{id}_{\mathbb{N}} * \mathbf{1} \;&\Longrightarrow\; \mu * \sigma \;=\; \mathrm{id}_{\mathbb{N}}. \end{aligned}$$

Angleško-slovenski slovar strokovnih izrazov

proper pravi
pure pravi, čisti
versor versor, enotski kvaternion
dot product skalarni produkt
by-product stranski učinek

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.