VARIACIJE NA MOIVREOVO TEMO

ANTON CEDILNIK

Biotehniška fakulteta
Univerza v Ljubljani

Math. Subj. Class. (2010): 12D05, 13-01

Že iz srednje šole poznano Moivreovo formulo za potenciranje kompleksnih števil posplošimo na vse variante dvorazsežne enotske algebre nad poljubnim poljem.

VARIATIONS ON A THEME OF DE MOIVRE

We generalize Moivre's formula for exponentiating complex numbers, well known from high school, to all variants of two-dimensional unital algebras over any field.

Uvod

Algebra – matematična struktura in ne poglavje matematike – je vektorski prostor z dodatno operacijo, imenovano množenje, ki je distributivna in homogena. Bolj podrobno: če je $\mathcal{A}$ vektorski prostor nad komutativnim obsegom (poljem) $\mathbb{F}$ in ima preslikava $(a,b) \in \mathcal{A}^2 \mapsto a \cdot b \in \mathcal{A}$ lastnosti

$$\forall (a,b,c) \in \mathcal{A}^3 : (a+b) \cdot c = a \cdot c + b \cdot c, a \cdot (b+c) = a \cdot b + a \cdot c,$$
$$\forall (\lambda, a, b) \in \mathbb{F} \times \mathcal{A}^2 : (\lambda a) \cdot b = a \cdot (\lambda b) = \lambda (a \cdot b),$$

potem urejeni par $(\mathcal{A}, \cdot)$ imenujemo $\mathbb{F}$-**algebra**.

Če ni nevarnosti nesporazuma, po stari navadi namesto $a \cdot b$ pišemo kar ab. Pa tudi λab namesto $\lambda(a \cdot b)$.

Najprej nekaj nujnih definicij. **Razsežnost** (dimenzija) algebre $(\mathcal{A}, \cdot)$ je kar dimenzija vektorskega prostora $\mathcal{A}$.

Algebra $(\mathcal{A}, \cdot)$ je **asociativna**, če je

$$\forall (a,b,c) \in \mathcal{A}^3 : (ab)c = a(bc),$$

in **komutativna,** če je

$$\forall (a,b) \in \mathcal{A}^2 : ab = ba.$$

Algebra $(\mathcal{A},\cdot)$ je **enotska** (unitalna), če v njej obstaja element $e \neq 0$ **(enota)** z lastnostjo

$$\forall a \in \mathcal{A} : ea = ae = a.$$

Algebri $(\mathcal{A},\cdot)$ in $(\mathcal{B},\circ)$ sta **izomorfni**, če obstaja taka obrnljiva linearna preslikava $U : \mathcal{A} \to \mathcal{B}$ (**izomorfizem**), da je

$$\forall (a,b) \in \mathcal{A}^2 : U(a \cdot b) = U(a) \circ U(b).$$

Izomorfnih algeber navadno sploh ne razlikujemo, saj se pri njih vse z algebrsko strukturo povezane reči ujemajo.

Zelo preprosto je dokazati, da je enotski algebri izomorfna algebra tudi enotska in da vsak izomorfizem ohranja enoto.

Izomorfni algebri imata seveda isto dimenzijo. Klasificirati algebre iz razreda algeber z določeno dimenzijo pomeni razdeliti ta razred na podrazrede tako, da sta poljubni algebri iz istega podrazreda izomorfni, poljubni algebri iz različnih podrazredov pa sta neizomorfni. Navadno želimo iz vsakega podrazreda odlikovati po en primerek, ki ga potem okličemo za kanonskega in je klasifikacija dana kar s spiskom teh kanonskih algeber.

Moivreova formula

Primer, ki je tu še posebej zanimiv, je **realna algebra kompleksnih števil** $(\mathbb{C},\cdot)$, torej množica vseh kompleksnih števil kot realen dvorazsežni vektorski prostor skupaj z običajnim množenjem kompleksnih števil. Zaradi razčiščevanja pojmov se splača omeniti: skalarji so tu realna števila, vektorji so kompleksna števila. V zapisu $\lambda ab = \lambda \cdot a \cdot b$ je leva pika množenje realnega in kompleksnega števila, desna pika pa množenje kompleksnih števil; piki torej predstavljata različni operaciji, leva je množenje vektorja s skalarjem, desna pa je množenje vektorjev.

Znano **Moivreovo formulo** je leta 1707 odkril francoski matematik Abraham de Moivre (abraám dəmuávr, 1667–1754). V sodobni obliki se takole glasi:

$$\forall (n,\varphi) \in \mathbb{Z} \times \mathbb{R} : (\cos\varphi + i\sin\varphi)^n = \cos(n\varphi) + i\sin(n\varphi).$$

Dokaz gre s popolno indukcijo. Ponovimo ga, ker bo model za dokazovanje v prihodnje.

$n = 0:$ Formula trivialno velja.

$n = k:$ Predpostavljamo: $(\cos\varphi + i\sin\varphi)^k = \cos(k\varphi) + i\sin(k\varphi)$

$$
\begin{aligned}
n = k+1: (\cos\varphi + i\sin\varphi)^{k+1} &= (\cos\varphi + i\sin\varphi)^k(\cos\varphi + i\sin\varphi)\\
&= [\cos(k\varphi) + i\sin(k\varphi)](\cos\varphi + i\sin\varphi)\\
&= [\cos(k\varphi)\cos\varphi - \sin(k\varphi)\sin\varphi] + i[\cos(k\varphi)\sin\varphi + \sin(k\varphi)\cos\varphi]\\
&= \cos((k+1)\varphi) + i\sin((k+1)\varphi)\&
\end{aligned}
$$

$n < 0:$ Če označimo $n = -m$ in je $m > 0,$ je

$$
\begin{aligned}
&(\cos\varphi + i\sin\varphi)^n = (\cos\varphi + i\sin\varphi)^{-m}\\
&= \left(\frac{1}{\cos\varphi + i\sin\varphi}\right)^m = \left(\frac{\cos\varphi - i\sin\varphi}{(\cos\varphi + i\sin\varphi)(\cos\varphi - i\sin\varphi)}\right)^m\\
&= (\cos\varphi - i\sin\varphi)^m = [\cos(-\varphi) + i\sin(-\varphi)]^m\\
&= \cos(-m\varphi) + i\sin(-m\varphi) = \cos(n\varphi) + i\sin(n\varphi)
\end{aligned}
$$

Najpomembnejša uporaba Moivreove formule je seveda potenciranje kompleksnih števil. Napišimo ustrezno formulo kar brez (splošno znanega) dokaza za kompleksno število $x + iy \neq 0:$

$$\forall n \in \mathbb{Z} : (x + iy)^n = r^n[\cos(n\varphi) + i\sin(n\varphi)],$$

kjer je $r = +\sqrt{x^2 + y^2}$ in $\cos\varphi = \frac{x}{r}, \sin\varphi = \frac{y}{r}$. Ta formula se lahko ob primerni interpretaciji uporabi tudi za ne-cele n, a ta zgodba nas tu ne bo zanimala.

Klasifikacija dvorazsežnih enotskih algeber

Kdaj so se matematiki začeli zanimati za dvorazsežne posplošitve realne algebre kompleksnih števil, mi ni uspelo ugotoviti. Najstarejša najdena letnica v tej zvezi je bila 1848 v [4]. Sprva so premišljevali le o spremenjeni naravi imaginarne enote i, potem pa se je z razvojem teorije vektorskih prostorov nad poljubnim poljem naravno odprlo vprašanje, kaj če realna števila nadomestimo s kakim drugim poljem.

Zastavimo si nalogo klasificirati vse dvorazsežne enotske algebre nad poljubnim poljem $\mathbb{F}$! Bazo algebre naj vedno sestavljata enota e in še en element u. Potem ima vsaka multiplikacijska tabela take algebre zelo preprosto obliko (glej tabelo 1). Skalarja λ in μ sta **strukturni konstanti** in sta v načelu še povsem poljubna, bo pa klasifikacija odvisna ravno od njiju.

$\cdot$	e	u
e	e	u
u	u	$\lambda e + \mu u$

Tabela 1. Dvorazsežna enotska algebra.

Preprosto je dokazati, da so vse te algebre komutativne in asociativne.

Le kot zanimivost omenimo še, da za vsak element $c = \alpha e + \beta u, (\alpha, \beta) \in \mathbb{F}^2$, velja kvadratična enačba $c^2 - T(c)c + N(c)e = 0$, kjer sta funkcionala T in N podana takole: $T(c) = 2\alpha + \beta\mu, N(c) = \alpha^2 + \alpha\beta\mu - \beta^2\lambda$. Dokaz je zelo preprost: v izpeljavi

$$\begin{aligned} 0 &= c^2 - T(c)c + N(c)e \\ &= [\alpha^2 e + 2\alpha\beta u + \beta^2(\lambda e + \mu u)] - T(c)[\alpha e + \beta u] + N(c)e \\ &= [\alpha^2 + \beta^2\lambda - T(c)\alpha + N(c)]e + [2\alpha\beta + \beta^2\mu - T(c)\beta]u \end{aligned}$$

morata v zadnjem delu oba koeficienta biti enaka nič zaradi linearne neodvisnosti elementov e in u. T je linearen (aditiven in homogen), N pa je multiplikativen in 2-homogen, tj. za a, b, c iz algebre in skalar δ velja:

$$\begin{aligned} T(a+b) &= T(a) + T(b), \\ T(\delta c) &= \delta T(c), \\ N(ab) &= N(a)N(b), \\ N(\delta c) &= \delta^2 N(c). \end{aligned}$$

Tudi nekakšno konjugiranje lahko uvedemo: $\overline{\alpha e + \beta u} := (\alpha + \beta\mu)e - \beta u$. Bralec bo zlahka dokazal naslednje relacije, kjer sta c in d elementa algebre, δ pa skalar:

$$\overline{c \pm d} = \overline{c} \pm \overline{d},\ \ \overline{\delta c} = \delta\overline{c},\ \ \overline{cd} = \overline{c}\,\overline{d}.$$
$$\overline{\overline{c}} = c,\ \ c + \overline{c} = T(c)e,\ \ c\overline{c} = N(c)e.$$

Imejmo še eno tako algebro, enota naj bo f, drugi element baze v pa naj ima kvadrat $v^2 = \sigma f + \tau v, (\sigma, \tau) \in \mathbb{F}^2$. Če sta algebri izomorfni, obstaja izomorfizem U z vrednostma $U(e) = f, U(u) = xf + yv, (x, y) \in \mathbb{F}^2$. Ker obrnljivi operator linearno neodvisna elementa preslika spet v linearno neodvisni sliki, mora biti $y \neq 0$. Naredimo tale račun:

$$\begin{aligned} (\lambda + \mu x)f + \mu y v &= U(\lambda e + \mu u) = U(u^2) \\ &= U(u)^2 = (xf + yv)^2 = (x^2 + \sigma y^2)f + (2xy + \tau y^2)v. \end{aligned}$$

Takoj sledita enačbi

$$\lambda + \mu x = x^2 + \sigma y^2, \quad \mu y = 2xy + \tau y^2.$$

Poenostavimo:

$$\lambda = -x^2 - \tau xy + \sigma y^2, \quad \mu = 2x + \tau y. \tag{1}$$

Povzemimo: algebri s paroma strukturnih konstant (λ, μ) in (σ, τ) sta izomorfni natanko tedaj, ko obstaja tak par $(x, y \neq 0) \in \mathbb{F}^2$, da sta enačbi (1) izpolnjeni.

Preden nadaljujemo, se spomnimo, kaj je karakteristika polja – označili jo bomo s simbolom char $\mathbb{F}$. Recimo, da velja sklep[1]

$$n \in \mathbb{N} \land \forall \delta \in \mathbb{F} : n\delta = 0 \;\Rightarrow\; n = 0.$$

Potem je char $\mathbb{F} = 0$. Nasprotno od tega pa obstaja tako najmanjše naravno število $n > 0$, da je za vsak δ iz $\mathbb{F}$ velja $n\delta = 0$, in tedaj je char $\mathbb{F} = n$. Izkaže se še, da je neničelna karakteristika nujno praštevilo. Več o tem najdemo v [2, str. 107].

Sistem (1) obravnavajmo najprej v primeru char $\mathbb{F} \neq 2$. Tedaj je $x = \frac{1}{2}\mu - \frac{1}{2}\tau y$ in

$$4\lambda + \mu^2 = (4\sigma + \tau^2)y^2. \tag{2}$$

Iz enačbe (2) razberemo, da je algebra s poljubnim parom strukturnih konstant (σ, τ) izomorfna algebri s parom $(4\sigma + \tau^2, 0)$ (izbrali smo $y = 2$), torej da smemo predpostavljati $\mu = \tau = 0$. Enačba (2) se močno poenostavi: $\lambda = \sigma y^2$, problem pa razpade na tri možnosti:

- $\sigma = 0$ in zato tudi $\lambda = 0$;
- σ ni kvadrat in tak je potem tudi λ;
- σ je neničelni kvadrat in potem je lahko $\lambda = 1$ pri izbiri $y = \sigma^{-1/2}$.

Povzemimo te ugotovitve z nekoliko spremenjenimi oznakami!

Izrek 1 (Klasifikacija dvorazsežnih enotskih algeber s karakteristiko $\neq 2$). *Če je algebra podana s tabelo 1, je ena od naslednjih tipov:*

A. char $\mathbb{F} \neq 2, \mu = \lambda = 0$.

---

[1] Ali je 0 naravno število ali ne, je bolj kot ne stvar okusa, saj enotnega mnenja med matematiki po svetu ni. V tem članku velja, da so naravna števila pač moči končnih množic. Torej $\mathbb{N} = \mathbb{Z}^+ \cup \{0\}$ in zato $0 \in \mathbb{N}$.

B. char $\mathbb{F} \neq 2, \mu = 0, \lambda$ *ni kvadrat; dve taki algebri s parametroma* λ_1 *in* λ_2 *sta izomorfni natanko tedaj, ko je* $\lambda_1\lambda_2$ *kvadrat.*

C. char $\mathbb{F} \neq 2, \mu = 0, \lambda = 1.$

Opozoriti je treba, da ta klasifikacija dejansko ni popolna, saj je neizomorfnih algeber tipa B lahko še mnogo – v primeru $\mathbb{F} = \mathbb{Q}$ (polje racionalnih števil) jih je celo neskončno. A kaj več se ne da povedati, če o obravnavanem polju nič ne vemo.

Zdaj pa se omejimo na primer char $\mathbb{F} = 2$. Spomnimo na tri nenavadne posledice take karakteristike: za vsak par $(\alpha, \beta) \in \mathbb{F}^2$ je $2\alpha = 0, -\alpha = \alpha, (\alpha + \beta)^2 = \alpha^2 + \beta^2$.

Sistem (1) se takole poenostavi:

$$\lambda = x^2 + \tau xy + \sigma y^2, \quad \mu = \tau y. \tag{3}$$

Če je $\tau = 0$, je tudi $\mu = 0$. Če pa je $\tau \neq 0$, lahko z izbiro $y = \tau^{-1}$ dobimo $\mu = 1$. Problem klasifikacije zato razpade na dva dela: $\mu = \tau = 0$ in $\mu = \tau = y = 1$. Nadaljevanje gre v istem slogu in brez odvečnih besed napišimo končni rezultat.

Izrek 2 (Klasifikacija dvorazsežnih enotskih algeber s karakteristiko 2). *Če je algebra podana s tabelo 1, je ena od naslednjih tipov:*

D. char $\mathbb{F} = 2,\ \mu = \lambda = 0.$

E. char $\mathbb{F} = 2,\ \mu = 0,\ \lambda$ *ni kvadrat; dve taki algebri s parametroma* λ_1 *in* λ_2 *sta izomorfni natanko tedaj, ko je rešljiva enačba* $\lambda_2 = x^2 + \lambda_1 y^2$ *z neznankama* x, y.

F. char $\mathbb{F} = 2,\ \mu = 1,\ \lambda = 0.$

G. char $\mathbb{F} = 2,\ \mu = 1,\ \forall x \in \mathbb{F} : x^2 + x + \lambda \neq 0$*; dve taki algebri s parametroma* λ_1 *in* λ_2 *sta izomorfni natanko tedaj, ko je rešljiva enačba* $\lambda_2 = x^2 + x + \lambda_1$ *z neznanko* x.

Tudi klasifikacija v izreku 2 ni popolna pri algebrah tipov E in G. Popolno klasifikacijo lahko dobimo le, če o polju vemo vsaj to, kako je z rešitvami kvadratičnih enačb.

Klasifikacija realnih algeber zelo preprosto sledi iz izreka 1. Le tri algebre obstajajo:

A. $\mathbb{F} = \mathbb{R},\ \mu = \lambda = 0.$

B. $\mathbb{F} = \mathbb{R},\ \mu = 0, \lambda = -1.$

C. $\mathbb{F} = \mathbb{R},\ \mu = 0, \lambda = 1.$

Elementom algebre A pravimo **dualna števila** in tistim iz algebre C **razcepno-kompleksna števila**. Algebra B je pa seveda kar algebra kompleksnih števil.[2]

Klasifikacija kompleksnih algeber je še bolj preprosta; samo dve sta:

A. $\mathbb{F} = \mathbb{C},\ \mu = \lambda = 0.$

C. $\mathbb{F} = \mathbb{C},\ \mu = 0,\ \lambda = 1$

Še zadnji primer, tokrat z najmanjšim poljem $\mathbb{Z}_2$, ki ima le elementa 0 in 1, seštevanje in množenje pa izvajamo po modulu 2:

$$0 + 0 = 1 + 1 = 0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0,$$
$$0 + 1 = 1 + 0 = 1 \cdot 1 = 1.$$

Potem z uporabo izreka 2 dobimo tole klasifikacijo s tremi kanonskimi algebrami:

D. $\mathbb{F} = \mathbb{Z}_2,\ \mu = \lambda = 0.$

F. $\mathbb{F} = \mathbb{Z}_2,\ \mu = 1,\ \lambda = 0.$

G. $\mathbb{F} = \mathbb{Z}_2,\ \mu = \lambda = 1.$

Tile posebni primeri primaknejo predzadnji kamenček h klasifikaciji, namreč eksistenco tipov algeber iz izrekov 1 in 2. Le še eksistenco tipa E bi bilo treba dokazati, a se bomo temu izognili; izkaže se namreč [2, str. 285], da je polje s karakteristiko 2, ki ima vsaj kakšen ne-kvadrat, nujno neskončno.

Potenciranje v dvorazsežnih enotskih algebrah

Če nam je Moivreova formula dana, je dokaz njene pravilnosti – kot smo videli na začetku – dokaj preprost. Podobno je s formulami za potenciranje v poljubni dvorazsežni enotski algebri. Zato bomo tu samo navedli vse formule, skoraj vse dokazovanje pa prepustili marljivemu bralcu.

Povsod naj bo $c = \alpha e + \beta u \neq 0, (\alpha, \beta) \in \mathbb{F}^2$ in $n \in \mathbb{Z}$. Trivialni potenci v vseh primerih: $c^0 = e, c^1 = c$.

A. $\alpha = 0: \ c^n = 0$ za $n > 1$
$\alpha \neq 0: \ c^n = \alpha^n e + n\alpha^{n-1}\beta u$

[2]Pedantno povedano: Algebra tipa B je izomorfna realni algebri kompleksnih števil.

B. $c^n = \frac{1}{2}\left[\left(\alpha+\beta\sqrt{\lambda}\right)^n + \left(\alpha-\beta\sqrt{\lambda}\right)^n\right]e + \frac{1}{2\sqrt{\lambda}}\left[\left(\alpha+\beta\sqrt{\lambda}\right)^n - \left(\alpha-\beta\sqrt{\lambda}\right)^n\right]u$
Formulo razumemo tako, kot da $\sqrt{\lambda}$ v resnici obstaja v $\mathbb{F}$; bolj strokovno pravimo, da računamo v enostavni korenski razširitvi polja $\mathbb{F}$ [2, str. 308]. Če res izračunamo tako potenco za neki konkreten n, v rezultatu $\sqrt{\lambda}$ ne nastopa več.

C. $c^n = \frac{1}{2}\left[(\alpha+\beta)^n + (\alpha-\beta)^n\right]e + \frac{1}{2}\left[(\alpha+\beta)^n - (\alpha-\beta)^n\right]u$, v primeru $\alpha^2 = \beta^2$ le za $n \geq 0$

D. $\alpha = 0: \ c^n = 0$ za $n > 1$
$\alpha \neq 0: \ c^{2n} = \alpha^{2n}e, c^{2n+1} = \alpha^{2n}(\alpha e + \beta u)$

E. $c^{2n} = (\alpha^2 + \beta^2\lambda)^n e, \ c^{2n+1} = (\alpha^2+\beta^2\lambda)^n(\alpha e + \beta u)$

F. $c^n = \alpha^n e + [\alpha^n + (\alpha+\beta)^n]u$, v primeru $\alpha(\alpha+\beta) = 0$ le za $n \geq 0$

G. $\beta = 0: \ c^n = a^n e$
$\beta \neq 0: \ c^n = \beta^n\left([B_{n+1} + (\gamma+1)B_n]e + B_n u\right)$, kjer je $\gamma := \alpha\beta^{-1}$ in $\delta := \gamma^2 + \gamma + \lambda$. Koeficienti B_n zadoščajo diferenčni enačbi

$$B_{n+2} + B_{n+1} + \delta B_n = 0, \quad B_0 = 0, \quad B_1 = 1.$$

Rešitev tega diferenčnega problema je (za $n > 0$):

$$B_{2n} = 1 + \sum_{k=1}^{n}\left[\binom{n - \operatorname{int}\frac{k+1}{2}}{n-k} + \binom{n-1-\operatorname{int}\frac{k}{2}}{n-k}\right]\delta^k,$$

$$B_{2n+1} = 1 + \sum_{k=1}^{n}\binom{n-\operatorname{int}\frac{k+1}{2}}{n-k}\delta^k, B_{-n} = \delta^{-n}B_n.$$

V formulah za tip G nastopa v binomskih simbolih funkcija **celi del** $\operatorname{int} x$, ki jo pogosto označujejo tudi s simbolom $\lfloor x \rfloor$. Ta funkcija priredi realnemu številu x največje celo število, ki ni večje od x.

Še tole mimogrede omenimo: koeficienti B_n zadoščajo še eni zanimivi identiteti: $B_{n+1}^2 + B_{n+1}B_n + \delta B_n^2 = \delta^n$. Dokaz je dokaj preprost in tu povejmo samo, da sledi iz računa $c^{n+1}c^{-(n+1)} = e$.

Formul za tip G doslej še nisem zasledil nikjer v matematični literaturi. Vem pa iz [3], da jih je leta 2014 izpeljal slovenski matematik Marko Petkovšek, zato bom te formule imenoval **Petkovškove formule**; glej tudi [4].

Pri tipih B, E in G se vse potence dajo neomejeno izračunati, v posebnem tudi potenca c^{-1} za $c \neq 0$, kar pomeni, da v takih algebrah lahko definiramo deljenje (zato jih tudi imenujemo **algebre z deljenjem**). Ker so te algebre asociativne in komutativne in imajo deljenje, so to dejansko polja, razširitve prvotnega polja $\mathbb{F}$ v istem smislu, kot je polje $\mathbb{C}$ razširitev polja $\mathbb{R}$. Iz $\frac{a}{b} = ab^{-1}$ in formul za potenciranje dobimo za $(\alpha, \beta, \gamma, \delta) \in \mathbb{F}^4, \gamma e + \delta u \neq 0$:

B. $\frac{\alpha e+\beta u}{\gamma e+\delta u} = \left(\gamma^2 - \delta^2\lambda\right)^{-1} \left[(\alpha\gamma - \beta\delta\lambda)\, e + (\beta\gamma - \alpha\delta)\, u\right]$

E. $\frac{\alpha e+\beta u}{\gamma e+\delta u} = \left(\gamma^2 + \delta^2\lambda\right)^{-1} \left[(\alpha\gamma + \beta\delta\lambda)\, e + (\beta\gamma + \alpha\delta)\, u\right]$

G. $\frac{\alpha e+\beta u}{\gamma e+\delta u} = \left(\gamma^2 + \gamma\delta + \delta^2\lambda\right)^{-1} \left[(\alpha\gamma + \alpha\delta + \beta\delta\lambda)\, e + (\beta\gamma + \alpha\delta)\, u\right]$

Za konec pa še nekaj besed o dokazovanju formul za potenciranje. Dokazi se – kot že rečeno – lahko naredijo na način, ki smo ga prikazali v razdelku Moivreova formula za originalno Moivreovo formulo. No, vsaj pri tipih B, E in G ni nobene bistvene razlike. Nekoliko več pazljivosti zahtevajo preostali tipi, ker je treba še ugotoviti, katere potence sploh obstajajo.

B. Russell, angleški matematik in filozof, je izrekel tole misel: *Kdaj pa kdaj se je dobro vprašati o sleherni stvari, ki se vam zdi samoumevna.* Sledimo tej misli in se vprašajmo, kaj sploh so potence – ne pozabimo namreč, da gre tu za »eksotično okolje« algebre in ne za neko številsko množico.

Enotski kolobar [2, str. 84] je taka posplošitev polja, v kateri ne zahtevamo eksistence inverznega elementa za neničelne elemente in torej deljenje ni vedno izvedljivo. Pa še komutativnosti množenja tudi ne zahtevamo več. Prav lahko je videti, da so vse algebre A – G taki kolobarji.

V kolobarju $\mathcal{K}$ z enoto e se potenciranje definira kot množenje enakih faktorjev:

$$\forall a \in \mathcal{K}\ \ \forall n \in \mathbb{N} : a^0 := e, a^{n+1} := aa^n.$$

Za te potence veljata osnovna zakona:

$$\forall a \in \mathcal{K}\ \ \forall (m,n) \in (\mathbb{N})^2 : a^m a^n = a^{m+n}, (a^m)^n = a^{mn}. \tag{4}$$

Od tod dalje pa velja splošno sprejet dogovor: Ostale potence s celoštevilskimi ali celo racionalnimi eksponenti naj bodo definirane tako, da zakona (4) ostaneta veljavna. S popolno indukcijo lahko še dokažemo

$$\forall (a,b) \in \mathcal{K}^2\ \ \forall n \in \mathbb{N} : [ab = ba \Rightarrow (ab)^n = a^n b^n = b^n a^n]. \tag{5}$$

Glede na to, da je polje realnih števil tudi enotski kolobar, je naravno vprašanje, zakaj v splošnem kolobarju privzamemo $0^0 = e$, pri delu z realnimi števili pa ne. Odgovor je preprost: zahteva $0^0 = 1$ povzroči nezveznost potenciranja, čemur se pa radi izognemo. Primer: Za funkcijo

$$f(x) := \begin{cases} (\ln|x|)^{-1} \cdot \ln 2 & x \neq 0 \\ 0 & x = 0 \end{cases} \tag{6}$$

velja

$$\lim_{x\to 0} |x|^{f(x)} = 2 \neq 1 = |0|^{f(0)}$$

Pri delu s številskimi kolobarji zato 0^0 pustimo nedefiniran.

Pomemben argument za smiselnost enačbe $0^0 = e$ je naslednji. V kolobarju lahko obstaja kakšen **nilpotent**, torej tak $r \in \mathcal{K}$, da je $r \neq 0 = r^k$ za neki $k \in \mathbb{Z}^+$ (v algebrah tipov A in D je u tak element). Potem mora veljati: $e = r^0 = r^{0\cdot k} = (r^k)^0 = 0^0$. Element 0 pa v nobenem kolobarju ne more imeti negativnega eksponenta, ker bi to vodilo v protislovje: $0 = 0 \cdot 0^{-1} = 0^1 \cdot 0^{-1} = 0^{1-1} = 0^0 = e$.

Potence neničelnega elementa z negativnimi eksponenti so najtesneje povezane z inverznim elementom: a^{-1} je definiran z identiteto $aa^{-1} = a^{-1}a = e$. Ti enačbi na splošno nista rešljivi in tak element potem nima potenc z negativnimi eksponenti. Če pa rešitev obstaja, je ena sama, ker če bi obstajali dve rešitvi $a^{-1} = b$ in $a^{-1} = c$, bi sledilo: $b = eb = (ca)b = c(ab) = ce = c$

Druge potence z negativnimi eksponenti so definirane z identiteto $a^{-n} = (a^{-1})^n$. Zaradi lastnosti (5) je $a^{-n}a^n = (a^{-1})^n a^n = a^n (a^{-1})^n = a^n a^{-n}$ in $(a^{-1})^n a^n = (a^{-1}a)^n = e^n = e$, zato $a^{-n} = (a^n)^{-1}$, kar potrjuje, da so take potence dobro definirane.

Kot primer dokazujmo formulo za potenciranje v algebri tipa C. Označimo $p = \frac{1}{2}(e+u)$ in $q = \frac{1}{2}(e-u)$. p in q sta linearno neodvisna in sta **idempotenta:** $p^2 = p$, $q^2 = q$, pa še $pq = 0$ in $\alpha e + \beta u = (\alpha+\beta)p + (\alpha-\beta)q$. Mimogrede: prav tale zadnja dekompozicija je vzrok, da elementom algebre tipa C nad realnimi števili rečemo razcepno-kompleksna števila.

S popolno indukcijo dokažemo, da je $(\delta p + \varepsilon q)^n = \delta^n p + \varepsilon^n q$ za vsako celo število n. Seveda mora v primeru $n < 0$ biti $\delta \neq 0 \neq \varepsilon$.

Elementi oblike δp ali εq pa ne morejo imeti negativnih eksponentov. Kot primer rešujmo enačbo za inverz elementa p. Obstajati morata taka skalarja x, y, da je $pp^{-1} = p(xp + yq) = e = p + q$. Sledi: $xp = p + q$, kar pa zaradi linearne neodvisnosti p in q ni mogoče.

LITERATURA

[1] M. Petkovšek in H. Zakrajšek, *Solving linear recurrence equations with polynomial coefficients, Computer algebra in quantum field theory*, Texts Monogr. Symbol. Comput., Springer, Vienna, 259–284, 2013.

[2] I. Vidav, *Algebra*, Mladinska knjiga, Ljubljana 1972.

[3] Osebni kontakt.

[4] *Split-complex/number*, dostopno na `en.wikipedia.org/wiki/Split-complex\_number`, ogled 2. 9. 2022.