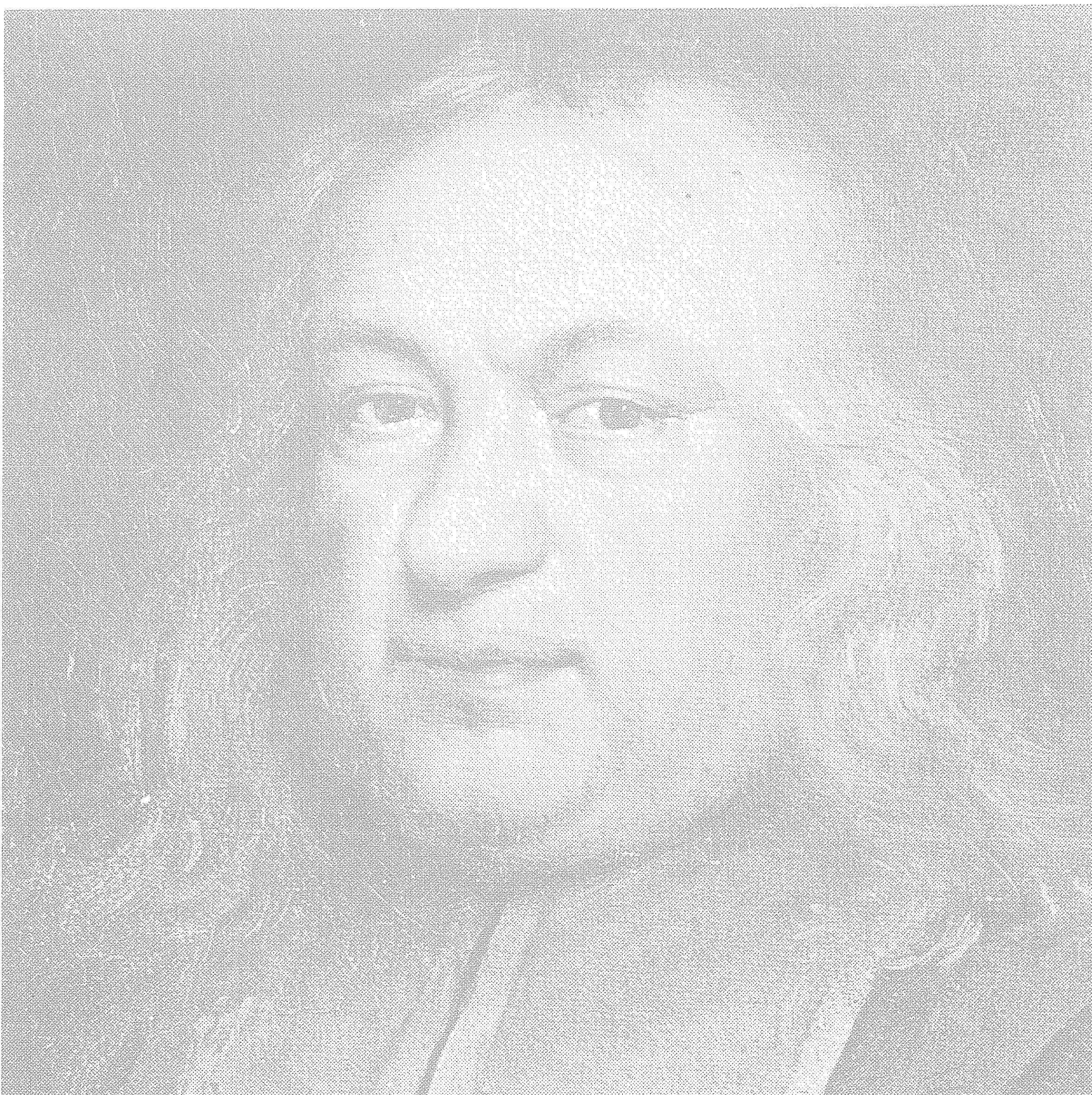


1994

Letnik 41

2

OBZORNIK ZA MATEMATIKO IN FIZIKO



OBZORNIK ZA MATEMATIKO IN FIZIKO

LJUBLJANA, MAREC 1994

letnik 41, številka 2, strani 33–64

Glasilo Društva matematikov, fizikov in astronomov Slovenije, 61111 Ljubljana, Jadranska c. 19, p.p. 64, telefonska št. (061) 265-061/53, žiro račun 50101-678-47233, devizna nakazila SKB banka d.d. Ljubljana, val-27621-42961/9, Ajdovščina 4, Ljubljana.

Uredniški odbor: Mirko Dobovišek (glavni urednik), Boris Lavrič (urednik za matematiko in odgovorni urednik), Martin Čopič (urednik za fiziko), Boštjan Jaklič (tehnični urednik).

Jezikovno pregledal Janez Juvan, računalniško oblikoval Martin Zemljič.

Člani društva prejemajo Obzornik brezplačno. Celoletna članarina 1.900,– SIT. Naročnina v knjigarnah in za ustanove 3.800,– SIT, za tujino 40 DEM. Posamezna številka za člane 400,– SIT, dvojna številka 800,– SIT, stare številke 300,– SIT.

Tisk: KURIR print d.o.o. Naklada 1500 izvodov.

Revijo sofinancirata Ministrstvo za znanost in tehnologijo ter Ministrstvo za šolstvo in šport.

Po mnenju MZT št. 415-52/92 z dne 5.2.1992 šteje revija med proizvode iz 13. točke tarifne št. 3 zakona o prometnem davku, za katere se plačuje 5% davek od prometa proizvodov.

© 1994 DMFA Slovenije – 1191

Poštnina plačana na pošti 61102 Ljubljana

VSEBINA — CONTENTS

Članki — Articles

Str.–Page

Fermatov problem končno rešen? — Fermat's last theorem finally proved?

(Ivan Vidav) 33–44

Urejeni številski obsegi — Ordered fields (Boris Lavrič) 45–50

Realne algebre, ki zadoščajo kvadratni enačbi — Real algebras satisfying

quadratic identity (Borut Zalar) 51–58

Radon v okolju — Radon in our environment (Andrej Likar) 59–63

Vesti — News

Prof. Djuro Kurepa in memoriam (Anton Suhadolc) III

Novi člani DMFA Slovenije v letu 1993 (Martina Koman) IV

Nove knjige — New books (Anton Suhadolc) 64–III

Na ovitku: Pierre Fermat, 1601–1665. Glej tudi članek na strani 33.

FERMATOV PROBLEM KONČNO REŠEN?

IVAN VIDAČ

Math. Subj. Class. (1991) 14H52, 11G05, 11F03

Članek vsebuje elementaren opis eliptičnih krivulj in modulskih funkcij in navaja nekaj osnovnih izrekov, ki so pomembni pri reševanju Fermatovega problema.

FERMAT'S LAST THEOREM FINALLY PROVED?

Elementary properties of elliptic curves and modular functions are described and some basic theorems relevant for the proof of the last Fermat's theorem are stated.

Lansko poletje se je razširila vest, da je angleški matematik Andrew Wiles, ki dela na univerzi v Princetonu, rešil s pomočjo teorije eliptičnih krivulj in modulskih funkcij slavní Fermatov problem, se pravi, da je dokazal zadnji Fermatov izrek, ki se glasi:

Naj bo n naravno število, večje od 2. Enačba

$$a^n + b^n = c^n \tag{1}$$

nima rešitve v celih od nič različnih številih a , b , c .

Fermat je to trditev zapisal okoli leta 1637 kot opombo na robu knjige *Arithmetica* grškega matematika Diofanta in dodal, da je našel zanjo čudovit dokaz, ki ga pa žal pozneje nikoli ni objavil.

Pripomba. Denimo, da za neki eksponent n enačba (1) ni rešljiva. Potem ni rešljiva pri nobenem naravnem r niti enačba

$$u^{nr} + v^{nr} = w^{nr}$$

v celih od nič različnih številih u , v , w . Vsaka taka rešitev bi namreč dala rešitev $a = u^r$, $b = v^r$, $c = w^r$ enačbe (1) v celih od nič različnih številih. Naravno število, večje od 2, ki ni potenca od 2, je deljivo vsaj z enim lihim praštevilom, če pa je potenca od 2, je deljivo s 4. Zato je dovolj dokazati Fermatov izrek za $n = 4$ in za vse eksponente $n = p$, ki so liha praštevila.

1. Oglejmo si prav na kratko glavne mejnike pri reševanju Fermatovega problema. Upravičeno smemo domnevati, da je imel Fermat neoporečen dokaz, in sicer z metodo neskončnega spusta, le za primer $n = 4$. Okoli sto let pozneje je Euler ugotovil pravilnost domneve pri $n = 3$. Eksponent $n = 5$ sta ugnala skoraj istočasno Dirichlet (1828) in Legendre (1830). Njuno dokazovanje je bilo precej zapleteno. Leta 1912 je Plemelj objavil zelo preprost dokaz za pete potence, in sicer kot lep zgled za uporabo obsega,

ki ga dobimo, če racionalnim številom dodamo $\sqrt{5}$. Lamé je leta 1839 skušal dokazati primer $n = 7$, pa je napravil napako, ki jo je odpravil Henri Lebesgue leta 1840.

Zares velik korak naprej je napravil Kummer leta 1847. Obravnaval je enačbo (1) v ciklotomskem obsegu, ker se dá v njem leva stran razstaviti na linearne faktorje. (Ciklotomski obseg je najmanjši algebraični obseg števil, ki vsebuje racionalna števila in vse korene enačbe $x^n - 1 = 0$.) Ker v kolobarjih celih algebraičnih števil ne velja vedno izrek o enolični faktorizaciji, je Kummer izdelal posebno teorijo idealov, da je premostil to težavo. S teorijo idealov mu je uspelo dokazati pravilnost Fermatovega izreka za vsa *regularna praštevila*.

Regularna praštevila se dajo najlažje opredeliti s pomočjo Bernoullijevih števil, ki jih dobimo, če razvijemo v Taylorjevo vrsto funkcijo $f(t) = \frac{t}{2} \cdot \frac{e^t + 1}{e^t - 1}$. Ker je f soda, nastopajo v tem razvoju samo sode potence od t :

$$\frac{t}{2} \cdot \frac{e^t + 1}{e^t - 1} = 1 + B_2 \frac{t^2}{2!} + B_4 \frac{t^4}{4!} + B_6 \frac{t^6}{6!} + \dots$$

Koeficienti B_{2k} se imenujejo Bernoullijeva števila. So racionalni in jih zato lahko pišemo v obliki okrajšanih ulomkov. Liho praštevilo p se imenuje *regularno*, če ne deli števca nobenega izmed okrajšanih ulomkov $B_2, \dots, B_{p-3}$. Do sto so regularna vsa liha praštevila z izjemo 37, 59 in 67. Ni znano, ali je regularnih praštevil neskončno. Pač pa je Jensen leta 1915 dokazal, da je neregularnih neskončno.

Nadaljnji pomemben napredek pri reševanju Fermatovega problema je bil dosežen, ko je nemškemu matematiku Faltingsu leta 1983 uspelo dokazati Mordellovo domnevo. Preden povemo, za kaj gre pri tej domnevi, potrebujemo nekaj pojasnil iz algebraične geometrije.

Algebraična krivulja v ravnini je definirana z enačbo

$$f(x, y) = 0, \tag{2}$$

kjer je $f(x, y)$ nekonstanten polinom s poljubnimi koeficienti. Krivuljo sestavljajo vse točke (x, y) , katerih koordinate x in y zadoščajo enačbi (2). Če je npr. $f(x, y)$ polinom druge stopnje, ki ni produkt dveh linearnih faktorjev, je pripadajoča krivulja stožnica.

Točka (a, b) na krivulji (2) je singularna, če sta v njej oba parcialna odvoda $f_x = \partial f / \partial x$ in $f_y = \partial f / \partial y$ enaka nič, če je torej

$$f(a, b) = 0, \quad f_x(a, b) = 0 \quad \text{in} \quad f_y(a, b) = 0.$$

Singularne so na primer vse dvojne in večkratne točke.

Pogosto nas zanima vedenje krivulje v neskončnosti. V ta namen preselimo obravnavo v projektivno ravnino, ki jo dobimo, če evklidski (afini)

ravnini dodamo točke v neskončnosti in premico v neskončnosti. Tudi točkam v neskončnosti je treba prirediti koordinate. To napravimo z uvedbo homogenih koordinat. Trojko X, Y, Z imenujemo homogene koordinate točke z običajnim (afinim) koordinatama x in y , če velja $x = X/Z$ in $y = Y/Z$. Seveda mora biti $Z \neq 0$. Točka v neskončnosti pa ima tretjo koordinato $Z = 0$. Določa jo razmerje prvih dveh koordinat X/Y .

Do enačbe krivulje v homogenih koordinatah pridemo tako, da vstavimo v (2) $x = X/Z$ in $y = Y/Z$ in potem enačbo pomnožimo še z Z^n (n je stopnja polinoma f). Zaznamujmo

$$F(X, Y, Z) = Z^n f(X/Z, Y/Z).$$

F je homogen polinom stopnje n spremenljivk X, Y, Z . Enačba krivulje (2) v homogenih koordinatah se glasi

$$F(X, Y, Z) = 0. \quad (2^*)$$

Točke v neskončnosti, ki leže na krivulji, dobimo, če postavimo $Z = 0$. Pripadajoča enačba $F(X, Y, 0) = 0$ je stopnje n za razmerje X/Y . Zato ima krivulja stopnje n največ n (realnih) točk v neskončnosti. Algebraično krivuljo z dodanimi točkami v neskončnosti imenujemo *projektivna krivulja*.

Enačbo (2) lahko obravnavamo tudi v obsegu kompleksnih števil. Zanima nas množica vseh kompleksnih parov (z, w) , ki zadoščajo enačbi

$$f(z, w) = 0. \quad (2^{**})$$

Par kompleksnih števil (z, w) , kjer je $z = x + iy$ in $w = u + iv$, si ponazorimo s točko s koordinatami (x, y, u, v) v štirirazsežnem evklidskem prostoru $\mathbb{R}^4$. Algebraična krivulja, to je množica vseh rešitev enačbe (2**), je pravzaprav neka ploskev v $\mathbb{R}^4$. Poljubno si namreč lahko izberemo koordinati x in y , se pravi dve števili, pišemo $z = x + iy$ in pri tem z izračunamo $w = u + iv$ iz enačbe (2**) (le-ta je v kompleksnem vselej rešljiva). Tudi zdaj dodamo točke v neskončnosti, ki jih seveda določajo kompleksne rešitve enačbe $F(X, Y, 0) = 0$. Če je krivulja (2**) brez singularnih točk, je ploskev, ki jo določa v štirirazsežnem prostoru množica vseh kompleksnih rešitev enačbe (2**) z dodanimi točkami v neskončnosti, sklenjena. To ploskev predstavimo v trirazsežnem prostoru s topološko ekvivalentno ploskvijo, po navadi s sfero, ki smo ji dodali nekaj ročajev. Število ročajev zaznamujemo z g in imenujemo *rod krivulje* (2**) oziroma (2). Rod je lahko 0 (ročajev ni, ploskev je sfera) ali pozitivno celo število. Rod g , ki meri zapletenost algebraične krivulje, se da opredeliti tudi za krivulje s singularnimi točkami.

Kako izračunamo rod? Če je krivulja brez singularnih točk (ne sme imeti niti kompleksnih singularnih točk niti singularnih točk v neskončnosti), dobimo g po obrazcu

$$g = \frac{1}{2}(n-1)(n-2), \quad (3)$$

kjer je n stopnja polinoma f . Pri stožnicah je $n = 2$, torej $g = 0$. Za nesingularne kubične krivulje ($n = 3$) je rod $g = 1$. Splošno imenujemo krivulje z rodом $g = 1$ *eliptične krivulje*. Vsaka nesingularna kubična krivulja je torej eliptična.

Točka (x, y) v ravnini je celoštevilsko, če sta njeni koordinati x in y celi števili, in racionalna, če sta racionalni števili. Racionalne in celoštevilске točke nas zanimajo predvsem na krivuljah, pri katerih ima polinom f v enačbi (2) racionalne oziroma cele koeficiente. Racionalni koordinati x in y izrazimo v obliki ulomkov

$$x = \frac{a}{c}, \quad y = \frac{b}{c}, \quad (*)$$

kjer so a, b, c cela števila. Vidimo, da so $X = a, Y = b$ in $Z = c$ homogene koordinate, ki so zdaj cela števila. Če leži točka (x, y) na krivulji (2), zadoščajo njene homogene koordinate a, b, c enačbi (2^*) . Tudi obratno je res: Imejmo celoštevilsko rešitev $X = a, Y = b, Z = c$ homogene enačbe (2^*) . Potem sta $x = a/c, y = b/c$ afini koordinati racionalne točke na krivulji (2). Kadar je $c = 0$, leži pripadajoča točka v neskončnosti. Tudi tako točko štejemo med racionalne točke.

Cela števila a, b, c , ki zadoščajo $(*)$, niso natanko določena z racionalnima koordinatama x in y . So pa določena do faktorja ± 1 , če zahtevamo, da nimajo skupnega faktorja, večjega od 1. V tem primeru imenujemo trojko a, b, c primitivna rešitev enačbe (2^*) . Vsaka racionalna točka na krivulji (2) določa torej dve primitivni celoštevilski rešitvi pripadajoče homogene enačbe (2^*) .

Za zgled si oglejmo krivuljo

$$x^n + y^n = 1. \quad (4)$$

Če jo zapišemo v homogenih koordinatah (postavimo $x = X/Z, y = Y/Z$ in pomnožimo z Z^n), dobimo

$$X^n + Y^n = Z^n. \quad (1^*)$$

To pa je enačba (1), zapisana z drugačnimi črkami. Zato imenujemo krivuljo (4) Fermatova krivulja. Po pravkar povedanem pripada vsaki celoštevilski rešitvi enačbe (1^*) racionalna točka na krivulji (4) (izjema je le trivialna rešitev $X = Y = Z = 0$), vsaka racionalna točka krivulje (4) pa določa dve primitivni rešitvi enačbe (1^*) .

Očitno ležita na krivulji (4) pri lihem eksponentu n tile racionalni točki: $x = 1, y = 0$ in $x = 0, y = 1$, poleg njiju pa še točka v neskončnosti s homogenimi koordinatami $X = 1, Y = -1, Z = 0$. Fermatova domneva trdi, da drugih racionalnih točk na krivulji (4) ni.

Fermatova krivlja je nesingularna in zato izračunamo njen rod po obrazcu (3). Pri $n = 3$ imamo $g = 1$, pri $n \geq 4$ pa $g \geq 3$.

Kaj lahko povemo na splošno o racionalnih in celoštevilskih točkah na algebraičnih krivuljah? Na stožnici je neskončno racionalnih točk, če je na njej vsaj ena (seveda vzamemo, da ima enačba stožnice racionalne koeficiente). Na krožnici je očitno kvečjemu končno mnogo celoštevilskih točk, na paraboli $y = x^2$ jih je neskončno in prav tako na nekaterih hiperbolah, npr. na hiperboli

$$x^2 - 2y^2 = 1.$$

Stožnice imajo rod $g = 0$. Kako je z racionalnimi in celoštevilskimi točkami na eliptičnih krivuljah, to je, na krivuljah roda $g = 1$? Na nekaterih eliptičnih krivuljah je racionalnih točk končno mnogo (oziroma ni nobene), spet na drugih jih je neskončno, na primer na nesingularni kubični krivulji

$$x^3 + y^3 = 7.$$

Pač pa je množica celoštevilskih točk — to je dokazal Siegel — na vsaki eliptični krivulji končna (ali prazna). In kako je na krivuljah z rodom $g > 1$? Angleški matematik Mordell je leta 1922 postavil domnevo, da je na taki algebraični krivulji množica racionalnih točk vselej končna. To domnevo se je posrečilo dokazati šele leta 1983 mlademu nemškemu matematiku Faltingsu. (Pravzazprav je Faltings dokazal neko domnevo, ki jo je postavil leta 1962 ruski matematik Šafarevič; nekaj let pozneje pa je ruski matematik Paršin pokazal, da velja Mordellova domneva, če je pravilna Šafarevičeva domneva.)

Kaj pove Faltingsov rezultat za Fermatovo domnevo? Ker ima Fermatova krivulja rod $g \geq 3$, če je $n > 3$, je torej pri takem n na njej končno število racionalnih točk. Vsaka racionalna točka pa določa, kakor smo zgoraj ugotovili, dve primitivni rešitvi enačbe (1). Torej ima enačba (1) pri $n > 3$ kvečjemu končno mnogo primitivnih rešitev. Povejmo, da je nekaj let pozneje Heath-Brown z izboljšanjem metod, ki jih je uporabljal Faltings, dokazal, da velja Fermatov zadnji izrek skoraj za vse eksponente n .

2. *Eliptične krivulje.* Vsaka eliptična krivulja, se pravi algebraična krivulja z rodom $g = 1$, se dá transformirati v krivuljo z enačbo

$$y^2 = x^3 + Ax^2 + Bx + C, \quad (5)$$

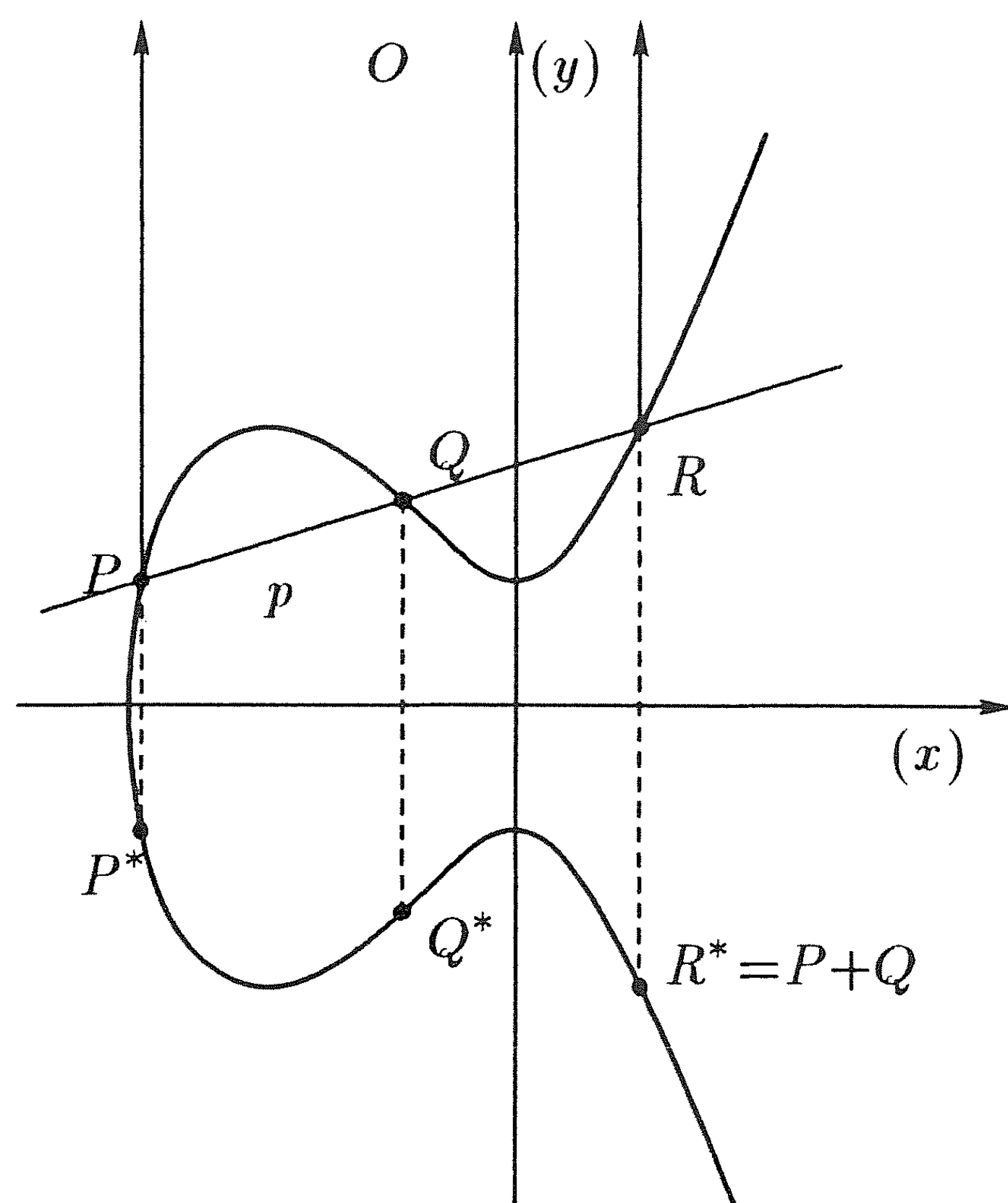
kjer so A, B, C konstante (Weierstrassova normalna oblika). Kubična krivulja z enačbo (5) pa je eliptična, če ima polinom na desni same različne ničle.

Krivulja (5) je očitno simetrična glede na abscisno os, ki jo seče v eni ali treh točkah; to je odvisno od tega, ali je le ena ničla polinoma na desni

realna ali so realne vse tri. Na sliki 1 seče krivulja abscisno os enkrat. V neskončnosti ima krivulja eno samo točko, namreč točko, kjer ordinatna os seče premico v neskončnosti. Zaznamujmo to točko z O . Njene homogene koordinate so $X = 0, Y = 1, Z = 0$. Zvezati končno točko P z O se pravi potegniti skozi P vzporednico z ordinatno osjo.

Množico vseh točk na eliptični krivulji (5) z O vred bomo označili z E . Torej sestavljajo E vse točke projektivne krivulje.

Ker je krivulja (5) tretje stopnje, jo seče vsaka premica največ v treh točkah. Zato lahko uvedemo v množici E binarno operacijo, in sicer takole: naj bosta P in Q poljubni točki na krivulji, torej $P, Q \in E$. Zvežimo P in Q s premico p . Le-ta ima s krivuljo poleg P in Q še eno skupno točko, ki jo imenujmo R (slika 1). (Če se P in Q ujemata, vzamemo za p tangento na krivuljo v točki P .) Tako smo dobili v množici E binarno operacijo, ki priredi točkama P in Q tretje presečišče R zveznice p s krivuljo. Ta operacija je očitno komutativna, vendar zanjo množica E ni grupa. Uvedimo zdaj novo operacijo, ki jo bomo imenovali seštevanje. Ker je krivulja (5) simetrična glede na os (x) , leži na njej



Slika 1.

hkrati s $P = (x, y)$ tudi simetrična točka $P^* = (x, -y)$. Simetrično točko R^* tretjega presečišča R imenujemo *vsota točk* P in Q in pišemo $P + Q = R^*$ (slika 1). Izkaže se, da je množica E za to binarno operacijo komutativna (Abelova) grupa. Vlogo elementa nič igra v njej točka O v neskončnosti. Velja namreč $P + O = P$ za vsako $P \in E$. Nasprotni element $-P$ točke P pa je simetrična točka P^* , torej $-P = P^*$. Če je $P = (x, y)$, je potemtakem $-P = (x, -y)$.

Kadar so koeficienti A, B, C racionalni, je eliptična krivulja definirana nad obsegom $\mathbb{Q}$ racionalnih števil. Tedaj ji rečemo *aritmetična eliptična krivulja*. Množico vseh racionalnih točk na njej označimo z $E(\mathbb{Q})$. Točko O v neskončnosti štejemo za racionalno (njene homogene koordinate $X = 0, Y = 1, Z = 0$ so cela števila), zato pripada množici $E(\mathbb{Q})$. Hitro se prepričamo, da je $E(\mathbb{Q})$ podgrupa grupe E . Očitno je namreč hkrati s P tudi $-P$ racionalna točka. Naj bosta zdaj $P = (x_1, y_1)$ in $Q = (x_2, y_2)$ poljubni točki iz $E(\mathbb{Q})$. Zveznica p ima enačbo $y = \alpha x + \beta$ z racionalnima

koeficientoma α in β . Če to vstavimo v (5), dobimo kubično enačbo za x z racionalnimi koeficienti. Ker sta dva njena korena racionalna (namreč abscisi x_1 in x_2 točk P in Q), je tudi tretji koren x_3 racionalen. Prav tako je racionalen $y_3 = \alpha x_3 + \beta$. Torej je tretje presečišče $R = (x_3, y_3)$ racionalna točka in isto velja za simetrično točko $R^* = (x_3, -y_3)$, ki je vsota $P + Q$. Množica $E(\mathbb{Q})$ je zaprta za seštevanje in je zato grupa.

Točka $P \in E(\mathbb{Q})$ ima končen red, če obstaja tako naravno število $n \geq 1$, da je $nP = O$ (tu pomeni nP krajši zapis za vsoto n enakih sumandov $P + P + \dots + P$). Najmanjše število s to lastnostjo se imenuje red točke P . Na primer O , ki je element nič naše grupe, ima red 1. Vse racionalne točke s končnim redom sestavljajo podgrupo T , ki ji pravimo *torzijska podgrupa* grupe $E(\mathbb{Q})$.

Katere točke imajo red 2? Naj bo $2P = P + P = O$. Potem je $-P = P$. Tudi obratno je res: Iz $-P = P$ izhaja enkost $2P = O$, tako da ima P red 2 (tu je P končna točka). Ker je $-P = (x, -y)$, če je $P = (x, y)$, vidimo, da velja $-P = P$ natanko tedaj, kadar je $-y = y$, se pravi, kadar je $y = 0$. Točka P leži na abscisni osi. Torej imajo red 2 točke, ki so presečišča krivulje z abscisno osjo. Presečišče $P = (x_1, 0)$ pripada grupi $E(\mathbb{Q})$, če je racionalna točka. Ker je x_1 ničla polinoma $x^3 + Ax^2 + Bx + C$ na desni v (5), vsebuje $E(\mathbb{Q})$ točko reda 2 le tedaj, kadar ima ta polinom vsaj eno racionalno ničlo.

Kakšna je lahko torzijska grupa pri raznih aritmetičnih krivuljah? Odgovor daje naslednji izrek, ki ga je dokazal Mazur (1977) in se glasi:

Izrek (Mazur). *Naj bo $E(\mathbb{Q})$ aritmetična eliptična krivulja. Njena torzijska grupa je ali*

- a) *ciklična grupa z močjo m , kjer je m bodisi eno izmed števil od 1 do 10 bodisi 12, ali*
- b) *direktni produkt ciklične grupe z dvema elementoma in ciklične grupe z $2m$ elementi, kjer je m lahko 1, 2, 3 ali 4.*

Za vsako izmed navedenih grup obstajajo aritmetične eliptične krivulje, ki imajo to grupo za torzijsko grupo.

Dokaz tega izreka je izredno zapleten.

Direktni produkt ciklične grupe z močjo 2 in ciklične grupe z močjo $2 \times 4 = 8$ ima 16 elementov. Vse druge v izreku navedene grupe štejejo manj elementov. Če smo torej na kakšni eliptični krivulji našli 17 racionalnih točk, je na njej neskončno racionalnih točk.

3. Modulske funkcije in parametrizacija eliptičnih krivulj. Naj bodo a , b , c , d dana cela števila, med katerimi velja zveza

$$ad - bc = 1. \quad (6)$$

Modulska transformacija γ je preslikava, ki priredi kompleksnemu številu z število z' , pri čemer je

$$z' = \gamma(z) = \frac{az + b}{cz + d}. \quad (7)$$

Število z ponazorimo s točko na kompleksni ravnini. Transformacija (7) preslika kompleksno ravnino vase. Vse modulske transformacije sestavljajo grupo, ki jo označimo z Γ . (Inverzna preslikava γ^{-1} od (7) je namreč modulska in prav tako tudi kompozitum $\gamma_1\gamma_2$ dveh takih transformacij γ_1 in γ_2 .)

Naj bo $z = x + iy$ in $z' = \gamma(z) = x' + iy'$. Preprost račun pokaže, da je

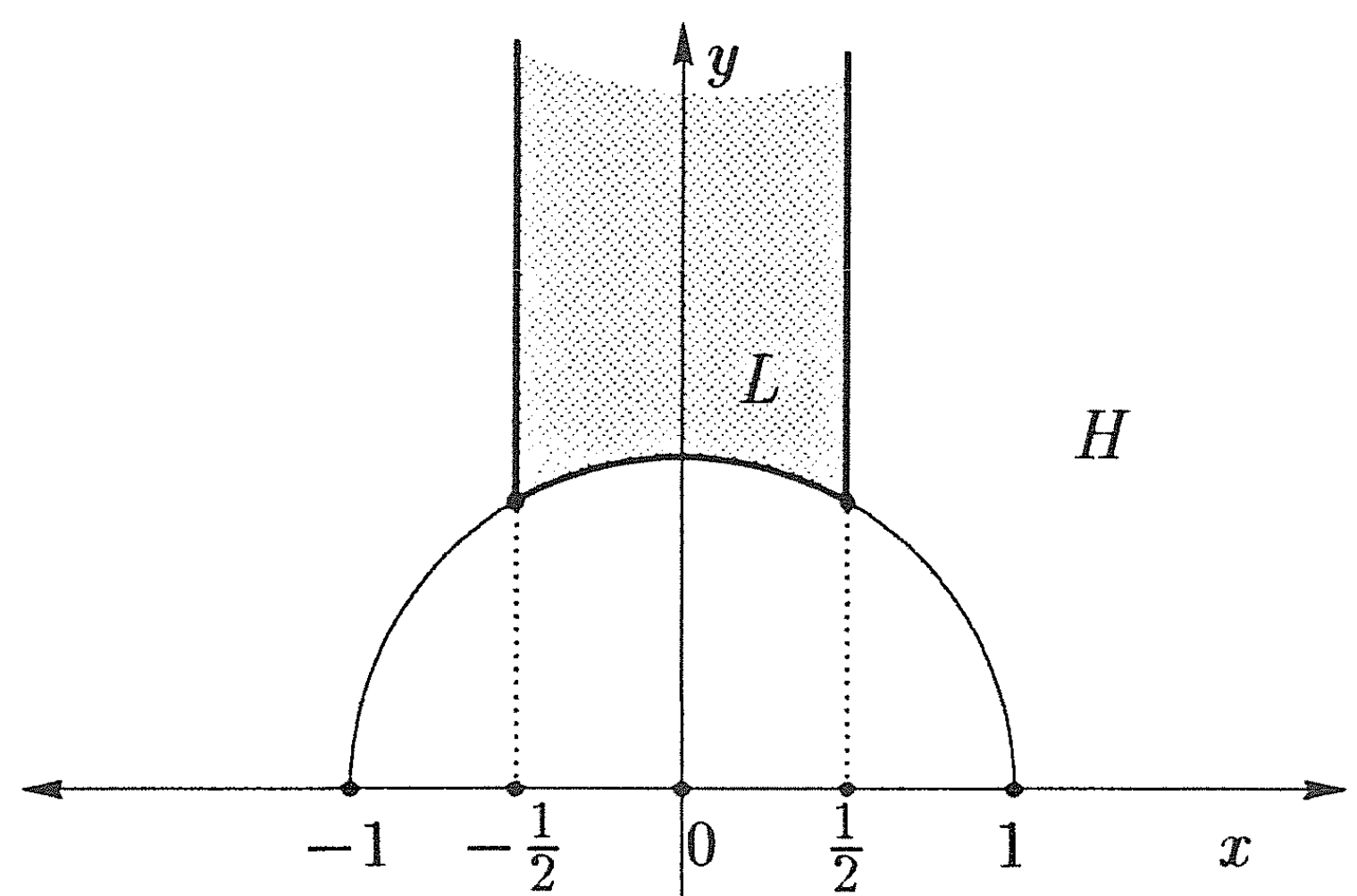
$$y' = \frac{y}{(cz + d)(c\bar{z} + d)}.$$

Ker je imenovalec na desni vselej pozitiven, imata y in y' isti znak. Zato preslika (7) točko z na zgornji polravnini (tam je $y > 0$) v točko z' na zgornji polravnini. Isto velja za spodnjo polravnino. Zaznamujmo zgornjo polravnino s H , torej

$$H = \{z = x + iy, y > 0\}.$$

Vsaka modulska transformacija γ bijektivno preslika polravnino H nase. Ker je γ na H holomorfná funkcija, je preslikava tudi konformna, se pravi, da ohranja kote.

Točki z in z' polravnine H imenujemo ekvivalentni, če obstaja modulska transformacija γ , ki preslika z v z' , torej če je $z' = \gamma(z)$ za kakšno $\gamma \in \Gamma$. Ker je Γ grupa, je ta relacija ekvivalenčna in razdeli množico točk polravnine H na ekvivalenčne razrede. *Osnovno območje* za grupo Γ je taka množica točk iz H , da je vsaka točka $z \in H$ ekvivalentna natanko eni točki z' iz osnovnega območja. Za osnovno območje



Slika 2.

lahko vzamemo lik L , ki je na sliki 2 osenčen. Sestavljajo ga točke, ki so zunaj enotnega kroga $x^2 + y^2 = 1$ in med premicama $x = -\frac{1}{2}$ ter $x = \frac{1}{2}$, poleg tega pa še del točk na robu. Modulske transformacije preslikajo osnovno območje L na množico likov, ki se med seboj ne prekrivajo, vsi skupaj pa natanko enkrat pokrijejo vso polravnino H .

Na polravnini H meromorfna funkcija φ se imenuje *modulska*, če izpolnjuje tale dva pogoja:

1. Velja

$$\varphi(\gamma(z)) = \varphi(z) \quad (8)$$

za vsak $z \in H$ in vsako modulsko transformacijo γ .

Ker je transformacija $z' = z + 1$ modulska (dobimo jo iz (7) pri $a = b = d = 1, c = 0$), pove enačba (8), da je $\varphi(z + 1) = \varphi(z)$. Torej je funkcija φ periodična s periodo 1 in se dá zato razviti v konvergentno Fourierovo vrsto. Definicijo modulske funkcije dopolnimo še s pogojem:

2. Fourierova vrsta za φ mora imeti določeno obliko, ki pa je tu ne bomo natančneje opisali. Ta pogoj pove, kako se vede φ v neskončnosti.

V zgornji definiciji smo zahtevali, naj velja enakost (8) za vse modulske transformacije. Pa naj bo Γ' kakšna podgrupa grupe Γ , in sicer taka, ki ima v Γ končen indeks r . To pomeni, da sestoji Γ iz r odsekov

$$\Gamma', \gamma_2\Gamma', \dots, \gamma_r\Gamma',$$

kjer so $\gamma_2, \dots, \gamma_r$ primerno izbrane transformacije iz Γ . Osnovno območje za grupo Γ' opredelimo kakor za celotno grupo Γ . Dobimo pa ga tako, da osnovnemu območju L grupe Γ pridružimo njegove slike $\gamma_2^{-1}(L), \dots, \gamma_r^{-1}(L)$.

Pojem modulske funkcije φ zdaj posplošimo takole: Enačba (8) naj velja le za transformacije γ iz podgrupe Γ' .

Eliptična krivulja (5) se dá parametrizirati z modulskimi funkcijami, če obstaja taka modulska podgrupa Γ' s končnim indeksom v Γ in taki modulski funkciji $\varphi(\tau), \psi(\tau)$, pripadajoči podgrupi Γ' , da velja za vsak $\tau \in H$ enakost

$$\psi(\tau)^2 = \varphi(\tau)^3 + A\varphi(\tau)^2 + B\varphi(\tau) + C.$$

Torej sta

$$x = \varphi(\tau), \quad y = \psi(\tau) \quad (9)$$

parametrični enačbi krivulje (5). Ker sta φ in ψ z izjemo polov na polravnini H holomorfni, pomeni parametrizacija konformno upodobitev polravnine H na eliptično krivuljo. (Spomnimo se, da je krivulja v obsegu kompleksnih števil v resnici ploskev.) Pravzaprav se že osnovno območje grupe Γ' preslika na vso krivuljo.

Katere eliptične krivulje se dajo parametrizirati na opisani način? Bely je dokazal, da natanko tiste, pri katerih so koeficienti A, B, C algebraična števila. (Število je algebraično, če je ničla kakšnega nekonstantnega polinoma s celimi koeficienti.)

Posebno vlogo imajo kongruenčne podgrupe grupe Γ . Opredelimo jih takole: naj bo N dano naravno število. Označimo z $\Gamma(N)$ množico vseh modulskih transformacij γ , pri katerih veljajo med koeficienti a, b, c, d kongruence

$$a \equiv d \equiv 1 \pmod{N}, \quad \text{in} \quad b \equiv c \equiv 0 \pmod{N}.$$

Ni težko ugotoviti, da je množica $\Gamma(N)$ grupa in da ima končen indeks v grupi Γ . *Kongruenčna podgrupa* je taka podgrupa Γ' grupe Γ , ki vsebuje kakšno podgrupo $\Gamma(N)$ pri primerno izbranem N . Pravimo, da je parametrizacija eliptične krivulje *aritmetičnega tipa*, če sta pripadajoči funkciji φ in ψ v (9) modulski za kakšno kongruenčno podgrupo Γ' . Eliptične krivulje, ki se dajo parametrizirati na opisani način, se odlikujejo s številnimi lastnostmi. Zato je umestno vprašanje, katere se dajo. Odgovor še ni znan. Taniyama, Weil in drugi so v tej zvezi postavili tole domnevo:

Domneva. (Taniyama-Weil). *Vsaka aritmetična eliptična krivulja (torej taka, v kateri so koeficienti A, B, C racionalni) premore parametrizacijo aritmetičnega tipa.*

Doslej so dokazali veljavnost te domneve za nekatere družine eliptičnih krivulj, na primer za vse krivulje s kompleksno multiplikacijo.

Vrnimo se zdaj k Fermatovemu problemu, Kakšno zvezo ima z njim teorija eliptičnih krivulj in modulskih funkcij? Denimo, da obstaja pri nekem praštevilskega eksponentu $n = p > 2$ netrivialna rešitev enačbe (1), torej da smo našli taka od nič različna cela števila a, b, c , ki zadoščajo zvezi $a^p + b^p = c^p$. Nekateri matematiki (Serre, Frey in drugi) so prišli na misel prirediti tej rešitvi eliptično krivuljo

$$y^2 = x(x - a^p)(x + b^p). \quad (10)$$

Ker jo je zlasti Frey raziskoval in odkril nekatere njene zanimive lastnosti, se zdaj imenuje Freyeva krivulja. Ničle polinoma na desni v (10) so $x_1 = 0$, $x_2 = a^p$ in $x_3 = -b^p$, se pravi cela števila. Zato so na Freyevi krivulji tri racionalne točke reda 2. Na prvi pogled se ne zdi enačba (10) nič posebnega. Toda Ribetu je uspelo leta 1986 dokazati tole:

če obstaja parametrizacija aritmetičnega tipa Freyevе krivulje, je na njej racionalna točka reda p .

Denimo zdaj, da je $p \geq 5$. Ker so na Freyevi krivulji tri racionalne točke reda 2, njena torzijska grupa ne more biti ciklična (v ciklični grupi ima namreč kvečjemu en element red 2). Po Mazurjevem izreku je torej torzijska grupa direkten produkt ciklične grupe z močjo 2 in ciklične grupe z močjo $2m$, kjer je m lahko 1, 2, 3 ali 4. Toda v nobeni od teh grup ni elementa reda $p \geq 5$. Tako smo prišli do protislovja. Torej:

če je pravilna Taniyama-Weilova domneva, velja zadnji Fermatov izrek za vse eksponente $p \geq 5$.

Ribetov dokaz je izredno zapleten in ga pisec tega članka ni preštudiral. Povejmo samo nekaj osnovnih idej. Na algebraični krivulji je diferencial prve vrste tak diferencial $R(x, y)dx$, ki je povsod holomorfen (R je racionalna funkcija spremenljivk x in y , ki sta povezani z enačbo (2)). Na eliptični

krivulji (5) je diferencial prve vrste dx/y . S parametrizacijo (9) ga na Freyevi krivulji izrazimo v obliki $\chi(\tau)d\tau$, kjer pomeni faktor $\chi(\tau)$ pri diferencialu $d\tau$ kvocient $\varphi'(\tau)/\psi(\tau)$. Funkcija $\chi(\tau)$ je holomorfna na vsej polravnini H , transformira pa se takole

$$\chi(\gamma(\tau)) = (c\tau + d)^2 \chi(\tau). \quad (11)$$

Tu je $\gamma(\tau) = (a\tau + b)/(c\tau + d)$ poljubna transformacija iz grupe Γ' . (Pravilo (11) dobimo z odvajanjem enačbe (8).) Na polravnini H holomorfna funkcija χ , za katero velja (11) za vsako transformacijo $\gamma \in \Gamma'$, se imenuje *modulska forma z utežjo 2*. V našem primeru je χ tudi periodična s periodo 1 in se dá zato razviti v Fourierovo vrsto. Izkaže se, da ima ta vrsta obliko

$$\chi(\tau) = e^{2\pi i\tau} + a_2 e^{4\pi i\tau} + a_3 e^{6\pi i\tau} + \dots$$

kjer so koeficienti a_j cela števila. Ribet je dognal, da so ti koeficienti po modulu p kongruentni istoležnim koeficientom Fourierove vrste neke znane modulske forme z utežjo 2. Od tod je potem sklepal, da obstaja na Freyevi krivulji racionalna točka z redom p .

Z isto metodo je mogoče obravnavati splošnejšo družino diofantskih enačb

$$Ax^n + y^n = z^n,$$

kjer je A dano naravno število. Pri pogoju, da velja Taniyama-Weilova domneva, se izkaže, da ta enačba ne premore od nič različne celoštevilске rešitve x, y, z za noben eksponent $n \geq 7$, če je koeficient A potenca od 2, od 3 ali od 7.

Ribetov rezultat je spodbudil Wilesa, da se je lotil raziskovanja na tem področju. Po sedmih letih napornega dela mu je uspelo dokazati Taniyama-Weilovo domnevo za družino semistabilnih aritmetičnih eliptičnih krivulj. Njegov dokaz obsega okoli 200 strani. Ker Freyeva krivulja sodi v omenjeno družino, je Wiles rešil Fermatov problem, seveda če ni napravil nobene napake. Njegovo delo zdaj proučujejo specialisti za ta področja. Piscu tega članka še ni znan izid.

Pripomba. Kaj so semistabilne eliptične krivulje? Ker so koeficienti pri aritmetični eliptični krivulji z enačbo (5) cela števila, lahko obravnavamo to enačbo v obsegu ostankov po poljubnem praštevilske modulu p . Pravimo, da smo enačbo reducirali po modulu p . Nekoliko površno povedano je krivulja (5) semistabilna, če ima polinom na desni v reducirani enačbi pri vsakem praštevilske modulu vsaj dve različni ničli.

Poglejmo še enkrat začetek in konec reševanja slavnega problema. Dokaz za četrte potence je kratek in ne zahteva nobenega posebnega znanja

iz teorije števil. Razume ga lahko vsak boljši srednješolec. Dokaz, ki velja za vse eksponente, pa je tako zapleten, da ga doumejo samo specialisti z ustreznih področij. Poleg splošne teorije eliptičnih krivulj in modulskih funkcij potrebujemo Mazurjev izrek o torzijskih grupah, Wilesov dokaz, da Taniyama-Weilova domneva drži za semistabilne eliptične krivulje, in Ribetov dokaz, da je Freyeva krivulja protislovna, če premore parametrizacijo aritmetičnega tipa. Knjiga, ki bi zajela te teorije z vsemi dokazi, bi bila zelo obsežna. V matematiki poznamo veliko problemov, ki so razumljivi tudi matematično neizobraženim ljudem, rešitve pa so zelo težke ali jih sploh še niso našli. Primer takega nerešenega problema je Goldbachova domneva, da je vsako sodo število vsota dveh praštevil. Morda obstaja splošno razumljiva matematična resnica, katere dokaz je v primerjavi z dokazom Fermatove domneve tako zapleten, kakor je dokaz te domneve zapleten v primerjavi z dokazom za četrte potence. Če bi taka matematična resnica obstajala, ali bi se mogel človek dokopati do njenega dokaza?

Dodatek. Po zadnjih informacijah (pisec se zanje zahvaljuje prof. J. Vrabcu) so odkrili vrzel v Wilesovem delu. Gre za neko neenačbo, katere veljavnost je potrebna pri nadaljnjem reševanju problema, dokaz te neenačbe pa je pomanjkljiv. Wiles je februarja povedal, da mu še ni uspelo premagati te ovire.

V začetku aprila se je razširila vest, da je N. Elkies našel rešitev enačbe (1) v celih od nič različnih številih, in sicer pri nekem zelo velikem eksponentu n , večjem od 10^{20} . Če bi se izkazalo, da je to res, Fermatov zadnji izrek ne bi veljal za vsak eksponent n in prav tako ne bi bila pravilna Taniyama-Weilova domneva. Zgoraj omenjena pomanjkljivost v Wilesovem dokazu se seveda tudi ne bi dala odpraviti. Ker pa se je ta vest razširila prve dni aprila, gre morda za prvoaprilsko šalo. (N. Elkies je pred nekaj leti odkril, da obstaja nešteto rešitev enačbe $x^4 + y^4 + z^4 = t^4$ v naravnih tujih si številih. S tem je ovrgel Eulerjevo domnevo, da ta enačba nima celih rešitev.)

LITERATURA

- [1] J. Grasselli, *Mordellova domneva dokazana*, Obzornik mat. fiz. **32** (1985), 33–37.
- [2] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, 1984.
- [3] B. Mazur, *Number Theory as Gadfly*, Amer. Math. Monthly **98** (1991), 593–610.
- [4] J. Plemelj, *Nerešljivost enačbe $x^5 + y^5 + z^5 = 0$ v obsegu $K(\sqrt{5})$* , Obzornik mat. fiz. **3** (1954), 135–138; prevod *Die Unlösbarkeit von $x^5 + y^5 + z^5 = 0$ im Körper $K(\sqrt{5})$* , Monatshefte f. Math. und Physik **23** (1912).
- [5] J. Silverman, J. Tate, *Rational points on Elliptic Curves*, Springer-Verlag, 1992.
- [6] I. Stewart, *Fermat's last time*, Trip. Scientific Amer., Nov. 1993, 85–88.

UREJENI ŠTEVILSKI OBSEGI

BORIS LAVRIČ

Math. Subj. Class. (1991) 66F25, 13J25

V članku obravnavamo urejenost na podobsegih obsega kompleksnih števil. Poiščemo vse arhimedske enostavne razširitve obsega racionalnih števil.

ORDERED FIELDS

In this note we consider orders on subfields of the complex number field. In particular, we find all archimedean simple extensions of the field of rational numbers.

1. Uvod

Zabeležimo najprej nekaj osnovnih pojmov.

Definicija 1. *Urejen kolobar* je kolobar $\mathcal{K}$ z dano podmnožico $\mathcal{K}^p \subset \mathcal{K}$, ki ustreza naslednjim zahtevam:

$$\mathcal{K} = -\mathcal{K}^p \cup \{0\} \cup \mathcal{K}^p, \quad -\mathcal{K}^p \cap \mathcal{K}^p = \emptyset, \quad (1)$$

$$\mathcal{K}^p + \mathcal{K}^p \subset \mathcal{K}^p, \quad \mathcal{K}^p \mathcal{K}^p \subset \mathcal{K}^p. \quad (2)$$

Relacijo urejenosti $<$ uvedemo z ekvivalenco

$$a < b \text{ (ali } b > a) \iff b - a \in \mathcal{K}^p, \quad a, b \in \mathcal{K}.$$

Množico $\mathcal{K}^p$ sestavljajo elementi $a \in \mathcal{K}$, ki jih imenujemo *pozitivni elementi* in zadoščajo pogoju $a > 0$, množico $-\mathcal{K}^p$ pa elementi $a \in \mathcal{K}$, ki jih imenujemo *negativni elementi* in zadoščajo pogoju $a < 0$. Zapis $a \geq 0$ pomeni $a > 0$ ali $a = 0$, analogen pomen pa ima zapis $a \leq 0$.

Če je urejen kolobar obseg, mu pravimo *urejen obseg*. Takó definirani pojem urejenega obsega se ujema z enako imenovanim pojmom v knjigi [4, III. 9], čeprav se definiciji za malenkost razlikujeta.

Naštejmo nekaj lastnosti urejenega kolobarja $\mathcal{K}$, ki sledijo neposredno iz definicije. Relacija $<$ je asimetrična, tranzitivna ter sovisna. Velja zakon *trihotomije*:

za vsak par $a, b \in \mathcal{K}$ velja natanko ena od možnosti $a < b$, $a > b$ in $a = b$.

Za poljubne elemente $a, b, c \in \mathcal{K}$ veljata sklepa

$$a < b \Rightarrow a + c < b + c,$$

$$a < b \text{ in } c > 0 \Rightarrow ac < bc \text{ in } ca < cb.$$

Kvadrat poljubnega neničelnega elementa iz $\mathcal{K}$ je pozitiven. Če ima $\mathcal{K}$ enoto 1, torej velja $1 > 0$. Inverz pozitivnega elementa iz $\mathcal{K}$ je pozitiven. Za vsak element $a \in \mathcal{K}$ lahko na naraven način opredelimo njegovo absolutno

vrednost: $|a| = a$, kadar je $a \geq 0$, in $|a| = -a$, kadar je $a < 0$. Zlahka vidimo, da za poljubna elementa a, b urejenega kolobarja velja

$$|a + b| \leq |a| + |b|, \quad |ab| = |a||b|.$$

Podkolobar urejenega kolobarja $\mathcal{K}$ podeduje urejenost od $\mathcal{K}$ in je z inducirano relacijo $<$ urejen kolobar.

Naj bosta $\mathcal{K}$ in $\mathcal{L}$ urejena kolobarja oziroma urejena obsega. Preslikava $\phi : \mathcal{K} \rightarrow \mathcal{L}$ je *izomorfizem* (urejenih kolobarjev oziroma urejenih obsegov), kadar je algebrski izomorfizem (kolobarjev oziroma obsegov) in urejenostni izomorfizem:

$$a < b \iff \phi(a) < \phi(b), \quad a, b \in \mathcal{K}.$$

Urejen kolobar $\mathcal{K}$ je zaradi zaprtosti množice pozitivnih elementov $\mathcal{K}^p$ za množenje in zakona trihotomije brez pravih deliteljev nič. Če je $\mathcal{K}$ komutativen, ga lahko po izreku 17 iz knjige [4, III. 8] vložimo v obseg ulomkov. Podrobnosti o takšni vložitvi nam razkrije naslednji rezultat:

Izrek 2. *Naj bo $\mathcal{K}$ komutativen urejen kolobar in $\mathcal{O}$ obseg ulomkov nad $\mathcal{K}$. Potem lahko obseg $\mathcal{O}$ na en sam način uredimo tako, da postane urejen obseg, ki na $\mathcal{K}$ inducira originalno urejenost.*

Dokaz. Denimo, da je obseg $\mathcal{O}$ urejen tako, da na $\mathcal{K}$ inducira originalno urejenost. Vzemimo poljuben element $c \in \mathcal{O}$ in ga zapišimo v obliki $c = a/b$, $a, b \in \mathcal{K}$. Iz enakosti $a = bc$ razberemo, da je c pozitiven natanko takrat, kadar sta elementa a in b bodisi oba pozitivna bodisi oba negativna. Od tod sledi, da je urejenost na $\mathcal{O}$ enolično določena s pogoji izreka in da množico $\mathcal{O}^p$ sestavljajo elementi $a/b \in \mathcal{O}$, $ab > 0$.

Dokažimo zdaj existenco zahtevane urejenosti na $\mathcal{O}$. Zadostuje ugotoviti, da množica

$$\mathcal{O}^p = \{a/b \in \mathcal{O} : (a > 0 \text{ in } b > 0) \text{ ali } (a < 0 \text{ in } b < 0)\}$$

ustreza pogojem iz (1) in (2).

Vzemimo poljuben neničeln element $a/b \in \mathcal{O}$. Če sta a in b hkrati pozitivna ali negativna, je $a/b \in \mathcal{O}^p$, v nasprotnem primeru pa $a/b \in -\mathcal{O}^p$, torej velja prva zahteva iz (1).

Zdaj pa vzemimo poljubna elementa a_1/b_1 in a_2/b_2 iz $\mathcal{O}^p$. Če velja $a_1/b_1 = -a_2/b_2$, potem je $a_1b_2 + a_2b_1 = 0$. Sumanda a_1b_2 in a_2b_1 sta hkrati pozitivna oziroma negativna, zato je vsota $a_1b_2 + a_2b_1$ bodisi pozitivna bodisi negativna, ni pa enaka 0. Množica $\mathcal{O}^p$ torej ustreza tudi drugemu pogoju iz (1).

Podobno lahko ugotovimo, da velja

$$(a_1b_2 + a_2b_1)/(b_1b_2) \in \mathcal{O}^p, \quad (a_1a_2)/(b_1b_2) \in \mathcal{O}^p,$$

iz česar sledi zaprtost množice $\mathcal{O}^p$ za seštevanje in za množenje, torej (2). ■

Kolobar celih števil $\mathbb{Z}$ le z naravno urejenostjo postane urejen kolobar. To urejenost lahko razširimo na obseg ulomkov $\mathbb{Q}$ na en sam način, tako da

le-ta postane urejen obseg. Razširjena urejenost je seveda naravna urejenost racionalnih števil. Vsak urejen obseg ima karakteristiko 0 in na svojem podobsegu $\mathbb{Q}$ inducira naravno urejenost.

Naj bo $\mathcal{K}$ urejen obseg. Potem njegova podmnožica $\mathcal{K}^p$ vsebuje enoto 1 in je zaprta za množenje ter za invertiranje. Zato z inducirano urejenostjo $\mathcal{K}^p$ postane urejena multiplikativna grupa v smislu definicije iz [4, II. 13].

2. Arhimedski obsegi

Definicija 3. Urejen kolobar $\mathcal{K}$ je *arhimedski*, kadar za vsak par pozitivnih elementov $a, b \in \mathcal{K}$ obstaja tak $n \in \mathbb{N}$, da je $b < na$.

Bralec se lahko brez težav prepriča, da je urejen obseg $\mathcal{K}$ arhimedski natanko takrat, kadar za poljuben element $a \in \mathcal{K}$ obstaja tak $n = n(a) \in \mathbb{N}$, da je $a < n$, torej arhimedsko urejen po definiciji iz [4, III. 9]. Zgledi arhimedskih urejenih kolobarjev so urejeni podkolobarji obsega realnih števil z naravno urejenostjo. Še več, do izomorfizma natančno so to vsi arhimedski kolobarji. Velja namreč naslednja posplošitev izreka 18 iz [4, III]. Elementarni dokaz tega rezultata najdemo v [1].

Izrek 4. (Pickert, [2]) *Urejen arhimedski kolobar $\mathcal{K}$ je izomorfen podkolobarju naravno urejenega obsega $\mathbb{R}$. Pri tem sta podkolobar in izomorfizem nanj enolično določena.*

Ker je množica racionalnih števil gosta na realni osi, iz izreka 2 brz sledi, da v arhimedskem obsegu $\mathcal{K}$ velja naslednji sklep:

Za vsak par $a, b \in \mathcal{K}$, ki ustreza pogoju $a < b$, obstaja tak $r \in \mathbb{Q}$, da je $a < r < b$.

Bralec se lahko hitro prepriča, da v nearhimedskem urejenem obsegu ta sklep ne velja. Oglejmo si še eno karakteristično lastnost arhimedskih obsegov.

Izrek 5. (Vaida, [3]) *Urejen obseg $\mathcal{K}$ je arhimedski natanko takrat, kadar je urejena multiplikativna grupa $\mathcal{K}^p$ arhimedska: za vsak par $a > 1$, $b > 1$ obstaja tak $n \in \mathbb{N}$, da je $a^n > b$.*

Dokaz. Naj bo $\mathcal{K}$ arhimedski in $a > 1$, $b > 1$. Potem obstaja tak $n \in \mathbb{N}$, da za $c = a - 1 > 0$ velja $nc > b$, in tedaj je

$$a^n = (1 + c)^n \geq 1 + nc > b.$$

Denimo, da $\mathcal{K}$ ni arhimedski. Poiščimo tak pozitiven $d \in \mathcal{K}$, da je $d > n$ za vsak $n \in \mathbb{N}$. Potem za $a = 1 + d^{-1}$ velja $1 < a < 1 + 1/n$ in zato je

$$a^n < \left(1 + \frac{1}{n}\right)^n < 3 \quad \forall n \in \mathbb{N},$$

torej urejena multiplikativna grupa $\mathcal{K}^p$ ni arhimedska. ■

Podobseg arhimedskega obsega je v inducirani urejenosti tudi sam arhimedski. Za algebraične razširitve velja tudi nasprotno.

Izrek 6. (Pickert, [2]) *Naj bo komutativen urejen obseg $\mathcal{L}$ algebraična razširitev podobsega $\mathcal{K}$, ki ga uredimo z inducirano urejenostjo. Potem je $\mathcal{L}$ arhimedski tedaj in le tedaj, kadar je $\mathcal{K}$ arhimedski.*

Dokaz. Če je $\mathcal{L}$ arhimedski, je očitno tak tudi $\mathcal{K}$. Denimo zdaj, da je $\mathcal{K}$ arhimedski, $\mathcal{L}$ pa ne. Izberimo tak $\alpha \in \mathcal{L}$, da velja $\alpha > n$ za vsak $n \in \mathbb{N}$. Potem je $\beta = \alpha^{-1} > 0$ in $\beta < 1/n$ za vsak $n \in \mathbb{N}$. Ker je β algebraičen nad $\mathcal{K}$, obstajajo elementi $a_0, a_1, \dots, a_k \in \mathcal{K}$, za katere velja

$$a_0 + a_1\beta + \dots + a_k\beta^k = 0, \quad a_0a_k \neq 0.$$

Vzemimo tak $n_0 \in \mathbb{N}$, da je $|a_j| < n_0$ za indekse $j = 0, 1, \dots, k$. Potem za vsak $n \in \mathbb{N}$ zaradi $\beta < (kn_0n)^{-1} < 1$ velja

$$0 < |a_0| \leq |a_1|\beta + \dots + |a_k|\beta^k < kn_0\beta < \frac{1}{n},$$

kar pa nasprotuje temu, da je $\mathcal{K}$ arhimedski. Če je $\mathcal{K}$ arhimedski, je torej tudi $\mathcal{L}$ arhimedski, izrek pa je s tem dokazan. ■

Posledica 7. *Vsak urejen obseg algebraičnih kompleksnih števil je arhimedski.*

Dokaz. Urejen obseg algebraičnih števil je algebraičen nad naravno urejenim podobsegom $\mathbb{Q}$, ta pa je arhimedski. ■

3. Urejene enostavne razširitve

Vemo že, da obseg racionalnih števil le z naravno urejenostjo postane urejen obseg. Z obsegom realnih števil $\mathbb{R}$ je podobno. Ker je v urejenem obsegu kvadrat vsakega neničelnega elementa pozitiven, tudi $\mathbb{R}$ edino z naravno urejenostjo postane urejen obseg. Vsak podobseg obsega $\mathbb{R}$ je naravno urejen z inducirano urejenostjo, vendar nasploh to ni edina urejenost na podobsegu. Oglejmo si primer.

Naj bo $\mathcal{K} = \mathbb{Q}(\sqrt{2})$ in $\phi : \mathcal{K} \rightarrow \mathcal{K}$ avtomorfizem, opredeljen s predpisom

$$\phi(r + s\sqrt{2}) = r - s\sqrt{2}, \quad r, s \in \mathbb{Q}.$$

Potem množica $\mathcal{K}^p = \{a \in \mathcal{K} : \phi(a) > 0\}$ ustreza (1) in (2). Obseg $\mathcal{K}$ skupaj s podmnožico $\mathcal{K}^p$ je urejen obseg, vendar se urejenost na $\mathcal{K}$ ne ujema z naravno. Se da $\mathcal{K}$ še kako urediti?

Kako pa je z urejenostjo na podobsegu obsega kompleksnih števil $\mathbb{C}$? Brž ko podobseg vsebuje imaginarno enoto i , ga zaradi $i^2 = -1 < 0$ ni mogoče urediti. Se sploh kak nerealen podobseg obsega $\mathbb{C}$ da urediti v urejen obseg? Spet posezimo po primeru.

Naj bo α nerealna rešitev enačbe $\alpha^3 = 2$, $\mathcal{K} = \mathbb{Q}(\alpha)$ in $\phi : \mathcal{K} \rightarrow \mathbb{Q}(\sqrt[3]{2})$ izomorfizem obsegov, ki α preslika v $\sqrt[3]{2}$. S podmnožico $\mathcal{K}^p = \{a \in \mathcal{K} : \phi(a) > 0\}$ v nerealen podobseg $\mathcal{K} \subset \mathbb{C}$ uvedemo strukturo urejenega obsega.

Poiščimo zdaj vse urejene enostavne algebraične razširitve obsega $\mathbb{Q}$.

Izrek 8. *Naj bo $\alpha \in \mathbb{C}$ algebraično število, $p(X) \in \mathbb{Q}[X]$ njegov minimalni polinom in m število realnih ničel polinoma $p(X)$. Potem lahko razširitev $\mathcal{K} = \mathbb{Q}(\alpha)$ uredimo v urejen obseg natanko na m načinov. Urejenosti na $\mathcal{K}$ so določene z množicami $\mathcal{K}_1^p, \dots, \mathcal{K}_m^p$, ki so opredeljene v dokazu tega izreka.*

Dokaz. Naj bodo $\alpha_1, \dots, \alpha_m$ realne ničle polinoma $p(X)$, k pa njegova stopnja. Za vsak indeks $j \in \{1, \dots, m\}$ zaznamujmo s ϕ_j izomorfizem obsegov $\mathcal{K} \rightarrow \mathbb{Q}(\alpha_j)$, ki ustreza pogoju $\phi_j(\alpha) = \alpha_j$. Bralec se brez težav lahko prepriča, da tak izomorfizem obstaja in je en sam. Podmnožice

$$\mathcal{K}_j^p = \{a \in \mathbb{Q}(\alpha) : \phi_j(a) > 0\}, \quad j = 1, \dots, m,$$

obsega $\mathcal{K}$ ustrezajo pogojem iz (1) in (2). Ker ima polinom $p(X)$ le enostavne ničle, so te množice med seboj različne, torej je možno $\mathcal{K}$ urediti vsaj na m načinov.

Naj bo zdaj $\mathcal{K} = \mathbb{Q}(\alpha)$ urejen obseg in $\mathcal{K}^p$ množica pozitivnih elementov iz $\mathcal{K}$. Po posledici 1 je urejen obseg $\mathcal{K}$ arhimedski in zato po izreku 4 izomorfen podobsegu naravno urejenega obsega $\mathbb{R}$. Zaznamujmo s ϕ izomorfizem $\mathcal{K} \rightarrow \mathbb{Q}(\phi(\alpha)) \subset \mathbb{R}$. Potem je očitno $\phi(\alpha)$ ničla polinoma $p(X)$. Ker je poleg tega $\phi(\alpha) \in \mathbb{R}$, obstaja tak $j \in \{1, \dots, m\}$, da je $\phi(\alpha) = \alpha_j$. Od tod sledi, da je $\phi = \phi_j$. Izomorfizem ϕ je tudi urejenostni izomorfizem, zato velja $\mathcal{K}^p = \mathcal{K}_j^p$, izrek pa je s tem dokazan. ■

Dokaz izreka 8 pove, da smemo vzeti $m = 0$. Torej algebraično razširitev $\mathbb{Q}(\alpha)$ lahko pretvorimo v urejen obseg natanko takrat, kadar ima minimalni polinom števila α vsaj eno realno ničlo. Ker ima vsak polinom $p(X) \in \mathbb{Q}(X)$ lihe stopnje vsaj eno realno ničlo, velja

Posledica 9. *Algebraična razširitev lihe stopnje nad $\mathbb{Q}$ z ustrezno urejenostjo postane urejen obseg.*

Uporabimo izrek 8 na poljubnem kvadratnem obsegu $\mathcal{K} = \mathbb{Q}(\sqrt{m})$, kjer je $m \in \mathbb{Z}$ nekvadrat. Minimalni polinom števila $\sqrt{m} \in \mathcal{K}$ je $p(X) = X^2 - m$. Za $m < 0$ po izreku 8 $\mathcal{K}$ ne more biti urejen obseg, za $m > 0$ pa lahko $\mathcal{K}$ uredimo natanko na dva načina.

Poiščimo zdaj vse arhimedske enostavne transcendentne razširitve obsega $\mathbb{Q}$. Naj bo τ dano kompleksno število, transcendentno nad $\mathbb{Q}$, in $\mathcal{K} = \mathbb{Q}(\tau)$. Vzemimo poljubno realno transcendentno število ζ in s ϕ_ζ zaznamujmo izomorfizem obsegov $\mathcal{K} \rightarrow \mathbb{Q}(\zeta)$, ki τ preslika v ζ . Potem množica

$$\mathcal{K}_\zeta^p = \{a \in \mathcal{K} : \phi_\zeta(a) > 0\}$$

ustreza pogojem iz definicije 1 in zato ureja obseg $\mathcal{K}$.

Izrek 10. Vse arhimedske urejenosti enostavne transcendentne razširitve $\mathcal{K} = \mathbb{Q}(\tau)$ so dane s podmnožicami pozitivnih elementov $\mathcal{K}_\zeta^p$, kjer ζ preteče vsa realna transcendentna števila. Pri različnih izbirah ζ dobimo različne urejenosti.

Dokaz. Ker je naravna urejenost na $\mathbb{Q}(\zeta)$ arhimedska, je takšna tudi urejenost, ki jo na $\mathcal{K}$ določa množica $\mathcal{K}_\zeta^p$. Naj bosta ζ in ξ realni transcendentni števili, $\xi < \zeta$, r pa racionalno število, ki ustreza pogoju $\xi < r < \zeta$. Potem je $\tau - r \in \mathcal{K}_\zeta^p \setminus \mathcal{K}_\xi^p$, torej sta urejenosti, ki ju določata $\mathcal{K}_\zeta^p$ in $\mathcal{K}_\xi^p$, različni.

Naj bo zdaj $\mathcal{K}^p$ množica pozitivnih elementov arhimedskega obsega $\mathcal{K}$. Po izreku 4 obstaja izomorfizem urejenega obsega $\mathcal{K}$ na naravno urejen podobseg $\mathcal{L} = \phi(\mathcal{K})$ obsega $\mathbb{R}$. Ker velja $\mathcal{L} = \mathbb{Q}(\phi(\tau))$ in je $\zeta = \phi(\tau)$ realno transcendentno število, je $\phi = \phi_\zeta$ in $\mathcal{K}^p = \mathcal{K}_\zeta^p$, torej smo z množicami $\mathcal{K}_\zeta^p$ opisali vse arhimedske urejenosti na $\mathcal{K}$. ■

Navedimo še zgled nearhimedskega urejenega kolobarja in obsega. Naj bo $\mathcal{K}$ komutativen urejen kolobar in $\mathcal{K}[X]$ kolobar polinomov s koeficienti iz $\mathcal{K}$. Potem katerokoli od množic

$$\left\{ \sum_k a_k X^k \in \mathcal{K}[X] : \exists n : a_n > 0 \text{ in } a_k = 0 \ \forall k > n \right\},$$

$$\left\{ \sum_k a_k X^k \in \mathcal{K}[X] : \exists n : a_n > 0 \text{ in } a_k = 0 \ \forall k < n \right\}$$

lahko razglasimo za množico pozitivnih elementov $\mathcal{K}[X]^p$, saj obe ustrezata pogojem definicije 1. Dobimo tako imenovani leksikografski urejenosti kolobarja $\mathcal{K}[X]$, ki ju po izreku 1 lahko razširimo na obseg ulomkov nad $\mathcal{K}[X]$, torej na obseg $\mathcal{K}(X)$ racionalnih funkcij s koeficienti iz $\mathcal{K}$. Ker za vsak $n \in \mathbb{N}$ v prvi leksikografski urejenosti velja $n < X$, v drugi pa $nX < 1$, sta obe nearhimedski.

Naj bo $\mathcal{K}$ komutativen urejen obseg in τ transcendenten element nad $\mathcal{K}$. Potem je obseg $\mathcal{K}(\tau)$ izomorfen obsegu $\mathcal{K}(X)$ racionalnih funkcij s koeficienti iz $\mathcal{K}$, ki ga znamo urediti na primer z leksikografsko urejenostjo. Ta ni arhimedska, torej vsako enostavno transcendentno razširitev $\mathcal{K}(\tau)$ lahko opremimo s strukturo nearhimedskega urejenega obsega.

LITERATURA

- [1] B. Lavrič, *Arhimedsko urejeni kolobarji*, Obzornik mat. fiz. **39** (1992) 73–78.
- [2] G. Pickert, *Einführung in die höhere Algebra*, Vandenhoeck & Ruprecht, Göttingen 1951.
- [3] D. Vaida, *Sur les corps partiellement ordonnés*, Com. Acad. Roumaine **9** (1959) 1243–1248.
- [4] I. Vidav, *Algebra*, DMFA Slovenije, Ljubljana 1989.

REALNE ALGEBRE, KI ZADOŠČAJO KVADRATNI ENAČBI

BORUT ZALAR

Math. Subj. Class. (1991) 17A45

Na elementaren način so opisani osnovni rezultati teorije kvadratičnih algeber. Po-udarek je na konstrukciji sledi, norme in konjugacije ter vektorski algebri, ki jo generira kvadratična algebra.

REAL ALGEBRAS SATISFYING QUADRATIC IDENTITY

We survey some results and methods of the theory of quadratic algebras for non-specialists. We describe constructions of trace, norm and conjugation in such algebras. We also discuss vector algebra generated by a quadratic algebra.

1. Uvod

Naj bo $\mathcal{A}$ realna, v splošnem neasociativna algebra z enoto, ki jo bomo označili z $\mathbb{I}$. Naj bo $x \in \mathcal{A}$. Oznaka x^2 naj pomeni $x \cdot x$.

Definicija 1. Algebro $\mathcal{A}$ imenujemo *kvadratična*, če za vsak $x \in \mathcal{A}$ obstajata taki števili $s_x, n_x \in \mathbb{R}$, da je $x^2 - 2s_x x + n_x \mathbb{I} = 0$.

Zgled 2. Na obseg kompleksnih števil glejmo kot na dvodimenzionalno realno algebro. Naj bo $z = \alpha + \beta i$ kompleksno število. Tedaj je

$$\begin{aligned} z^2 &= (\alpha^2 - \beta^2) + 2\alpha\beta i = (-\alpha^2 - \beta^2) + \\ &\quad + 2\alpha^2 + 2\alpha\beta i = (-\alpha^2 - \beta^2) + \\ &\quad + 2\alpha(\alpha + \beta i) = -|z|^2 + 2(\operatorname{Re} z)z. \end{aligned}$$

Če vzamemo $n_z = |z|^2$ in $s_z = \operatorname{Re} z$, potem vidimo, da je obseg kompleksnih števil realna kvadratična algebra.

Faktor -2 nastopa v definiciji 1 zato, da se pri tem osnovnem zgledu kvadratične algebre število s_x ujema s funkcijo „realni del“.

Zgled 3. Algebri kvaternionov in oktonionov, opisani v [5] in [6], sta kvadratični. Podobno kot pri kompleksnih številih je $n_x = \|x\|^2$ in $s_x = \operatorname{Re} x$, kjer je $\| \cdot \|$ običajna evklidska norma v $\mathbb{R}^4$ oziroma $\mathbb{R}^8$.

Zgled 4. Naj bo $\mathcal{A}$ algebra realnih matrik dimenzije 2×2 . Če je $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, je

$$X^2 + \alpha X + \beta I = \begin{pmatrix} a^2 + bc + \alpha a + \beta & b(a + d + \alpha) \\ c(a + d + \alpha) & d^2 + bc + \alpha d + \beta \end{pmatrix}.$$

Če vzamemo $\alpha = -a - d = -\text{sled}(X)$ in $\beta = ad - bc = \det(X)$, dobimo, da je $\mathcal{A}$ kvadratična algebra. V resnici je to poseben primer znanega Cayley-Hamiltonovega izreka, ki pravi, da je vsaka matrika ničla svojega karakterističnega polinoma. Ta je v primeru dvorazsežnega vektorskega prostora stopnje največ dva.

Pripomba 5. Algebre realnih matrik dimenzije $n \times n$ za $n \geq 3$ niso kvadratične. To tudi sledi iz Cayley-Hamiltonovega izreka. Če namreč vzamemo matriko, ki ima paroma različne lastne vrednosti, potem je njen karakteristični polinom, ki je hkrati tudi minimalni, stopnje $n > 2$, in zato taka matrika ne more biti ničla nobenega kvadratnega polinoma.

Zgled 6. Naj bo $\mathcal{V}$ realen pred-Hilbertov prostor z abstraktnim vektorskim produktom $\times$ (glej [7]) in naj bo $\mathcal{A} = \mathbb{R}\mathbb{I} \oplus \mathcal{V}$. Če definiramo v $\mathcal{A}$ produkt s predpisom

$$(\alpha\mathbb{I} + x)(\beta\mathbb{I} + y) = (\alpha\beta - \langle x, y \rangle)\mathbb{I} + (\alpha y + \beta x + x \times y),$$

potem je

$$(\alpha\mathbb{I} + x)^2 - 2\alpha(\alpha\mathbb{I} + x) + (\alpha^2 + \|x\|^2)\mathbb{I} = 0,$$

kar pomeni, da je $s_{\alpha+x} = \alpha$ in $n_{\alpha+x} = \alpha^2 + \|x\|^2$.

2. Sled in norma

Prvo naravno vprašanje, ki ga poraja definicija 1, je problem enoličnosti števil s_x in n_x .

Pripomba 7. Če je $\lambda \in \mathbb{R}$, potem za $x = \lambda\mathbb{I}$ števili n_x in s_x nista enolično določeni. Če vzamemo poljuben $\alpha \in \mathbb{R}$, je $x^2 + \alpha x - (\lambda^2 + \alpha\lambda)\mathbb{I} = 0$, kar pomeni, da je s_x lahko katerokoli realno število.

Na srečo velja naslednja preprosta trditev:

Trditev 8. Naj bo $\mathcal{A}$ kvadratična algebra z enoto $\mathbb{I}$ in naj bosta x in $\mathbb{I}$ linearno neodvisna. Tedaj sta števili s_x in n_x enolično določeni.

Dokaz. Naj bo $x^2 + \alpha x + \beta\mathbb{I} = x^2 + \gamma x + \delta\mathbb{I}$. Tedaj je $(\alpha - \gamma)x + (\beta - \delta)\mathbb{I} = 0$, in ker sta ta dva vektorja linearno neodvisna, sledi $\alpha = \gamma$ in $\beta = \delta$. ■

Naš namen je definirati funkciji $s, n : \mathcal{A} \rightarrow \mathbb{R}$. Zaradi opombe 7 si moramo vrednost teh funkcij na elementih oblike $x = \lambda\mathbb{I}$ predpisati sami. V duhu zgledov, ki smo jih navedli, je naravno, če jih definiramo na naslednji način:

$$s(x) = \begin{cases} s_x; & \text{če sta } x \text{ in } \mathbb{I} \text{ linearno neodvisna} \\ \lambda; & \text{če je } x = \lambda\mathbb{I} \end{cases}$$

$$n(x) = \begin{cases} n_x; & \text{če sta } x \text{ in } \mathbb{I} \text{ linearno neodvisna} \\ \lambda^2; & \text{če je } x = \lambda\mathbb{I}. \end{cases}$$

Na ta način dobimo sled $s : \mathcal{A} \rightarrow \mathbb{R}$ in normo $n : \mathcal{A} \rightarrow \mathbb{R}$. Beseda norma mogoče ni najbolj posrečena, ker napeljuje na misel, da je $n(x)$ pozitivno število, kar pa ni nujno res. Ker je ta terminologija že uveljavljena v literaturi, jo bomo uporabljali tudi v tem članku. Oglejmo si nekaj lastnosti sledi in norme.

Trditev 9. *Sled je linearen funkcional. Norma je kvadratičen funkcional, kar pomeni, da zadošča paralelogramskemu pravilu $n(x + y) + n(x - y) = 2n(x) + 2n(y)$.*

Dokaz. Najprej si oglejmo poseben primer, ko so $\mathbb{I}, x, y$ linearno neodvisni. Iz definicije kvadratične algebre dobimo enakosti

$$x^2 - 2s(x)x + n(x)\mathbb{I} = 0, \quad (1)$$

$$y^2 - 2s(y)y + n(y)\mathbb{I} = 0, \quad (2)$$

$$(x + y)^2 - 2s(x + y)x - 2s(x + y)y + n(x + y)\mathbb{I} = 0, \quad (3)$$

$$(x - y)^2 - 2s(x - y)x + 2s(x - y)y + n(x - y)\mathbb{I} = 0. \quad (4)$$

Če izrazimo x^2 in y^2 s pomočjo (1) in (2) ter nato seštejemo (3) in (4), dobimo

$$2[2s(x) - s(x + y) - s(x - y)]x + 2[2s(y) - s(x + y) + s(x - y)]y + [n(x + y) + n(x - y) - 2n(x) - 2n(y)]\mathbb{I} = 0.$$

Ker so $\mathbb{I}, x, y$ linearno neodvisni, so vsi trije oklepaji enaki 0, iz česar sledi, da je $s(x + y) = s(x) + s(y)$ in $n(x + y) + n(x - y) = 2n(x) + 2n(y)$.

Nadalje si oglejmo primer, ko so $\mathbb{I}, x, y$ linearno odvisni, medtem ko para $\{\mathbb{I}, x\}$ in $\{\mathbb{I}, y\}$ nista linearno odvisna. Tedaj lahko zapišemo $y = \alpha\mathbb{I} + \beta x$, kjer $\beta \neq 0$. Po definiciji sledi in norme velja $x^2 - 2s(x)x + n(x)\mathbb{I} = 0$. Od tod lahko direktno izračunamo

$$y^2 - 2[\alpha + \beta s(x)]y + [\alpha^2 + 2\alpha\beta n(x) + \beta^2 n(x)]\mathbb{I} = 0.$$

Po trditvi 8 je $s(y) = \alpha + \beta s(x)$ in $n(y) = \alpha^2 + 2\alpha\beta n(x) + \beta^2 n(x)$. Podobno izračunamo še $s(x + y)$, $n(x + y)$, $n(x - y)$ in ko dobljene rezultate primerjamo, ugotovimo da je $s(x + y) = s(x) + s(y)$ in tudi zelena formula za $n(x)$ je izpolnjena.

Preostaneta nam še primera, ko je bodisi $x = \lambda\mathbb{I}$ ali $y = \lambda\mathbb{I}$, ki ju uženemo s podobnim prijemom kot zgoraj. S tem je aditivnost dokazana. Za konec še homogenost. Če sta $\{1, x\}$ linearno neodvisna, nam $x^2 - 2s(x)x + n(x)\mathbb{I} = 0$ pove, da za poljuben $\lambda \in \mathbb{R}$ velja $(\lambda x)^2 - 2\lambda s(x)(\lambda x) + \lambda^2 n(x)\mathbb{I} = 0$ in po definiciji sledi in norme je $s(\lambda x) = \lambda s(x)$, $n(\lambda x) = \lambda^2 n(x)$. Če je $x = \alpha\mathbb{I}$, potem je

$$s(\lambda x) = s(\lambda\alpha\mathbb{I}) = \lambda\alpha = \lambda s(x), \\ n(\lambda x) = n(\lambda\alpha\mathbb{I}) = \lambda^2\alpha^2 = \lambda^2 n(x)$$

in dokaz je končan. ■

Ni odveč opomba, da nam ta trditev dodatno potrdi smiselnost definicije $s(\alpha \mathbb{I}) = \alpha$ ter $n(\alpha \mathbb{I}) = \alpha^2$. Definirajmo $\mathcal{V}$ kot množico tistih elementov iz $\mathcal{A}$, ki imajo ničelno sled. Direktna posledica prejšnje trditve je

Trditev 10. $\mathcal{V}$ je vektorski podprostor v $\mathcal{A}$ in $\mathcal{A} = \mathbb{R}\mathbb{I} \oplus \mathcal{V}$.

Vsak element kvadratične algebre lahko torej pišemo v obliki $x = \alpha \mathbb{I} + v$, kjer je $\alpha \in \mathbb{R}$ in $v \in \mathcal{V}$. Temu razcepu rečemo *razcep elementa x v vsoto skalarja in vektorja*. Naslednje naravno vprašanje, ki se zastavlja, je zveza med normo in sledjo.

Trditev 11. Med normo in sledjo velja zveza $n(x) = 2s(x)^2 - s(x^2)$. Poleg tega je $n(x^2) = n(x)^2$.

Dokaz. Ker je $x^2 = 2s(x)x - n(x)\mathbb{I}$, je

$$\begin{aligned} (x^2)^2 &= 4s(x)^2x^2 + n(x)^2\mathbb{I} - 4s(x)n(x)x = \\ &= 4s(x)^2x^2 + n(x)^2\mathbb{I} - 2n(x)(x^2 + n(x)\mathbb{I}) = \\ &= x^2(4s(x)^2 - 2n(x)) - n(x)^2\mathbb{I}. \end{aligned}$$

Če sta $\mathbb{I}, x^2$ linearno neodvisna, potem je po trditvi 8 $s(x^2) = 2s(x)^2 - n(x)$ in $n(x^2) = n(x)^2$.

Od zdaj naprej naj bosta x^2 in $\mathbb{I}$ linearno odvisna. Ločiti moramo dve možnosti. Če sta tudi $\mathbb{I}, x$ linearno odvisna, je $x = \alpha \mathbb{I}$. Tedaj je $s(x) = \alpha$, $s(x^2) = \alpha^2$, $n(x) = \alpha^2$ in $n(x^2) = \alpha^4$. Obe zeleni formuli je treba trivialno preveriti. Če pa sta $\mathbb{I}, x$ linearno neodvisna, nam osnovna enakost $x^2 - 2s(x)x + n(x)\mathbb{I} = 0$ pove, da je $x^2 + n(x)\mathbb{I} = 0$ in $s(x) = 0$. Ker je $x^2 = -n(x)\mathbb{I}$, je $s(x^2) = -n(x)$. To nam pove, da je $2s(x)^2 - s(x)^2 = 0 + n(x)$. Po definiciji norme je $n(x^2) = (-n(x))^2 = n(x)^2$, in dokaz je končan. ■

Posledica 12. Na algebri $\mathcal{A}$ obstaja taka simetrična bilinearna forma $\langle \cdot, \cdot \rangle : \mathcal{A} \times \mathcal{A} \rightarrow \mathbb{R}$, da je $\langle x, x \rangle = n(x)$ za vsak $x \in \mathcal{A}$.

Dokaz. Definiramo $\langle x, y \rangle = 2s(x)s(y) - \frac{1}{2}s(xy + yx)$. Ta preslikava je zaradi trditve 9 bilinearna. Po trditvi 11 je $\langle x, x \rangle = n(x)$. ■

3. Vektorska algebra

Najprej bomo izpeljali zvezo med množenjem, normo in sledjo.

Trditev 13. Za poljubna $x, y \in \mathcal{A}$ velja $xy + yx = -2\langle x, y \rangle \mathbb{I} + 2s(x)y + 2s(y)x$, kjer je $\langle x, y \rangle$ bilinearna forma iz posledice 12.

Dokaz. S pomočjo trditve 9 dobimo

$$\begin{aligned}(x + y)^2 &= 2s(x + y)(x + y) - \langle x + y, x + y \rangle \mathbb{I} = 2s(x)x + 2s(y)y + \\ &\quad + 2s(x)y + 2s(y)x - \langle x, x \rangle \mathbb{I} - \langle y, y \rangle \mathbb{I} - 2\langle x, y \rangle \mathbb{I} = \\ &= x^2 + y^2 + 2s(x)y + 2s(y)x - 2\langle x, y \rangle \mathbb{I}.\end{aligned}$$

Od tod takoj sledi želeni rezultat. ■

Posledica 14. Vse komutativne kvadratične algebre so oblike $\mathcal{A} = \mathbb{R}\mathbb{I} \oplus \mathcal{V}$, pri čemer je množenje dano s formulo $(\alpha\mathbb{I} + u)(\beta\mathbb{I} + v) = \alpha\beta\mathbb{I} - \langle u, v \rangle \mathbb{I} + \alpha v + \beta u$, kjer je $\langle \cdot, \cdot \rangle$ neka simetrična bilinearna forma na $\mathcal{V}$.

Dokaz. Brez težav preverimo, da je vsaka algebra take oblike komutativna in kvadratična. Da je vsaka komutativna kvadratična algebra te oblike, pa sledi direktno iz trditve 10 in trditve 13, če upoštevamo komutativnost. V primeru komutativne algebre se namreč enakost iz trditve 13 reducira na $xy = -\langle x, y \rangle \mathbb{I} + s(x)y + s(y)x$. Če zdaj vstavimo $x = \alpha\mathbb{I} + u$ in $y = \beta\mathbb{I} + v$ in upoštevamo $\langle \mathbb{I}, u \rangle = \langle \mathbb{I}, v \rangle = 0$ ter $s(u) = s(v) = 0$, dobimo željeni rezultat. ■

Produkt dveh vektorjev ni nujno vektor, zato $\mathcal{V}$ ni nujno podalgebra v $\mathcal{A}$. Kljub temu lahko v $\mathcal{V}$ na naraven način uvedemo množenje s pomočjo trditve 9. Preslikava $\circ : \mathcal{V} \times \mathcal{V} \rightarrow \mathcal{V}$, dana s predpisom $x \circ y = xy - s(xy)\mathbb{I}$, je zaradi omenjene trditve bilinearna. Iz iste trditve tudi sledi, da je $s(x \circ y) = 0$, kar po definiciji pomeni, da je $x \circ y \in \mathcal{V}$. Par $(\mathcal{V}, \circ)$ imenujemo *vektorska algebra*. Izmed njenih lastnosti navedimo samo najosnovnejšo.

Trditev 15. Vektorski produkt $\circ$ je antikomutativen.

Dokaz. Vzemimo poljubna $u, v \in \mathcal{V}$. Po trditvi 13 je, upoštevaje $s(u) = s(v) = 0$,

$$\begin{aligned}u \circ v + v \circ u &= (uv + vu) - s(uv)\mathbb{I} - s(vu)\mathbb{I} = \\ &= -2\langle u, v \rangle \mathbb{I} - s(uv)\mathbb{I} - s(vu)\mathbb{I}.\end{aligned}$$

Ker je leva stran enačbe vektor, desna pa skalar, je $u \circ v + v \circ u = 0$. ■

Iz zgornjega dokaza dobimo kot stranski produkt še:

Posledica 16. Za vsaka $u, v \in \mathcal{V}$ je $s(uv + vu) = -2\langle u, v \rangle$.

4. Konjugiranje

Ena od pomembnih lastnosti kompleksnih števil je obstoj konjugiranja $z \mapsto \bar{z}$. Podobno preslikavo imajo tudi kvaternioni in oktonioni, kjer zaradi nekomutativnosti množenja velja $\bar{z}\bar{w} = \overline{wz}$, kar je v splošnem različno od $\bar{z}\bar{w}$. V skladu s tem definiramo konjugiranje na splošni realni algebri $\mathcal{A}$ takole:

Definicija 17. Linearno preslikavo $\bar{\cdot} : \mathcal{A} \rightarrow \mathcal{A}$ imenujemo *konjugiranje*, če za vsaka $x, y \in \mathcal{A}$ velja $\overline{\overline{x}} = x$ in $\overline{xy} = \bar{y}\bar{x}$.

V kvadratični algebri $\mathcal{A} = \mathbb{R}\mathbb{I} \oplus \mathcal{V}$ je naravni kandidat za konjugiranje preslikava, definirana z $\alpha\mathbb{I} + v = \alpha\mathbb{I} - v$. Tako je na primer pri kompleksnih številih, kvaternionih in oktonionih. Očitno je, da ta preslikava zadošča pogoju $\overline{\overline{x}} = x$ za vsak $x \in \mathcal{A}$, zato nas zanima, pri kakšnih dodatnih pogojih velja $\overline{xy} = \bar{y}\bar{x}$.

Trditev 18. Naj bo $\mathcal{A} = \mathbb{R}\mathbb{I} \oplus \mathcal{V}$ kvadratična algebra in naj bo dana preslikava $\alpha\mathbb{I} + u = \alpha\mathbb{I} - u$. Tedaj je preslikava $x \mapsto \bar{x}$ konjugiranje natanko tedaj, ko sled zadošča pogoju $s(xy) = s(yx)$ za vsaka $x, y \in \mathcal{A}$. Poleg tega za vsak $x \in \mathcal{A}$ veljajo formule:

- (i) $x\bar{x} = \bar{x}x = n(x)\mathbb{I}$,
- (ii) $x + \bar{x} = 2s(x)\mathbb{I}$,
- (iii) $s(\bar{x}) = s(x)$, $n(\bar{x}) = n(x)$.

Dokaz. Pišimo $x = \alpha\mathbb{I} + u$, $y = \beta\mathbb{I} + v$. Tedaj je $\bar{x} = \alpha\mathbb{I} - u$, $\bar{y} = \beta\mathbb{I} - v$. Nadalje imamo, upoštevaje trditev 15,

$$\begin{aligned}\overline{xy} &= (\alpha\beta\mathbb{I} + \beta u + \alpha v + s(uv)\mathbb{I} + u \circ v)^- = \\ &= \alpha\beta\mathbb{I} + s(uv)\mathbb{I} - \beta u - \alpha v - u \circ v, \\ \bar{y}\bar{x} &= (\beta\mathbb{I} - v)(\alpha\mathbb{I} - u) = \alpha\beta\mathbb{I} + s(vu)\mathbb{I} - \alpha v - \beta u + v \circ u, \\ \overline{xy} - \bar{y}\bar{x} &= s(uv)\mathbb{I} - s(vu)\mathbb{I}.\end{aligned}$$

Torej je preslikava $x \mapsto \bar{x}$ konjugiranje natanko tedaj, ko velja $s(uv) = s(vu)$ za vsaka $u, v \in \mathcal{V}$. Dokazati moramo še, da od tod sledi tudi $s(xy) = s(yx)$ za vsaka $x, y \in \mathcal{A}$. Ker je sled linearna, je

$$s(xy) - s(yx) = (\alpha\beta + s(uv)) - (\alpha\beta + s(vu)) = 0,$$

saj je $s(u) = s(v) = s(u \circ v) = 0$, ker so elementi u, v in $u \circ v$ vektorji.

Ker je $u^2 = -n(u)\mathbb{I}$ za vsak $u \in \mathcal{V}$, je $x\bar{x} = \bar{x}x = \alpha^2\mathbb{I} - u^2 = \alpha^2\mathbb{I} + n(u)\mathbb{I}$. Po trditvi 11 je

$$\begin{aligned}n(x) &= n(\alpha\mathbb{I} + u) = 2s(\alpha\mathbb{I} + u)^2 - s((\alpha\mathbb{I} + u)^2) = \\ &= 2\alpha^2 - s(\alpha^2\mathbb{I} - n(u)\mathbb{I} + 2\alpha u) = 2\alpha^2 - \alpha^2 + n(u),\end{aligned}$$

iz česar sledi $x\bar{x} = n(x)\mathbb{I}$.

Da je $x + \bar{x} = 2s(x)\mathbb{I}$ in $s(\bar{x}) = s(x)$, je očitno. Enakost $n(\bar{x}) = n(x)$ tudi sledi iz trditve 11, saj je

$$n(\bar{x}) = n(\alpha\mathbb{I} - u) = 2\alpha^2 - s(\alpha^2\mathbb{I} - n(u)\mathbb{I} - 2\alpha u) = \alpha^2 + n(u) = n(x).$$

5. Asociativne algebre

Če je kvadratična algebra asociativna, potem imata njena norma in sled avtomatično nekaj posebnih lastnosti.

Trditev 19. *Naj bo $\mathcal{A}$ asociativna kvadratična algebra. Tedaj je*

- (i) $s(xy) = s(yx)$ za vsaka $x, y \in \mathcal{A}$,
- (ii) $n(xy) = n(x)n(y)$ za vsaka $x, y \in \mathcal{A}$.

Dokaz. Vzemimo poljubna $u, v \in \mathcal{V}$. Tedaj je $(uv)u = u(vu)$. Če to identiteto zapišemo s pomočjo vektorskega produkta, dobimo najprej

$$(s(uv)\mathbb{I} + u \circ v)u = u(s(vu)\mathbb{I} + v \circ u),$$

nato pa

$$s(uv)u + s((u \circ v)u)\mathbb{I} + (u \circ v) \circ u = s(vu)u + s(u(v \circ u))\mathbb{I} + u \circ (v \circ u).$$

Po trditvi 15 je $(u \circ v) \circ u = -u \circ (u \circ v) = u \circ (v \circ u)$. Zgornja enakost se zato poenostavi v

$$[s(uv) - s(vu)]u = -s((u \circ v)u)\mathbb{I} + s(u(v \circ u))\mathbb{I}. \quad (5)$$

Ker je na eni strani enakosti vektor, na drugi pa skalar, sledi $s(uv) = s(vu)$. Iz dokaza trditve 18 vemo, da je tedaj tudi $s(xy) = s(yx)$ za vsaka $x, y \in \mathcal{A}$.

Če upoštevamo pravkar dokazano simetričnost sledi, dobimo iz trditve 15 in (5) še

$$s(u(v \circ u)) = s((u \circ v)u) = s(u(u \circ v)) = -s(u(v \circ u)),$$

iz česar sledi, da je $s(u(v \circ u)) = 0$. To pomeni, da je

$$u \circ (v \circ u) = u(v \circ u) \quad (6)$$

za vsaka $u, v \in \mathcal{V}$. Za dokaz identitete (ii) bomo morali izraziti vse količine z bilinearno formo $\langle \cdot, \cdot \rangle$ iz posledice 12. Če v formulo $n(x) = 2s(x)^2 - s(x^2)$ iz trditve 11 vstavimo $x + y$ in upoštevamo (i), dobimo $\langle x, y \rangle = 2s(x)s(y) - s(xy)$ za poljubna $x, y \in \mathcal{A}$. Ker je $s(u) = s(v) = 0$, dobimo

$$s(uv) = -\langle u, v \rangle, \quad (7)$$

$$\langle u, u \circ v \rangle = 0 \quad (8)$$

za vsaka $u, v \in \mathcal{V}$. Če (8) lineariziramo, kar pomeni, da vstavimo namesto u element $u + w$, kjer je $w \in \mathcal{V}$, dobimo

$$\langle u, v \circ w \rangle = \langle u \circ v, w \rangle \quad (9)$$

za vse $u, v, w \in \mathcal{V}$. Zdaj izračunamo, upoštevaje (6), (7) in (9),

$$\begin{aligned} n(uv) &= \langle uv, uv \rangle = \langle s(uv)\mathbb{I} + u \circ v, s(uv)\mathbb{I} + u \circ v \rangle = \\ &= s(uv)^2 + \langle u \circ v, u \circ v \rangle = \langle u, v \rangle^2 + \langle (u \circ v) \circ u, v \rangle = \\ &= \langle u, v \rangle^2 - \langle u \circ (u \circ v), v \rangle = \langle u, v \rangle^2 - \langle u(u \circ v), v \rangle = \\ &= \langle u, v \rangle^2 - \langle u^2v - s(uv)u, v \rangle = \langle u, v \rangle^2 + \langle u, u \rangle \langle v, v \rangle + \\ &\quad + s(uv) \langle u, v \rangle = \langle u, u \rangle \langle v, v \rangle = n(u)n(v). \end{aligned}$$

Za konec vzemimo še $x = \alpha\mathbb{I} + u$, $y = \beta\mathbb{I} + v$. Tedaj je

$$\begin{aligned} n(xy) &= n((\alpha\mathbb{I} + u)(\beta\mathbb{I} + v)) = \\ &= \langle \alpha\beta\mathbb{I} + \alpha v + \beta u + uv, \alpha\beta\mathbb{I} + \alpha v + \beta u + uv \rangle = \\ &= \alpha^2\beta^2 + \alpha^2n(v) + \beta^2n(u) + n(u)n(v) + \\ &\quad + 2\alpha\beta\langle \mathbb{I}, uv \rangle + 2\alpha\beta\langle u, v \rangle + 2\alpha\langle v, uv \rangle + 2\beta\langle u, uv \rangle = \\ &= n(x)n(y) + 2\alpha\langle v, uv \rangle + 2\beta\langle u, uv \rangle + 2\alpha\beta(\langle \mathbb{I}, uv \rangle + \langle u, v \rangle). \end{aligned}$$

Če upoštevamo (8), dobimo

$$\langle u, uv \rangle = \langle u, s(uv)\mathbb{I} + u \circ v \rangle = s(uv)\langle u, \mathbb{I} \rangle = 0.$$

Podobno je $\langle v, uv \rangle = 0$. Na koncu, upoštevaje (7), dobimo še

$$\langle \mathbb{I}, uv \rangle = \langle \mathbb{I}, s(uv)\mathbb{I} + u \circ v \rangle = s(uv) = -\langle u, v \rangle.$$

To pomeni, da so zadnji trije členi v računu iz prejšnjega odstavka enaki 0, zato je $n(xy) = n(x)n(y)$. ■

S pomočjo [6] in pravkar dokazanega bomo izpeljali še primer struktur-nega izreka.

Trditev 20. *Naj bo $\mathcal{A}$ asociativna kvadratična algebra. Če je norma $n(x)$ strogo pozitivno definitna, je $\mathcal{A}$ izomorfna realnim številom, kompleksnim številom ali kvaternionom.*

Dokaz. Naj bo $\langle \cdot, \cdot \rangle$ simetrična bilinerna forma iz posledice 12. Ker je po predpostavki $\langle x, x \rangle = n(x) > 0$ za $x \neq 0$, je $\langle x, y \rangle$ skalarni produkt na $\mathcal{A}$. Ker je

$$\langle xy, xy \rangle = n(xy) = n(x)n(y) = \langle x, x \rangle \langle y, y \rangle,$$

je $\mathcal{A}$ algebra z absolutno vrednostjo in enoto. Po [6, izrek, stran 162] sledi želeni rezultat.

LITERATURA

- [1] A. Elduque, *Alternative quadratic algebras*, J. Math. Phys. **31** (1990) 1–5.
- [2] K. McCrimmon, *Algebras with scalar involution*, Pacific J. Math. **116** (1985) 85–109.
- [3] J. M. Osborn, *Quadratic division algebras*, Trans. Amer. Math. Soc. **105** (1962) 202–221.
- [4] R. D. Schafer, *Introduction to Nonassociative algebras*, Academic Press, 1966.
- [5] B. Zalar, *O oktonionih*, Obzornik mat. fiz. **39** (1992) 79–84.
- [6] B. Zalar, *Algebre z absolutno vrednostjo*, Obzornik mat. fiz. **39** (1992) 161–166.
- [7] B. Zalar, *Abstraktni vektorski produkt*, Obzornik mat. fiz. **40** (1993) 155–161.

RADON V OKOLJU

ANDREJ LIKAR

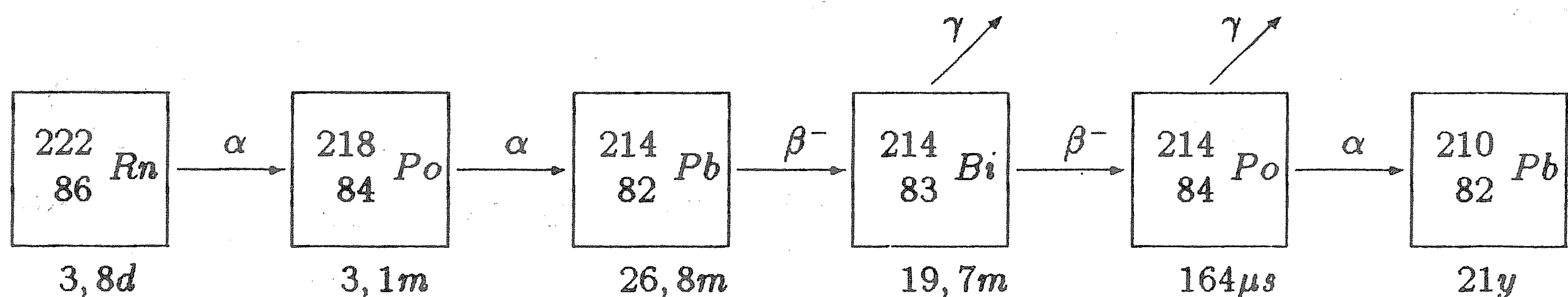
PACS 25.85

V sestavku osvetlimo pojav radona v okolju. Obravnavamo njegov razpad v kratkožive potomce, ki so zdravju nevarni in omenimo najpogostejše postopke pri merjenju specifične aktivnosti radona v zraku.

RADON IN OUR ENVIRONMENT

We discuss the decay of radon in the environment to its short lived daughters which are hazardous to our health. Some common measuring techniques for determination of specific activity of radon in air are presented as well.

Radon (^{222}Rn), toron (^{220}Rn) in aktinon (^{219}Rn) so izotopi žlahtnega plina $_{86}\text{Rn}$, ki nastajajo v naravi z razpadom α radija. Začetki razpadnih verig, ki vodijo do treh različnih izotopov radija, so ^{238}U , ^{232}Th in ^{235}U . Te elemente od nekdaj vsebuje zemeljska skorja, saj njihovi razpolovni časi niso veliko manjši od starosti Zemlje. Povprečno specifično aktivnost ^{238}U v zemlji cenimo na 25 Bq/kg, na prav toliko tudi ^{232}Th , specifična aktivnost ^{235}U pa je le 1 Bq/kg. Toron ($t_{1/2} = 56\text{s}$) in aktinon ($t_{1/2} = 4\text{s}$) imata v primeri z radonom ($t_{1/2} = 3,83\text{ dni}$) kratek razpolovni čas, zato velik del atomov razpade, še preden z difuzijo iz tal dosežejo ozračje. Vpliv torona in aktinona na zdravje ljudi zato večinoma lahko zanemarimo.



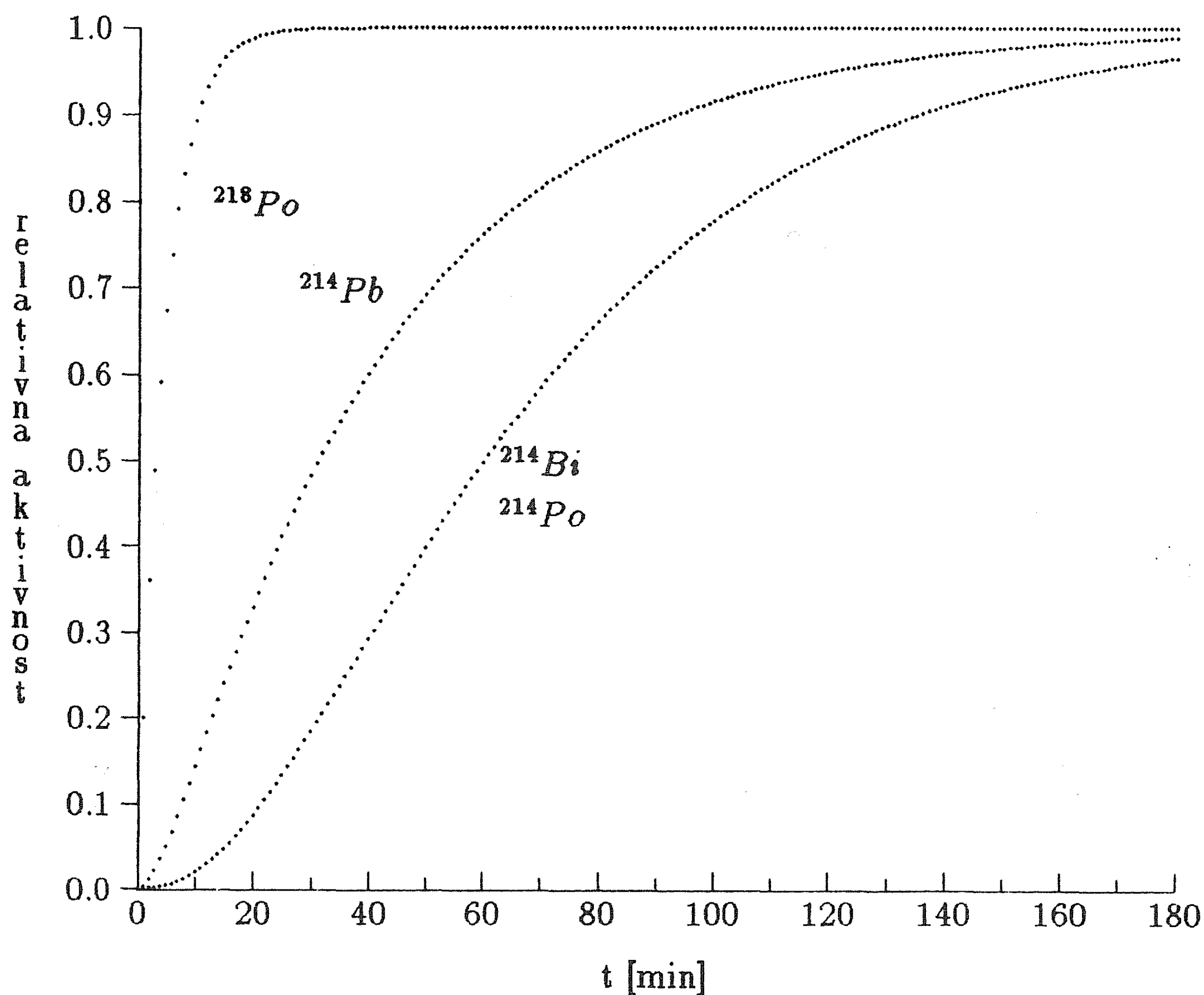
Slika 1. Radonov razpadni niz.

Radon razpada z oddajanjem delcev α po vrsti v kratkožive potomce ^{218}Po , ^{214}Pb , ^{214}Bi in ^{214}Po (slika 1). Izotop ^{210}Pb je sicer tudi nestabilen, a ima razmeroma velik razpolovni čas 21 let. Zato ga obravnavamo, kot da je stabilen. Naraščanje aktivnosti radonovih potomcev opišejo enačbe radioaktivnih nizov:

$$\frac{dN_n}{dt} = \frac{N_{n-1}}{\tau_{n-1}} - \frac{N_n}{\tau_n}.$$

Z N_{n-1} smo označili število atomov predhodnika, z N_n pa število atomov opazovanega izotopa. Razpadni čas τ je povezan z razpolovnim časom: $\tau = t_{1/2}/\ln 2$. Relativna aktivnost kratkoživih potomcev v svežem radonu

se spreminja s časom (slika 2). Aktivnost radona je konstantna, saj lahko zanemarimo njegovo razpadanje zaradi dolgega razpolovnega časa v primeri s potomci. Aktivnosti vseh kratkoživih potomcev so po treh urah enake aktivnosti radona.



Slika 2. Naraščanje aktivnost kratkoživih radonovih potomcev s časom. Pri $t = 0$ imamo le radon. Ravnovesje dosežemo po treh urah.

Kratkoživi radonovi potomci [1] so ob nastanku pozitivno nabiti. V ozračju z 10^4 prašnimi delci v cm^3 se vežejo na delce s pogostostjo 10^{-2} s^{-1} , kar pomeni, da je po nekaj minutah okrog 90% potomcev vezanih. V zelo zakajenih sobah je za to treba le nekaj sekund. Nevezani atomi se s pogostostjo 1/min usedajo na površine v prostoru (stene, tla...), vezani atomi pa le z 1/h. Zato v stanovanjskih prostorih radon ni v ravnovesju s potomci. Odmik od ravnovesja je odvisen od mnogih dejavnikov, na primer od vlažnosti zraka in stopnje ventilacije v prostoru. Radonovih potomcev je v zraku manj kot v ravnovesju. V rovih rudnikov urana z močno ventilacijo preprečujejo nastanek radonovih potomcev.

Vdihavanje zraka z radonovimi potomci je zdravju nevarno. Pljuča zbirajo prašne delce kot filter, potomci pa z delci α poškodujejo občutljivo tkivo. Sam radon zanemarljivo prispeva k obsevanju. Človek je radonu izpostavljen povsod, najbolj pa v zaprtih prostorih. Radon izpuhteva iz sten in tal in se posebno pozimi nabira v slabo zračenih prostorih. Vdihavanje radonovih potomcev prispeva v nekaterih področjih sveta do 50% k celotni obsevalni dozi zaradi naravnih in umetnih radioaktivnih izvirov. Precej radona se sprošča zaradi človekove dejavnosti. Pri pridobivanju in predelavi

urana ter skladiščenju jalovine se izpuhtevanje radona na nekaterih mestih poveča. Radon se sprošča tudi pri sežiganju premoga, zemeljskega plina in uporabi zemeljske toplote. Njegov pogubni vpliv na zdravje so prvi izkusili rudarji v Češkem rudogorju že v 16. stoletju. Za pljučnim rakom so zbolele tri četrtine rudarjev. Vzrok te „gorske bolezni“ so odkrili šele v dvajsetih letih tega stoletja.

O vplivu radona na zdravje ne bomo govorili podrobneje. Kljub temu ocenimo tveganje, da bomo zboleli zaradi povečane koncentracije radona. Denimo, da letno prejmemo zaradi radona dozo 3 mSv, ki je že ustrezno preračunana na celo telo. Toliko povprečno prejmejo na primer na Švedskem. Tveganje, da bomo zboleli, ocenimo s $5 \cdot 10^{-2} \text{ Sv}^{-1}$ po opazovanju ljudi, ki so prejeli večje doze sevanja. Če živimo 60 let, je tveganje:

$$T = 5 \cdot 10^{-2} \text{ Sv}^{-1} 60 \text{ let } 3 \cdot 10^{-3} \text{ Sv/leto} = 10^{-2}.$$

To je primerljivo s tveganjem, da bomo v Sloveniji žrtev v prometni nesreči:

$$T = 60 \text{ let } 700 \text{ leto}^{-1} 2 \cdot 10^6 = 2 \cdot 10^{-2}.$$

Če pomislimo, da so posamezniki zaradi višjih koncentracij radona izpostavljeni tudi mnogo večjim tveganjem, je skrb za zmanjševanje radona v bivalnih prostorih razumljiva. Za primerjavo povejmo, da kadilec, ki pokadi zavoječek cigaret dnevno, tvega glede pljučnega raka toliko kot nekadilec, ki živi v prostoru s specifično aktivnostjo radona 750 Bqm^{-3} (100 primerov/1000 prebivalcev v 60 letih). Iz navedenih podatkov sledi, da pri celoletnem bivanju v prostoru s specifično aktivnostjo radona nekaj deset Bqm^{-3} prejmemo dozo enega mSv.

Do podobnega rezultata pridemo tudi po tejle poti. Denimo, da so potomci v ravnovesju z radonom. Specifične aktivnosti radona in potomcev so zato enake. Od potomcev, ki jih z dihanjem zajamemo v pljuča, sevata žarke α ^{218}Po in ^{214}Po . Število atomov slednjega je v zraku zanemarljivo majhno v primeri z ^{218}Po zaradi kratkega razpolovnega časa. Potomca ^{218}Po in iz njega nastali ^{214}Po sevata delce α z energijo $\sim 5 \text{ MeV}$, potomca ^{214}Pb , ^{214}Bi pa posredno, ko razpadeta do ^{214}Po še po $\sim 5 \text{ MeV}$. Človek vdihne povprečno 1 m^3 zraka v eni uri, torej $24 \times 365 \text{ m}^3$ letno. Računamo, da se v pljučih zadržijo vsi vdihani potomci in tam razpadejo v dolgoživi iztop ^{210}Pb . Njihovo število sledi iz enačbe $N_n = \frac{dN_n}{dt} \tau_n$, v kateri smo z A_n označili specifično aktivnost n -tega potomca, ki je v ravnovesju enaka specifični aktivnosti radona. Z navedenimi podatki izračunamo skupno energijo delcev α v kubičnem metru zraka, ki jo izsevajo potomci do popolnega razpada, ko dotoka novih ni več. Z natančnim računom dobimo $5,57 \cdot 10^{-9} \text{ Jm}^{-3}$ za vsak Bq m^{-3} radona [3]. V pljučih z maso $\sim 1 \text{ kg}$ se torej letno sprosti $24 \times 365 \text{ m}^3 \times 5,57 \cdot 10^{-9} \text{ Jm}^{-3} = 4,9 \cdot 10^{-5} \text{ J}$ energije. Tolikšna je absorbirana doza v grayih (Gy). Pri oceni ekvivalentne doze v sievertih (Sv) upoštevamo, da je sevanje α je pri enaki sproščeni energiji v kilogramu tkiva ~ 20

krat nevarnejše od sevanja γ , zato, pomnožimo sproščeno energijo z 20. S faktorjem 0,1 upoštevamo delež pljuč k celotnemu tveganju, da zbolimo, s faktorjem 0,5 pa ocenimo odmik od ravnovesja. Vse to prinese efektivno ekvivalentno dozo $\sim 0,05$ mSv letno za vsak Bqm^{-3} radona v zraku.

Specifične aktivnosti radona v zraku so najnižje nad oceani, zaledeneli površinami in otoki, pod 1 Bqm^{-3} , nad kopnim med 1 in 10 Bqm^{-3} , v zaprtih prostorih med 10 in 1000 Bqm^{-3} , v jamah, rudnikih in nekaterih toplicah pa dosežejo do nekaj tisoč Bqm^{-3} in več. Specifične aktivnosti radona ni mogoče dovolj natančno napovedati z računskimi modeli. V mnogih državah zato sistematično merijo njegovo koncentracijo predvsem v vrtcih, šolah in stanovanjskih hišah. Meritve specifične aktivnosti radona v 730 vrtcih v Sloveniji [2] so pokazale, da je v 72% vseh igralnic aktivnost nižja kot 100 Bqm^{-3} , v 15 % so našli vrednosti med 100 in 200 Bqm^{-3} , v 6 % pa med 200 in 400 Bqm^{-3} . V enem od vrtcev pa so izmerili okrog 6000 Bqm^{-3} in so ga zato ustrezno sanirali. V razvitem svetu upoštevajo z zakoni predpisane meje, ko se odločajo o sanacijah zgradb.

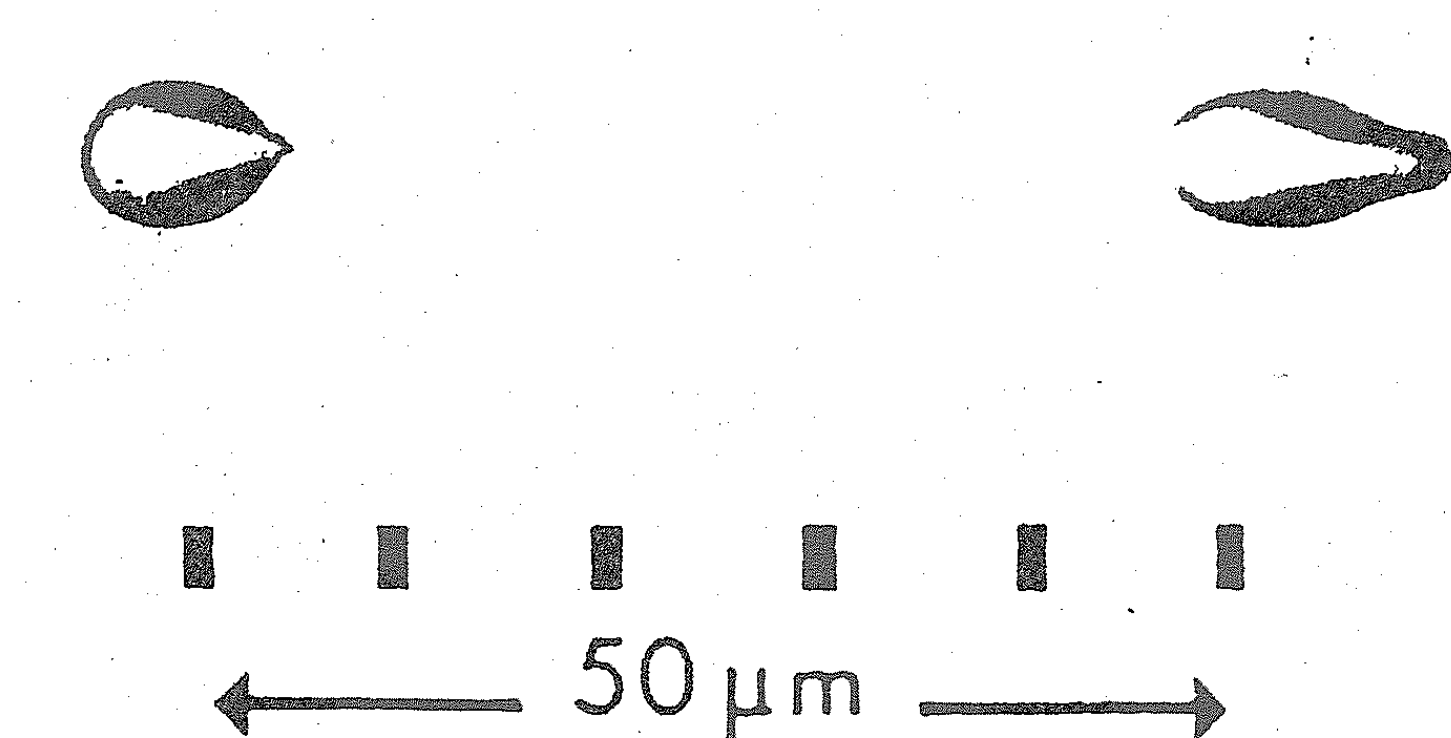
Oglejmo si nekaj metod za merjenje radona v zraku. Merilne metode temeljijo na štetju delcev α , ki jih sevajo radon in še dva potomca, ali fotonov γ dveh potomcev.

Preprosta je metoda s scintilacijsko celico. Posodo s prostornino okrog 0,2 l znotraj prevlečejo s scintilatorjem (cinkovim sulfidom), na eni strani pa naredijo okno za fotopomnoževalko. Delci α pri prehodu skozi scintilator sprožijo bliske z valovno dolžino 600 nm, ki jih šteje fotopomnoževalka. Zrak z radonom zajamejo v stekleno posodo, v laboratoriju pa z njim prepihajo celico. Meriti začnejo po treh urah, ko je radon v ravnovesju s potomci. Ozadje, to je pogostost bliskov, ki niso povezani z razpadom radona in potomcev, je v taki celici okoli 1/min. Če je v celici zrak s specifično aktivnostjo 250 Bqm^{-3} in štejemo eno uro, dobimo 420 ± 20 bliskov od radona in ozadja in 60 ± 8 bliskov iz ozadja. Pri računanju smo privzeli, da enemu razpadu radona ustreza povprečno okrog dvema bliskoma v celici. Temu pravimo „izkoristek celice“. Ne smemo pozabiti, da na en razpad radona pridejo trije delci α , zato je izkoristek lahko večji od ena. Razlika prešteti sunkov je 360 ± 22 , torej merimo aktivnost radona z napako 6%. Pri manjših aktivnostih so časi merjenja bistveno daljši, zato v tem primeru radon iz večje količine zraka koncentrirajo s hladno pastjo s tekočim dušikom (77K). Radon zmrzne pri temperaturi 193 K.

Pri drugem načinu merjenja prečrpajo zrak z znano prostornino skozi filter iz steklenih vlaken, ki zadrži skoraj vse radonove potomce in merijo energijo izsevanih delcev α . Ta je značilna za posamezne potomce. S tem določijo aktivnost potomcev v zraku, na aktivnost radona pa ne morejo zanesljivo sklepati. Zanimiva je metoda z dvema filtroma. V prvem zadržijo potomce iz zraka, v drugem pa s polprevodniškim merilnikom štejejo razpade potomca ^{218}Po , ki nastane z razpadom radona na poti med obema filtroma.

V stanovanjskih prostorih odloča o izpostavljenosti stanovalcev povprečna specifična aktivnost v daljšem razdobju. Metoda z zbiranjem radona na aktivnem oglju in metoda z jedrskimi sledmi sta namenjeni prav takim merjenjem.

Pri prvi segrevajo posodice z ogljem nekaj ur pri temperaturi nekaj nad 100°C , da izženejo adsorbirani radon in vodo [4]. Nato posodice ohladijo in tesno zaprejo. V prostoru posodice odprejo in za nekaj dni izpostavijo zraku. Tesno zaprte posodice nato v laboratoriju po treh urah, ko je radon v ravnovesju s potomci, postavijo na spektrometer γ . Fotone sevata ^{214}Bi in ^{214}Po takoj po razpadu β^{-} ^{214}Pb in ^{214}Bi . Iz izmerjene aktivnosti določijo specifično aktivnost radona v prostoru, v katerem je bila posodica odprta.



Slika 3. Z jedkanjem nastanejo vidne sledi delcev α na površini plastične folije.

Detektor delcev α je pri metodi jedrskih sledi košček plastične folije [5]. Delci α pustijo v foliji sledi, ki postanejo z jedkanjem v vročem NaOH vidne (slika 3). Štetje značilnih sledi opravijo z računalnikom na osnovi slike, ki jo posreduje televizijska kamera [4]. Njihovo število je sorazmerno s časom ekspozicije in specifično aktivnostjo radona v zraku. Detektor moramo zaščititi pred radonovimi potomci v zraku. Zato ga položimo v plastično posodo z zelo ozko špranjo – difuzijsko oviro, ki zadrži potomce, v posodo pa spusti le radon. Take dozimetre izpostavijo radonu v prostoru od enega do treh mesecev in z njimi merijo aktivnosti nad 1 Bqm^{-3} .

LITERATURA

- [1] *Ionizing Radiation: Sources and Biological Effects*, United Nation Scientific Committee on the Effects of Atomic Radiation. Report to the General Assembly, United Nations, New York 1982.
- [2] Janja Vaupotič, *Radon v vrtcih v Sloveniji*, Magistrsko delo, Ljubljana, 1992.
- [3] Milko J. Križman, *Vpliv obratovanja rudnika Žirovski vrh na povišanje koncentracije radona in njegovih kratkoživih potomcev v zraku v neposredni okolici*, Magistrsko delo, Kragujevac 1990.
- [4] A. Lindholm, *privatno sporočilo*
- [5] Tomaž Šutej, *Razvoj dozimetra za določanje radona v zraku z detektorji jedrskih sledi*, Magistrsko delo, Ljubljana, 1988

NOVE KNJIGE

DEVLIN K., Nova zlata doba matematike, Sigma 53, DMFA Slovenije, Ljubljana 1993. 272 strani

V naslovu omenjena nova zlata doba matematike se nanaša na čas od leta 1960 do približno 1982. Matematika se je namreč v tem času še posebno intenzivno razvijala. Intenzivno se je razvijala tudi zadnjih 2500 let, z izjemo daljšega časovnega intervala v srednjem veku. Kot primer razdobja, v katerem so bili dosežki posebno pomembni, moremo šteti čas okoli 300 let pr. Kr., ko je nastala prva aksiomatično zgrajena matematična disciplina, evklidska geometrija. Za drugo pomembno zlato dobo matematike bi večina matematikov štela čas, ko sta Newton in Leibniz razvila infinitezimalni račun.

Avtor šteje obdobje 1960–1982 za zlato dobo najmanj iz dveh razlogov. V tem času so se razvile moderne matematične discipline, v klasičnih področjih matematike pa so matematiki rešili nekaj zelo starih, težkih problemov; v teh disciplinah je šel razvoj v globino. Avtor si je zadal nalogo predstaviti nepoklicnemu matematiku in ljubitelju matematike nekaj teh novih rezultatov, predvsem pa posredovati lepoto dosežkov in deliti z bralcem silno navdušenje in čudenje nad doseženimi rezultati.

O modernih področjih je s takim ciljem bolj težko pripovedovati; lažje je poljudno predstaviti stare, pogosto lahko razumljive probleme, katerih rešitev je tudi stoletja kljubovala naporom matematikov.

Prvo poglavje govori o teoriji števil, o praštevilih in njihovi uporabi v kriptografiji. Drugo govori o množicah, o aksiomatični metodi v matematiki, o neskončnosti in o problemih matematične logike. Tretje poglavje podaja zgodovinski pregled razvoja pojma realnega in kompleksnega števila, zatem opiše, kako je v sedemdesetih letih prišlo do rešitve starega problema razrednega števila, do dokaza domneve, ki jo je postavil za Gauss. Četrto poglavje govori o modernem področju, o kaosu, kar je postalo res zanimivo področje šele z razvojem zmogljivih računalnikov. Peto poglavje nas vpele v teorijo grup; cilj je opis dokaza izreka o klasifikaciji enostavnih grup. Dokaz tega izreka je nastajal desetletja in ga sestavlja okoli 500 člankov s skupnim obsegom približno 15000 strani. Tudi ta dokaz je bil dokončno izpeljan v sedemdesetih letih. Šesto poglavje je posvečeno reševanju enačb v celih številih. Glavni dosežek v sedemdesetih letih je bil negativen odgovor na 10. Hilbertov problem: ni nobenega postopka, ki bi za vsako Diofantsko enačbo v končno mnogo korakov ugotovil, ali je rešljiva ali ne. Tudi sedmo poglavje pripoveduje o več kot sto let starem problemu: ali je možno s štirimi barvami dobro pobarvati vsak zemljevid. Dokaz tega izreka so, ob bistveni pomoči računalnika, našli v sedemdesetih letih. Osmo poglavje pripoveduje o slavnem zadnjem Fermatovem problemu. Še danes se ne ve, ali je ta problem res rešen. Deveto poglavje je nekoliko zahtevnejše. Opisuje teorijo analitičnih funkcij in njeno zvezo s problemi iz teorije števil. Na koncu poglavja najdemo opis poti, po kateri so v sedemdesetih letih prišli do dokaza, ki je potrdil sto let staro Bieberbachovo hipotezo. Deseto poglavje opisuje

razmeroma moderno področje, topologijo. Govori o vozlih, o ploskvah v prostoru in o posplošitvi tega pojma, o mnogoterostih v večdimenzionalnem prostoru. Vrhunec poglavja je opis Poincaréjeve domneve in kako so v osemdesetih letih dokazali, da ta domneva ne drži, npr. v štiridimenzionalnem prostoru. Zadnje poglavje opisuje probleme učinkovitosti algoritmov, torej probleme iz modernega področja teoretičnega računalništva.

Menim, da je avtorju zastavljeni cilj lepo uspel. Dostopno je opisal nekaj najpomembnejših dosežkov matematike, predvsem v zadnjih 30 letih; uspelo mu je tudi posredovati navdušenje matematikov nad opisanimi izrednimi dosežki.

Knjiga je zanimivo branje za matematika, za študente matematike, za srednjošolce in tudi za druge ljubitelje matematike.

Anton Suhadolc

VESTI

PROF. DJURO KUREPA IN MEMORIAM

V decembru lanskega leta smo izvedeli, da je v tragičnih okoliščinah preminil slovenskim matematikom dobro znan matematik akademik prof. Djuro Kurepa.

Rodil se je kot štirinajsti otrok 16. avgusta 1907 v Glini. Študiral je na univerzi v Zagrebu in Parizu. Doktoriral je na Sorboni leta 1935 pod mentorstvom M. Frecheta. Tema doktorske disertacije je bila iz področja teorije delno urejenih množic. Tej temi je ostal zvest tudi pozneje. Med več kot 50 članki, ki jih je objavil v mednarodnih matematičnih revijah, so morda najpomembnejši iz področja teorije množic. Prof. Kurepa je bil od leta 1938 do leta 1945 docent, pozneje profesor na zagrebški univerzi, od leta 1965 do upokojitve leta 1977 pa redni profesor na beograjski univerzi. Bil je mentor pri 42 doktorskih disertacijah iz matematike. Pri njem sta doktorirala tudi pri nas zelo znana matematika prof. Svetozar Kurepa in prof. Sibe Mardešić. Poleg poučevanja je bil prof. Kurepa izjemno delaven matematik. Priobčil je prek 100 člankov strokovne vsebine. Rad se je udeleževal matematičnih konferenc, simpozijev, posvetov in objavil več deset prispevkov s takih srečanj. Kot gost je predaval na univerzah po vsej Evropi in tudi na mnogih ameriških univerzah. Bil je tudi izjemno plodovit pisec srednješolskih učbenikov. V soavtorstvu je napisal, če ne štejemo mnogih ponatisov, okoli 30 srednješolskih in nekaj univerzitetnih učbenikov. Poleg naštetih publikacij je objavil še nekaj sto poljudnih prispevkov, prigradnih sestavkov, sestavkov o problematiki pouka matematike, iz šahovskega sveta in nekaj zanimivih avtobiografskih sestavkov. Tudi v OMF je objavil članek z naslovom Diskretum in kontinuum, leta 1986 je napisal 14 strani dolg sestavek v Matematičnem vestniku, posvečen profesorju Plemlju.

Prof. Kurepa je bil član mnogih matematičnih društev, uredniških odborov, kongresnih odborov itd. Napisal je tudi okoli 1000 recenzij knjig. Za neutrudno delo je dobil mnoga domača in inozemska priznanja.

Prof. Djuro Kurepa je za seboj pustil sled, ki bo še dolgo časa vidna v matematični skupnosti.

Anton Suhadolc

NOVI ČLANI DMFA SLOVENIJE V LETU 1993

Lani se je v Društvo matematikov, fizikov in astronomov Slovenije včlanilo 83 novih članov, društvo je zapustilo 31 članov. Novi člani društva so:

- | | |
|------------------------------|---------------------------------|
| 1631. BABIČ Vitomir | 1673. MATI Danica |
| 1632. BARBIČ Lenart | 1674. MEDVEŠČEK Janja |
| 1633. BENIGER JAPELJ Petra | 1675. MERZEL Franci |
| 1634. BENKO Dragomir | 1676. MIKLAVC Adolf |
| 1635. BORŠTNIK Branko | 1677. MOČIVNIK Primož |
| 1636. BOŠTJANČIČ Angela | 1678. MOČIVNIK PATERNOST Helena |
| 1637. BRATKO Dušan | 1679. MUHIČ Zinka |
| 1638. CESAR Zdenka | 1680. NAGODE Franc |
| 1639. CVELBAR Uroš | 1681. NOVAK Karmen |
| 1640. DERGANČ Jure | 1682. OGRIZEK Sandi |
| 1641. DOBNIKAR Jure | 1683. PADEŽNIK Franci |
| 1642. DOLENC Sašo | 1684. PAVLIN Marta |
| 1643. FABIČ PETRAČ Irena | 1685. PEKLAJ Vanja |
| 1644. FURMAN Darinka | 1686. PLANINC Igor |
| 1645. GABROVEC Peter | 1687. PLANTAN Jožica |
| 1646. GOJČIČ Zlatka | 1688. POLJANEC Ksenija |
| 1647. GORNIK Bojan | 1689. POTOKAR Milan |
| 1648. GRAHEK Mateja | 1690. POVALEJ Lilijana |
| 1649. HAJNŠEK Tanja | 1691. PREŠEREN Rok |
| 1650. HAREJ Vesna | 1692. PREVORČIČ Simona |
| 1651. HORVAT Darja | 1693. PUPIS Vesna |
| 1652. IRT Gregor | 1694. RAJIČ Jaro |
| 1653. IVANUŠA Robert | 1695. ROBBA Severin |
| 1654. JAKOBČIČ Andrej | 1696. ROSA Irena |
| 1655. KLEMENČIČ Janez | 1697. RUTER Andrej |
| 1656. KOBAL Ivan | 1698. SLAPAR Marko |
| 1657. KOCON Jože | 1699. SOLARIČ Ladislav |
| 1658. KOKLIČ Rudolf | 1700. SUHADOLNIK Alojz |
| 1659. KOSI Irena | 1701. SUŠAK Branko |
| 1660. KOTNIK Masimiljan | 1702. ŠOLMAJER Tomaž |
| 1661. KOVAČ GREGORČIČ Irena | 1703. ŠUBIČ Aleš |
| 1662. KOVAČEC MARAŠEK Simona | 1704. ŠUŠTERŠIČ Luka |
| 1663. KOZOLE Alojz | 1705. ŠVAGAN Majda |
| 1664. KREJAN Alenka | 1706. TRATNIK Uroš |
| 1665. KRIŽAN Peter | 1707. URBIČ Tomaž |
| 1666. KULČAR Igor | 1708. VERČKO Ivan |
| 1667. LAVRIČ Majda | 1709. VIČAR Zorko |
| 1668. LAZAR Samo | 1710. ZAVRTANIK Danilo |
| 1669. LESAR Antontija | 1711. ZAZULA Mojca |
| 1670. LUKŠIČ Marija | 1712. ZDOLŠEK Marija |
| 1671. LUZAR Alenka | 1713. ZUPAN Aleš |
| 1672. MARINČEK Jože | |

Martina Koman