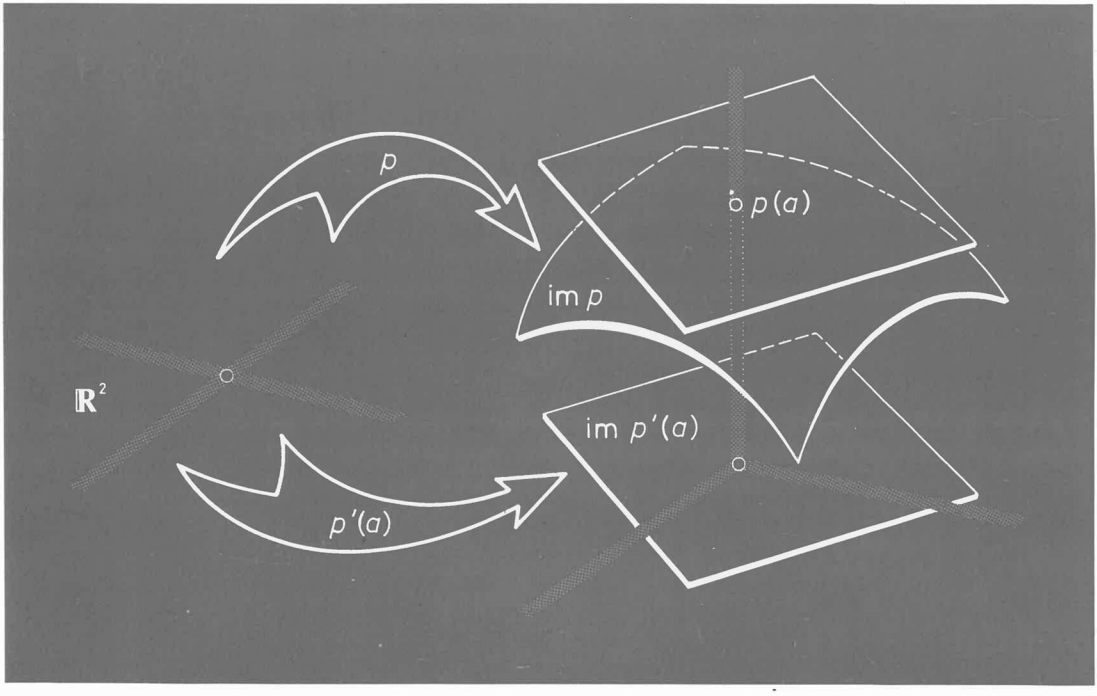
R-177/87-1/2
ODPISANO

IZDAJA DRUSTVO MATEMATIKOV, FIZIKOV IN ASTRONOMOV SR SLOVENIJE

YU ISSN 0473-7466

1987
Letnik 34
1/2

OBZORNIK ZA MATEMATIKO IN FIZIKO



LETNIK 34 — ŠTEVILKA 1/2

OBZORNIK ZA MATEMATIKO IN FIZIKO

LJUBLJANA, JANUAR 1987

Uredniški odbor: Janez Strnad — urednik za fiziko in odgovorni urednik, Milan Hladnik — urednik za matematiko, Ciril Velkovrh — urednik.

Odbor svetovalcev: Robert Blinc, Alojz Kodre, Peter Legiša, Anton Moljk, Mitja Rosina, Tomaž Skulj, Anton Suhadolc, Ivan Vidav

Jezikovni pregled Marija Janežič, slike Miha Štalec.

Naročnina: za posameznike 3000.— din (za člane društva je že vračunana članarina), za dijake in študente 1500.— din, za ustanove in podjetja 6000.— din, za tujino 20 $, posamezna številka 1000.— din, dvojna številka 2000.— din.

Dopise pošiljajte in list naročajte na naslov: Društvo matematikov, fizikov in astronomov SRS — Podružnica Ljubljana — Obzornik za matematiko in fiziko, 61111 Ljubljana, Jadranska cesta 19, p. p. 64, telefon št. (061) 265-061/53, žiro račun 50101-678-47233, devizni račun pri Ljubljanski banki št. 50100-620-107-257300-5694/4.

Tisk: Tiskarna Ljudske pravice v Ljubljani. Naklada 1600 izvodov. Izdajo revije sofinancirata ISS in RSS.

© 1987 DMFA SRS — 839

Poštnina plačana na pošti 61102 Ljubljana

ODPISANO

2-177/87-1/2

Inv. 129509

VSEBINA — CONTENTS

Str. — Page

Članki — Articles

Prijateljska števila — Amicable numbers (Jože Grasselli) . . . . . 1— 7
Kubične krivulje — Cubic curves (Ivan Vidav) . . . . . 9—22
Nova pot do Lebesgua — Lebesgue in a new way (Niko Prijatelj) . . . . 23—33
Geometrijska podoba odvoda — Differentiation from the geometric point of view (France Križanič) . . . . . 35—52
Fizikalne razmere v zvezdah — Physical conditions in stars (Tomaž Zwitter) 53—55
Višina vesoljskih teles — The altitude of heavenly bodies (Marijan Prosen) 56—58

Nove knjige — New books

(Marko Petkovšek, Alojzij Vadnal, Andrej Čadež, Peter Legiša, Drago Bajc, Bojan Mohar, Sandi Klavžar, Drago Bajc, Martin Čopič, Janez Rakovec, Mladen Houška, Ivan Vidav) 7, 21, 22, 33, 52, 55, 58, 59, 61, 62

Utrinki

Kako dosežete, da postane fizika samouničevalna (Janez Strnad) 64

Domače vesti — Home news

Mednarodni kongres matematikov, Berkeley 1986 (Dušan Repovš) . . . . 64—III
11. seminar iz fizike: Medicina in fizika — vabilo (Janez Strnad) IV

Na ovitku: Slika 6. (Glej članek na str. 35.)

PRIJATELJSKA ŠTEVILA

JOŽE GRASSELLI

Math. Subj. Class. (1985) 10 A 40

Članek opisuje nekaj važnejših ugotovitev o prijateljskih številih.

AMICABLE NUMBERS

An exposition of some facts about amicable numbers is given.

1. Vsakemu naravnemu številu a, ki je večje od 1, pripadata vsota vseh njegovih pravih deliteljev

$$s(a) = \sum d \quad ; \quad d|a \quad , \quad 1 \leqq d < a$$

in vsota vseh njegovih pozitivnih deliteljev

$$\sigma(a) = \sum d \quad ; \quad d|a \quad , \quad 1 \leqq d \leqq a$$

Vrednosti $s(a)$ in $\sigma(a)$ sta naravni števili in se razlikujeta za a

$$s(a) = \sigma(a) - a \tag{1}$$

Zaradi te povezave je mogoče obravnavanje vsote $s(a)$ prevesti na obravnavo za $\sigma(a)$. To se večkrat naredi, ker se vsota $\sigma(a)$ pri znani kanonični izrazitvi števila a izraža enostavneje kot vsota s(a). Naj bo namreč

$$a = p^m \ldots q^n$$

kjer so $p, \ldots, q$ različna praštevila, $m, \ldots, n$ naravna števila. Vsak pozitivni delitelj števila a je zajet ravno enkrat v vsoti, ki jo dobimo, ko v izrazu

$$(1 + p + p^2 + \ldots + p^m) \ldots (1 + q + q^2 + \ldots + q^n)$$

opravimo vsa množenja. Ker so v oklepajih vsote geometričnih zaporedij, imamo

$$\sigma(a) = \frac{p^{m+1} - 1}{p - 1} \ldots \frac{q^{n+1} - 1}{q - 1} \tag{2}$$

2. Primerjajmo po velikosti a in $s(a)$ in upoštevajmo še povezavo (1). Naravno število a je

deficientno, če je $s(a) < a$ oz. $\sigma(a) < 2a$
abundantno, če je $s(a) > a$ oz. $\sigma(a) > 2a$
popolno, če je $s(a) = a$ oz. $\sigma(a) = 2a$

Deficientnih števil je neskončno. Med njimi so npr. že vsa praštevila p, saj je $s(p) = 1 < p$.

Tudi abundantnih števil je neskončno. Mednje sodijo npr. tudi vsa števila $3 \cdot 2^n$, $n \geqq 2$. Po (2) je namreč

$$\sigma(3 \cdot 2^n) = 4(2^{n+1} - 1) = 6 \cdot 2^n + 2 \cdot 2^n - 4 > 2 \cdot (3 \cdot 2^n)$$

---

* Prvi štirje prispevki so zapisi predavanj na 11. društvenem seminarju iz matematike, ki je bil januarja 1986 v Ljubljani.

Najmanjše popolno število je 6. Res je $s(6) = 1 + 2 + 3 = 6$.

Domnevajo, da je popolnih števil neskončno. Dokaza, ki bi to domnevo potrjeval, še ni.

Pač pa je poznana zgradba sodih popolnih števil. Opisuje jo Evklid-Eulerjevo pravilo:

Sodo število c je popolno natančno tedaj, kadar ima obliko

$$c = 2^{n-1}(2^n - 1) \tag{3}$$

in je $2^n - 1$ praštevilo.

Že Evklid omenja, da je število c iz (3) popolno, kadar je $2^n - 1$ praštevilo. Seveda je c tudi sodo število, saj mora biti $n \geqq 2$, če naj bo $2^n - 1$ praštevilo. Euler je pokazal, da sodo popolno število ne more imeti drugačne oblike, kot je ta Evklidova. Oboje izhaja iz opredelitve popolnega števila in iz (2).

Če je eksponent n sestavljeno število, npr. $n = st$, kjer sta s, t od 1 večji naravni števili, $2^n - 1 = 2^{st} - 1$ gotovo ni praštevilo, saj ima pravi delitelj $2^s - 1 > 1$. Ko iščemo soda popolna števila, je torej dovolj, da v (3) teče n po praštevilih.

Vendar v splošnem $2^n - 1$ ni praštevilo, ko je eksponent n praštevilo. Zgled: $2^{11} - 1 = 2047 = 23 \cdot 89$. Zato je treba za vsak praštevilski eksponent n posebej ugotoviti, ali je $2^n - 1$ praštevilo ali ne. Pri tem se je mogoče naslanjati na tale kriterij, ki ga je podal v prejšnjem stoletju Lucas ([6], str. 225):

Naj bo n praštevilo, $r_1 = 4$, $r_{j+1} = r_j^2 - 2$ za $j = 1, 2, \ldots, n-1$. Število $2^n - 1$ je praštevilo, če je

$$r_{n-1} \equiv 0 \pmod{2^n - 1}$$

in sestavljeno, če je

$$r_{n-1} \not\equiv 0 \pmod{2^n - 1}$$

Kriterij zahteva že pri majhnih n veliko računanja. Pri večjih n ga je bilo mogoče uporabiti šele, ko so se pojavili moderni računalniki.

Praštevila oblike $2^n - 1$ imenujemo Mersennova. Do leta 1983 je bilo najdenih 28 Mersennovih praštevil in z njimi po (3) prav toliko sodih popolnih števil. Največje tedaj znano Mersennovo praštevilo je bilo

$$2^{86243} - 1$$

V desetiškem zapisu ima prek 25 000 mest in je bilo takrat tudi največje znano praštevilo.

Dosti manj kot o sodih se ve o lihih popolnih številih. Našli niso doslej še nobenega. Niso pa mogli dokazati, da lihih popolnih števil ni. Dognali so le, da so liha popolna števila, če obstajajo, zelo velika. Tako po nekaterih ocenah pod 10^{200} ni nobenega lihega popolnega števila ([5], str. 25).

3. Če naravno število a ni popolno, je $s(a) \neq a$. Ali je pri kakšnem a morda $s(s(a)) = a$? To vprašanje nas pripelje do prijateljskih števil.

Od 1 večji in med sabo različni naravni števili a, b sestavljata **prijateljski par**, če je

$$s(a) = b \text{ in } s(b) = a \tag{4}$$

Števili a, b sami imenujemo tedaj **prijateljski**. Zaradi (4) je

$$s(s(a)) = s(b) = a \text{ in } s(s(b)) = s(a) = b$$

Če upoštevamo (1), se pogoj (4) glasi

$$\sigma(a) = \sigma(b) = a + b \tag{5}$$

Zgled prijateljskega para dajeta števili 220 in 284. Iz praštevilske razcepitve

$$220 = 2^2 . 5 . 11, \quad 284 = 2^2 . 71$$

po (2) izračunamo

$$\sigma(220) = 7 . 6 . 12 = 504 = 220 + 284$$
$$\sigma(284) = 7 . 72 = 504 = 220 + 284$$

in pogoj (5) je izpolnjen.

Prijateljski par 220, 284 so poznali že davno. Nekateri menijo, da ga je odkril Pitagora. Drugi spet navajajo razloge, po katerih naj bi za ta par vedeli vsaj 500 let pred Pitagoro. Poimenovanje prijateljska števila pripisujejo Pitagori.

4. Dolgo je bil 220, 284 edini poznani prijateljski par. Seveda se je zastavljalo vprašanje, ali je še kaj prijateljskih parov.

Delni odgovor vsebuje pravilo za iskanje prijateljskih števil, ki ga je v 9. stoletju postavil Thabit ibn Kurrah iz Bagdada ([4], str. 39). Pravilo se da povedati takole:

Naj bo n naravno število večje od 1. Če so števila

$$\begin{aligned} p &= 3 . 2^{n-1} - 1 \\ q &= 3 . 2^n - 1 \\ r &= 9 . 2^{2n-1} - 1 \end{aligned} \tag{6}$$

praštevila, sestavljata števili

$$\begin{aligned} a &= 2^n pq \\ b &= 2^n r \end{aligned} \tag{7}$$

prijateljski par.

O veljavnosti pravila se lahko bralec prepriča sam, upoštevaje (2). Pri uporabi Thabitovega pravila so težave podobne kot pri Evklid-Eulerjevem pravilu za popolna števila. Za večje n pač ni preprosta stvar dognati, ali so p, q, r v (6) praštevila ali ne.

Thabit sam je uporabil svoje pravilo le za $n = 2$. Tedaj je

$$p = 3 . 2 - 1 = 5, \quad q = 3 . 2^2 - 1 = 11, \quad r = 9 . 2^3 - 1 = 71$$

Ker so to sama praštevila, sta števili, določeni po (7)

$$a = 2^2 . 5 . 11 = 220, \quad b = 2^2 . 71 = 284$$

prijateljski. Dobljen je že znani Pitagorov par.

Ko so se v 17 stoletju v Evropi spet začeli zanimati za prijateljska števila, Thabitovega pravila niso poznali. Toda Fermat in malo pozneje Descartes sta to pravilo vsak zase na novo odkrila.

Fermat je pri $n = 4$ iz (6) in (7) prišel do prijateljskega para

$$2^4 . 23 . 47 = 17\,296, \quad 2^4 . 1151 = 18\,416$$

Pred kratkim so opazili, da navaja ta par v nekem svojem spisu Maročan Ibn al Banna že okrog leta 1300.

Descartes je vzel $n = 7$ in ugotovil, da so tedaj p, q, r iz (6) praštevila. To mu je dalo prijateljski par

$$2^7 \cdot 191 \cdot 383 = 9\,363\,584, \quad 2^7 \cdot 73\,727 = 9\,437\,056$$

Tako se je po več kot 2000 letih število znanih prijateljskih parov povzpelo na tri.

V zadnjem času so Thabitovo pravilo preizkusili za vse $n \leqq 20\,000$. Izkazalo se je, da se dobe prijateljski pari le za $n = 2, 4, 7$, ko imamo Pitagorov, Fermatov in Descartesov par. Seveda da se ne da od tod nič sklepati, kaj je pri $n > 20\,000$.

5. Po Descartesu je preteklo približno sto let, da so spet našli nova prijateljska števila. Posrečilo se je to Eulerju.

Najprej se je Euler vprašal po vseh prijateljskih parih

$$a = 2^n pq, \quad b = 2^n r \tag{8}$$

kjer so p, q, r različna liha praštevila in n naravno število. Takšne pare smo srečali že v Thabitovem pravilu, vendar imajo tam praštevila p, q, r predpisano obliko (6). Eulerja je njegovo vprašanje privedlo do neke diofantske enačbe, ki je ni bilo težko rešiti. Poglejmo!

Da bosta števili (8) prijateljski, mora po (5) veljati

$$\sigma(2^n pq) = \sigma(2^n r)$$

Vrednosti na obeh straneh se dasta izraziti po obrazcu (2), saj so 2, p, q, r različna praštevila. Dobimo

$$(p + 1)\,(q + 1) = r + 1 \tag{9}$$

in ko se vzame

$$p + 1 = x, \quad q + 1 = y \tag{10}$$

se (9) lahko zapiše

$$xy = r + 1 \tag{11}$$

Po zahtevi (5) mora še biti

$$\sigma(2^n pq) = 2^n pq + 2^n r$$

ali

$$(2^{n+1} - 1)\,(p + 1)\,(q + 1) = 2^n(pq + r)$$

Če se tu upošteva, da je po (10) in (11)

$$pq + r = 2xy - x - y$$

se pride na enačbo

$$xy = 2^n(x + y)$$

ki se da pisati tudi takole

$$(x - 2^n)\,(y - 2^n) = 2^{2n} \tag{12}$$

Od tod se vidi, da je treba 2^{2n} izraziti kot produkt dveh različnih celih števil, saj sta x, y po (10) različna naravna. Hitro se še pokaže, da morata faktorja na levi biti tudi večja od 1. Ker se da 2^{2n} razcepiti v produkt dveh naravnih od 1 večjih faktorjev le na način

$$2^{2n} = 2^{n-k} \cdot 2^{n+k}$$

kjer je k naravno število, manjše od n, je rešitev za (12)

$$x = 2^n + 2^{n-k}, \quad y = 2^n + 2^{n+k}$$

Iz (10) in (11) pri $m = n - k$ potem izhaja

$$\begin{aligned} p &= 2^m(2^k + 1) - 1 \\ q &= 2^m(2^k + 2^{2k}) - 1 \\ r &= 2^{2m}(2^k + 2^{2k+1} + 2^{3k}) - 1 \end{aligned} \tag{13}$$

Tako smo pri Eulerjevem pravilu:

Če so pri naravnih m, k števila iz (13) praštevila, dajeta števili

$$\begin{aligned} a &= 2^{m+k}pq \\ b &= 2^{m+k}r \end{aligned} \tag{14}$$

prijateljski par.

Za $m = n - 1$, $k = 1$ preide Eulerjevo pravilo v Thabitovo pravilo. Je pa seveda Eulerjevo pravilo splošnejše od Thabitovega.

Euler z zgornjim pravilom ni našel nobenega novega prijateljskega para. Pozneje je Legendre pokazal, da sta p, q iz (13) za $m = 1$, $k = 7$ praštevili. Ali je število r tedaj praštevilo ali ne, ni mogel dognati. Čez nekaj let je Čebyšev ugotovil, da je pri tej izbiri tudi r praštevilo. Tako je bil za $m = 1$, $k = 7$ po (13) in (14) najden prej še neznani prijateljski par. V zadnjem času so po Eulerjevem pravilu s pomočjo računalnikov prišli še do enega novega prijateljskega para.

Na podoben način kot zgornje pravilo je Euler izpeljal še več drugih pravil za iskanje prijateljskih parov ([4], str. 42 sl.). Z njimi je odkril 59 novih prijateljskh parov. Večino Eulerjevih parov sestavljajo kar velika števila. Ni pa med njimi majhnega para

$$1184 = 2^5 \cdot 37, \quad 1210 = 2 \cdot 5 \cdot 11^2$$

ki so ga našli šele sredi prejšnjega stoletja.

6. Do nedavnega so se pri iskanju prijateljskih števil naslanjali le na Eulerjeva pravila. Pred nekaj leti pa je Borho odkril pravilo, po katerem je mogoče iz znanih prijateljskih parov prihajati do novih prijateljskih parov ([2]). Pravilo pravi:

Imejmo tak prijateljski par

$$a = cu, \quad b = cs \tag{15}$$

da je s praštevilo, c in u tuja, c in s tuja. Če je

$$u + s + 1 = p \tag{16}$$

praštevilo in sta pri naravnem n tudi

$$\begin{aligned} q &= (u + 1)\, p^n - 1 \\ r &= (u + 1)(s + 1)\, p^n - 1 \end{aligned} \tag{17}$$

praštevili, dajeta števili

$$\begin{aligned} a_1 &= ap^nq \\ b_1 &= cp^nr \end{aligned} \tag{18}$$

prijateljski par.

Da Borhovo pravilo drži, se ni težko prepričati. Tukaj tega ne bomo preverjali. Tudi ne bomo opisovali, kako je bilo pravilo odkrito. Obrnimo se kar k zgledu.

Vzemimo Pitagorov prijateljski par. Razcepitev, ki jo pravilo zahteva, se glasi

$$a = 220 = 4 \cdot 55, \quad b = 284 = 4 \cdot 71$$

tako da je glede na (15)

$$c = 4, \quad u = 55, \quad s = 71 \tag{19}$$

Ker sta števili

$$s = 71 \text{ in } p = u + s + 1 = 55 + 71 + 1 = 127 \tag{20}$$

praštevili, je Pitagorov par ustrezen kot izhodišče za Bohrovo pravilo.

Po (19) in (20) je $u + 1 = 56$, $s + 1 = 72$, $c = 4$, $p = 127$. Ko to upoštevamo v (17) in (18), lahko v našem primeru zaradi $a = 220$ Borhovo pravilo takole povemo:

Naj teče n po naravnih številih. Vsakič, ko sta

$$q = 56 \cdot 127^n - 1$$
$$r = 56 \cdot 72 \cdot 127^n - 1$$

praštevili, dajeta števili

$$a_1 = 220 \cdot 127^n q$$
$$b_1 = 4 \cdot 127^n r$$

prijateljski par.

Za $n = 1$ imamo

$$q = 56 \cdot 127 - 1 = 7111 = 13 \cdot 547$$

Ker q ni praštevilo, pri $n = 1$ ne pridemo do prijateljskega para.

Za $n = 2$ je

$$q = 56 \cdot 127^2 - 1 = 903\,223$$
$$r = 56 \cdot 72 \cdot 127^2 - 1 = 65\,032\,127$$

Da se pokazati, da sta ta q, r praštevili. Zato je par

$$a_1 = 220 \cdot 127^2 \cdot 903\,223$$
$$b_1 = 4 \cdot 127^2 \cdot 65\,032\,127$$

prijateljski.

Pitagorov prijateljski par pa ni edini, ki premore tako razcepitev (15), da so faktorji c, u, s paroma tuji, s in $u + s + 1$ pa praštevili. Takih parov je med takrat znanimi prijateljskimi pari Borho naštel vsaj 22. Iz vsakega teh parov je zato mogoče izhajati in po (17) in (18) iskati nove prijateljske pare, ko gre n po naravnih številih. Iz vsakega teh parov izhaja podobno pravilo kot zgoraj iz Pitagorovega para.

7. Sedaj je znanih okrog 1100 prijateljskih parov ([2], [8]. Od tega so približno 900 parov odkrili po letu 1945. V zadnjih dvajsetih letih si iskalci izdatneje pomagajo z računalniki.

8. Prevladuje prepričanje, da je prijateljskih števil neskončno mnogo. Dokazali pa tega še niso.

Ve pa se, da postajajo prijateljska števila zmeraj redkejša, ko se pomikamo po naraščajočih naravnih številih. Naj bo $A(x)$ število prijateljskih števil, ki ne presegajo x. Količnik $A(x)/x$ potem meri delež prijateljskih števil med števili do x. Za ta količnik je Erdös dognal, da konvergira proti nič, ko raste x proti neskončno ([5], str. 31). Od tod se tudi vidi, da postajajo prijateljska števila bolj in bolj redka. Pravimo še, da ima množica prijateljskih števil gostoto nič.

Tudi množica praštevil ima gostoto nič. Vendar so prijateljska števila dosti redkeje posejana med naravnimi števili kot praštevila. Znano je, da vrsta iz recipročnih praštevil divergira. Za vrsto iz recipročnih prijateljskih števil pa je pred kratkim Pomerance dognal, da konvergira ([9]).

LITERATURA

[1] M. M. Artjuhov, *K problemam družestvennyh čisel,* Acta Arith. **27** (1974), 281—291.

[2] W. Borho, *Befreundete Zahlen. Lebendige Zahlen,* Birkhäuser Verlag, Basel, Boston, Stuttgart 1981.

[3] W. Borho, *Eine Schranke für befreundete Zahlen mit gegebener Teileranzahl,* Math. Nachr. **63** (1974), 297—301.

[4] L. E. Dickson, *History of the Theory of Numbers,* Vol. I. Reprint. Chelsea, New York 1971.

[5] R. K. Guy, *Unsolved Problems in Number Theory,* Springer Verlag, New York, Heidelberg, Berlin 1981.

[6] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers,* Clarendon Press, Oxford 1975.

[7] H. J. Kanold, *Über befreundete Zahlen* I, II, III. Math. Nachr. **9** (1953), 243—248; **10** (1953), 99—111. Journ. reine ang. Math. **234** (1969), 207—215.

[8] E. L. Lee, J. S. Madachy, *The History and Discovery of Amicable Numbers* I, II, III. Journ. Rec. Math. 5 (1972), 77—93; 153—173; 231—249.

[9] C. Pomerance, *On the distribution of amicable numbers* I, II. Journ. reine ang. Math. **293/94** (1977), 217—222; **325** (1981), 183—188.

NOVE KNJIGE

KOZAK Jernej, Podatkovne strukture in algoritmi, Ljubljana, DMFA SRS 1986, 392 str. — (Matematika-Fizika : Zbirka univerzitetnih učbenikov in monografij ; 27). Cena 6250.— din (5000.— din).

Druga izdaja se po obliki močno razlikuje od prve. Ko jo vzamemo v roke, smo prijetno presenečeni nad ličnostjo stavka, ki se po kvaliteti približuje knjigotisku. Avtor je besedilo nadvse skrbno oblikoval na računalniško vodenem marjetičnem pisalnem stroju. Moti le znak za relacijo vsebovanosti množic, ki ga na marjetkah ni in je nadomeščen kar s črko C. Vsebina je doživela nekaj manjših sprememb in izboljšav; med njimi naj omenim le to, da so v novi izdaji vsi algoritmi izdelani do kraja in ne vsebujejo več vstavkov v naravnem jeziku. Algoritmi so zapisani v izpeljanki paskala, tako da jih je mogoče z neznatnim trudom spremeniti v programe in pognati na računalniku.

Za knjigo velja vse, kar je o njej zapisal T. Pisanski v OMF **31** (1984) 3. Zaradi njene pomembnosti za slovensko računalništvo pa naj dodam še nekaj misli.

Knjiga je — če ne štejemo uvoda in dodatka — razdeljena na dva dela. Prvi govori o podatkovnih strukturah, drugi, obsežnejši, pa o algoritmih. Podatkovne strukture so podane s t.i. algebrajsko specifikacijo, v kateri so lastnosti operacij nad strukturo definirane aksiomatično. Tak način podajanja je zelo »čist« in precizen. Pogrešamo morda le kratko opombo o polnosti, ki naj bralca prepriča, da našteti aksiomi zadoščajo za določitev rezultata poljubnega končnega zaporedja operacij.

Pri obravnavi algoritmov postavi avtor v ospredje metode reševanja problemov oz. načrtovanja algoritmov: »deli in vladaj«, požrešno metodo, dinamično programiranje, sestopanje ter »razveji in omeji«. Vsaki od metod je posvečeno eno poglavje. Tako podatkovne strukture kot metode načrtovanja algoritmov so bogato ilustrirane s številnimi zgledi, ki so zanimivi tudi sami po sebi in v njih najdemo rešitve številnih pomembnih problemov. Nekateri problemi so rešeni na več načinov in zato naletimo nanje v različnih poglavjih, npr. problem najkrajših poti, problem nahrbtnika in problem trgovskega potnika. Posebna odlika knjige so tabele z izmerjenimi povprečnimi časi teka posameznih algoritmov pri različno velikih nalogah z naključno izbranimi podatki. Na podlagi teh meritev je ocenjen vodilni člen časovne zahtevnosti, kar je zlasti zanimivo pri različnih rešitvah istega problema.

Tu in tam bi si pri razlagi in dokazih pravilnosti algoritmov želeli več jasnosti. Pri dokazovanju pravilnosti se v literaturi še ni izoblikoval slog, ki bi bil splošno sprejet kot najprimernejši. Osnovni alternativi sta formalni dokaz in neformalni dokaz. Avtor se tu nagiba bolj k drugi možnosti. Slabost prve je v tem, da so formalni dokazi količkaj bolj zapletenih algoritmov obupno dolgi in nepregledni; slabost druge pa, da nas »dokaz« o pravilnosti algoritma pogosto ne prepriča nič bolj kot algoritem sam. Morda je, kot običajno, najboljša srednja pot — neformalni dokaz, ki pa je dosledno opremljen z vsemi netrivialnimi sestavinami formalnega dokaza, kot so invariante zank ter pogoji na ključnih mestih v algoritmu. Sicer pa bodimo optimisti in upajmo, da bodo v nekaj letih sistemi za avtomatično dokazovanje izrekov ob navedbi pravilnih invariant sposobni rutinsko preverjati pravilnost nekaj strani dolgih algoritmov.

Vsakemu poglavju so dodane številne naloge, ki širijo in dopolnjujejo obravnavano snov. V dodatku najdemo tudi rešitve nekaterih nalog.

Knjiga je bogata zakladnica algoritmov in podatkovnih struktur in ji ne moremo očitati nobenega spregleda. Avtorjev glavni cilj je privzgojiti bralcu algoritmično mišljenje, ga naučiti sistematičnosti pri načrtovanju algoritmov in ga navaditi na kritično vrednotenje in primerjanje algoritmov glede na njihovo zahtevnost. Ta cilj je dosežen in avtorju lahko priznamo, da je opravil veliko delo.

Omenim naj še, da je imel avtor pri iskanju strokovnih izrazov srečno roko in je obogatil slovensko izrazoslovje z nekaj dobro izbranimi izrazi.

Knjiga bo dobrodošla vsakomur, ki se kakorkoli srečuje z računalnikom. Prva izdaja je bila tako rekoč razgrabljena in tudi drugi lahko napovemo podobno usodo.

Marko Petkovšek

KUBIČNE KRIVULJE

IVAN VIDAV

Math. Subj. Class. (1980) 10 B 10, 14 H, 14 K 07

Članek vsebuje elementaren opis kubičnih krivulj. Opredeljene so eliptične krivulje in grupna struktura na teh krivuljah. Obravnava teče v obsegu $\mathbb{R}$, deloma v obsegu $\mathbf{Q}$.

CUBIC CURVES

This article contains an elementary exposition of the theory of cubic curves. Elliptic curves are defined. The group structure on these curves and on the set of their rational points is described.

1. Pregled kubičnih krivulj. Eliptične krivulje

Algebraična krivulja je krivulja z enačbo

$$f(x, y) = 0 \tag{1}$$

kjer je $f(x, y)$ poljuben polinom spremenljivk x in y. Če je npr. f druge stopnje, je (1) enačba stožernice. Kubično krivuljo dobimo, če vzamemo za f polinom tretje stopnje, torej

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Ky + L = 0 \tag{2}$$

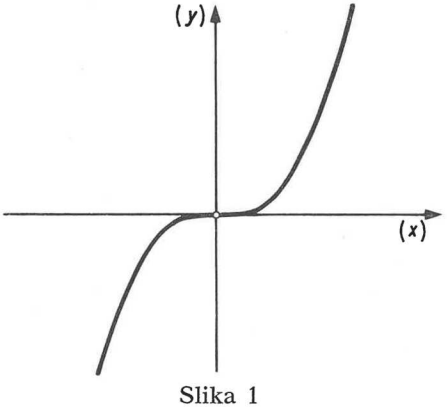
Koeficientov $A, B, \ldots, L$ je kar deset. So poljubna dana števila, vendar A, B, C in D ne smejo biti vsi enaki 0.

Preprost primer kubične krivulje je kubična parabola z enačbo $y = x^3$. Srečamo jo pri risanju elementarne funkcije $f(x) = x^3$. Zanimiva je zato, ker je njen odvod $f'(x) = 3x^2$ v izhodišču $x = 0$ enak 0, pa kljub temu funkcija tam nima lokalnega ekstrema. Izhodišče je za kubično parabolo prevojna točka (obračaj). Tangenta je tu kar abscisna os, krivulja pa leži na obeh straneh tangente (Sl. 1). V splošnem imenujemo prevoj tako točko na krivulji $y = f(x)$, kjer je drugi odvod $f''(x)$ enak 0.

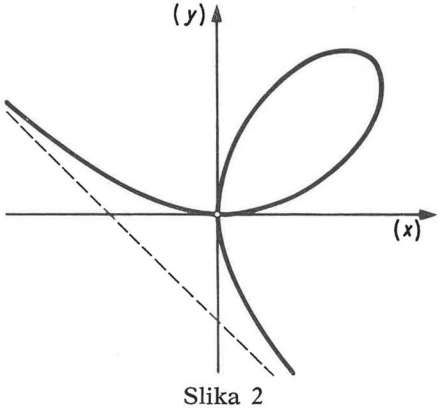
Nadaljnji primer kubične krivulje je Kartezijev list, ki ima enačbo

$$x^3 + y^3 - 3axy = 0, \quad a > 0 \tag{3}$$

Zanj je značilno, da napravi zanko. Izhodišče je dvojna točka (Sl. 2).



Slika 1



Slika 2

V teoriji eliptičnih funkcij in integralov pa srečamo krivulje z enačbo

$$y^2 = 4x^3 - g_2x - g_3 \tag{4}$$

kjer sta g_2 in g_3 konstanti. Tudi to so kubične krivulje.

Polinom $f(x, y)$ na levi v (2) je lahko razcepen ali nerazcepen. Če je razcepen, razpade na produkt najmanj dveh faktorjev $f(x, y) = g(x, y)\ h(x, y)$, od katerih je eden, npr. g, linearen, h pa kvadraten. Iz enačbe $f(x, y) = 0$ dobimo dve enačbi $g(x, y) = 0$ in $h(x, y) = 0$. Prva pomeni premico, druga stožernico. Tudi polinom h se da včasih razstaviti v dva linearna faktorja, polinom f pa tedaj razpade na tri linearne faktorje. Kubična krivulja torej lahko razpade na premico in stožernico ali na tri premice.

Razcepnost polinoma je odvisna od obsega, v katerem obravnavamo enačbo. Velja pa tole: Če je polinom tretje stopnje z realnimi koeficienti razcepen v obsegu kompleksnih števil, razpade vsaj na dva faktorja tudi v obsegu $\mathbb{R}$.

Odslej bomo privzeli, da je polinom f na levi v (2) nerazcepen. Enačba pomeni v tem primeru pravo kubično krivuljo.

Po navadi vzamemo v ravnini pravokoten koordinatni sistem. Kubično krivuljo sestavljajo vse točke, katerih koordinate (x, y) zadoščajo enačbi (2). Koordinati x in y sta realni števili in prav tako so realni vsi koeficienti od A do L. Delamo torej v obsegu $\mathbb{R}$. V teoriji eliptičnih funkcij pa obravnavamo enačbo (4) v obsegu C. Zanimajo nas poljubni kompleksni pari (z, w), ki ustrezajo enačbi

$$w^2 = 4z^3 - g_2z - g_3 \tag{4*}$$

Tudi koeficienta g_2 in g_3 sta lahko kompleksna. Še vedno imenujemo množico vseh rešitev (z, w) krivulja, čeprav v dobesednem smislu ni krivulja. Pišimo namreč $z = x + iy$, $w = u + iv$. Par (z, w) določa realno četverko (x, y, u, v), to pa je točka v štirirazsežnem evklidskem prostoru. Ker si lahko $z = x + iy$ poljubno izberemo in potem izračunamo $w = u + iv$ iz enačbe (4*), je množica vseh rešitev (x, y, u, v) neka ploskev v štirirazsežnem prostoru.

Včasih pa so koeficienti v enačbi (1) racionalna števila in zanimajo nas rešitve (x, y), kjer sta x in y racionalna. Tako točko imenujemo racionalna točka na krivulji (1). Za zgled vzemimo enačbo

$$x^3 + y^3 = 1 \tag{5}$$

Naj bo (x, y) racionalna točka na tej krivulji. Izrazimo števili x in y v obliki ulomkov s skupnim imenovalcem $x = a/c$, $y = b/c$, kjer so a, b, c cela števila in seveda $c \neq 0$. Ker velja (5), je med a, b, c zveza

$$a^3 + b^3 = c^3 \tag{6}$$

Fermatova domneva je za tretje potence pravilna: V vsaki celoštevilski rešitvi enačbe (6) je eno izmed števil a, b, c enako 0. Ker $c \neq 0$, je zato $a = 0$ ali $b = 0$. V prvem primeru je $x = 0$, $y = 1$, v drugem pa $x = 1$ in $y = 0$. Torej ležita na krivulji (5) samo dve racionalni točki (0, 1) in (1, 0).

Vzemimo točko (x, y) na algebraični krivulji (1) in postavimo v njej tangento. Smerni koeficient tangente y' dobimo z odvajanjem enačbe (1), torej iz enačbe $f_x + y'f_y = 0$. Tu pomenita $f_x = \partial f/\partial x$ in $f_y = \partial f/\partial y$ parcialna odvoda. Zaznamujmo z (X, Y) koordinati poljubne točke na tangenti. Potem je

$$(X - x)f_x + (Y - y)f_y = 0 \tag{7}$$

enačba tangente v točki (x, y). Odvoda f_x in f_y vzamemo seveda v dotikališču. Tangenta je natanko določena v vsaki točki krivulje, kjer nista oba odvoda f_x in f_y enaka 0. Če je npr. $f_y = 0$ in $f_x \neq 0$, se enačba (7) glasi $X - x = 0$. Tangenta je pravokotna na abscisno os.

Tako točko algebraične krivulje, kjer sta oba odvoda $f_x = f_y = 0$, imenujemo *singularna točka*. Za Kartezijev list je npr. izhodišče $(0, 0)$ singularna točka. V tem primeru je $f(x, y) = x^3 + y^3 - 3axy$ in od tod

$$f_x(x, y) = 3(x^2 - ay), \quad f_y(x, y) = 3(y^2 - ax)$$

Res je $f_x(0, 0) = f_y(0, 0) = 0$. Izhodišče je dvojna točka, skoznjo gre Kartezijev list dvakrat. Tangenti sta v dvojni točki dve, ena je abscisna os, druga ordinatna os (Sl. 2).

Kako se vede kubična krivulja, ko se točka na njej oddaljuje v neskončnost? Da to spoznamo, preselimo obravnavo v projektivno ravnino. Projektivno ravnino dobimo tako, da dodamo evklidski ravnini točke v neskončnosti in premico v neskončnosti. Tudi točkam v neskončnosti priredimo koordinate. V ta namen uvedemo homogene koordinate. Absciso x in ordinato y zapišemo v obliki kvocientov $x = x_1/x_3$ in $y = x_2/x_3$. Števila x_1, x_2, x_3 imenujemo homogene koordinate točke, ki ima običajni koordinati x in y. Pri tem mora biti $x_3 \neq 0$. Točka je seveda odvisna le od razmerja koordinat x_1, x_2, x_3. Če pa je $x_3 = 0$, pomeni trojka $(x_1, x_2, 0)$ homogene koordinate točke v neskončnosti. Vsaka trojka (x_1, x_2, x_3) določa torej neko točko v projektivni ravnini. Edina izjema je trojka $(0, 0, 0)$, ki ne določa nobene točke. Ker imajo vse točke v neskončnosti koordinato x_3 enako 0, je $x_3 = 0$ enačba premice v neskončnosti.

Enačbo kubične krivulje v homogenih koordinatah dobimo tako, da vstavimo $x = x_1/x_3$ in $y = x_2/x_3$ v (2) in nato pomnožimo enačbo z x_3^3. Torej

$$Ax_1^3 + Bx_1^2x_2 + Cx_1x_2^2 + Dx_2^3 + Ex_1^2x_3 + Fx_1x_2x_3 + Gx_2^2x_3 + Hx_1x_3^2 + Kx_2x_3^2 + Lx_3^3 = 0 \qquad (2^*)$$

Na levi stoji homogen polinom tretje stopnje spremenljivk x_1, x_2, x_3, ki ga bomo označili s $\Phi(x_1, x_2, x_3)$. Če nas zanimajo točke v neskončnosti, ki leže na kubični krivulji, vstavimo $x_3 = 0$ v enačbo (2*). Dobimo

$$Ax_1^3 + Bx_1^2x_2 + Cx_1x_2^2 + Dx_2^3 = 0$$

Lega točke v neskončnosti $(x_1, x_2, 0)$ je odvisna samo od kvocienta x_1/x_2. Zgornja enačba pa je enačba tretje stopnje za x_1/x_2. Vsaj en njen koren je realen, lahko vsi trije. Zato ima kubična krivulja vsaj eno realno točko v neskončnosti, največ pa tri. Zgled: Enačba krivulje (5) je v homogenih koordinatah $x_1^3 + x_2^3 = x_3^3$. Če vstavimo $x_3 = 0$, dobimo enačbo $x_1^3 + x_2^3 = 0$, ki nam da za kvocient x_1/x_2 eno samo realno vrednost -1. Krivulja (5) ima torej eno samo realno točko v neskončnosti. Ker je razmerje $x_1/x_2 = -1$ racionalno število, štejemo točko v neskončnosti za racionalno.

V homogenih koordinatah se enačba tangente na krivuljo glasi

$$X_1\Phi_{x_1} + X_2\Phi_{x_2} + X_3\Phi_{x_3} = 0 \qquad (8)$$

Tu so (X_1, X_2, X_3) homogene koordinate poljubne točke na tangenti, $\Phi_{x_1} = \partial\Phi/\partial x_1$, $\Phi_{x_2} = \partial\Phi/\partial x_2$, $\Phi_{x_3} = \partial\Phi/\partial x_3$ so parcialni odvodi, ki jih je treba vzeti v dotikališču (x_1, x_2, x_3). Če je $x_3 = 0$, leži dotikališče v neskončnosti. Pripa-

dajočo tangento imenujemo *asimptota krivulje*. Za zgled vzemimo spet Kartezijev list, pri katerem je $\Phi = x_1^3 + x_2^3 - 3ax_1x_2x_3$ in

$$\Phi_{x_1} = 3(x_1^2 - ax_2x_3), \quad \Phi_{x_2} = 3(x_2^2 - ax_1x_3), \quad \Phi_{x_3} = -3ax_1x_2$$

Kartezijev list seče premico v neskončnosti v točki s koordinatami $x_1 = 1$, $x_2 = -1$, $x_3 = 0$. Enačba (8) se v tej točki glasi $3X_1 + 3X_2 + 3aX_3 = 0$. Če jo prepišemo v običajne koordinate, tako da postavimo $x = X_1/X_3$, $y = X_2/X_3$, dobimo enačbo asimptote na Kartezijev list

$$x + y + a = 0$$

Po enačbi (8) je tangenta določena v vsaki točki, končni ali neskončni, kjer niso vri trije parcialni odvodi Φ_{x_1}, Φ_{x_2}, Φ_{x_3} enaki nič. Taka točka, kjer je $\Phi_{x_1} = \Phi_{x_2} = \Phi_{x_3} = 0$, pa je singularna za krivuljo. Singularna je seveda lahko tudi točka v neskončnosti.

Vsaka razcepna kubična krivulja ima vsaj eno realno ali kompleksno singularno točko. Če razpade npr. na premico in stožernico, je presečišče premice s stožernico singularna točka.

Ni težko videti, da ima nerazcepna kubična krivulja kvečjemu eno singularno točko in da je singularna točka realna, če so koeficienti v enačbi realni.

Definicija. Kubična krivulja, ki nima singularne točke (niti v končnosti niti v neskončnosti), se imenuje eliptična krivulja.

Zgled za eliptično krivuljo je (5). Pripadajoči homogeni polinom je tu $\Phi = x_1^3 + x_2^3 - x_3^3$. Vsi parcialni odvodi $\Phi_{x_1} = 3x_1^2$, $\Phi_{x_2} = 3x_2^2$, $\Phi_{x_3} = -3x_3^2$ so hkrati enaki nič le pri $x_1 = x_2 = x_3 = 0$. Trojka $(0, 0, 0)$ pa ne določa točke v projektivni ravnini. Torej (5) nima singularne točke in je eliptična krivulja.

Na kubični paraboli $y = x^3$ ni nobene singularne točke v končnosti. Račun pa pokaže, da seče ta krvulja premico v neskončnosti v singularni točki. Zato kubična parabola ni eliptična krivulja.

Imejmo poljubno premico z enačbo

$$ax + by + c = 0 \tag{9}$$

Poiščimo presečišča te premice s krivuljo (2). Pri tem privzemimo, da je (2) nerazcepna krivulja, ki ne razpade v premico in stožernico ali v tri premice. Koordinate presečišč poiščemo tako, da iz (9) izračunamo npr. y in to vstavimo v (2). Dobimo za x enačbo tretje stopnje. Zato seče premica kubično krivuljo v splošnem v treh točkah. Seveda je lahko realno eno samo presečišče, drugi dve sta konjugirano kompleksni. Včasih je enačba za x nižje stopnje. V tem primeru moramo račun ponoviti v homogenih koordinatah. Presečišče premice (9) s kubično krivuljo je namreč lahko tudi točka v neskončnosti.

Enačba tretje stopnje, ki jo dobimo za absciso presečišča, more imeti večkratne korene. Če je npr. x_1 dvakratni koren in y_1 pripadajoča ordinata, je premica (9) tangenta na kubično krivuljo v točki (x_1, y_1). Dotikališče (x_1, y_1) šteje za dve presečišči. Če pa ima enačba tretje stopnje en sam trojni koren, imenujemo točko (x_1, y_1) prevoj. Prevoj šteje za tri presečišča. Premica (9) je tudi v tem primeru tangenta na krivuljo, vendar se v prevojni točki tesneje prilega krivulji kakor v običajni točki. Tangenta v običajni točki seče kubično krivuljo še v eni točki. Tangenta v prevojni točki pa nima s kubično krivuljo nobene druge skupne točke.

Na stožernici ni prevojnih točk. Že v začetku pa smo videli, da je izhodišče prevojna točka na kubični paraboli $y = x^3$. Kako je s prevojnimi točkami na poljubni kubični krivulji? Če iščemo absciso (ali ordinato) prevojne točke na krivulji (2), nas račun privede na enačbo devete stopnje (glej [4], str. 80). Torej je lahko na kubični krivulji devet prevojnih točk. Vendar pa niso vse realne. Toda enačba devete stopnje z realnimi koeficienti ima vselej vsaj en realen koren. Zato je na vsaki kubični krivulji najmanj ena realna prevojna točka. Če leži na krivulji singularna točka, je ne štejemo med prevojne točke.

Vemo, da lahko preslikamo s primerno izbrano projektivno transformacijo katerokoli točko projektivne ravnine v katerokoli drugo točko. Isto velja za premice (glej [3], str. 126—130). Pa naj bo P realna prevojna točka na krivulji (2) in premica p tangenta v P. S projektivno transformacijo preslikajmo tangento p v premico $x_3 = 0$, tj. premico v neskončnosti, točko P pa v točko s homogenimi koordinatami $(0, 1, 0)$. V tej točki ordinatna os seče premico v neskončnosti. Preslikana krivulja ima enačbo

$$Ax^3 + Ex^2 + Fxy + Gy^2 + Hx + Ky + L = 0 \qquad (*)$$

Ker prevoj (0, 1, 0) ni singularna točka, je koeficient $G \neq 0$; to pokaže kratek račun. Z afino transformacijo zdaj brez težave prevedemo krivuljo (*) v krivuljo s preprosto enačbo (glej [4], str. 81)

$$y^2 = x^3 - Ax - B \qquad (10)$$

ki je podobna enačbi (4). Ker sodijo afine transformacije med projektivne, dobimo torej vse kubične krivulje tako, da preslikamo krivulje (10) s projektivnimi transformacijami. Zato je dovolj, če proučimo krivulje (10).

Polinom $x^3 - Ax - B$ na desni enačbe (10) ima lahko same med seboj različne ničle ali tudi večkratne ničle. To je odvisno od njegove diskriminante, tj. od izraza $D = 4A^3 - 27B^2$. Če je $D \neq 0$, so vse tri ničle med seboj različne, če je $D = 0$, sta vsaj dve enaki. Oglejmo si najprej primer $D \neq 0$. Dve možnosti sta: Vse ničle x_1, x_2, x_3, so realne ali je le ena realna, npr. x_1, drugi dve pa konjugirano kompleksni: $x_3 = \bar{x}_2$.

V prvem primeru uredimo ničle po velikosti, tako da je $x_1 < x_2 < x_3$. Enačba (10) se glasi

$$y^2 = (x - x_1)(x - x_2)(x - x_3) \qquad (Ia)$$

Izraz na desni je pozitiven, če leži x med x_1 in x_2 ali pa, če je $x > x_3$. Krivulja sestoji zato iz dveh delov. Tisti del, ki leži med x_1 in x_2, je sklenjen, drugi del, kjer je $x > x_3$, se razteza v neskončnost (Sl. 3). Abscisna os je simetrala krivulje. Povsod obstaja tangenta. V točkah A_1, A_2, A_3, kjer krivulja seče os (x), je tangenta pravokotna na to os.

Pri konjugirano kompleksnih ničlah imamo enačbo

$$y^2 = (x - x_1)(x - x_2)(x - \bar{x}_2) \qquad (Ib)$$

Produkt zadnjih dveh faktorjev na desni je pozitiven za vsak realen x. Zato je desna stran pozitivna, če je $x > x_1$. Krivulja sestoji iz enega samega dela (Sl. 4).

Krivulji (Ia) in (Ib) nimata singularnih točk in sta zato eliptični krivulji.

Pripomba. Prepričati se moramo, da tudi v neskončnosti ni singularnosti. Edina točka v neskončnosti, ki leži na krivulji (10), je (0, 1, 0,) in je prevoj.

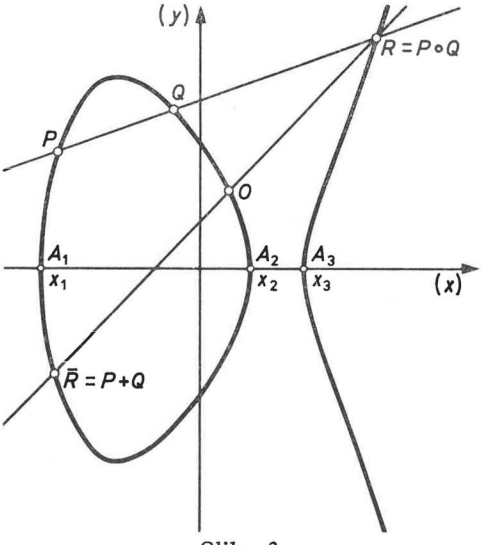
Tangenta v tej točki pa je premica v neskončnosti $x_3 = 0$. Zato ta točka za krivuljo (10) ni singularna.

Če ima polinom na desni v (10) večkratne ničle, so vse realne. Oglejmo si najprej primer, ko je ena ničla dvojna. Tudi zdaj sta dve možnosti: Dvojna je manjša ničla ali dvojna je večja. V prvem primeru imamo enačbo

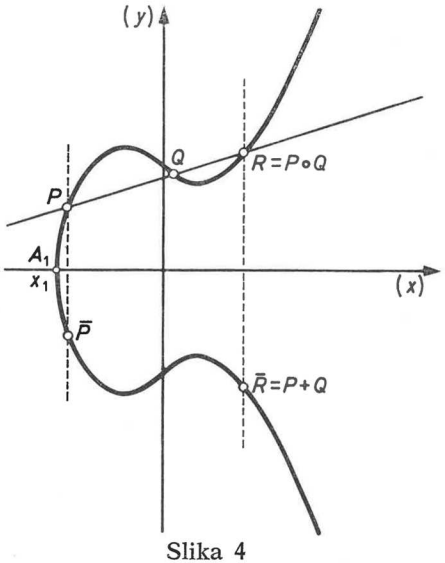
$$y^2 = (x - x_1)^2 (x - x_2), \quad x_1 < x_2 \tag{IIa}$$

V drugem pa

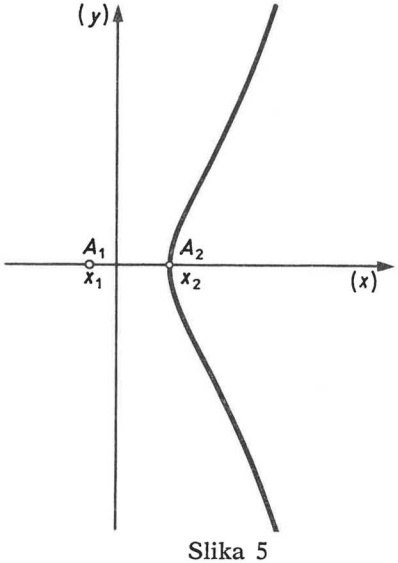
$$y^2 = (x - x_1) (x - x_2)^2, \quad x_1 < x_2 \tag{IIb}$$



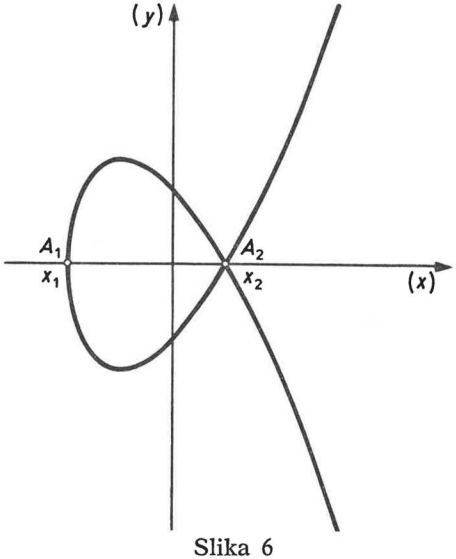
Slika 3



Slika 4



Slika 5



Slika 6

Mislimo si lahko, da (IIa) nastane iz (Ia) tako, da zlezeta skupaj ničli x_1 in x_2, (IIb) pa tako, da zlezeta skupaj x_2 *in* x_3. V prvem primeru se sklenjeni del krivulje stisne v eno samo točko. Graf funkcije (IIa) sestoji iz točke $x = x_1$ na abscisni osi in iz dela, ki se razteza v neskončnost in kjer je $x > x_2$. Izolirana točka $(x_1, 0)$ ni regularna, zato je (IIa) kubična krivulja s singularnostjo (Sl. 5). V drugem primeru pa se oba dela krivulje združita v točki x_2 na abscisni osi. Krivulja napravi zanko (Sl. 6). Točka $(x_2, 0)$ je dvojna. Skoznjo gresta dve veji krivulje, ki sta grafa funkcij

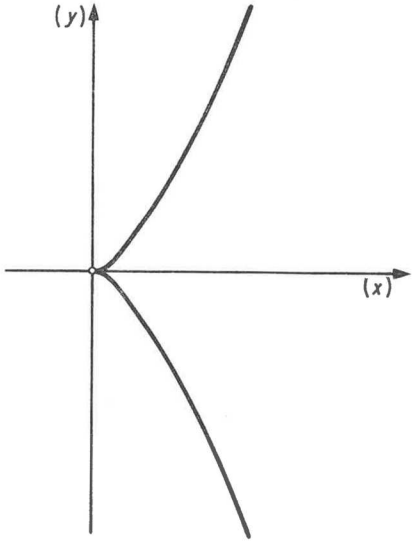
$$f_1(x) = (x - x_2)\sqrt{x - x_1} \quad \text{in} \quad f_2(x) = -(x - x_2)\sqrt{x - x_1}$$

Obakrat vzamemo na desni pozitivni koren. Odvoda teh funkcij sta v točki $x = x_2$ končna in med seboj različna: $f_1'(x_2) = \sqrt{x_2 - x_1}$ in $f_2'(x_2) = -\sqrt{x_2 - x_1}$. Kubična krivulja ima v dvojni točki dve tangenti, na vsako vejo po eno. Dvojna točka je seveda singularna. Torej (IIa) in (IIb) nista eliptični krivulji.

Zadnja možnost je ta, da so vse ničle x_1, x_2, x_3 med seboj enake. Ker je njihova vsota enaka 0, saj v polinomu $x^3 - Ax - B$ ni člena z x^2, so vse tri enake 0. V tem primeru se enačba glasi

$$y^2 = x^3 \qquad \text{(III)}$$

Krivulja (Sl. 7) ima v izhodišču ost. Izhodišče je seveda singularna točka.



Slika 7

Tako smo pregledali vse možne kubične krivulje. Ugotovili smo, da pomeni enačba (10) eliptično krivuljo, če je diskriminanta $D \neq 0$.

V čem se razlikujejo eliptične krivulje od kubičnih krivulj s singularnostjo? Postavimo $x = x_2 + t^2$ v enačbo (IIa). Dobimo $y^2 = t^2(t^2 + x_2 - x_1)^2$ in od tod

$$x = t^2 + x_2, \quad y = t(t^2 + x_2 - x_1) \qquad \text{(11)}$$

To sta parametrični enačbi krivulje (IIa). Ko zavzame parameter t vse realne vrednosti, opiše točka (x, y), ki jo dobimo iz (11), natanko enkrat vso krivuljo (IIa), razen izolirane točke. Enak parametrični enačbi ima tudi krivulja (IIb), saj smemo v njej zamenjati x_1 in x_2. Parametrični enačbi krivulje (III) pa sta $x = t^2$, $y = t^3$. Značilno za kubične krivulje s singularno točko je to, da ima vsaka taka krivulja parametrični enačbi, kjer sta x in y racionalni funkciji parametra t. Pri enačbah (IIa), (IIb) in (III) sta x in y celo polinoma. Eliptične krivulje pa nimajo parametrične enačbe, kjer bi bila x in y racionalni funkciji parametra. Premorejo pa tudi te krivulje parametrične enačbe. Koordinati x in y se izražata z eliptičnimi funkcijami parametra. Eliptične funkcije so, podobno kakor racionalne, povsod enolične funkcije.

2. Grupna struktura na eliptični krivulji

Naj bo dana nerazcepna kubčna krivulja z enačbo (2). Označimo z E množico vseh njenih točk. K E štejemo tudi točke v neskončnosti. V množico E lahko uvedemo binarno operacijo takole: Naj bosta P in Q poljubna elementa iz E, tedaj točki na krivulji (2). Zveznica PQ seče krivuljo v treh točkah, poleg P in Q še v tretji točki R (Sl. 3). Kadar je premica PQ tangenta na krivuljo v točki P, šteje dotikališče P za dve presečišči in je $R = P$. Podobno je $R = Q$, če je sekanta PQ tangenta v točki Q. Kadar pa točki P in Q sovpadata, je treba vzeti za sekanto PQ tangento v točki P. V vseh primerih je tretje presečišče R natanko določeno s P in Q. Zato imenujemo R kompozitum točk P in Q in pišemo $R = P \circ Q$.

Pripomba. Iz množice točk na kubični krivulji, ki ni eliptična, je treba izločiti singularno točko S. Singularna točka S šteje za dve točki na krivulji. Če je npr. $P = Q = S$, zveznica PQ ni določena, saj v singularni točki S tudi tangenta ni določena. Vzemimo zdaj poljubni od S različni točki P, $Q \in E$. Sekanta PQ ne gre skozi S. V nasprotnem primeru bi imela premica PQ štiri presečišča s krivuljo, namreč poleg P in Q še S, ki šteje za dve točki na krivulji. To pa ni mogoče. Torej je naša binarna operacija določena na množici $E - \{S\} = E_{ns}$.

Nastane vprašanje, ali je množica točk E na eliptični krivulji oz, množica E_{ns} na krivulji s singularnostjo, grupa za to operacijo. Odgovor je nikalen. Za to operacijo ni nevtralnega elementa. Nevtralni element bi bila namreč taka točka $N \in E$, da bi veljalo $P \circ N = P$ za vsako točko $P \in E$. Pa denimo, da bi taka točka N obstajala. Potegnimo skozi N premico, ki seče krivuljo v treh točkah, tedaj poleg N še v P in Q. Po naši definiciji je kompozitum $P \circ N = Q$. Ker $Q \neq P$, točka N ni nevtralni element za operacijo.

Do grupne operacije pridemo takole: Izberimo si na krivulji poljubno točko O. (Če je na krivulji singularna točka S, naj bo $S \neq O$.) Točko $R = P \circ Q$ zvežimo z O, zveznica OR naj seče krivuljo tretjič v točki $\overline{R}$. Torej $\overline{R} = R \circ O$. Točko $\overline{R}$ proglasimo za vsoto točk P in Q in pišimo $\overline{R} = P + Q$ (sl. 3). Tako smo dobili v množici E oz. v E_{ns} novo binarno operacijo, seštevanje. Neposredno iz definicije je razvidno, da sta obe operaciji komutativni: $P \circ Q = Q \circ P$ in prav tako $P + Q = Q + P$. Med seboj sta povezani takole: $P + Q = (P \circ Q) \circ O$.

Množica E oz. E_{ns} je za seštevanje grupa, če velja asociativnostni zakon, obstaja nevtralni element in če ima vsak element P nasprotni element $\overline{P}$. Nevtralni element je točka O. Zvežimo namreč poljubno točko P z O. Zveznica OP seče krivuljo tretjič v točki $R = P \circ O$. Da dobimo vsoto $P + O$, moramo R zvezati z O in poiskati tretje presečišče zveznice z E. To pa je ravno točka P. Torej $P + O = P$ in O je nevtralni element za seštevanje, ki ga po navadi imenujemo element nič.

Ugodno je vzeti za O eno od prevojnih točk na krivulji. To bomo odslej tudi storili. Spet naj bo P poljubna točka na E oz. E_{ns}. Tretje presečišče zveznice OP s krivuljo imenujmo $\overline{P}$, tedaj $\overline{P} = P \circ O$. Poiščimo vsoto $P + \overline{P}$. Premica $P\overline{P}$ seveda seče krivuljo tretjič v točki O, torej $P \circ \overline{P} = O$. Po definiciji vsote je $P + \overline{P} = (P \circ \overline{P}) \circ O = O \circ O$. Za zveznico OO je treba vzeti tangento v O.

Ker je O prevojna točka, šteje dotikališče O za tri presečišča. Zato je $O \circ O = O$ in od tod $P + \overline{P} = O$. Torej je $\overline{P}$ nasprotni element od P. Dokazati bi bilo treba še zakon asociativnosti za seštevanje. Dokaz pa je precej zapleten in ga zato opustimo.

Za zgled vzemimo kubično parabolo $y = x^3$. Naj bosta $P = (x_1, y_1)$ in $Q = (x_2, y_2)$ poljubni točki na njej. Potem je $y_1 = x_1^3$ in $y_2 = x_2^3$. Smerni koeficient sekante PQ je enak $(y_2 - y_1)/(x_2 - x_1) = x_1^2 + x_1 x_2 + x_2^2$, enačba sekante pa

$$y = x_1^3 + (x_1^2 + x_1 x_2 + x_2^2)(x - x_1)$$

Abscise presečišč s krivuljo $y = x^3$ dobimo iz enačbe

$$x^3 - (x_1^2 + x_1 x_2 + x_2^2)\, x + x_1 x_2 (x_1 + x_2) = 0$$

Dva korena te enačbe sta x_1 in x_2. Ker v njej ni člena z x^2, je vsota vseh treh korenov enaka 0. Zato je tretji koren $x_3 = -(x_1 + x_2)$. Točka $R = P \circ Q$ ima potemtakem koordinati $x_3 = -(x_1 + x_2)$, $y_3 = -(x_1 + x_2)^3$. Izhodišče je prevojna točka na kubični paraboli. Vzemimo izhodišče za točko 0. Če poljubno točko $T = (x, y)$ na krivulji zvežemo z izhodiščem, seče zveznica krivuljo tretjič v simetrično ležeči točki glede na izhodišče, tedaj v točki $\overline{T} = (-x, -y)$. Od tod sledi, da ima točka $\overline{R} = P + Q$ absciso $x_1 + x_2$. Na kubični paraboli $y = x^3$ je lega vsake točke določena z absciso. Absciso vsote $P + Q = \overline{R}$ dobimo preprosto tako, da seštejemo abscisi x_1 in x_2 točk P in Q, ki sta sumanda. To pa pomeni, da je grupa točk na kubični paraboli izomorfna aditivni grupi realnih števil. (Točka v neskončnosti je za kubično parabolo singularna in jo zato izločimo iz množice točk.)

Več dela je pri računanju koordinat točke $\overline{R} = P + Q$ na poljubni kubični krivulji. Račun se precej poenostavi, če vzamemo enačbo v obliki (10). Naj bo to eliptična krivulja. Njena točka v neskončnosti $(0, 1, 0)$ je prevoj, ki naj bo točka O. Ker je O presečišče ordinatne osi s premico v neskončnosti, so premice skozi O vzporednice z ordinatno osjo. Izjema je seveda premica v neskončnosti, ki pa ne sodi v evklidsko ravnino. Točki $R = P \circ Q$ in $\overline{R} = P + Q$ ležita simetrično glede na abscisno os (sl. 4). Zveznica $R\overline{R}$ gre namreč skozi O in je zato vzporedna z ordinatno osjo, abscisna os pa je simetrala krivulje (10). Če je $P = (x, y)$ poljubna končna točka na E, je simetrična točka $\overline{P} = (x, -y)$ nasprotni element od P. Res je zveznica $P\overline{P}$ vzporedna z osjo (y) in gre zato skozi O (sl. 4). Od tod sledi $P + \overline{P} = O$.

Naj imata $P, Q \in E$ koordinate $P = (x_1, y_1)$ in $Q = (x_2, y_2)$. Absciso x_3 točke $\overline{R} = P + Q$ izračunamo po formuli

$$x_3 = (y_2 - y_1)^2/(x_2 - x_1)^2 - x_1 - x_2 \qquad (12)$$

Ordinato y_3 pa dobimo iz enačbe premice PQ. Formula (12) velja tedaj, ko sta P in Q končni točki in $x_1 \neq x_2$. Če je $x_1 = x_2$ in $P \neq Q$, ležita P in Q simetrično glede na os (x). V tem primeru je $Q = \overline{P}$ nasprotni element od P in $P + Q = P + \overline{P} = O$, kakor smo videli. Če pa P in Q sovpadata, nadomestimo v formuli (12) smerni koeficient sekante $(y_2 - y_1)/(x_2 - x_1)$ s smernim koeficientom tangente v točki P.

Doslej smo obravnavali krivulje nad obsegom $\mathbb{R}$. Nič drugače ni nad obsegom C. Množica vseh kompleksnih parov (z, w), ki zadoščajo enačbi (4*) — tej množici je treba dodati točko $(0, 1, 0)$ v neskončnosti — je grupa za seštevanje. Absciso in ordinato točke $P + Q$ izračunamo po istih formulah kakor v realnem primeru.

Kako pa je, če se omejimo na obseg racionalnih števil? Tedaj po navadi privzamemo, da so koeficienti v enačbi (2) cela števila. Množico vseh racionalnih točk na krivulji (2) označimo z $E(Q)$. Če sta P in Q racionalni točki, ima premica PQ enačbo z racionalnimi koeficienti. Ker so tudi v enačbi (2) racionalni koeficienti, dobimo za absciso presečišč enačbo tretje stopnje z racionalnimi koeficienti. Ta enačba ima dva racionalna korena, namreč abscisi točk P in Q. Zato je tudi tretji koren racionalen. To pomeni, da je točka $R = P \circ Q$ racionalna. Za nevtralni element O vzamemo racionalno točko. Potem je vsota $P + Q = (P \circ Q) \circ O$ racionalnih točk P in Q racionalna točka. Isto velja za točko $\overline{P}$, ki je nasprotni element od P. Zato tudi množica $E(Q)$ oz. $E_{ns}(Q)$ racionalnih točk na kubični krivulji sestavlja za seštevanje grupo.

Kakšna je lahko množica racionalnih točk, ki leže na algebraični krivulji z racionalnimi koeficienti? Imejmo najprej stožernico. Če je na njej vsaj ena racionalna točka, je takih točk neskončno. Res, naj bo $T_0 = (x_0, y_0)$ racionalna točka na stožernici. Vsaka premica skozi T_0 z racionalnim smernim koeficientom seče stožernico drugič v racionalni točki. Za absciso (oz. ordinato) presečišča dobimo namreč kvadratno enačbo z racionalnimi koeficienti, ki ima racionalen koren x_0 (oz. y_0). Potem je tudi drugi koren racionalen. Seveda se lahko zgodi, da na stožernici ni nobene racionalne točke, čeprav so vsi koeficienti v njeni enačbi racionalni. Zgled za to je krožnica $x^2 + y^2 = 3$.

Pri kubičnih krivuljah je stvar z racionalnimi točkami bolj zapletena. Videli smo npr., da so na krivulji $x^3 + y^3 = 1$ natanko tri racionalne točke, če štejemo zraven tudi točko v neskončnosti. Podobno kot stožernice pa se vedejo kubične krivulje s singularnostjo. Na vsaki taki kubični krivulji, ki ima enačbo z racionalnimi koeficienti, leži nešteto racionalnih točk. Pokazati se da najprej, da je singularna točka S racionalna. Ker šteje S za dve točki krivulje, seče vsaka premica, ki gre skozi S, kubično krivuljo samo še v eni točki. In če ima ta premica racionalen smerni koeficient, sta koordinati drugega presečišča racionalni. Torej je res racionalnih točk neskončno.

Pri eliptičnih krivuljah pa imamo tele možnosti:

a) racionalnih točk ni. Zgled za to je krivulja $x^3 + 2y^3 = 7$;

b) racionalnih točk je končno mnogo, kakor na krivulji $x^3 + y^3 = 1$;

c) racionalnih točk je neskončno.

Naj ima eliptična krivulja (10) cele koeficiente. Na njej leži točka v neskončnosti $(0, 1, 0)$, ki ima celoštevilske homogene koordinate in jo zato štejemo med racionalne točke. Množica racionalnih točk $E(Q)$ na krivulji (10) ni prazna, za seštevanje pa je Abelova grupa. V primeru (b) je $E(Q)$ končna grupa. Koliko elementov ima lahko ta grupa na posameznih eliptičnih krivuljah? Izkaže se, da ni veliko možnosti. B. Mazur je namreč l. 1976 dokazal, da je v grupi $E(Q)$, če je končna, vselej manj kot 17 elementov. Če smo torej našli na kakšni eliptični krivulji 17 racionalnih točk, leži na njej neskončno racionalnih točk.

V vsaki Abelovi grupi lahko definiramo produkt nP celega števila n s poljubnim elementom P. Če je n naravno število, je nP krajša pisava za vsoto $P + P \ldots + P$, kjer je sumandov n. Če pa je $n = -m$ negativen, pomeni $(-m)P$ nasprotni element od mP. Element P ima končen red, če obstaja tako naravno število $n \geq 1$, da je $nP = 0$. V končni grupi imajo vsi elementi končen red. V vsaki Abelovi grupi pa sestavljajo vsi elementi s končnim redom že zase grupo, ki jo imenujemo torzijska podgrupa dane grupe. Torzijska podgrupa je gotovo prava podgrupa, če obstajajo elementi, ki nimajo končnega reda.

Ni težko videti, da za vsako prevojno točko P na eliptični krivulji velja $3P = 0$. Zato ima vsaka prevojna točka $P \neq O$ red 3. Točke A_1, A_2, A_3, kjer eliptična krivulja (Ia) seče os (x) (sl. 3), pa imajo red 2. Mazur je dokazal, da ima tudi torzijska podgrupa grupe $E(Q)$ vselej manj kot 17 elementov.

Grupa $E(Q)$ je končno generirana, če obstaja v njej končno število točk $P_1, \ldots, P_s$ z lastnostjo, da se da vsaka točka $P \in E(Q)$ zapisati v obliki vsote $P = m_1 P_1 + \ldots + m_s P_s$, kjer so koeficienti m_i cela števila. Ni vsaka Abelova grupa končno generirana, npr. aditivna grupa racionalnih števil ni. Že H. Poincaré je postavil domnevo, da je grupa $E(Q)$ na vsaki eliptični krivulji končno generirana. Domnevo se je posrečilo dokazati l. 1922 angleškemu matematiku L. J. Mordellu in se zdaj imenuje Mordellov izrek.

Racionalne točke $P_1, \ldots, P_r$ na eliptični krivulji so linearno neodvisne, če je enačba $m_1 P_1 + \ldots + m_r P_r = 0$ izpolnjena le tedaj, ko so vsi koeficienti m_i enaki nič. Maksimalno število linearno neodvisnih točk se imenuje *rang* grupe $E(Q)$. Mordellov izrek pove, da je rang vedno končen. Pri končnih grupah je seveda enak nič. Nerešeno je vprašanje, ali obstajajo eliptične krivulje s poljubno velikim rangom. Vsekakor pa je lahko rang precej velik, saj je našel J. F. Mestre leta 1982 eliptično enačbo, pri kateri je rang najmanj enak 12.

Pri nekaterih eliptičnih krivuljah je grupa $E(Q)$ neskončna ciklična. To pomeni, da obstaja na krivulji racionalna točka P s tole lastnostjo: Točke nP so pri različnih n med seboj različne in vse točke v $E(Q)$ dobimo, ko preteče n vsa cela števila. Zgled za tako krivuljo je [1]

$$y^2 + y = x^3 - x$$

Na njej leži racionalna točka $P = (0, 0)$ in vse racionalne točke so oblike nP, $n \in \mathbb{Z}$. Dokaz te trditve pa nikakor ni preprost.

Denimo, da poznamo na eliptični krivulji racionalno točko $P_0 = (x_0, y_0)$. Potem je tudi $P_1 = P_0 \circ P_0$ racionalna točka. Prav tako je racionalna točka $P_2 = P_1 \circ P_1$ itd. Če postavimo $P_{k+1} = P_k \circ P_k$, dobimo zaporedje racionalnih točk P_k, $k = 0, 1, 2, \ldots$ To zaporedje konstruiramo seveda tako, da postavimo v točki P_k tangento na eliptično krivuljo. Točka P_{k+1} je presečišče te tangente s krivuljo. Ni rečeno, da so vse točke P_k med seboj različne. Vendar se v nekaterih primerih da dokazati, da so različne. Na takih eliptičnih krivuljah smo našli neskončno racionalnih točk. Grupa $E(Q)$ pa ima rang najmanj 1. Za zgled vzemimo krivuljo

$$x^3 + y^3 = a \qquad (13)$$

Naj bo število a na desni celo, večje od 2 in brez kubičnega delitelja. Tedaj velja tole: Če je na (13) kakšna racionalna točka P_0, je racionalnih točk neskončno, ker so vsi členi zgornjega zaporedja P_k med seboj različne točke [2]. Npr. na krivulji $x^3 + y^3 = 9$ leži racionalna točka $P_0 = (2, 1)$. Zato je na njej neskončno racionalnih točk. Vsaka racionalna rešitev $x = u/w$, $y = v/w$ te enačbe pa da rešitev enačbe

$$u^3 + v^3 = 9w^3 \tag{14}$$

v celih številih u, v, w. Torej ima (14) neskončno celoštevilskih rešitev, ki niso med seboj proporcionalne. Po opisani metodi dobimo na krivulji $x^3 + y^3 = 9$ točko $P_1 = (20/7, -17/7)$. Ta nam da tole rešitev enačbe (14): $u = 20$, $v = -17$, $w = 7$.

Kako pa je z rešitvami (x, y) algebraične enačbe (1), kjer sta x in y celi števili? Seveda vzamemo, da so koeficienti cela števila. Najprej si poglejmo krivulje druge stopnje. Na elipsi je množica celoštevilskih točk gotovo končna. Na nekaterih hiperbolah pa leži neskončno celoštevilskih točk. Zgled je hiperbola $x^2 - 2y^2 = 1$. Na njej je točka s koordinatama $x = 3$, $y = 2$. Nadaljnje celoštevilske rešitve dobimo tako, da izraz $(3 + 2\sqrt{2})^n$, kjer je eksponent n naravno število, razvijemo. Racionalni del je abscisa in koeficient pri $\sqrt{2}$ ordinata celoštevilske točke na krivulji $x^2 - 2y^2 = 1$. Pri $n = 2$ imamo npr. $(3 + 2\sqrt{2})^2 = 17 + 12\sqrt{2}$. Torej $x = 17$, $y = 12$.

Na eliptičnih krivuljah je množica celoštevilskih točk vselej končna, lahko tudi prazna. To je posledica globokega izreka o diofantskih aproksimacijah, ki so ga dokazali A. Thue, C. Siegel in K. Roth. Čeprav je množica celoštevilskih rešitev končna, pa nikakor ni lahka naloga poiskati vse take točke pri dani eliptični enačbi. Za zgled si oglejmo krivuljo [1]

$$y^2 = x^3 - 7x + 10 \tag{15}$$

Takoj ugotovimo, da leže na njej točke $A = (1, 2)$, $B = (2, 2)$, $C = (1, -2)$ in $D = (2, -2)$. (Zadnji dve sta simetrični k prvima dvema glede na abscisno os.) Zveznica dveh izmed teh točk seče krivuljo tretjič v racionalni točki, ki pa nima vselej celoštevilskih koordinat. Vendar ugotovimo brez težave tole: Če zvežemo dve taki celoštevilski točki, da je smerni koeficient sekante celo število, ima tretje presečišče spet cele koordinate. Npr. sekanta BC ima smerni koeficient 4. Krivuljo seče tretjič v točki $G = (13, 46)$. Če tako ravnamo, dobimo brez posebne težave s poskušanjem 26 točk s celimi koordinatami na krivulji (15). To so točke

$$(-3, 2), (-2, 4), (-1, 4), (1, 2), (2, 2), (3, 4), (5, 10), (9, 26), (13, 46), (31, 172),$$
$$(41, 262), (67, 548), (302, 5248)$$

Poleg teh so na krivulji še vse simetrične točke z isto absciso in nasprotno ordinato. Ali so to vse celoštevilske rešitve enačbe (15), ne vem. Vsekakor pa leži na krivulji(15) neskončno racionalnih točk, ker je že celoštevilskih točk 26, tedaj več kakor 16.

Teorija eliptičnih krivulj je izredno zanimiva, toda težka in zelo obsežna. Povezana je na eni strani s teorijo eliptičnih funkcij, na drugi strani pa s teorijo števil. V članku smo spoznali le najpreprostejše lastnosti. Pogled na

posamezne tipe kubičnih krivulj (slike od 3 do 7) nam ne odkrije na njih nič posebnega. Saj ne vidimo grupne strukture, še manj pa, ali leže na taki krivulji racionalne in celoštevilske točke. Kaj šele, da bi s slike razbrali veljavnost Mordellovega izreka! Zato je teorija eliptičnih krivulj lep primer za trditev, da je matematika abstraktna umetnost: Slike nam ne povedo, kako bogato strukturo imajo te krivulje.

LITERATURA

[1] R. Hartshorne, *Algebraic Geometry*, New York, Springer Verlag, 1977.
[2] K. Ireland—M. Rosen, *A Classical Introduction to Modern Number Theory*, New York, Springer Verlag, 1982.
[3] I. Vidav, *Afina in projektivna geometrija*, Zbirka Matematika—Fizika, Ljubljana 1981.
[4] B. L. van der Waerden, *Einführung in die Algebraische Geometrie*, Berlin, Verlag Julius Springer, 1939.

NOVE KNJIGE

WAERDEN, B. L. von der, A History of Algebra. From al-Khwarizmi to Emmy Noether. Springer Verlag, Berlin, Heidelberg, New York, Tokio 1985, XII + + 272 strani.

V prvem, najdaljšem poglavju podaja pisec zgodovinski razvoj reševanja algebrajskih enačb višjih stopenj od prvih začetkov pri Arabcih do dokončne rešitve celotne problematike z Galoisovo teorijo. Med arabskimi matematiki so posebno skrbno obdelani al-Khaarizmi, Tabit ben Qurra in Omar Khayyam. Tem slede italijanski matematiki: Leonardo da Pisa (Fibonacci), Benedetto Biaggio, Mazzinghi, Pacioli, Dardi da Pisa, Scipione del Ferro, Cardano, Tartaglia, Ferrari in Bombelli; pri teh se zanimivo bere, kako so se pretolkli do reševanja kubičnih in bikvadratnih enačb.

Nato slede opisi dosežkov pomembnih matematikov, ki jih pravzaprav poznamo iz učbenikov: Viète, Fermat, Descartes, Waring, Vandermonde, Abel in zlasti Gauss s svojo popolno rešitvijo krožnodelitvenih enačb in s svojim fundamentalnim teoremom algebre. Krona poglavja je Galois s svojo genialno teorijo, ki pa hkrati že odpira pot v drugo, razmeroma kratko poglavje o razvoju teorije grup.

V poglavju o grupah je prikazan razvoj poznavanja substitucijskih grup, transformacijskih grup, abstraktnih grup in struktur končnih grup; ob tem so bolj izčrpno obdelani matematiki: Klein, Lie, Kronecker, Cayley, Hölder, Jordan, Cartan in Weyl.

V tretjem poglavju je prikazan najprej razvoj specialnih algeber oziroma hiperkompleksnih sistemov: Hamiltonovih kvaternionov, Gravesovih oktonionov itd. Temu sledi prikaz o razvoju splošnih algebrajskih struktur in nato prikaz razvoja karakterjev Abelovih in končnih grup.

Z zgodovinskega vidika je delo odlično, ker izčrpno navaja in dostikrat tudi citira uporabljene originalne vire in v zadostni meri napotuje bralca na dopolnilno literaturo.

Alojzij Vadnal

NOVE KNJIGE

BOGOYAVLENSKY O. I., Methods of the qualitative theory of dynamical systems in astrophysics and gas dynamics, Berlin, Springer Verlag, 1985, 301 str.

Pred desetimi ali petnajstimi leti smo bili navajeni misliti na analitično mehaniko kot na dovršeno umetnino, ki ji ni več kaj posebnega dodati. V zadnjem desetletju pa se je dramatično pokazalo, da je mehanika še kako živa in lahko nudi orodje za reševanje problemov, ki jih do sedaj sploh nismo prištevali vanjo. Zdi se mi, da je ta napredek vsaj posredno stimulirala Thomova teorija katastrof za tiste čase dokaj neortodoksnim pogledom: ni važno, kako se posamezna trajektorija zasuče, ampak je bolj pomembno, na kakšen način trajektorije sistema povezujejo fazni prostor. Od razmeroma nejasnih predstav o tem, kako naj opišemo povezave v faznem prostoru, smo danes prišli do povsem ostre klasifikacije kritičnih točk in njihovih lastnosti.

Knjiga Metode kvalitativne teorije dinamičnih sistemov v astrofiziki in dinamiki plinov je monografija, v kateri ugledni avtor predstavlja uporabnost novih metod mehanike na področju kozmologije in dinamike plinov.

Kozmološki modeli, ki jih avtor obravnava, so t.i. Bianchijevi prostori. To so prostori, ki jih dobimo kot rešitve Einsteinovih enačb, če predpostavljamo, da je vesolje prostorsko homogeno, vendar ne nujno izotropno. Po taki predpostavki obstaja Lijeva grupa transformacij, katere orbite ležijo v trirazsežnem podprostoru. Na ta način je zamrznjena večina dinamičnih spremenljivk prostor-časa; vse, kar se zgodi v eni točki prostora, se mora na enak način zgoditi povsod. Edine dinamične spremenljivke, ki potem še ostanejo, so tiste, ki niso zamrznjene s simetrijsko grupo in jih lahko opišemo z največ tremi generaliziranimi koordinatami, ki opisujejo lokalno anizotropnost prostora.

Podobno avtor zamrzne tudi večino dinamičnih spremenljivk gravitacijsko vezanega plina in tako študira dinamiko sferno simetričnega kolapsa z metodami hamiltonove mehanike. V knjigi je na novo obravnavan problem gravitacijsko vezanega rotirajočega plina, katerega dinamične prostostne stopnje so vezane z zahtevo, naj bo gibanje »sebi podobno« to je, vse količine, ki opisujejo lokalno stanje plina, so funkcije enega samega parametra, ki je funkcija lege in časa.

Knjiga Metode kvalitativne teorije dinamičnih sistemov ni lahko branje. Vsebuje sicer dovolj informacij, da bralec lahko ponovi večino izpeljav, vendar pa bomo v njej našli le malo komentarja o fizikalni naravi obravnavanega problema ali o sklepih, ki bi sledili iz navedenih rezultatov. Knjiga, ki bi govorila o tej plati problemov, do zdaj še ni bila napisana in to daje pričujoči monografiji njen čar in izziv.

Andrej Čadež

NOVA POT DO LEBESGUA

NIKO PRIJATELJ

Math. Subj. Class. (1980) 26 A 42

Članek obravnava Mc Shanovo definicijo tako imenovanega gauge-integrala, ki je ekvivalenten Lebesguovemu integralu.

LEBESGUE IN A NEW WAY

In this article Mc Shane's definition of his gauge-integral, which is equivalent to the Lebesgue integral, is exposed.

0

V klasični teoriji realnih funkcij je temeljni pojem integrala prvič natanko opredelil šele *Riemann* leta 1854. Buren razvoj te teorije prav na prehodu v naše stoletje pa je brž pokazal, da je Riemannov integral vendarle preskromno sredstvo za potrebe, ki so se pojavile v novih okoliščinah. To pomanjkljivost je razmeroma zgodaj, namreč že leta 1902, odpravil *Lebesgue*. Čeravno je Lebesguovo odkritje sprožilo plaz novih spekulacij, ki so naposled vodile celo do nove samostojne matematične discipline, tako imenovane teorije mere, pa je tudi res, da je Lebesguov integral postal in ostal vogelni kamen sodobne matematične analize.

Zato je kajpada razumljivo prizadevanje, ki je zmeraj bolj očitno, da bi se ta premik od Riemanna k Lebesgu, ki je bil v matematiki izveden že na začetku našega stoletja, vsaj ob njegovem sklepu uresničil tudi v matematičnem pouku. Da se dobro razumemo: Lebesguov integral je že nekaj desetletij obvezna postavka v visokošolskih učnih programih študija matematike po vsem civiliziranem svetu. Toda v ogromni večini primerov so ti programi tako zasnovani, da vsebujejo prvo leto tudi nadrobno obravnavo Riemannovega integrala in njegovo uporabo. Ta del programa se navadno pokriva s programom študija matematike za naravoslovce in tehnike, katerim je poznanje Lebesgua večidel sploh »prihranjeno«. No, in omenjeno prizadevanje po posodobitvi pouka matematike je preprosto v tem, da bi se v visokošolskih programih za matematike *in* naravoslovce Riemannov integral že na samem začetku nadomestil z Lebesguovim.

Naravni nasledek te želje so sevé vse pogostnejši poskusi nekaterih matematikov, da bi odkrili če že ne »kraljevske« pa vsaj kolikor mogoče »zložno« pot do Lebesguovega integrala. Če se namreč obravnavanje Riemannovega integrala odlikuje po naravnost elegantni preprostosti, pa je že sam pristop do Lebesguovega dosti bolj zapleten. To je kajpak povsem razumljivo in do neke mere tudi neogibno, saj tudi gre za dosti bolj pretanjen in premeten pojem. Avtor enega zadnjih takih poskusov je znani ameriški matematik *E. J. McShane*, ki si je zadal tole konkretno nalogo: *Najti táko pot do Lebesguovega integrala, ki bi bila kar se le da podobna klasični poti do Riemannovega in ki bi se tudi po težavnosti »vzpona« razločevala od le-te samo toliko, kolikor je to nujna posledica dejstva, da gre pač za mnogo bolj zahtevno matematično konstrukcijo.* Njegova dokončna rešitev te naloge je nadrobno izdelana in obrazložena v zajetni knjigi **Unified Integration, Academic Press, Inc. 1983, 607 str.**

V tej knjigi konstruira McShane na želeni način integral, ki ga imenuje *gauge-integral* in za katerega dokaže, da je ekvivalenten Lebesguovemu integralu. Najprej opredeli seveda integral na realni osi in izpelje v vseh podrobnostih njegove temeljne lastnosti, potem pa ga razširi tudi na n-razsežne prostore $\mathbb{R}^n$. Mimo tega pokaže uporabo integralov pri diferencialnih enačbah in verjetnostnem računu, govori o krivuljnem integralu in površini ploskev, o vektorskih prostorih, Fourierovih vrstah in Fourierovi transformaciji, v zadnjem poglavju pa opiše še klasično pot do Lebesguovega integrala, ki izhaja iz teorije mere. Skratka, vsebina knjige povsem odgovorja njenemu obsegu.

V temle kratkem zapisu želimo samo nakazati pot, po kateri je avtor knjige prišel do definicije »novega« integrala, ki je torej ekvivalenten Lebesguovemu.

1

Da bi napravili podobnosti predvsem pa tudi bistvene razločke med definicijama Riemannovega in »novega«, alias Lebesguovega, integrala dobro razvidne, izberimo tole definicijo Riemannovega integrala:

Naj bo realna funkcija f definirana na *kompaktnem intervalu* $[a, b]$. Če je D kakšna delitev $a = x_0 < x_1 < \ldots < x_{i-1} < x_i \ldots < x_n = b$ intervala $[a, b]$, označimo z Δx_i dolžino i-tega podintervala $[x_{i-1}, x_i]$ te delitve, torej $\Delta x_i = x_i - x_{i-1}$, in z d_D dolžino najdaljšega podintervala delitve D. Izberimo *poljubno* točko ξ_i na vsakem podintervalu $[x_{i-1}, x_i]$ delitve D in napravimo vsoto

$$R(f, D) = \sum_{i=1}^{n} f(\xi_i)\, \Delta x_i$$

Potem rečemo: Če obstaja tako realno število $\mathbf{I}$, da moremo najti k vsakemu realnemu $\varepsilon > 0$ tak realen $\delta > 0$, da velja ocena

$$|R(f, D) - \mathbf{I}| < \varepsilon$$

za *vsako* delitev D intervala $[a, b]$, za katero je $d_D < \delta$, in pri *poljubni* izbiri točk ξ_i na podintervalih $[x_{i-1}, x_i]$, potem je funkcija f na intervalu $[a, b]$ Riemannovo integrabilna in število $\mathbf{I}$ je njen Riemannov integral na tem intervalu.

Če naj se zdaj po McShanu dokopljemo do podobne definicije Lebesguovega integrala, je potrebno opraviti še nekaj priprav.

Predvsem moramo opozoriti, da se bomo od vsega začetka gibali vzdolž *dopolnjene realne osi* $\mathbb{R}^*$, ki jo dobimo, če množici realnih števil $\mathbb{R}$ dodamo še elementa $-\infty$ in $+\infty$- ki seveda nista realni števili. Množico $\mathbb{R}^* = \mathbb{R} \cup \{-\infty, +\infty\}$ lahko brž *linearno uredimo,* če linearno urejenost »<« realnih števil $\mathbb{R}$ razširimo še na nova elementa, in sicer z zahtevama, da bodi

$$-\infty < +\infty \text{ in } -\infty < x < +\infty \text{ za vsak } x \in \mathbb{R}$$

Znamenito dejstvo, da ima vsaka neprazna množica v $\mathbb{R}$, ki je navzdol (navzgor) omejena, infimum (supremum) v $\mathbb{R}$, se poenostavi v resnico, da ima sploh vsaka neprazna množica v $\mathbb{R}^*$ infimum in supremum v $\mathbb{R}^*$. Nasprotno pa moremo le *delno* razširiti na $\mathbb{R}^*$ obe operaciji vsoto in produkt, ki sta definirani na vsem $\mathbb{R}$ in ki napravljata $\mathbb{R}$ za komutativen obseg. Ti operaciji v $\mathbb{R}$ sta namreč dopolnjeni v $\mathbb{R}^*$ le s temi dogovori:

$$(-\infty) + (-\infty) = -\infty \quad , \quad (+\infty) + (+\infty) = +\infty$$
$$x + (-\infty) = (-\infty) + x = -\infty \quad , \quad x + (+\infty) = (+\infty) + x = +\infty$$

za vsak $x \in \mathbb{R}$

$$(-\infty) \cdot (-\infty) = (+\infty) \cdot (+\infty) = +\infty \quad ,$$
$$(-\infty) \cdot (+\infty) = (+\infty) \cdot (-\infty) = -\infty$$
$$x \cdot (-\infty) = (-\infty) \cdot x = -\infty \quad , \quad x \cdot (+\infty) = (+\infty) \cdot x = +\infty$$

za vsak $x > 0$ iz $\mathbb{R}$

$$x \cdot (-\infty) = (-\infty) \cdot x = +\infty \quad , \quad x \cdot (+\infty) = (+\infty) \cdot x = -\infty$$

za vsak $x < 0$ iz $\mathbb{R}$

V teoriji integracije, in o tej tukaj govorimo, dodamo tem »standardnim« dogovorom vedno še enega, nekolikanj nenavadnega, da bodi namreč

$$0 \cdot (-\infty) = (-\infty) \cdot 0 = 0 \cdot (+\infty) = (+\infty) \cdot 0 = 0$$

Na dlani je, da $\mathbb{R}^*$ ni več obseg.

Razume se, da imamo v $\mathbb{R}^*$ opraviti tudi z *intervali*, katerih eno ali celo obe krajišči sta lahko $-\infty$ ali $+\infty$. Ako sta torej $a, b \in \mathbb{R}^*$, imamo, podobno kot v $\mathbb{R}$, na izbiro tele 4 tipe intervalov: zaprt interval $[a, b] = \{x \in \mathbb{R}^*, a \leqq x \leqq b\}$, *na desno odprt* interval $[a, b[= \{x \in \mathbb{R}^*, a \leqq x < b\}$, *na levo odprt interval* $]a, b] = \{x \in \mathbb{R}^*, a < x \leqq b\}$ in seveda še *odprt* interval $]a, b[= \{x \in \mathbb{R}^*, x < x < b\}$. Brž ko je $a > b$, so vsi intervali z levim krajiščem a in desnim krajiščem b prazna množica $\emptyset$, kar je sevé neposredno razvidno iz zgornjih opredelitev intervalov. Če sta $a, b \in \mathbb{R}$, potem pravimo, da je ustrezni interval *omejen*. Brž ko je $a < b$, ima vsak od teh štirih tipov intervalov I z levim krajiščem a in desnim krajiščem b *dolžino* ali *mero* $m(I) = b - a$. Če je levo krajišče $-\infty$ ali desno $+\infty$, postavimo $m(I) = +\infty$, in če premore interval eno samo točko ali pa je prazna množica, je $m(I) = 0$. Očitno imamo lahko prazno množico za odprt interval, saj je $]a, a[= \emptyset$ za vsak $a \in \mathbb{R}^*$. Podobno je tudi $]a, a] = [a, a[= \emptyset$, toda $[a, a] = \{a\}$.

Mimo intervalov, ki so prazna množica, sodijo med odprte množice običajne topologije v $\mathbb{R}$ še vsi neprazni odprti intervali v $\mathbb{R}$. No, v $\mathbb{R}^*$ pa spadajo k odprtim množicam običajne topologije poleg intervalov, ki so prazna množica, in vseh odprtih intervalov še tile neprazni intervali: $[-\infty, a[$ z $a \in \mathbb{R}$ ali $a = +\infty$, $]a, +\infty]$ z $a \in \mathbb{R}$ ali $a = -\infty$ in pa seveda $\mathbb{R}^* = [-\infty, +\infty]$. Če naj torej velja tudi v $\mathbb{R}^*$, da sodijo med odprte množice običajne topologije natanko tisti neprazni intervali, ki so odprti, potem moramo pač proglasiti tudi pravkar navedene intervale za odprte. Ker zoper to ni nobenega logičnega pomisleka, tako tudi napravimo.

Naj bosta spet $a, b \in \mathbb{R}^*, a < b$ in I interval kateregakoli tipa z levim krajiščem a in desnim krajiščem b. Potem označimo z $\overline{I}$ *zaprtje* intervala I v $\mathbb{R}^*$, ki je v vsakem primeru zaprti interval $[a, b]$. Če pa je $a \geqq b$, potem je zaprtje intervala kar enako intervalu. Se pravi, da je $\overline{[a, a]} = [a, a] = \{a\}$, v vsakem drugem primeru pa sta interval I in njegovo zaprtje $\overline{I}$ prazna množica.

Če je x poljubna točka v $\mathbb{R}^*$, imenujemo vsak *odprt* interval I, ki vsebuje točko x, okolica točke x. Tako je na primer za vsak $a \in \mathbb{R}$ interval $[-\infty, a[$ okolica točke $-\infty$, interval $]a, +\infty]$ okolica točke $+\infty$ in interval $[-\infty,$

$+\infty]$, se pravi $\mathbb{R}^*$, okolica sploh vsake točke $x \in \mathbb{R}^*$. V nadaljnjem bomo torej z besedo *okolica* vedno označevali le neprazne, odprte intervale, ki so potemtakem okolice vsake točke, ki jo vsebujejo.

Tudi sicer bomo imeli še in še opravka z intervali, pri katerih pa nas bo zanimala v glavnem le njihova dolžina ali mera. Da bi se izognili dolgoveznemu pojasnjevanju in ponavljanju, se odločimo takole: Če ne gre za okolice in če ne bomo posebej zahtevali drugače, naj bodo naprej vsi intervali *na levo odprti*, se pravi, da ne vsebujejo levega krajišča, pač pa desno, *v kolikor to krajišče ni* $+\infty$. Če pa je desno krajišče $+\infty$, *bodi ustrezni interval tudi na desno odprt*. S tem dogovorom dosežemo, da so vsi intervali, ki nas poleg okolic še zanimajo, pa naj bodo že omejeni ali ne, podmnožice realne osi $\mathbb{R}$.

Do McShanove definicije integrala nam je zdaj treba napraviti le še 5 korakov, s katerimi bomo po vrsti opredelili tiste temeljne pojme, na katerih sloni definicija.

1. *korak*: Naj bodo $I_1, I_2, \ldots I_n$ dani *paroma disjunktni* intervali v $\mathbb{R}$, x_1, $x_2, \ldots x_n$ pa poljubno izbrane točke v $\mathbb{R}^*$. Potem imenujemo končno množico urejenih parov

$$P = \{(x_1, I_1), (x_2, I_2), \ldots (x_n, I_n)\} \tag{1}$$

obeleženo delitev unije $\bigcup_{i=1}^{n} I_i$. Za intervale I_i, ki so po dogovoru na levo odprti, rečemo, da so intervali, za točke x_i pa, da so *evaluacijske točke* obeležene delitve P.

2. *korak*: Bodi dana kakšna obeležena delitev (1) in naj bo f funkcija iz $\mathbb{R}^*$ v $\mathbb{R}^*$. Potem imenujemo vsoto

$$S(f, P) = \sum_{i=1}^{n} f(x_i) \cdot m(I_i) \tag{2}$$

če seveda obstaja, *delitvena vsota funkcije f glede na obeleženo delitev P*.

3. *korak*: Naj bo A podmnožica v $\mathbb{R}^*$. Potem imenujemo *družino okolic na* A vsako funkcijo α, ki priredi vsaki točki $x \in A$ neko okolico $\alpha(x)$ te točke.

Družina okolic na A je potemtakem vsaka funkcija α, ki ima za domeno množico A, za kodomeno vse okolice točk $x \in A$, in ki priredi vsaki točki $x \in A$ določno njeno okolico.

4. *korak*: Naj bo α kakšna družina okolic na $\mathbb{R}^*$ in (1) obeležena delitev unije $\bigcup_{i=1}^{n} I_i$, ki je vsebovana v $\mathbb{R}$. Potem rečemo, da je obeležena delitev P *α-gosta*, če je za vsak $i = 1, 2, \ldots n$ zaprtje $\overline{I}_i$ intervala I_i vsebovano v okolici $\alpha(x_i)$, če je torej

$$\overline{I}_i \subseteq \alpha(x_i) \quad \text{za} \quad i = 1, 2, \ldots n \tag{3}$$

5. *korak*: Naj bo B podmnožica realne osi $\mathbb{R}$ in f *realna* funkcija, definirana na kakšni domeni $C \subseteq \mathbb{R}^*$ tako, da je $B \subseteq C$. Napravimo *realno* funkcijo f_B: $\mathbb{R}^* \to \mathbb{R}$ s predpisom

$$f_B(x) = \begin{cases} f(x), & \text{če je} \quad x \in B \\ 0, & \text{če je} \quad x \in \mathbb{R}^* - B \end{cases} \tag{4}$$

in vzemimo v pretres *vse obeležene delitve realne osi* $\mathbb{R}$, se pravi vse obeležene delitve (1),pri katerih je unija delitvenih intervalov I_i *vsa realna os* $\mathbb{R}$. In zdaj se dogovorimo:

Če obstaja tako realno število **L**, da moremo najti k vsakemu realnemu $\varepsilon > 0$ tako družino okolic α na $\mathbb{R}^*$, da velja ocena

$$|S(f_B, P) - \mathbf{L}| < \varepsilon \tag{5}$$

za vsako delitveno vsoto funkcije f_B glede na obeleženo delitev P realne osi, ki je α-gosta, potem je funkcija f na množici B Lebesguovo integrabilna in število **L** je njen Lebesguov integral na B.

Preden dopolnimo to definicijo še z neogibno potrebnimi pojasnili in pripombami, moramo najprej premisliti, če nam sploh kaj pove. Ta definicija ima namreč smisel samo, če je res, *da obstaja k vsaki družini okolic α na $\mathbb{R}^*$ vsaj ena α-gosta obeležena delitev P realne osi* $\mathbb{R}$. Brž ko bi namreč za kakšno družino okolic α^* na $\mathbb{R}^*$ ne obstajala nobena α^*-gosta obeležena delitev realne osi $\mathbb{R}$, bi bil seveda za to družino okolic α^* pogoj (5) na prazno izpolnjen, in to za vsak realen $\varepsilon > 0$, za vsako realno funkcijo f, za vsako podmnožico $B \subseteq R$, ki je v domeni funkcije f, in za vsako realno število **L**. To pa pomeni, da bi bila vsaka realna funkcija f integrabilna na vsaki podmnožici B, ki je v njeni domeni, in da bi bil njen integral vsako realno število **L**. Na dlani je, da je tak pojem integrala povsem neraben in zato nesmiseln. V zadnjem razdelku bomo pokazali, da Mc Shanova definicija nima te usodne hibe.

Zdaj pa dodajmo še nekaj pojasnil in pripomb.

(A) Če naj se sploh lotimo verifikacije ocene (5), potem moramo biti seveda gotovi, da delitvene vsote $S(f_B, P)$ obstajajo in so končne, brž ko se nanašajo na α-goste obeležene delitve P realne osi $\mathbb{R}$, za primerno izbrane družine okolic α na $\mathbb{R}^*$. Ne smemo namreč pozabiti, da nastopajo pri obeleženih delitvah realne osi tudi neomejeni intervali, katerih dolžina ali mera je sevé $+\infty$. Vendar pa nam to ne more povzročiti nobenih nevšečnosti, če se omejimo le na take družine okolic α na $\mathbb{R}^*$, pri katerih je okolica $\alpha(x)$ *omejena za vsak* $x \in \mathbb{R}^*$, *za katerega je* $f_B(x) \neq 0$. V tem primeru so namreč vsi sumandi *končne* vsote $S(f_B, P)$ tudi *končni*. Kajti, če je v produktu $f_B(x_i) \cdot m(I_i)$ prvi faktor od nič različno realno število, je tudi drugi faktor končen, saj je obeležena delitev P α-gosta, in zato je zaprtje $\overline{I}_i$ intervala I_i vsebovano v *omejeni* okolici $\alpha(x_i)$. Če pa je prvi faktor $f_B(x_i) = 0$, potem je po naših dogovorih tudi produkt $f_B(x_i) \cdot m(I_i) = 0$, ne glede na to, kolikšen je $m(I_i)$. Potemtakem je delitvena vsota $S(f_B, P)$ res končna.

Da opisane družine okolic α na $\mathbb{R}^*$ res obstajajo, je brž razvidno, če upoštevamo tole: funkcija f_B je po definiciji na množici $\mathbb{R}^* - B$ identično enaka nič; ker je B podmnožica realne osi $\mathbb{R}$, to pomeni, da je $f_B(-\infty) = f_B(+\infty) = 0$.

(B) Seveda je mogoče pokazati: če je funkcija f integrabilna na množici B, je njen integral **L** na B enolično določen. Razume se, da veljajo tudi vse »standardne« lastnosti integralov, ki jih poznamo iz elementarne teorije. Bodi prepuščeno bravcu, da ugotovi, v koliki meri je McShanova definicija Lebesguovega integrala res podobna definiciji Riemannovega integrala, ki smo jo ponovili na začetku razdelka. Tukaj opozorimo raje le na bistvene razločke, iz katerih je neposredno razvidno, na kako skromnih predpostavkah sloni Mc Shanova definicija.

Za množico $B \subseteq \mathbb{R}$, po kateri integriramo, *ne* zahtevamo, da je omejena in seveda tudi *ni* potrebno, da je interval. Če B je interval z levim krajiščem a in

desnim krajiščem $b > a$, ki je lahko tudi neomejen, potem je integral kakšne funkcije na tem intervalu, v kolikor seveda obstaja, neodvisen od tega, za kateri tip intervala se odločimo.

Tudi realna funkcija f ni treba, da je omejena na integracijski množici $B \subseteq \mathbb{R}$, kakor je to pri Riemannovem integralu, pa se vseeno lahko zgodi, da Lebesguov integral obstaja.

Iz obeh zgornjih odstavkov je potemtakem razvidno, da so z novo definicijo integrala zajeti tudi tako imenovani *izlimitirani* integrali, ki so znana elementarna posplošitev Riemannovega integrala. Vendar je treba povedati, da velja to le za izlimitirane integrale, ki so absolutno konvergentni.

Intervale I_i, ki nastopajo v obeleženih delitvah P realne osi $\mathbb{R}$, lahko sevé indeksiramo v poljubnem vrstnem redu in ne nujno od leve proti desni. Niti ni potrebno, da so vsi ti intervali neprazni. Zato govorimo nasploh o delitvah in ne o porazdelitvah. Prazni delitveni intervali kajpak ničesar ne prispevajo k prirejeni delitveni vsoti in jih potemtakem lahko tudi zavržemo. Vendar je včasih vseeno ugodno, če jih pri delitvah dopuščamo.

Evaluacijske točke x_i, ki nastopajo pri obeleženih delitvah P v urejenih parih z delitvenimi intervali I_i, *nikakor ni treba, da bi bile vsebovane v ustreznih intervalih* I_i *niti ne v njihovih zaprtjih* $\overline{I}_i$. Prav tako tudi *ni neogibno,* da bi bile evaluacijske točke, ki so prirejene različnim delitvenim intervalom, med seboj različne. Včasih je celo zaželeno, da ima več različnih urejenih parov dane obeležene delitve iste evaluacijske točke.

Vsaka družina okolic α na $\mathbb{R}^*$ priredi vsakemu $x \in \mathbb{R}^*$ določno okolico $\alpha(x)$ točke x. Ker smo vzeli, da je $\alpha(x)$ neprazen, odprt interval, ki vsebuje točko x, je na dlani, da je $m(\alpha(x)) > 0$. Vendar pa pri tem *ne zahtevamo,* da obstaja tak realen $\delta > 0$, da bi veljalo $m(\alpha(x)) \geqq \delta$ za vsak $x \in \mathbb{R}^*$. Drugače povedano, dopuščamo tudi možnost, da je $\inf \{m(\alpha(x)), x \in \mathbb{R}^*\} = 0$.

(C) Pokažimo še na preprostem zgledu, kako ta teorija deluje. V ta namen si izberimo enostavno funkcijo, ki zmore na $\mathbb{R}$ le dve vrednosti in je definirana takole:

$$f(x) = \begin{cases} 1, & \text{če je } x \text{ racionalno število} \\ 0, & \text{če je } x \text{ iracionalno število} \end{cases}$$

za množico B pa vzemimo interval

$$B = [0, 1]$$

Ker je potemtakem funkcija f nezvezna v vsaki točki intervala $[0, 1]$, vemo, da ni Riemannovo integrabilna na tem intervalu. Poskusimo torej srečo z Lebesguom.

Pa napravimo funkcijo f_B: $\mathbb{R}^* \to \mathbb{R}$, kakor nam veleva 5. korak, s predpisom:

$$f_B(x) = \begin{cases} f(x), & \text{če je } x \in B \\ 0, & \text{če je } x \in \mathbb{R}^* - B \end{cases}$$

Se pravi, da ima f_B vrednost 1 v vseh racionalnih točkah intervala $[0, 1]$ in vrednost 0 povsod drugjé na $\mathbb{R}^*$. Naj bo zdaj dan poljubno izbrani realni $\varepsilon > 0$ in določimo družino okolic α na $\mathbb{R}^*$ takole:

Če je x racionalno število na intervalu $[0, 1]$, ga zapišimo v obliki reduciranega ulomka p/q, za $x = 0$ bodi to $0/1$, in definirajmo

$$\alpha(x) =]x - \varepsilon/2^{p+q+2},\ x + \varepsilon/2^{p+q+2}[\tag{6}$$

Za vsak drug $x \in \mathbb{R}^*$ pa širokosrčno postavimo kar

$$\alpha(x) = \mathbb{R}^* \tag{7}$$

saj je v tem primeru seveda $f_B(x) = 0$.

Naj bo

$$P = \{(x_1, I_1), (x_2, I_2), \ldots (x_n, I_n)\} \tag{8}$$

poljubna α-gosta obeležena delitev realne osi $\mathbb{R}$ in ocenimo prirejeno delitveno vsoto $S(f_B, P)$. Kakor smo že omenili, lahko indeksiramo intervale I_i v poljubnem vrstnem redu. Pa začnimo s tistimi, če jih sploh kaj je, katerih evaluacijske točke so racionalna števila na intervalu $[0, 1]$. Recimo, da so to pari $(x_1, I_1), (x_2, I_2), \ldots (x_h, I_h)$. Potem pa pridejo na vrsto še drugi pari $(x_{h+1}, I_{h+1}), \ldots (x_n, I_n)$. Ker ima f_B v točkah $x_1, x_2, \ldots x_h$ vrednost 1 in v točkah $x_{h+1}, \ldots x_n$ vrednost 0, je potemtakem delitvena vsota $S(f_B, P)$ po (2) enaka

$$S(f_B, P) = \sum_{i=1}^{h} m(I_i) \tag{9}$$

Če je $h = 0$, se pravi, če nobena evaluacijska točka ni racionalno število na intervalu $[0, 1]$, potem je očitno

$$S(f_B, P) = 0 \tag{a}$$

V nasprotnem primeru pa razmišljamo takole:

Ker je obeležena delitev P po hipotezi α-gosta, so zaradi (3) seveda mere intervalov I_i manjše, kvečjemu enake meram ustreznih okolic $\alpha(x_i)$. Če je torej x_i racionalno število na intervalu $[0, 1]$, zapisano v obliki reduciranega ulomka p/q, potem takoj razberemo iz (6), da je

$$m(I_i) \leqq \varepsilon/2^{p+q+1} \tag{10}$$

No, ker pa nastopajo v končni vsoti (9) samo intervali, ki so prirejeni racionalnim evaluacijskim točkam iz intervala $[0, 1]$, je ta končna vsota zanesljivo manjša od vsote neskončne dvojne vrste, katere splošni člen je

$$a_{pq} = \varepsilon/2^{p+q+1}$$

Ker gre za vrsto s pozitivnimi členi, je izid tega seštevanja neodvisen od vrstnega reda sumandov. Zato lahko najprej seštevamo pri negibnem p po $q = 1, 2, 3, \ldots$ in dobimo vsoto

$$\sum_{q=1}^{\infty} a_{pq} = \varepsilon/2^{p+1}$$

potem pa seštejemo še tako dobljene delne vsote po $p = 0, 1, 2, \ldots$, kar nam da

$$\sum_{p=0}^{\infty} \sum_{q=1}^{\infty} a_{pq} = \varepsilon$$

Tako dobimo torej oceno

$$0 < S(f_B, P) < \varepsilon \tag{b}$$

Iz (a) in (b) smemo potemtakem skleniti, da je v vsakem primeru

$$|S(f_B, P) - 0| = S(f_B, P) < \varepsilon$$

brž ko je obeležena delitev P α-gosta. To pa se pravi, da je funkcija f na intervalu $[0, 1]$ Lebesguovo integrabilna in da je njen integral $\mathbf{L} = 0$.

2

Pokažimo naposled še temeljno resnico, ki sploh napravi McShanovo definicijo integrala smiselno, da obstaja namreč k *vsaki* družini okolic α na $\mathbb{R}^*$ *vsaj ena* α-gosta obeležena delitev P realne osi $\mathbb{R}$. Zvesto posnemaje McShana, bomo dokazali celo še nekaj več, in sicer tole:
(T) Naj bo α poljubna dana družina okolic na $\mathbb{R}^*$, B pa na levo odprt neprazen interval v $\mathbb{R}$. Potem obstaja taka α-gosta obeležena delitev P intervala B, da je za vsak urejen par $(x_i, I_i) \in P$ evaluacijska točka x_i v zaprtju ustreznega intervala I_i, da je torej $x_i \in \overline{I}_i$.

Preden se lotimo dokazovanja tega izreka, pokažimo še naslednjo lemo, ki jo bomo uporabili pri dokazu:
(L) Naj bodo $P_1, P_2, \ldots P_p$ obeležene delitve podmnožic $C_1, C_2, \ldots C_p$, ki so paroma disjunktne. Potem je unija $P = \bigcup_{j=1}^{p} P_j$ obeležena delitev unije $C = \bigcup_{j=1}^{p} C_j$.

Če zapišemo za vsak $j = 1, 2, \ldots p$ eksplicitno

$$P_j = \{(x_{1j}, I_{1j}), (x_{2j}, I_{2j}), \ldots (x_{n_j j}, I_{n_j j})\}$$

potem so seveda točke $x_{1j}, x_{2j}, \ldots x_{n_j j}$ iz $\mathbb{R}^*$, intervali $I_{1j}, I_{2j}, \ldots I_{n_j j}$ so paroma disjunktni in na levo odprti v $\mathbb{R}$ in C_j *je* kajpada unija $C_j = \bigcup_{i=1}^{n_j} I_{ij}$ (glejte 1. korak). Ker pa so po hipotezi množice $C_1, C_2, \ldots C_p$ paroma disjunktne, sta disjunktna tudi poljubna intervala $I_{ij} \in P_j$ in $I_{mn} \in P_n$, brž ko je $j \neq n$. Potemtakem so res v uniji

$$P = \bigcup_{j=1}^{p} P_j = \{(x_{ij}, I_{ij}),\ j = 1, 2, \ldots p \text{ in } i = 1, 2, \ldots n_j \text{ pri negibnem } j\}$$

vse točke x_{ij} iz $\mathbb{R}^*$, intervali I_{ij} pa paroma disjunktni in na levo odprti v $\mathbb{R}$. To pa se pravi (glejte 1. korak), da je P obeležena delitev unije

$$\bigcup_{j=1}^{p} \left(\bigcup_{i=1}^{n_j} I_{ij} \right) = \bigcup_{j=1}^{p} C_j = C$$

S tem je lema (L) dokazana.

Dokaz izreka (T), ki je nekoliko zapleten, pa je takle:

Najprej priredimo vsakemu naravnemu številu $n \geqq 1$ določeno porazdelitev realne osi $\mathbb{R}$, in sicer takole: poleg intervalov $]-\infty, -2^n]$ in $]2^n, +\infty[$ naj tvorijo to porazdelitev še na levo odprti intervali, ki jih dobimo tako, da interval $]-2^n, 2^n]$ razdrobimo na 2^{2n+1} intervalov enake dolžine ali mere 2^{-n}. Če označimo s $K(n)$ množico intervalov te porazdelitve, potem so torej elementi te množice natanko tile intervali:

$I(n, 0) =]-\infty, -2^n]$
$I(n, i) =]-2^n + (i-1) \cdot 2^{-n}, -2^n + i \cdot 2^{-n}]$ za $i = 1, 2, \ldots 2^{2n+1}$
$I(n, 2^{2n+1} + 1) =]2^n, +\infty[$

Preprost premislek nam brž pove, da dobimo intervale množice $K(n+1)$ z *nadaljnjo drobitvijo* intervalov množice $K(n)$. Odtod pa seveda takoj sledi: če pripadata interval I' množici $K(n')$, interval I'' množici $K(n'')$ in je $n'' \geqq n'$, potem sta intervala I' in I'' bodisi disjunktna ali pa je $I'' \subseteq I'$.

Glede na te porazdelitve realne osi $\mathbb{R}$, ki so določene z množicami intervalov $K(1), K(2), \ldots K(n), \ldots$, bomo zdaj pokazali tole trditev:
(T*) Če je α poljubna dana družina okolic na $\mathbb{R}^*$, B pa na levo odprt neprazen interval v $\mathbb{R}$, potem obstaja taka α-gosta obeležena delitev P^* intervala B, da velja za vsak element $(x_i, I_i) \in P^*$, da je I_i bodisi prazen ali pa je enak preseku intervala B s kakšnim intervalom, ki pripada kateri od množic $K(1), K(2), \ldots, K(n), \ldots$, in je $x_i \in \overline{I}_i$. Take α-goste obeležene delitve bomo v nadaljevanju imenovali na kratko *izbrane*.

Če se nam posreči dokazati trditev (T*), potem smo s tem dokazali že tudi izrek (T). Iz *izbrane* α-goste obeležene delitve P^* intervala B dobimo namreč takoj tudi α-gosto obeleženo delitev P tega intervala, kakršno zahteva izrek (T), brž ko brišemo v delitvi P^* vse morebitne elemente (x_i, I_i) s praznimi intervali I_i.

Dokažimo trditev (T*) tako, da pokažemo, da nas njena negacija vodi do protislovja. Izhajajmo torej iz *domneve*, da ne obstaja nobena *izbrana* α-gosta obeležena delitev intervala B. Pa napravimo preseke $B \cap I(1,i)$ za vse $i = 0, 1, 2, \ldots 2^3 + 1$, ki so seveda spet na levo odprti disjunktni intervali, nekateri morda tudi prazni. Za hip *privzemimo*, da bi obstajala k vsakemu nepraznemu intervalu $B \cap I(1, i)$ kakšna *izbrana* α-gosta obeležena delitev P_i^* tega intervala. Ker je unija teh disjunktnih nepraznih intervalov kajpada natanko interval B, je po lemi (L) unija prirejenih delitev P_i^* obeležena delitev P intervala B. Oglejmo si to delitev natančneje. Vsak par $(x_k, I_k) \in P$ z nepraznim intervalom I_k spada potemtakem v natanko eno *izbrano* α-gosto obeleženo delitev P_i^* določenega nepraznega intervala $B \cap I(1, i)$. Zato je seveda

$$\overline{I}_k \subseteq \alpha(x_k) \quad , \quad x_k \in \overline{I}_k \tag{a}$$

in I_k je enak preseku intervala $B \cap I(1, i)$ s kakšnim intervalom $I(p, j)$, ki pripada eni od množic $K(1), K(2), \ldots K(n), \ldots$, se pravi, da je

$$I_k = (B \cap I(1, i)) \cap I(p, j) \tag{11}$$

Ker pa je $I_k \neq \emptyset$, mora biti, kakor že vemo, $I(p, j) \subseteq I(1, i)$ in tako dobimo iz (11), da je tudi

$$I_k = B \cap I(p, j) \tag{b}$$

Iz (a) in (b) pa lahko neposredno sklenemo, da je konstruirana obeležena delitev P intervala B α-gosta in *izbrana*. No, ker pa po naši *domnevi* ne obstaja nobena *izbrana* α-gosta obeležena delitev intervala B, je očitno mogoč en sam zaključek: *privzetje*, ki nas je vodilo do konstrukcije obeležene delitve P intervala B, je nezdružljivo z našo *domnevo*. To pa se pravi:

Brž ko ne obstaja nobena *izbrana* α-gosta obeležena delitev intervala B, je tudi med intervali $B \cap I(1,0)$, $B \cap I(1,1)$, ... $B \cap I(1, 2^3 + 1)$ vsaj en neprazen interval, za katerega prav tako ni nobene *izbrane* α-goste obeležene delitve. Pa vzemimo, da je $B \cap I(1, i_1)$ tak interval in ga naprej označimo z B_1. Bodi torej

$$\emptyset \neq B_1 = B \cap I(1, i_1) \subseteq B$$

In zdaj ponovimo to igro na intervalu B_1. Napravimo preseke $B_1 \cap I(2, i)$ za vse $i = 0, 1, 2, \ldots 2^5 + 1$, ki so spet na levo odprti disjunktni intervali, nekateri tudi prazni. Ker ne obstaja nobena *izbrana* α-gosta obeležena delitev intervala B_1, vemo iz pravkar opravljenega premisleka, da mora biti tudi med intervali $B_1 \cap I(2,0)$, $B_1 \cap I(2,1)$, ... $B_1 \cap I(2, 2^5 + 1)$ vsaj en neprazen interval, za katerega prav tako ni nobene *izbrane* α-goste obeležene delitve. Recimo, da je $B_1 \cap I(2, i_2)$ tak interval, in ga naprej označimo z B_2. Bodi torej

$$\emptyset \neq B_2 = B_1 \cap I(2, i_2) \subseteq B_1$$

To igro očitno lahko ponovimo neomejenokrat. Če označimo še začetni interval B zdaj raje z B_0, dobimo potemtakem neko zaporedje vloženih na levo odprtih in nepraznih intervalov v $\mathbb{R}$

$$B_0 \supseteq B_1 \supseteq B_2 \supseteq \ldots \supseteq B_n \supseteq \ldots \tag{12}$$

pri katerem je za vsak $n = 0, 1, 2, \ldots$

$$B_{n+1} = B_n \cap I(n+1, i_{n+1})$$

za primerno izbran $i_{n+1} \in \{0, 1, 2, \ldots 2^{2n+3} + 1\}$. In seveda ne smemo pozabiti, da za noben člen tega zaporedja ne obstaja nobena *izbrana* α-gosta obeležena delitev. Zaporedju (12) priredimo zdaj še zaporedje zaprtij $\overline{B}_n$, ki je zaporedje vloženih nepraznih in zaprtih intervalov v $\mathbb{R}^*$

$$\overline{B}_0 \supseteq \overline{B}_1 \supseteq \overline{B}_2 \supseteq \ldots \supseteq \overline{B}_n \supseteq \ldots \tag{13}$$

Tukaj se sevé spomnimo znanega izreka iz realne analize, da je pri vsakem zaporedju vloženih nepraznih intervalov v $\mathbb{R}$, ki so *omejeni* in *zaprti*, vsaj ena točka $y \in \mathbb{R}$ vsem tem intervalom skupna. No, bravec pa se brž lahko sam prepriča, da je analogno pri vsakem zaporedju vloženih nepraznih intervalov v $\mathbb{R}^*$, ki so *zaprti*, vsaj ena točka $y \in \mathbb{R}^*$ vsem tem intervalom skupna. Potemtakem obstaja točka $y \in \mathbb{R}^*$, ki je vsebovana v vseh členih $\overline{B}_n$ zaporedja (13). Če pišemo bolj določno $\overline{B}_n = [a_n, b_n]$ z $a_n, b_n \in \mathbb{R}^*$ in $a_n \leqq b_n$, obstaja torej taka točka $y \in \mathbb{R}^*$, da je $y \in [a_n, b_n]$ za vsak $n \in \mathbb{N}$.

Zdaj pa razločujmo 3 možnosti:

1. *možnost*: $y = -\infty$

V tem primeru mora biti seveda $a_n = -\infty$ za vsak $n \in \mathbb{N}$. Iz $B_{n+1} =]-\infty, b_{n+1}] = B_n \cap I(n+1, i_{n+1}) \subseteq I(n+1, i_{n+1})$ pa razberemo, da je $I(n+1, i_{n+1} =]-\infty, -2^{n+1}]$. Potemtakem je $\overline{B}_{n+1} \subseteq [-\infty, -2^{n+1}]$. Ker gre -2^{n+1} z naraščajočim n proti $-\infty$, je torej zagotovo $\overline{B}_{n+1} \subseteq \alpha(-\infty) = \alpha(y)$ za vse *dovolj velike* $n \in \mathbb{N}$.

2. *možnost*: $y = +\infty$

Zdaj mora biti kajpak $b_n = +\infty$ za vsak $n \in \mathbb{N}$. No, iz $B_{n+1} =]a_{n+1}, +\infty[= B_n \cap I(n+1, i_{n+1}) \subseteq I(n+1, i_{n+1})$ pa vidimo, da je $I(n+1, i_{n+1}) =]2^{n+1}, +\infty[$. Potemtakem je $\overline{B}_{n+1} \subseteq [2^{n+1}, +\infty]$ in ker gre seveda 2^{n+1} z naraščajočim n proti $+\infty$, je zanesljivo $\overline{B}_{n+1} \subseteq \alpha(+\infty) = \alpha(y)$ za vse *dovolj velike* $n \in \mathbb{N}$.

3. *možnost*: $y \in \mathbb{R}$.

Ker je za *dovolj velike* $n \in \mathbb{N}$ gotovo res, da je $-2^{n+1} < y < 2^{n+1}$, lahko iz $B_{n+1} =]a_{n+1}, b_{n+1}] = B_n \cap I(n+1, i_{n+1}) \subseteq I(n+1, i_{n+1})$ in pa $y \in \overline{B}_{n+1}$ zaključimo, da $I(n+1, i_{n+1})$ ni niti $]-\infty, -2^{n+1}]$ niti $]2^{n+1}, +\infty[$. Torej je $I(n+1, i_{n+1})$ v tem primeru očitno neki interval dolžine $2^{-(n+1)}$. Zato je dolžina intervala $\overline{B}_{n+1}$, se pravi razlika $b_{n+1} - a_{n+1} \leqq 2^{-(n+1)}$. Ker pa je $y \in \overline{B}_{n+1}$, torej $a_{n+1} \leqq y \leqq b_{n+1}$ za vsak $n \in \mathbb{N}$, vidimo, da gresta a_{n+1} in b_{n+1} z naraščajočim n proti y. Odtod pa spet sledi, da je gotovo $\overline{B}_{n+1} = [a_{n+1}, b_{n+1}] \subseteq \alpha(y)$ za vse *dovolj velike* $n \in \mathbb{N}$.

Kakor smo pokazali v vseh treh primerih, ki lahko nastopijo, je vedno mogoče najti *dovolj pozen* člen $\overline{B}_{n+1}$ v zaporedju (13), za katerega velja $\overline{B}_{n+1} \subseteq \alpha(y)$. Zdaj pa istoležnemu členu B_{n+1} v zaporedju (12), ki je na levo odprt neprazen interval v $\mathbb{R}$, priredimo obeleženo delitev P, ki ima en sam par, namreč (y, B_{n+1}), se pravi, da je $P = \{(y, B_{n+1})\}$. Oglejmo si to delitev P malo pobliže. No, ker je $\overline{B}_{n+1} \subseteq \alpha(y)$, je P očitno α-gosta obeležena delitev intervala B_{n+1}. Toda res je tudi $y \in \overline{B}_{n+1}$ in iz $B_{n+1} = B_n \cap I(n+1, i_{n+1})$ takoj spoznamo, da velja tudi $B_{n+1} = B_{n+1} \cap I(n+1, i_{n+1})$. To dvoje pa nam pove, da je P *izbrana* α-gosta obeležena delitev intervala B_{n+1}. In tako smo prišli do protislovja, saj vemo, da za noben člen zaporedja (12) ne obstaja nobena *izbrana* α-gosta obeležena delitev. Ker pa je vir tega protislovja *domneva*, da ne obstaja nobena *izbrana* α-gosta obeležena delitev začetnega intervala B, moramo pač to *domnevo* zavrniti. To pa sevé ne pomeni nič drugega, kot da je trditev (T*) resnična. S tem pa je nazadnje dokazan tudi izrek (T).

NOVE KNJIGE

GRASSELLI J., Linearna algebra, Vadnal A., Linearno programiranje — Ljubljana, DMFA SRS, 1986, 188 str. Jamnik R., Trigonometrijske vrste, Stieltjesov integral, Lebesguov integral — Ljubljana, DMFA SRS, 1986, 120 str. Krušič B., Dvojni in mnogoterni integral, Vidav I., Diferencialna geometrija v prostoru, Vencelj M., Vektorska analiza — Ljubljana, DMFA SRS, 1986, 136 str. Jamnik R., Verjetnostni račun in statistika — Ljubljana, DMFA SRS, 1986, 156 str.

(Matematika — Fizika, Zbirka univerzitetnih učbenikov in monografij; 23, 24, 25, 26.)

Znani učbenik Višja matematika II, prvič izdan leta 1975, je zdaj izšel v obliki štirih knjig. Prva med njimi vsebuje poglavji Linearna algebra (avtor Jože Grasselli) in Linearno programiranje (pisec Alojzij Vadnal). Linearna

algebra začne z vektorskimi prostori, slede linearne preslikave ter obravnava realnih in kompleksnih prostorov s skalarnim produktom. Poučimo se lahko o grupi obrnljivih matrik, o spektralni razčlenitvi normalnih operatorjev na končno razsežnih prostorih ter o bilinearnih in kvadratnih formah. Na koncu so na kratko povzete še osnovne lastnosti metričnih in Hilbertovih prostorov. Več kot sto nalog z rešitvami zaokroža to poglavje.

Linearno programiranje začne z lastnostmi konveksnih množic. Po formulaciji problema sledi reševanje z metodo simpleksov. Na koncu imamo še povezavo z dualnim problemom.

Drugo knjigo je napisal Rajko Jamnik. Vsebuje tri dele: Trigonometrijske vrste, Stieltjesov in Lebesguov integral. Zvemo, kako in kdaj lahko funkcijo na nekem intervalu razvijemo v Fourierovo vrsto po kotnih funkcijah. Sledi obravnava Fourierovega integrala. V drugem delu se seznanimo s funkcijami z omejenim totalnim razmahom, nato pa s Stieltjesovim integralom in primeri uporabe.

Lebesguov integral je najprej definiran za stopničaste realne funkcije realne spremenljivke, nato pa za t. im. sumabilne funkcije (ki pravzaprav sestavljajo prostor L_1). Za take funkcije so dokazani izreki o zamenjavi limite in integrala in Fubinijev izrek. Merljiva funkcija je definirana kot funkcija, ki je skoraj povsod limita zaporedja stopničastih funkcij. Množica na realni osi je merljiva, če je njena karakteristična funkcija merljiva. Vse to je uporabljeno pri obravnavi prostora $L_2(E)$, ker je E podmnožica realne osi. Dokazano je, da je L_2 Hilbertov prostor in (z Bernsteinovimi polinomi), da je trigonometrijski sistem ortonormirana baza prostora $L_2(-\pi, \pi)$.

Tretjo knjigo so napisali trije avtorji. Bogdan Krušič na klasičen način obravnava dvojni, trojni in mnogoterni integral in njegovo uporabo pri računanju težišč, vztrajnostnih momentov ter površin ploskev.

Diferencialno geometrijo v prostoru je napisal Ivan Vidav. Obravnavane so vektorske funkcije skalarnega argumenta, krivulje v prostoru, fleksija in torzija ter Frenetove formule.

Pri ploskvah se seznanimo z obema fundamentalnima formama, ukrivljenostjo, glavnimi smermi ter Gaussovo ukrivljenostjo. Obdelane so še družine ploskev in njihove ogrinjalke ter krivočrtne koordinate v prostoru.

Marija Vencelj je avtorica poglavja o vektorski analizi. V njem pridemo do Gaussovega in Stokesovega izreka. Obdelane so še sestavljene vektorske operacije ter Laplaceov operator v ortogonalnih krivočrtnih koordinatah.

Zadnja knjiga je Verjetnostni račun in statistika izpod peresa pokojnega profesorja Rajka Jamnika. Na lahko razumljiv način so tu obdelani osnovni pojmi verjetnostnega računa, zaporedja neodvisnih poskusov, slučajne spremenljivke in slučajni vektorji ter njihove številske karakteristike, na koncu pa še limitni izreki. Matematična statistika obravnava statistične hipoteze, preskuse značilnosti, korelacijo in regresijo.

Na koncu te kratke predstavitve povejmo še, da vsa poglavja vsebujejo naloge z rešitvami in seznam literature, vsaka od knjig pa tudi stvarno kazalo.

Peter Legiša

GEOMETRIJSKA PODOBA ODVODA

FRANCE KRIŽANIČ

Math. Subj. Class (1985) 26 B 12, 99 A 20

Matematika za fizike v enem svojih ljubljanskih tečajev že v prvem semestru pogleda na odvod s treh strani.

DIFFERENTIATION FROM THE GEOMETRIC POINT OF VIEW

In the first course of calculus differentiation can be looked at from three different points of view.

Predgovor

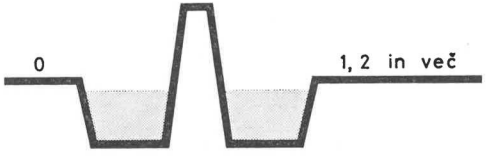
Ta članek je napisan kot berila, lahko se zgražate nad njim, ne da bi ga prebrali.

Snov je iz sredine matematične analize, zato ne začenja z aksiomi. Seveda pa, kakor vsaka analiza, temelji na aksiomih za realna števila (ponovimo: $\mathbb{R}$ je poln urejen obseg). Aksiome zamolči, ne more pa brez definicij, tudi takih — aksiomatskih. Za prostor večteric $\mathbb{R}^n$, na primer ve, da je n-razsežni vektorski prostor.

Ko smo še mi hodili v šolo, smo šteli

$$1,\ 2 \text{ in več} \tag{1}$$

Enica je pomenila Matematiko I in funkcije ene spremenljivke, 2 in več pa Matematiko II in funkcije dveh ali več spremenljivk. Šteli smo tudi v levo, toda vmes je bil visok zid z globokima jarkoma ob strani



(2)

Ničla tostran zidu je pomenila gimnazijo in nič spremenljivk. Vse je obstalo, nič se ni spreminjalo, povsod so bile same konstante. In koliko jih je bilo, na vsaki strani logaritemskih tablic po tristo! Zato smo jih tudi ogovarjali spoštljivo: logaritmi. Edninsko rabo logaritem smo spoznali šele na univerzi. Kdor je preplaval oba jarka, preplezal zid in prišel suh iz vode, je zvedel, da je logaritem funkcija.

Danes — od tod dalje ne berite — štejemo drugače

$$1,\ n,\ \infty \tag{3}$$

Mislimo pa: enorazsežni, večrazsežni, neskončnorazsežni prostor. Spremenljivka (ta je ena sama) teče pač enkrat po $\mathbb{R}$, drugič po $\mathbb{R}^n$, tretjič po kakem neskončnorazsežnem prostoru. Vse to bruc-uporabnik, v moji šoli fizik, sreča v prvem letu. Meje v (3) so zabrisane, 1 je posebni (pa čeprav prav posebni) primer n, n je lahko (zgodi se pač) tudi ∞. In še — zame najlepše, za druge gvišna smrt — zidu ni več in jarkov ne. Enica v (3) se je razlezla daleč v srednjo šolo, tu in tam je za seboj potegnila 2 in 3. Visoka šola se lahko krepkeje opre na srednjo in seže dalj. Osnovni tečaj matematike za uporabnike (od fizikov do vsakršnih tehnikov) skriva velike notranje rezerve. Odvod ni zadnja med njimi.

Kaj je, kar odvajamo, in kako si to predstavljamo

Ko bruca pripeljemo do odvoda, že dobro pozna preslikave med večrazsežnimi prostori. Seznanimo se z njimi še mi. Vzemimo preslikavo s startnim prostorom $\mathbb{R}^m$ in s ciljnim prostorom $\mathbb{R}^n$

$$f : \mathbb{R}^m \to \mathbb{R}^n \qquad f : x \mapsto f(x) \tag{4}$$

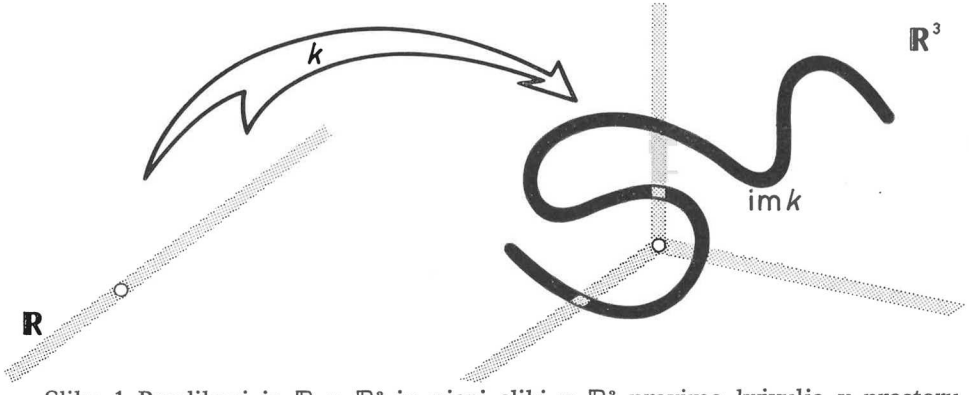
Na široko, v koordinatah, je to n funkcij m spremenljivk

$$\begin{Vmatrix} x_1 \\ x_2 \\ \dots \\ x_m \end{Vmatrix} \mapsto \begin{Vmatrix} f_1(x_1, x_2, \dots, x_m) \\ f_2(x_1, x_2, \dots, x_m) \\ \dots\dots\dots\dots\dots \\ f_n(x_1, x_2, \dots, x_m) \end{Vmatrix} \tag{5}$$

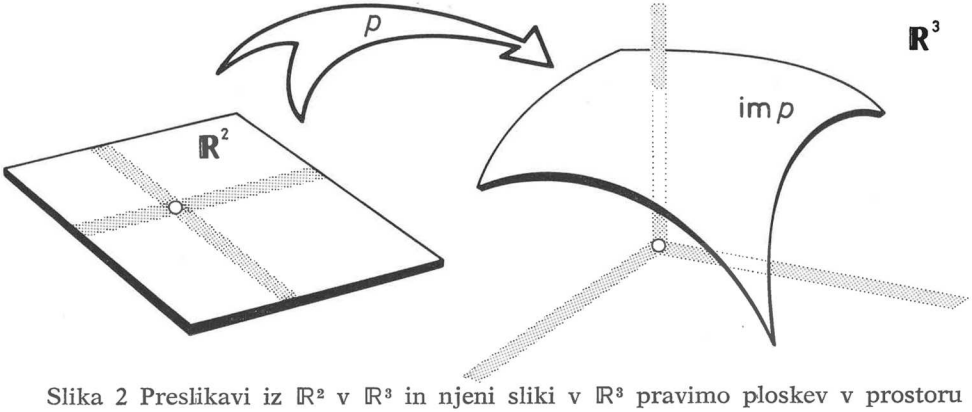
Nazorne pripomočke, s katerimi pričaramo preslikavo (4), iščemo v prostorih, med katerima slika, in v njunem premem produktu. Nazorni pripomoček je že spet — množica. Množica pač, ki jo znamo v kakem preprostem primeru videti.

V ciljnem prostoru $\mathbb{R}^n$ leži *slika* (image) preslikave f, množica njenih vrednosti

$$\operatorname{im} f = \{y \ ; \ y = f(x)\} \tag{6}$$



Slika 1 Preslikavi iz $\mathbb{R}$ v $\mathbb{R}^3$ in njeni sliki v $\mathbb{R}^3$ pravimo krivulja v prostoru



Slika 2 Preslikavi iz $\mathbb{R}^2$ v $\mathbb{R}^3$ in njeni sliki v $\mathbb{R}^3$ pravimo ploskev v prostoru

V preprostih zgledih lahko sliko narišemo. Taki zgledi so pač preslikave med prostori nizkih razsežnosti. Najprej sprejmimo tradicionalne oznake: enorazsežno spremenljivko označimo s t, dvorazsežno z urejenim parom (u, v) ali z ustreznim koordinatnim stolpcem, trorazsežni spremenljivki pa izberimo vektorski znak, krajevni vektor $\mathbf{r}$ v $\mathbb{R}^3$. V kanonski bazi je to pač koordinatni stolpec, s koordinatami x, y, z, če bo treba.

Začnimo s preslikavama

$$k : \mathbb{R} \to \mathbb{R}^3 \qquad k : t \mapsto \mathbf{r}(t) \tag{7}$$

$$p : \mathbb{R}^2 \to \mathbb{R}^3 \qquad p : (u, v) \mapsto \mathbf{r}(u, v) \tag{8}$$

Slika prve je krivulja, slika druge pa ploskev v prostoru. Tako se pač dogovorimo. Včasih je raba še bolj ohlapna: kar preslikavi (7) pravimo *krivulja* in preslikavi (8) *ploskev*.*

Fizikalni pogled na preslikavo (7) je ostrejši, v njej vidi gibanje, krivulja — slika je tir gibanja, iz (7) pa preberemo še vozni red, v vsakem trenutku t lahko zvemo, kje na tiru je gibajoča se točka.

Svinčnik kdaj laže seže v startni prostor. V njem rišemo inverzne slike množic. Inverzna slika množice $\mathcal{M} \subset \mathbb{R}^n$ je množica $f^{-1}\mathcal{M} \subset \mathbb{R}^m$, ki jo f preslika v $\mathcal{M}$

$$f^{-1}\mathcal{M} = \{x\,;\, f(x) \in \mathcal{M}\} \tag{9}$$

Najbolj zgovorne so inverzne slike enotočkastih množic — *nivojnice* ali *točkovnice* preslikave f

$$f^{-1}\{b\} = \{x\,;\, f(x) = b\} \tag{10}$$

Z drugimi besedami: Točkovnica $f^{-1}\{b\}$ je (najobsežnejša) množica, na kateri zavzame f vrednost b. In še: Na točkovnici $f^{-1}\{b\}$ je f konstanta, enaka b.

Po običajni definiciji preslikave so točkovnice disjunktne množice. Če so vse točkovnice enotočkaste, je f obrnljiva; definiramo lahko inverzno preslikavo f^{-1}. Unija vseh točkovnic je obratna (inverzna) slika preslikave,** $f^{-1}\,\mathbb{R}^n$.

Kak zgled prav gotovo poznamo, če ne drugega, nivojnice norme

$$\mathbb{R}^3 \to \mathbb{R} \qquad \mathbf{r} \mapsto |\mathbf{r}| \tag{11}$$

Nivojnica $f^{-1}\{b\}$ je obla s polmerom b, če je $b > 0$; je enotočkasta množica $\{0\}$, če je $b = 0$; in je prazna, če je $b < 0$.

Nivojnice so lahko bolj muhaste, na sliki 3 vidimo Cayleyev ali Whitneyev dežnik, $f^{-1}\{0\}$ za

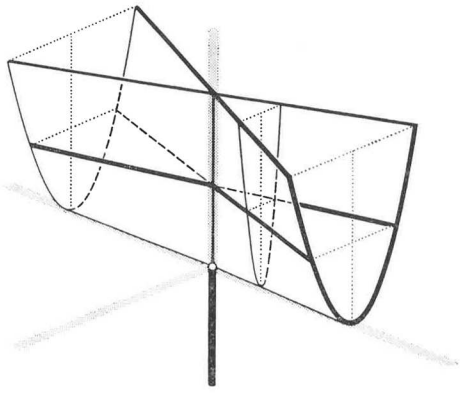
$$f : \mathbb{R}^3 \to \mathbb{R} \qquad f : (x, y, z) \mapsto x^2 - y^2 z \tag{12}$$

---

* Seveda, ožje teorije zahtevajo od obeh preslikav kaj več. Topologija prizna le tisto krivuljo ali ploskev, ki ustreza zvezni preslikavi (zvezni pač v vsaki točki, kjer je definirana). Diferencialna geometrija in analiza obravnavata le (večkrat) odvedljive preslikave, svoje prve korake pa usmerjata le med gladke — odvedljive in v vsaki točki regularne (glej (48)) — preslikave.

** Z drugo besedo: definicijsko območje ali domena. Preslikavo bomo vselej zapisali, kakor da je definirana na vsem začetnem prostoru, za vse pojme in račune, kar jih bomo srečali, pa bo dovolj, da definicijsko območje obsega okolico izbrane točke. (Izbrani točki bo največkrat ime a.)

Oba zgleda, (11) in (12), slikata v $\mathbb{R}$. Spomnimo se, da pravimo takim preslikavam v geometriji in v fiziki *skalarna polja*, v linearni algebri in v funkcionalni analizi pa *funkcionali*. Za klasično analizo je funkcional ali skalarno polje funkcija več spremenljivk iz (1). Zanjo ima stolpec na desni strani (5) eno samo vrstico.



Slika 3 Whitneyev ali Cayleyev dežnik, množica z enačbo $x^2 - y^2 z = 0$. Presek z ravnino $z = c$ je: par premic, če je $c > 0$, dvakrat šteta ordinatna os, če je $c = 0$, in točka $(0, 0, c)$, če je $c < 0$. Presek z ravnino $y = c$, $c \neq 0$, je parabola, tem ožja, čim bliže osi (z) sečemo dežnik

Preslikavo (4) lahko upodobimo še na tretji način, z njenim **grafom**, z množico graf $f \subset \mathbb{R}^m \times \mathbb{R}^n$

$$\text{graf } f = \{(x, y) \ ; \ y = f(x)\} = \{(x, f(x)) \ ; \ x \in \mathbb{R}^m\} \tag{13}$$

Tisto reč, ki ji v nazorni geometriji pravimo ploskev v prostoru, pričaramo v analizi na tri načine. Izbirajmo:

Ploskev je slika preslikave $\mathbb{R}^2 \to \mathbb{R}^3$.
Ploskev je točkovnica preslikave $\mathbb{R}^3 \to \mathbb{R}$
Ploskev je graf preslikave $\mathbb{R}^2 \to \mathbb{R}$.

Katera od teh trditev je najsplošnejša, najbolj res? Nobena. Pravi odgovor zvemo v teoriji mnogoterosti, kar pa spet zahteva aksiome, pa saj ga ne bomo potrebovali. Pokažimo le, da je graf najmanj splošen, predelamo ga lahko bodisi v sliko (druge preslikave) bodisi v točkovnico (tretje preslikave).

Vzemimo (4). Priredimo ji dve novi preslikavi, F in Φ. Prva naj startni prostor dvigne v premi produkt obeh prostorov, druga naj premi produkt spusti v ciljni prostor

$$F : \mathbb{R}^m \to \mathbb{R}^m \times \mathbb{R}^n \qquad F : x \mapsto (x, f(x)) \tag{14}$$

$$\Phi : \mathbb{R}^m \times \mathbb{R}^n \to \mathbb{R}^n \qquad \Phi : (x, z) \mapsto f(x) - z \tag{15}$$

Očitno je

$$\text{graf } f = \text{im } F \qquad \text{graf } f = \Phi^{-1}\{0\} \tag{16}$$

Pomožni preslikavi narišimo skupaj

$$\begin{array}{ccc} & \mathbb{R}^m \times \mathbb{R}^n & \\ {\scriptstyle F}\nearrow & & \searrow{\scriptstyle \Phi} \\ \mathbb{R}^m & & \mathbb{R}^n \end{array} \tag{17}$$

Kaj neki je njuna superpozicija?

Predavanja iz matematike so v prvem letniku fizike zasnovana tako, da teče linearna algebra vzporedno z analizo. Zato lahko bruc kar sam od sebe navrže še linearne zglede (če jih ne pozna že iz srednje šole). Vzemimo preslikavo

$$A : \mathbb{R}^m \to \mathbb{R}^n \tag{18}$$

(Kaj je to, povedo aksiomi, daleč naokrog se jim izognimo!) Bruc ve, da točkovnico $A^{-1}\{0\}$ za linearno preslikavo odlikujemo s posebnim imenom, *jedro* (kernel) ji pravimo, in označimo

$$A^{-1}\{0\} = \ker A \tag{19}$$

Slika im A je podprostor v ciljnem prostoru $\mathbb{R}^n$, jedro $\ker A$ je podprostor v startnem prostoru, graf A pa je podprostor v njunem premem produktu.

Kaj pa je točkovnica $A^{-1}\{b\}$, če je $b \neq 0$? Točka v njej, $x \in A^{-1}\{b\}$, zadošča enačbi (sistemu enačb) $Ax = b$. Točke iz jedra rešijo homogeno enačbo $Ax = 0$. Brž ko poznamo jedro, potrebujemo pri izbranem $b \neq 0$ le še eno rešitev nehomogene enačbe. Naj bo a taka rešitev, $Aa = b$. Tedaj

$$A^{-1}\{b\} = a + \ker A$$

Z besedami: Točkovnica $A^{-1}\{b\}$ je afini prostor nad jedrom preslikave A. (*Afini prostor* nad vektorskim prostorom definiramo tako, kakor smo definirali ravnino in trorazsežni evklidski prostor v berilih.)***

Za zgled vzemimo v $\mathbb{R}^3$ skalarno množenje s konstantnim vektorjem

$$\mathbb{R}^3 \to \mathbb{R} \qquad \mathbf{r} \mapsto \mathbf{a} \cdot \mathbf{r} \tag{20}$$

To je pač linearni funkcional ali linearno skalarno polje. Njegovo jedro sestavljajo vektorji, ki so pravokotni na $\mathbf{a}$. Brž ko je $\mathbf{a} \neq 0$, je jedro funkcionala (20) ravnina, ki gre skozi 0 in ima vektor $\mathbf{a}$ na normali. V število $b \in \mathbb{R}$ pa (20) preslika vse vektorje, ki zadoščajo enačbi $\mathbf{a} \cdot \mathbf{r} = b$. Naj bo $\mathbf{r}_0$ eden med njimi, $\mathbf{a} \cdot \mathbf{r}_0 = b$. V b se tedaj preslika z (20) vsak $\mathbf{r}$, ki zadošča enačbi $\mathbf{a} \cdot (\mathbf{r} - \mathbf{r}_0) = 0$.

Nivojnica linearnega skalarnega polja (20) je torej ravnina (skozi $\mathbf{r}_0$), ki je vzporedna jedru. Nivojnice polja (20) sestavljajo šop vzporednih ravnin.

Namesto linearne preslikave (18) opazujmo afino

$$f : \mathbb{R}^m \to \mathbb{R}^n \qquad f : x \mapsto Ax + a \tag{21}$$

*** Ponovimo z drugimi besedami: Afini prostor nad vektorskim prostorom $\mathscr{V}$ je množica (točk) $\mathscr{P}$, opremljena s surjektivnima preslikavama

$$\mathscr{P} \times \mathscr{P} \to \mathscr{V},\ (a, b) \mapsto a - b \qquad \mathscr{P} \times \mathscr{V} \to \mathscr{P},\ (a, \mathbf{v}) \mapsto a + \mathbf{v}$$

ki zadoščata aksiomom:

$$a - a = 0 \qquad (a - b) + (b - a) = 0 \qquad (a - b) + (b - c) + (c - a) = 0$$
$$(a + \mathbf{v}) - a = \mathbf{v}$$

Afinemu prostoru $\mathscr{P}$ pripišemo obseg skalarjev in razsežnost vektorskega prostora $\mathscr{V}$.

Naj bo $a \in \mathscr{P}$ in $\mathscr{M} \subset \mathscr{V}$. Z $a + \mathscr{M}$ označimo tedaj množico vseh točk $a + \mathbf{v}$, kjer $\mathbf{v}$ preteče $\mathscr{M}$. Če je $\mathscr{M}$ podprostor v $\mathscr{V}$, imenujemo $a + \mathscr{M}$ podprostor v afinem prostoru $\mathscr{P}$ ali kar afini podprostor skozi točko a. Razsežnost podprostora $a + \mathscr{M}$ je spet razsežnost vektorskega podprostora $\mathscr{M}$.

Slika afine preslikave (21) je afini podprostor v $\mathbb{R}^n$, vzporeden sliki linearne preslikave A. Prav tako je s točkovnicami in z grafom afine preslikave.

Preslikave sestavljamo. Imejmo dve preslikavi, druga naj začne, kjer prva konča

$$g : \mathbb{R}^l \to \mathbb{R}^m \qquad f : \mathbb{R}^m \to \mathbb{R}^n \tag{22}$$

Z njima sestavimo superpozicijo $f \circ g$, ki gre naravnost iz $\mathbb{R}^l$ v $\mathbb{R}^n$

$$f \circ g : \mathbb{R}^l \to \mathbb{R}^n \tag{23}$$

Računsko plat sestavljanja dobro poznamo, oglejmo si ga še na sliki. Vse, kar moramo opaziti, je

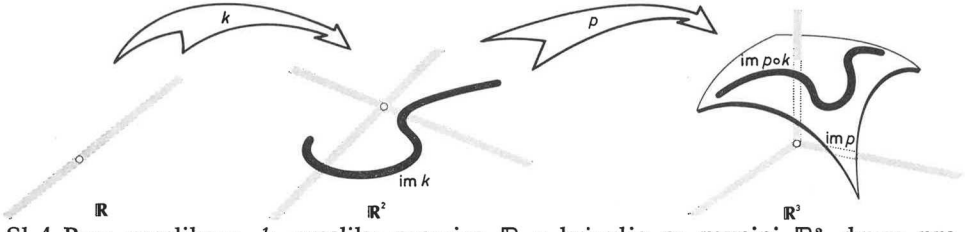
$$\operatorname{im} f \circ g \subset \operatorname{im} f \tag{24}$$

Dokaz je preprost: Elementu $z \in \operatorname{im} f \circ g$ najdemo x, da je $z = (f \circ g)(x)$, tedaj je $y = g(x)$ tak element, da je $z = f(y)$. Vsak z iz $\operatorname{im} f \circ g$ leži v $\operatorname{im} f$. Res je (24).

Za zgled, kar na sliki, sestavimo ravninsko krivuljo in ploskev v prostoru. Njuna superpozicija je prostorska krivulja

$$k : \mathbb{R} \to \mathbb{R}^2 \qquad p : \mathbb{R}^2 \to \mathbb{R}^3 \qquad p \circ k : \mathbb{R} \to \mathbb{R}^3$$

Zanju preberemo (24) takole: krivulja $p \circ k$ leži na ploskvi $\operatorname{im} p$. Ali: superpozicija $p \circ k$ je krivulja na ploskvi p.

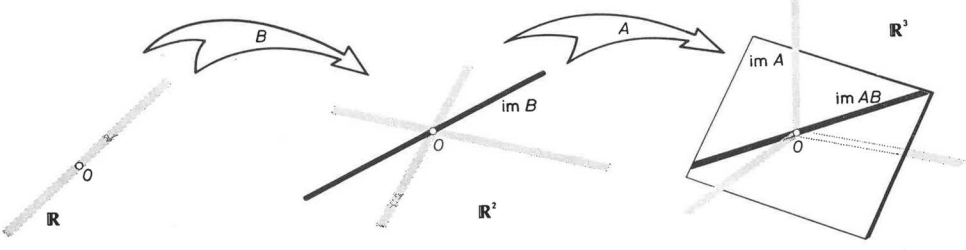


Sl. 4 Prva preslikava, k, preslika premico $\mathbb{R}$ v krivuljo na ravnini $\mathbb{R}^2$, druga preslikava, p, preslika ravnino $\mathbb{R}^2$ na ploskev v prostoru $\mathbb{R}^3$. Superpozicija obeh preslika premico $\mathbb{R}$ v prostorsko krivuljo $\operatorname{im} p \circ k$, ki leži na ploskvi $\operatorname{im} p$

Superpozicijo linearnih preslikav označimo kar s praznim znakom in ji rečemo produkt. Naj bosta A in B linearni preslikavi

$$B : \mathbb{R}^l \to \mathbb{R}^m \qquad A : \mathbb{R}^m \to \mathbb{R}^n$$

Njun produkt AB slika iz $\mathbb{R}^l$ v $\mathbb{R}^n$ linearno, (24) preberemo z besedami: Podprostor $\operatorname{im} AB$ leži v podprostoru $\operatorname{im} A$. Za zgled naj bo kar slika. Ali je vselej tako, kot je narisano?



Sl. 5 Linearna preslikava B preslika $\mathbb{R}$ v premico na ravnini $\mathbb{R}^2$, linearna preslikava A pa $\mathbb{R}^2$ na ravnino v $\mathbb{R}^3$. Slika zgovorno pove, kaj napravi z $\mathbb{R}$ produkt AB

Preprosto nazorno spoznanje (24) bo eden temeljnih kamnov naše razmišljave. Pripravimo si še drugega, ki govori o sliki in o inverzni sliki.

Vzemimo spet preslikavi (22) in inverzno sliko njune superpozicije. Iz $(f \circ g)(x) = b \Leftrightarrow f(g(x)) = b \Leftrightarrow g(x) \subset f^{-1}\{b\}$ povzamemo

$$\operatorname{im} g \subset f^{-1}\{b\} \Leftrightarrow \operatorname{im} f \circ g = \{b\} \tag{25}$$

Kdaj pravimo, da je preslikava v točki odvedljiva, in kaj je njen odvod

Imejmo

$$f : \mathbb{R}^m \to \mathbb{R}^n \qquad f : x \mapsto f(x) \tag{26}$$

Lepša, bolj ubrana bi bila teorija, če bi stopili za korak v splošnejše, vzeli bi preslikavo med dvema afinima prostoroma, startni bi bil nad $\mathbb{R}^m$, ciljni nad $\mathbb{R}^n$. Vseeno ostanimo pri (26).

Pribijmo $a \in \mathbb{R}^m$, dodajmo mu vse mogoče $h \in \mathbb{R}^m$ in opazujmo, kako se s h premika slika. V prirastku vrednosti $f(a + h) - f(a)$ spreminjajmo le h. Brž ko se dá prirastek razdeliti v dva dela tako, da se prvi spreminja s h linearno, drugi pa gre proti 0 hitreje kot h, pravimo, da je f v a odvedljiva.

Ponovimo: (26) je odvedljiva v $a \in \mathbb{R}^m$, brž ko je

$$\mathbb{R}^m \to \mathbb{R}^n \qquad h \mapsto f(a + h) - f(a) = Ah + o(h) \tag{27}$$

Preslikava A je linearna, ostanek pa gre proti 0 hitreje kot h

$$A \in \operatorname{Lin}(\mathbb{R}^m, \mathbb{R}^n) \qquad \lim_{h \to 0} o(h)/|h| = 0$$

Linearni preslikavi A pravimo *odvod* preslikave f v točki a in jo označimo z $f'(a)$.

Ne prezrimo: Preslikavo (26), ki je odvedljiva v točki a, spremlja *linearna preslikava* $f'(a)$

$$f : \mathbb{R}^m \to \mathbb{R}^n \qquad f'(a) : \mathbb{R}^m \to \mathbb{R}^n \tag{28}$$

Z novo oznako še enkrat prepišimo (27)

$$f(a + h) - f(a) = f'(a)h + o(h) \tag{29}$$

Prvi člen na desni moramo znati prav prebrati, $f'(a)h \in \mathbb{R}^n$ je vektor, v katerega preslika linearna transformacija $f'(a)$ vektor h iz $\mathbb{R}^m$.

Prostora $\mathbb{R}^m$ in $\mathbb{R}^n$ napnimo na kanonski bazi. V izbranih bazah ustreza linearni preslikavi $f'(a)$ matrika, ki jo imenujemo po Jacobiju in jo označimo z $\operatorname{Jac} f(a)$. Bolj pikolovsko bi morali zapisati $(\operatorname{Jac} f)(a)$ in prebrati: *Jacobijeva matrika* preslikave f v točki a. Toda, kjer bi bilo pisanja preveč (na primer že v (30)), bomo šli v nasprotno smer in oznako oklestili do $\operatorname{Jac} f$. Točko a bomo zamolčali, pozabili pa ne. V vsem članku nas bo zanimal le odvod v posamezni točki.

Preslikavo (26) zapišimo na široko s (5), pa je njena Jacobijeva matrika

$$\operatorname{Jac} f = \begin{Vmatrix} \partial f_1/\partial x_1, & \partial f_1/\partial x_2, & \ldots, & \partial f_1/\partial x_m \\ \partial f_2/\partial x_1, & \partial f_2/\partial x_2, & \ldots, & \partial f_2/\partial x_m \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \partial f_n/\partial x_1, & \partial f_n/\partial x_2, & \ldots, & \partial f_n/\partial x_m \end{Vmatrix} \tag{30}$$

Elementom Jacobijeve matrike pravimo *parcialni odvodi*. V posebnih primerih — na primer v (32) in v (35) — bomo uporabljali zanje krajše oznake.

Kadar sta bazi pribiti, radi poistovetimo linearno preslikavo in ustrezno matriko. Tako ravnamo tudi z odvodom in z Jacobijevo matriko za (26)

$$f'(a) = \operatorname{Jac} f(a) \tag{31}$$

Vendar pazimo: Tudi ko sta bazi izbrani, moramo (31) prebrati drugače, kot je zapisano. Linearna preslikava $f'(a)$ ni matrika, ampak množenje (stolpcev iz $\mathbb{R}^m$) z matriko $\operatorname{Jac} f(a)$.

Preletimo nekaj zgledov. Začnimo s krivuljo v prostoru. Namesto s (7) jo zapišimo v koordinatah

$$k : \mathbb{R} \to \mathbb{R}^3 \qquad k : t \mapsto \begin{Vmatrix} x(t) \\ y(t) \\ z(t) \end{Vmatrix}$$

Ustrezna Jacobijeva matrika ima en sam stolpec. Ker je neodvisna spremenljivka t enorazsežna, označimo parcialne odvode na navaden način, s piko

$$\operatorname{Jac} k(a) = \begin{Vmatrix} \dot{x}(a) \\ \dot{y}(a) \\ \dot{z}(a) \end{Vmatrix} \tag{32}$$

V vektorski pisavi (7) zapišemo tudi Jacobijevo matriko (32) kot vektor

$$\operatorname{Jac} k(a) = \dot{\mathbf{r}}(a) \tag{33}$$

Toda pazimo: odvod — linearna preslikava $k'(a)$ je množenje (števila h) z vektorjem $\dot{\mathbf{r}}(a)$

$$k'(a) : h \mapsto h\dot{\mathbf{r}}(t) \tag{34}$$

Drugi zgled naj bo skalarno polje

$$f : \mathbb{R}^3 \to \mathbb{R} \qquad f : \begin{Vmatrix} x \\ y \\ z \end{Vmatrix} \mapsto f(x, y, z)$$

Jacobijeva matrika zanj ima eno samo vrstico

$$\operatorname{Jac} f(\mathbf{a}) = \|f_x(\mathbf{a}), f_y(\mathbf{a}), f_z(\mathbf{a})\| \tag{35}$$

Tudi vrstico obravnavamo kot vektor, imenujemo jo gradient skalarnega polja v točki $\mathbf{a}$ in jo označimo z $\operatorname{grad} f(a)$. Spet samo zato, ker sta bazi pribiti, identificiramo

$$f'(\mathbf{a}) = \operatorname{grad} f(\mathbf{a}) = \operatorname{Jac} f(\mathbf{a}) \tag{36}$$

In pazimo: odvod $f'(\mathbf{a})$ — linearna preslikava iz $\mathbb{R}^3$ v $\mathbb{R}$ — je skalarno množenje (vektorja $\mathbf{h}$) z vektorjem $\operatorname{grad} f(\mathbf{a})$

$$f'(\mathbf{a}) : \mathbf{h} \mapsto \mathbf{h} \,.\, \operatorname{grad} f(\mathbf{a}) \tag{37}$$

Za tretji zgled naj bo ploskev v prostoru. Tudi to zapišimo najprej v koordinatah

$$p : \mathbb{R}^2 \to \mathbb{R}^3 \qquad p : \begin{Vmatrix} u \\ v \end{Vmatrix} \mapsto \begin{Vmatrix} x(u, v) \\ y(u, v) \\ z(u, v) \end{Vmatrix}$$

Ustrezna Jacobijeva matrika ima dva stolpca in tri vrstice

$$\operatorname{Jac} p = \begin{Vmatrix} x_u , x_v \\ y_u , y_v \\ z_u , z_v \end{Vmatrix}$$

V vektorskem zapisu (8) bomo Jacobijevo matriko videli kot par vektorjev — parcialnih odvodov krajevnega vektorja

$$\operatorname{Jac} p = \|\mathbf{r}_u , \mathbf{r}_v\| \tag{38}$$

Odvod $p'(a)$ kot linearna preslikava je pač množenje (stolpca h, k) z matriko

$$p'(\mathbf{a}) : \begin{Vmatrix} h \\ k \end{Vmatrix} \mapsto \begin{Vmatrix} x_u , x_v \\ y_u , y_v \\ z_u , z_v \end{Vmatrix} \begin{Vmatrix} h \\ k \end{Vmatrix} = \begin{Vmatrix} hx_u + kx_v \\ hy_u + ky_v \\ hz_u + kz_v \end{Vmatrix}$$

V stolpcu na desni razpoznamo linearno kombinacijo vektorjev (38). Ponovimo

$$p'(\mathbf{a}) : \begin{Vmatrix} h \\ k \end{Vmatrix} \mapsto h\,\mathbf{r}_u + k\,\mathbf{r}_v \tag{39}$$

Pripravimo si še izrek o odvajanju superpozicije. Imejmo preslikavi

$$g : \mathbb{R}^l \to \mathbb{R}^m \qquad f : \mathbb{R}^m \to \mathbb{R}^n$$

Brž ko je preslikava g odvedljiva v točki $a \in \mathbb{R}^l$, preslikava f pa v točki $g(a) = b \in \mathbb{R}^m$, je superpozicija $f \circ g$ odvedljiva v točki a in

$$(f \circ g)'(a) = f'(b)g'(a) \tag{40}$$

Dokaz ni dosti drugačen od tistega za enorazsežni primer, prinese kvečjemu kako tehnično težavo.**** Pomembneje je, da znamo (40) prebrati. Na desni je produkt linearnih preslikav, ta pa ni komutativen, zato moramo paziti na vrstni red faktorjev. Pisava in branje (40) pa tudi nekaj prikrijeta. Pozabimo na dogovor, da pravimo superpoziciji linearnih preslikav produkt. Tedaj povemo lepše:

Odvod superpozicije je superpozicija odvodov

$$(f \circ g)'(a) = f'(b) \circ g'(a)$$

Najraje bomo odvajanje superpozicije opisali z dvema komutativnima trikotnikoma preslikav. V prvega zapišimo definicijo superpozicije, v drugega — v trikotnik linearnih preslikav — pa izrek o odvajanju superpozicije

---

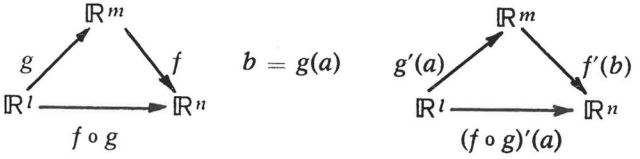
**** Imenujmo $g'(a) = A$ in $f'(b) = B$. Razčlenimo $g(a + h) = b + k$, ocenimo $k = Ah + o(h)$, računajmo

$$(f \circ g)\ (a + h) - (f \circ g)\ (a) = f(g(a + h))) - f(b) = f(b + k) - f(b) = Bk + o(k)$$

Povzemimo

$$(f \circ g)\ (a + h) - (f \circ g)\ (a) = BAh + Bo(h) + o(k)$$

Pokazati moramo le še, da je $Bo(h) + o(k) = o(h)$. To delo bo opravil bralec sam (ali pa bo odprl [4] na strani 341) in tako do konca dokazal (40).



(41)

Izrek ponovimo še v koordinatah: *Jacobijeva matrika superpozicije je produkt Jacobijevih matrik*

$$\text{Jac}\,(f \circ g)\,(a) = \text{Jac}\,f(b)\,\text{Jac}\,g(a)$$

Najpomembnejši posebni primer bo $l = 1$, ko je prva preslikava g krivulja v m-razsežnem prostoru

$$k : \mathbb{R} \to \mathbb{R}^m \qquad k : t \mapsto k(t)$$

Superpozicija $f \circ k$ je krivulja v n-razsežnem prostoru. Odvod krivulje je množenje z vektorjem; bodimo površni, pa nam bo odvod krivulje kar vektor, odvod krivulje k vektor $k'(a)$, odvod krivulje $f \circ k$ pa vektor $(f \circ k)'(a)$. Iz (40) preberemo: Vektor $(f \circ k)'(a)$ dobimo tako, da vektor $k'(a)$ preslikamo z linearno transformacijo $f'(b)$

$$(f \circ k)'(a) = f'(b)k'(a) \tag{42}$$

Za prvi zgled vzemimo krivuljo na ploskvi, $m = 2$, $n = 3$. Vektor $k(t)$ na ravnini zapišimo s koordinatnim stolpcem u, v, točko v trorazsežnem prostoru pa s krajevnim vektorjem $\mathbf{r}$. Stolpec $u(a)$, $v(a)$ označimo z $\mathbf{b}$. Tedaj po (38) in tako kot v (32)

$$p'(\mathbf{b}) = \|\mathbf{r}_u(\mathbf{b}) \,,\, \mathbf{r}_v(\mathbf{b})\| \qquad k'(a) = \left\| \begin{matrix} \dot{u}(a) \\ \dot{v}(a) \end{matrix} \right\|$$

Od tod pa po (42) in po prav takem računu, kot nas je pripeljal do (39)

$$p'(\mathbf{b})\, k'(a) = \dot{u}(a)\, \mathbf{r}_u(\mathbf{b}) + \dot{v}(a)\, \mathbf{r}_v(\mathbf{b}) \tag{43}$$

V klasičnem zapisu

$$\frac{\mathrm{d}}{\mathrm{d}t}\mathbf{r}(u(t),\ v(t)) = \dot{u}(t)\, \mathbf{r}_u(u(t),\ v(t)) + \dot{v}(t)\, \mathbf{r}_v(u(t),\ v(t)) \tag{44}$$

Za zadnji zgled naj bo $m = 3$ in $n = 1$. Preslikava f je skalarno polje, superpozicija $f \circ k$ pa meri vrednost polja vzdolž krivulje. Odvod (Jacobijeva matrika) krivulje je stolpec (32), odvod skalarnega polja je vrstica (35), njun produkt pač

$$f'(\mathbf{b})\, k'(a) = \dot{x}(a)\, f_x(\mathbf{b}) + \dot{y}(a)\, f_y(\mathbf{b}) + \dot{z}(a)\, f_z(\mathbf{b}) \tag{45}$$

Na desni je skalarni produkt vrstice grad f(**b**) in stolpca $\dot{\mathbf{r}}(a)$ ali kar skalarni produkt dveh vektorjev

$$f'(\mathbf{b})\, k'(a) = \dot{\mathbf{r}}(a) \,.\, \text{grad}\, f(\mathbf{b}) \tag{46}$$

V klasičnem zapisu

$$\frac{\mathrm{d}}{\mathrm{d}t} f(\mathbf{r}(t)) = \dot{\mathbf{r}}(t) \,.\, \text{grad}\, f(\mathbf{r}(t)) \tag{47}$$

Slika in nivojnice odvoda

Vemo, kaj odvajamo; kar odvajamo, si znamo predstavljati, ponazorimo si še odvod.

Ali naj še enkrat ponovimo, da govorimo o preslikavi f, ki je odvedljiva v točki a?

Preslikava f slika iz $\mathbb{R}^m$ v $\mathbb{R}^n$, med istima postoroma deluje tudi linearna preslikava $f'(a)$. Začnimo z nazorno predstavo v ciljnem prostoru, tam leži slika $\operatorname{im} f$, tam bomo našli tudi sliko $\operatorname{im} f'(a)$. Slika linearne preslikave je podprostor v $\mathbb{R}^n$, razsežnosti slike pravimo *rang* linearne preslikave, rang ne more preseči dimenzij prostorov, med katerima slika

$$\operatorname{rang} f'(a) \leqq \min\{m, n\}$$

Točka a je *pravilna (regularna)* za preslikavo f, če ima odvod v njej maksimalni možni rang

$$a \text{ pravilna za } f \Leftrightarrow \operatorname{rang} f'(a) = \min\{m, n\} \tag{48}$$

Točka, v kateri je rang nižji, je *kritična* ali *singularna* za f.

Singularne točke so zanimivejše od regularnih, toda v naš spis ne sodijo. Ustavimo se le ob posebnih zgledih $m = 1$ ali $n = 1$. Tedaj je največji možni rang odvoda enak 1, nižji od 1 je le rang 0. Linearna preslikava z rangom 0 je sama 0. Brž ko je $m = 1$ ali $n = 1$, je odvod v singularni točki enak 0, $f'(a) = 0$. To velja za krivulje v prostoru ($m = 1$), za skalarna polja nad njim ($n = 1$) in seveda za realne funkcije realne spremenljivke ($m = n = 1$).

Odslej nas bodo zanimale le regularne točke, ko bomo rekli a, bomo mislili (48). Imenujmo

$$r = \operatorname{rang} f'(a)$$

Linearna preslikava $f'(a)$ preslika prostor $\mathbb{R}^m$ v r-razsežni podprostor prostora $\mathbb{R}^n$. Vsi podprostori pa gredo skozi točko 0. Ko a preteče vse regularne točke, preteče $\operatorname{im} f'(a)$ šop r-razsežnih podprostorov v $\mathbb{R}^n$ (ni rečeno, da je to šop vseh takih podprostorov).

Radi bi kar se da hitro kaj narisali, zato se spustimo k enostavnemu zgledu, k ploskvi v prostoru

$$p : \mathbb{R}^2 \to \mathbb{R}^3 \qquad p : (u, v) \mapsto \mathbf{r}(u, v) \tag{49}$$

Njeno Jacobijevo matriko — odvod — zapišemo s parom vektorjev

$$p'(\mathbf{a}) = \|\mathbf{r}_u(\mathbf{a}),\ \mathbf{r}_v(\mathbf{a})\|$$

V regularni točki je rang Jacobijeve matrike enak 2, vektorja $\mathbf{r}_u$ in $\mathbf{r}_v$ sta linearno neodvisna, slika odvoda, $\operatorname{im} f'(a)$, je ravnina skozi izhodišče, napeta na vektorja $\mathbf{r}_u(\mathbf{a})$ in $\mathbf{r}_v(\mathbf{a})$.

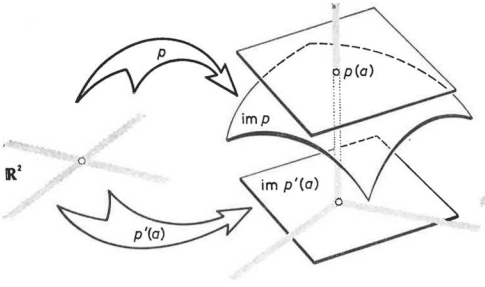
Množici regularnih točk preslikave (49) ustreza v $\mathbb{R}^3$ šop ravnin skozi izhodišče. Na vsako ravnino postavimo normiran normalni vektor $\boldsymbol{\nu}$, da bo trirob $\mathbf{r}_u$, $\mathbf{r}_v$, $\boldsymbol{\nu}$ pozitivno orientiran. Namesto ravnin rišimo njihove normale $\boldsymbol{\nu}$, tako dobimo Gaussovo upodobitev ploskve (49) na oblo.

Ponovimo kar s splošnimi besedami, do kod smo prišli. Slike odvodov $f'(a)$ gredo skozi točko 0. Razženimo jih, tisto, ki ustreza točki a, premaknimo vzporedno za $f(a)$. Od linearne preslikave $f'(a)$ se zatecimo k afini

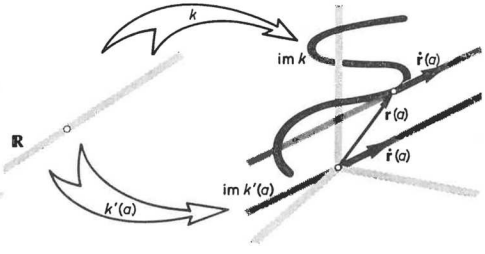
$$\mathbb{R}^m \to \mathbb{R}^n \qquad h \mapsto f(a) + f'(a)\,h \tag{50}$$

Slika afine preslikave (50) je r-razsežni afini podprostor, ki gre skozi točko $f(a)$ in je vzporeden podprostoru $\operatorname{im} f'(a)$. Sliki preslikave (50) pravimo *tangentni prostor* na $\operatorname{im} f$ v točki $f(a)$.

V zgledu (49) torej vsako ravnino iz šopa slik $\operatorname{im} p'(\mathbf{a})$ vzporedno premaknemo tako, da gre skozi točko $\mathbf{r}(\mathbf{a})$ na ploskvi. Tako dobimo pač tangentno ravnino na ploskev.



Sl. 6 S p preslikamo $\mathbb{R}^2$ na ploskev v prostoru, s $p'(a)$ pa na ravnino skozi izhodišče. Ravnino vzporedno premaknimo za $p(a)$, pa dobimo tangentno ravnino na ploskev $\operatorname{im} p$ v točki $p(a)$. Tangentna ravnina je slika afine preslikave (glej I. str. ovitka)



Sl. 7 S k preslikamo $\mathbb{R}$ v prostorsko krivuljo, s $k'(a)$ pa v premico skozi izhodišče. Premico vzporedno premaknimo za $\mathbf{r}(a)$, tako dobimo tangento, ki se krivulje dotika v $\mathbf{r}(a)$. Odvod $\dot{\mathbf{r}}(a)$ je vektor na tangenti

Nič drugače ni s krivuljo. Tangenta, ki se je dotika v točki $\mathbf{r}(a)$, je slika afine preslikave

$$\mathbb{R} \to \mathbb{R}^3 \qquad h \mapsto \mathbf{r}(a) + h\dot{\mathbf{r}}(a)$$

Vektor $\dot{\mathbf{r}}(a)$ leži torej na tangenti skozi točko $\mathbf{r}(a)$.

Prav tako je s krivuljo v m-razsežnem prostoru, v točki $k(a)$ se je dotika slika afine transformacije

$$\mathbb{R} \to \mathbb{R}^m \qquad h \mapsto k(a) + k'(a)h$$

Najzanimivejše spoznanje pa nas čaka ob sestavljenem zgledu, ob krivulji $f \circ k$ v n-razsežnem prostoru. Ponovimo v mislih, kar smo zapisali s trikotnikoma (41), in zapišimo, kako je tedaj po (24) s slikami

$$\operatorname{im} f \circ k \subset \operatorname{im} f \qquad \operatorname{im} (f \circ k)'(a) \subset \operatorname{im} f'(b)$$

Sliki odvodov sta podprostora, premaknimo ju vzporedno, da dobimo afina podprostora skozi točko $f(b) = (f \circ k)\,(a)$

$$(f \circ k)\,(a) + \operatorname{im} (f \circ k)'(a) \subset f(b) + \operatorname{im} f'(b)$$

Z besedami: *Tangenta na krivuljo* $\operatorname{im} f \circ k$ *leži v tangentnem prostoru na* $\operatorname{im} f$.

Po oprijemljiv zgled stopimo navzdol k $m = 2$ in $n = 3$. Tedaj je $p \circ k$ krivulja na ploskvi im p, njena tangenta leži na tangentni ravnini ploskve. Na to smo že pripravljeni, vektor na tangenti, ki se krivulje im $p \circ k$ dotika v točki $p(b)$ — vektor $(p \circ k)'(a) = p'(b)\, k'(a)$ — smo v (43) razčlenili po baznih vektorjih ravnine, ki se ploskve im p dotika v isti točki.

Sl. 8 Krivulja na ploskvi, tangenta na krivuljo — na tangentni ravnini ploskve

Ozrimo se še nazaj, v startni prostor $\mathbb{R}^m$. Kaj o odvodu lahko tam zagledamo? V $\mathbb{R}^m$ leži jedro linearne preslikave $f'(a)$. Razsežnost jedra je $m - r$, to si sposodimo pri linearni algebri. Nivojnice linearne preslikave $f'(a)$ so afini podprostori, vzporedni ker $f'(a)$. Skozi točko $a \in \mathbb{R}^m$ poteka nivojnica preslikave $f'(a)$

$$a + \ker f'(a) \tag{51}$$

Naloga za vajo: V kaj preslika $f'(a)$ množico (51)?

Skozi točko a narišimo še nivojnico preslikave f

$$f^{-1}\{f(a)\} \tag{52}$$

Afini podprostor (51) se v točki a dotika nivojnice (52).

Tako se pač dogovorimo, dogovor pa podprimo z izrekom:

Tangente vseh krivulj, ki potekajo skozi a po točkovnici (52), *leže v afinem podprostoru* (51).

Imenujmo $f(a) = b$ in vzemimo krivuljo k, ki gre skozi točko a in leži na $f^{-1}\{b\}$. Brez škode denimo $k(0) = a$, iz (25) pa preberimo: krivulja im k leži na $f^{-1}\{b\}$ natanko takrat, ko je superpozicija $f \circ k$ konstantna

$$\text{im } k \subset f^{-1}\{b\} \Leftrightarrow \text{im } f \circ k = \{b\} \tag{53}$$

Odvod konstantne preslikave je enak 0, odvod superpozicije je superpozicija odvodov

$$(f \circ k)' = 0 \qquad\qquad (f \circ k)'(0) = f'(a)\, k'(0)$$

Prepišimo (53) za odvode

$$\text{im } f'(a) \circ k'(0) = \{0\} \Leftrightarrow \text{im } k'(0) \subset \ker f'(a) \tag{54}$$

Inverzna slika točke $\{0\}$ je pač jedro linearne preslikave $f'(a)$. Premaknimo podprostora v točko $k(0) = a$

$$k(0) + \text{im } k'(0) \subset a + \ker f'(a)$$

Izrek je dokazan. Z njim smo dobili nazorno oporo za odvod preslikave že v startnem prostoru. Ponovimo:

Tangentni prostor na nivojnico preslikave f v točki a je afini prostor nad jedrom odvoda $f'(a)$.

Najzanimivejši utegne biti odvod skalarnega polja

$$f : \mathbb{R}^3 \to \mathbb{R}$$

Videli smo, da je točka a regularna zanj, če je rang $f'(a)$ enak 1, razsežnost jedra je $m - r = 3 - 1 = 2$. Preslikava $f'(\mathbf{a})$ je to pot kar množenje z vektorjem grad $f(\mathbf{a})$

$$f'(\mathbf{a}) : \mathbf{h} \mapsto \mathbf{h} \,.\, \operatorname{grad} f(\mathbf{a})$$

Jedro preslikave $f'(\mathbf{a})$ je pravokotno na vektor grad $f(\mathbf{a})$. Zato:

Gradient grad $f(\mathbf{a})$ je pravokoten na nivojnico polja f, ki gre skozi točko $\mathbf{a}$.

Graf odvoda

$f : \mathbb{R}^m \to \mathbb{R}^n$ naj bo odvedljiva v točki a. Videli smo, da je tangentni prostor na sliko $\operatorname{im} f$ v točki a vzporeden sliki odvoda, $\operatorname{im} f'(a)$, tangentni prostor na točkovnico $f^{-1}\{f(a)\}$ pa jedru odvoda, $\ker f'(a)$. Ali se bomo kaj začudili, da je tangentni prostor na graf preslikave f v točki $(a, f(a))$ vzporeden grafu linearne preslikave $f'(a)$?

Graf preslikave je podmnožica, graf odvoda pa podprostor v $\mathbb{R}^m \times \mathbb{R}^n$. Ponovimo

$$\operatorname{graf} f'(a) = \{(h, f'(a)h) \,;\, h \in \mathbb{R}^m\} \tag{55}$$

Dokažimo: *Grafa preslikave f se v točki $(a, f(a))$ dotika afini podprostor* nad grafom odvoda $f'(a)$

$$(a, f(a)) + \operatorname{graf} f'(a) = \{(a + h, f(a) + f'(a)h) \,;\, h \in \mathbb{R}^m\} \tag{56}$$

Po dokaz pojdimo k že znanim rečem. V grafu preslikave f smo zagledali sliko, če smo le prav pogledali iz $\mathbb{R}^m$ v $\mathbb{R}^m \times \mathbb{R}^n$, ali pa točkovnico, če smo se ozrli na $\mathbb{R}^m \times \mathbb{R}^n$ iz $\mathbb{R}^n$. Pripravili smo preslikavi

$$\mathbb{R}^m \xrightarrow{F} \mathbb{R}^m \times \mathbb{R}^n \xrightarrow{\Phi} \mathbb{R}^n$$

Elementu iz startnega prostora smo rekli x, elementu iz ciljnega z (črko y smo preskočili prihodnjemu zgledu na ljubo). Elemente premega produkta pišimo kot urejene pare, kdaj pa kdaj pa kot stolpce ali bločne matrike. Preslikavi F in Φ smo definirali z

$$F : x \mapsto \begin{Vmatrix} x \\ f(x) \end{Vmatrix} \qquad \Phi : \begin{Vmatrix} x \\ z \end{Vmatrix} \mapsto f(x) - z \tag{57}$$

Videli smo, da je graf $f = \operatorname{im} F = \Phi^{-1}\{0\}$.

Ali znamo preslikavi (57) odvajati? Šlo bo, ko pripravimo prirastka njunih vrednosti. Prvo odvajamo v točki a, drugo v (a, c). Spremembo argumenta označimo prvič s h, drugič s h, l

$$F(a + h) - F(a) = \begin{Vmatrix} a + h \\ f(a + h) \end{Vmatrix} - \begin{Vmatrix} a \\ f(a) \end{Vmatrix} = \begin{Vmatrix} h \\ f(a + h) - f(a) \end{Vmatrix}$$

$$\Phi(a + h, c + l) - \Phi(a, c) = f(a + h) - (c + l) - f(a) + c = f(a + h) - f(a) - l$$

Upoštevajmo, da je f odvedljiva v a

$$F(a+h) - F(a) = \begin{Vmatrix} h \\ f'(a)h \end{Vmatrix} + o(h)$$

$$\Phi(a+h, c+l) - \Phi(a,c) = f'(a)h - l + o(h,l)$$

Res je F odvedljiva v a in Φ v (a,c). Hkrati opazimo, da je odvod $\Phi'(a,c)$ neodvisen od c, zato ga na kratko označimo kar s $\Phi'(a)$

$$F'(a) : h \mapsto \begin{Vmatrix} h \\ f'(a)h \end{Vmatrix} \qquad \Phi'(a) : \begin{Vmatrix} h \\ l \end{Vmatrix} \mapsto f'(a)h - l \tag{58}$$

Poglejmo z ene, poglejmo z druge, pa vidimo

$$\operatorname{im} F'(a) = \operatorname{graf} f'(a) = \ker \Phi'(a) \tag{59}$$

Res je, kar smo trdili v začetku: Tangentni prostor na graf f v točki a je pač afini prostor nad im $F'(a)$ ali nad ker $\Phi'(a)$, nazadnje tudi nad graf $f'(a)$. Tangentni prostor na graf f v točki a je (56).

(58) berimo še naprej. Odvoda $F'(a)$ in $\Phi'(a)$ označimo z bločnima matrikama, prvega s stolpcem, drugega z vrstico linearnih operatorjev

$$F'(a) = \begin{Vmatrix} \mathrm{Id}_m \\ f'(a) \end{Vmatrix} \qquad \Phi'(a) = \|f'(a), -\mathrm{Id}_n\| \tag{60}$$

Z Id_k smo označili identiteto v $\mathbb{R}^k$ (ali k-vrstno kvadratno matriko, ki ima po glavni diagonali enice, drugod pa ničle).

Očitno je $\Phi'(a)\,F'(a) = 0$. To nas ne sme presenetiti, saj je $\Phi \circ F = 0$, zato $\Phi'(a, f(a))\,F'(a) = 0$, odvod $\Phi'(a,c)$ pa neodvisen od c.

Poglejmo (59), poglejmo (60), pa se nam bo odprlo, kako se vidi tangentni prostor na graf od znotraj, kako od zunaj:

Tangentni prostor, ki se dotika grafa preslikave f v točki $(a, f(a))$, je napet na stolpce matrike $F'(a)$ in je pravokoten na vrstice matrike $\Phi'(a)$.

Za zgled vzemimo skalarno polje na ravnini

$$f : \mathbb{R}^2 \to \mathbb{R} \qquad f : (x,y) \mapsto f(x,y)$$

Polje naj bo odvedljivo v točki $(a,b) \in \mathbb{R}^2$. S tem zgledom v mislih smo preskakovali črke v abecedi. Kjer je bil v splošnem element a, bo v zgledu urejen par števil (a,b), element c pa bo postal število c. Po stari navadi označimo

$$f(a,b) = c \qquad f_x(a,b) = p \qquad f_y(a,b) = q$$

Gradient polja v točki (a,b) je torej vrstica

$$\operatorname{grad} f(a,b) = \|p, q\| \tag{61}$$

Matrika Id_m šteje dve vrstici, Id_n eno samo, odvoda (60) sta

$$F'(a) = \begin{Vmatrix} 1, 0 \\ 0, 1 \\ p, q \end{Vmatrix} \qquad \Phi'(a) = \|p, q, -1\| \tag{62}$$

Graf polja je ploskev v prostoru $\mathbb{R}^3 = \mathbb{R}^2 \times \mathbb{R}$, na njej leži točka (a,b,c). Tangentno ravnino na graf v (a,b,c) opišimo na tri načine, naprej kot graf

afine preslikave, (56). Tam, kjer je v splošnem a, zapišemo par a, b, kjer je bila vrednost $f(a)$, je $f(a, b) = c$. Prav tako je namesto h par (h, k), odvod $f'(a, b)$ je skalarno množenje z vrstico (61)

$$f'(a, b) : (h, k) \mapsto ph + qk$$

Nazadnje: Tangentna ravnina na graf f v točki (a, b, c) je graf afine preslikave

$$(h, k) \mapsto (a + h, b + k, c + ph + qk) \tag{63}$$

Dodajmo še: Tangentna ravnina na graf f gre skozi točko (a, b, c) in je napeta na stolpca matrike $F'(a)$, na

$$\begin{Vmatrix} 1 \\ 0 \\ p \end{Vmatrix} \quad \text{in} \quad \begin{Vmatrix} 0 \\ 1 \\ q \end{Vmatrix} \tag{64}$$

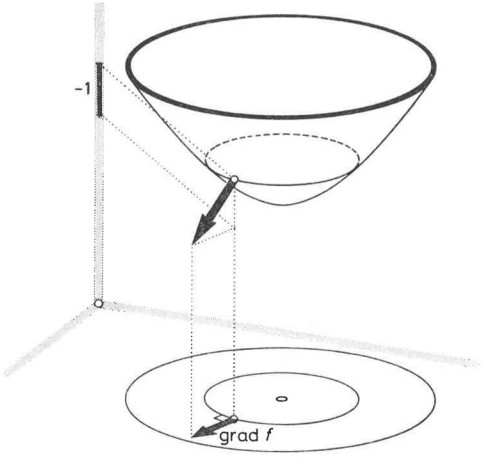
In: Tangentna ravnina na graf f gre skozi točko (a, b, c) in je pravokotna na vrstico $\Phi'(a)$, na

$$\|p, q, -1\| \tag{65}$$

Vsi trije opisi nas pripeljejo do istega spoznanja: Točka (x, y, z) na tangentni ravnini (na graf f skozi (a, b, c)) zadošča enačbi

$$z - c = p(x - a) + q(y - b) \tag{66}$$

Da je to res, bo — trikrat! — videl bralec sam.



Sl. 9 Graf skalarnega polja in tangentna ravnina naj. Koordinatna ravnina (x, y) je startni prostor, na njej rišemo nivojnice (točkovnice) polja
Dotikališče je (a, b, c). Presek grafa z ravnino $z = c$ je krivulja, vzporedna točkovnici $f^{-1}\{c\}$. Na normali grafa leži vektor, ki ima projekcijo na os (z) enako -1, projekcijo na ravnino (x, y) pa grad $f(a, b)$. Gradient je pravokoten na točkovnico

Zglede, ponovimo, smo izbirali tako, da je bila predstava kar se dá živa. Če je f slikala iz manj razsežnega v več razsežni prostor $(m < n)$, smo narisali sliko v ciljnem prostoru. Preslikavo iz več razsežnega v manj razsežni prostor $(m > n)$ smo si ponazorili s točkovnicami. Seveda smo lahko kaj narisali le, če sta bili obe razsežnosti dovolj majhni, 1, 2 ali 3. Kadar vsota obeh razsežnosti ni presegala 3, smo si pomagali še z grafom.

Prav na konec smo odrinili najpreprostejši zgled, $m = n = 1$. Enorazsežne množice niso tako zgovorne, zato le kdaj pa kdaj narišemo kako sliko ali točkovnico. Pomislimo na primer na linearno funkcijo (afino preslikavo)

$$f : \mathbb{R} \to \mathbb{R} \qquad f : x \mapsto kx + n \tag{67}$$

Dvoje je mogoče: ali je $k \neq 0$ ali pa $k = 0$. Prvič je $\operatorname{im} f = \mathbb{R}$, vse nivojnice pa so enotočkaste (zakaj že?). Drugič je slika enotočkasta, $\operatorname{im} f = \{n\}$, ves $\mathbb{R}$ pa je ena sama točkovnica, $f^{-1}\{n\} = \mathbb{R}$. Nariši še sliko in točkovnice za $x \mapsto \sin x$.

Slika in točkovnice so nas razočarale, vseeno pa bi si radi predstavili realno funkcijo

$$f : \mathbb{R} \to \mathbb{R} \qquad f : x \mapsto f(x) \tag{68}$$

En sam rešnji pripomoček nam lahko pomaga, graf. Ob njem si tudi ponazorimo odvod $f'(a)$. Denimo pač, da je f v a odvedljiva. Pomislimo še, da je identiteta v $\mathbb{R}$ kar množenje s številom 1, potem pa iz splošnega potegnimo posebno:

Tangento, ki se dotika grafa (v a odvedljive) funkcije (68) opišemo na tri načine:

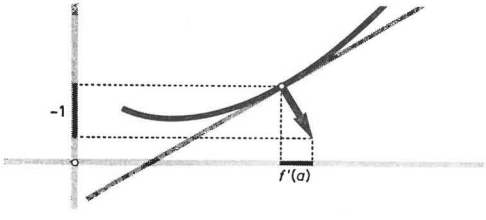
Tangenta je graf afine preslikave

$$x \mapsto (x - a)\, f'(a) + f(a)$$

Na tangenti leži vektor — stolpec, na normali pa vektor — vrstica

$$\begin{Vmatrix} 1 \\ f'(a) \end{Vmatrix} \qquad \|f'(a), -1\|$$

Vsi trije pojejo isto staro pesem: *število $f'(a)$ je smerni koeficient tangente.*



Sl. 10 Graf funkcije. Funkcija je odvedljiva v točki a. Točka $(a, f(a))$ leži na grafu. Vektor, ki ima projekcijo na abscisno os enako $f'(a)$, projekcijo na ordinatno os pa -1, leži na normali grafa skozi $(a, f(a))$

Sklepne pripombe

1. Obravnavali smo odvod v pribiti točki, $f'(a)$. Spreminjanje točke x v $f'(x)$ bi nas zaneslo na prag globalne analize, v teorijo mnogoterosti.

2. Spis sem sestavil na svojo roko, nedelegatsko. Oddelek zanj ne odgovarja.

3. Seminar smo začeli po francosko sentimentalno, pa ga tako še končajmo, s trpkim opozorilom Laurenta Schwartza [6]

Comme on l'a souvent dit, il n'est pas de
«Mathématiques sans larmes»
á l'usage des physiciens et des ingénieurs.

Pri nas so tudi matematiki inženirji.

LITERATURA

[1] J. Grasselli, *O odvodu v linearnih topoloških prostorih,* Obzornik mat. fiz. **16** (1969) 56—58.

[2] H. C. Kennedy, *Karl Marx and the Foundations of Differential Calculus,* Historia Mathematica **4** (1977) 303—318.

[3] T. Klinc, *Zapiski predavanj iz matematike,* Fakulteta za strojništvo l. 1986. Ljubljana

[4] F. Križanič, *Vektorska in tenzorska analiza,* MK, Ljubljana 1966.

[5] S. Lang, *Undergraduate Analysis,* Springer Verlag, New York—Heidelberg—Berlin 1983.

[6] L. Schwartz, *Analyse Mathématique* I, II, Hermann, Paris 1967.

[7] J. A. Thorpe, *Elementary Topics in Differential Geometry,* Springer Verlag, New York—Heidelberg—Paris 1979.

NOVE KNJIGE

FINN R., Equilibrium Capillary Surfaces. Berlin, Springer Verlag 1986.

Vsebina: Uvod. Simetrična kapilarna cev. Simetrična ležeča kaplja. Viseča kaplja. Asimetrični primer. Primerjalna načela in njihova uporaba. Breztežne kapilarne ploskve. Eksistenčni izreki. Kapilarni kot ob dotiku. Identitete in izoperimetrične zveze. Bibliografija (226 enot). Kazalo.

Delo obravnava teorijo o ravnovesnih pojavih površinske napetosti in je prva sodobna tovrstna knjiga. Obdelava je pretežno matematična, čeprav se knjiga loteva tudi specifično fizikalnih vprašanj ter prinaša izrecne ocene o poteku pojavov ter o mejah, med katerimi se gibljejo napake. Vsebuje tudi eksperimentalne potrditve.

Poudarek knjige je na pojavih, ki bi si jih ne nadejali (npr. neenakomerna ali nezvezna odvisnost od parametrov) in na izsledkih, ki ne izvirajo brez nadaljnjega iz perturbacijskih postopkov ali razvojev. Ključno vlogo ima tu načelo maksimuma, prilagojeno nelinearnim enačbam. Knjiga bi morala privlačiti ne samo matematike, ki se zanimajo za povprečno ukrivljenost, ampak tudi fizike in tehnike, ki bi radi posodobili svoje znanje o kapilarnih pojavih.

Drago Bajc

FIZIKALNE RAZMERE V ZVEZDAH

TOMAŽ ZWITTER

A 97.10.Cv

S preprostim sklepanjem bomo ugotovili, kakšne so razmere v notranjosti zvezd. To je osnova za numerične modele, s katerimi pojasnimo opazovane lastnosti zvezd. Za primer bomo predstavili rezultate modela masivne homogene zvezde, ki je namenjen pedagoški rabi.

PHYSICAL CONDITIONS IN STARS

Conditions in stellar interiors will be simply inferred. This is the basis for numerical models by which the observed properties of stars are explained. As an example the results of a model of a massive homogeneous star made for pedagogical purpose are presented.

Včasih so ljudje zvezde le opazovali, njihovih lastnosti pa niso poskušali fizikalno razlagati. Vzrok je bil preprost. Po ničemer niso mogli sklepati, da na zvezdah veljajo enaki fizikalni zakoni kot na Zemlji. Prvi korak je naredil William Huggins, ki je v šestdesetih letih prejšnjega stoletja opazoval zvezdne spektre. Opazil je, da imajo spektri vročih plinov v laboratoriju enake črte, kot jih najdemo v zvezdnih spektrih. Naredil je odločilen sklep, da so na zvezdah enaki elementi kot na Zemlji. To je pripeljalo do poskusov opisovanja lastnosti zvezdne snovi z znanimi fizikalnimi zakoni.

Sonce je (nam) najbližja zvezda, zato si bomo pomagali z njegovimi lastnostmi. Geološka merjenja na Zemlji so pokazala, da se lastnosti Sonca v zadnji milijardi let niso bistveno spremenile. Torej je Sonce v stacionarnem stanju. Na ekvatorju se zavrti okoli svoje osi v 25 dneh. Centrifugalni pospešek je mnogo manjši od gravitacijskega. Zato lahko upamo, da vrtenje ni bistvenega pomena za ravnovesje na Soncu, in ga obravnavamo kot krogelno simetrično nerotirajočo zvezdo.

Ocenimo velikosti nekaterih fizikalnih količin v zvezdah, ki nam bodo pomagale spoznati lastnosti snovi. Povprečna gostota Sonca je

$$\langle \varrho \rangle = M/(4\pi R^3/3) = 1 \text{ g/cm}^3$$

Tlak v zvezdi mora uravnovešati težo zunanjih plasti, saj bi se sicer velikost zvezde spreminjala, tega pa pri Soncu ne opazimo. Zato je

$$dp/dr = -\varrho(r)\, G\, M(r)/r^2$$

$M(r)$ je masa znotraj lupine s polmerom r. Središčni tlak je približno enak

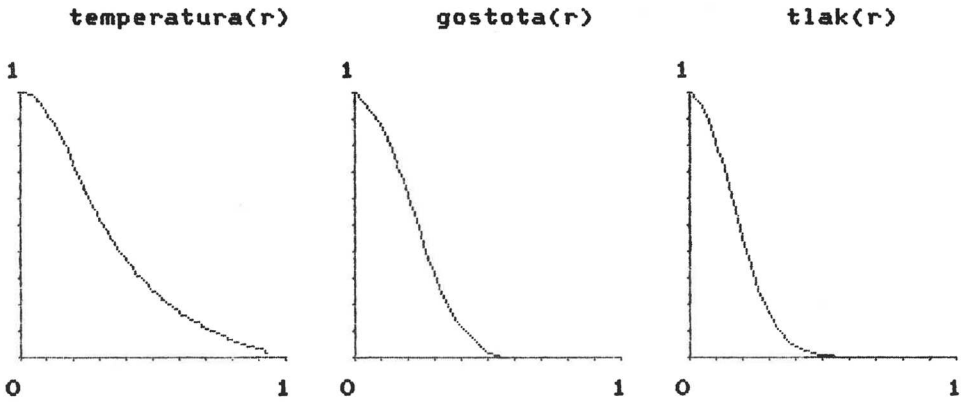
$$P_c/R \cong \langle \varrho \rangle\, G\, M/R^2$$

$$P_c \cong 3\, G\, M^2/(4\pi R^4) = 3 \cdot 10^9 \text{ bar}$$

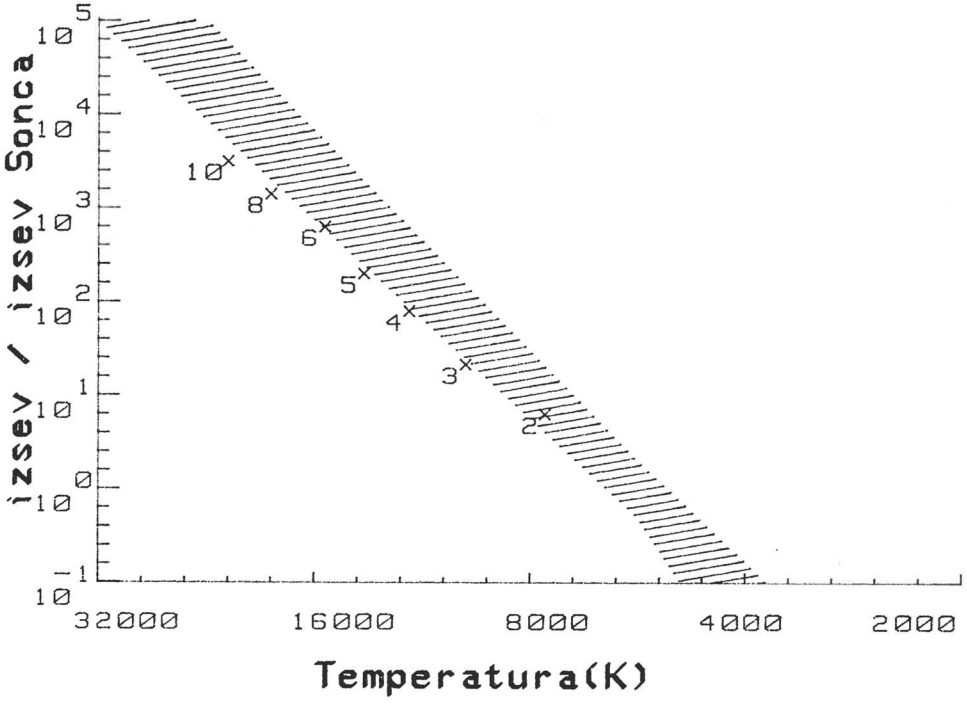
Vstavili smo izmerjeno maso in polmer Sonca.

Analiza zvezdnih spektrov pokaže, da sestavlja zvezde predvsem vodik, ki je na površini delno ioniziran. Temperatura v notranjosti je višja kot na površini, zato privzamemo, da sestavlja zvezde popolnoma ioniziran plin. Točnejše ocene pokažejo, da so trki med delci dovolj redki, da lahko obravnavamo plin kot idealen. Številska gostota delcev je enaka vsoti gostot vodikovih jeder in elektronov, to je dvakratni gostoti protonov. Z enačbo idealnega plina lahko ocenimo središčno temperaturo Sonca

$$T_c = P_c/(n\, k_B) \cong G\, M\, m_P/(2\, R\, k_B) = 10^7 \text{ K}$$



Sl. 1. Rezultati modela za zvezdo s petimi masami Sonca in homogenim sestavom 90 masnih odstotkov vodika, 9 odstotkov helija in 1 odstotkom težjih elementov. Polmer zvezde je 2,34 polmera Sonca, izsev pa 257 izsevov Sonca. Središčne vrednosti temperature, gostote in tlaka so: $2{,}35 \cdot 10^7$ K, 18,5 g/cm^3 in $6{,}77 \cdot 10^{10}$ bar. Efektivna temperatura površja je 15000 K



Sl. 2. Glavna veja H-R diagrama masivnih zvezd. Osenčeno področje je opazovana glavna veja. Križci so izračunane lege homogenih zvezd z enako sestavo kot na sl. 1. Številke pomenijo mase zvezd. Slabše ujemanje je posledica razvoja in vrtenja zvezd, ki ju model ne upošteva

Temperature v središčih zvezd so torej okoli deset milijonov stopinj.

Sonce seva moč $4 \cdot 10^{26}$ W. Geološka merjenja pokažejo, da se ta izsev v zadnji milijardi let ni bistveno spremenil. Zanima nas, od kod Soncu toliko energije. Še pred 50 leti so poskušali izsev Sonca razlagati s krčenjem Sonca ali z zajemanjem snovi iz okoliškega medzvezdnega prostora. Pokazalo se je, da bi krčenje lahko zagotovilo tolikšen izsev le za nekaj deset milijonov let. Če bi Sonce požiralo medzvezdno snov, bi moralo biti te toliko, da bi prah opazili tudi v okolici Zemlje. To pa ni res.

Edini možni energijski vir so torej jedrske reakcije. Pri zlivanju vodika v helij se spremeni 8 odstotkov mase v energijo. Masa zgorelega vodika v zadnji milijardi let je torej enaka

$$\triangle m_{\text{vodik}} = L_{\text{Sonce}} \cdot \text{čas}/(0.08\, c^2) = 1.8 \cdot 10^{27}\ \text{kg} \cong 10^{-3}\, M_{\text{Sonce}}$$

Ker je Sonce pretežno iz vodika, lahko z jedrskimi reakcijami pojasnimo njegov izsev. Sonce je v stacionarnem stanju, zato je izsev Sonca enak proizvodnji energije pri jedrskih reakcijah v njegovi notranjosti.

Zvezde gorijo le blizu središča, saj je hitrost jedrskih reakcij močno odvisna od temperature. Kontaktno prevajanje v notranjosti proizvedene energije proti površini zaradi premajhne gostote snovi ni pomembno. Energija se prenaša s sevanjem, če pa temperatura pada dovolj strmo, se razvije konvekcija.

S temi ugotovitvami lahko naredimo model zvezde in izračunane rezultate primerjamo z izmerjenimi. Sistem enačb, ki opisuje hidrostatično ravnovesje, stanje snovi ter prenašanje in proizvodnjo energije, je rešljiv le numerično. Primer rezultatov takega računalniškega programa kažeta sl. 1 in 2.

V večini zvezd gori vodik, vrtijo se počasi in so praktično v stacionarnem stanju. Za take zvezde znamo narediti računske modele, katerih rezultati se zelo dobro ujemajo z izmerjenimi. Zato lahko rečemo, da fiziko takih zvezd dobro razumemo. To pa ne velja za zvezde spremenljivke, pulzarje in rdeče orjakinje. Tu čaka astrofizike še veliko dela.

LITERATURA

[1] A. Čadež, *Fizika zvezd*, DMFA SRS, Ljubljana 1979.

[2] J. P. Cox, R. P. Giuli, *Principles of Stellar Structure*, Gordon and Breach, New York 1968.

[3] M. Schwarzschild, *Structure and Evolution of the Stars*, Princeton University Press, Princeton 1958.

NOVE KNJIGE

GROSSMAN I., Magnus W., Grupe i njihovi grafovi, Školska knjiga, Zagreb, 1975. (Moderna matematika)

Knjiga predstavlja osnovni uvod v teorijo grup. Njena posebnost je pristop k obravnavi grup — avtorja jih preučujeta s pomočjo prirejenih Cayleyevih grafov, ki mnogo nazorneje kot abstrakten opis prikazujejo grupe in njihovo zgradbo. Zato knjiga ne bo pretežka niti mlajšim bralcem. Vsekakor pa bo predstavljala prijetno in koristno branje vsem, ki jih zanima geometrija, topologija, teorija grafov ali (kombinatorna) teorija grup.

Bojan Mohar

VIŠINA VESOLJSKIH TELES

MARIJAN PROSEN

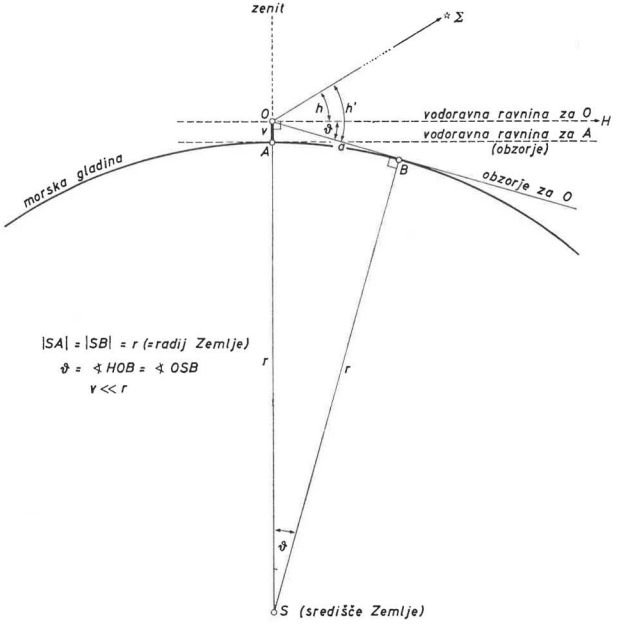
95.40 + s

Prispevek opiše merjenje višine vesoljskih teles, kot ga lahko obravnavamo v srednji šoli.

THE ALTITUDE OF HEAVENLY BODIES

In the article the measurement of the altitude of heavenly bodies suitable for treatment in secondary school is described.

Merjenje višine vesoljskih teles spada med osnovne naloge opazovalne astronomije. Z izmerjeno višino zvezd npr. lahko natančno določimo zemljepisno dolžino in širino kraja. Vzemimo, da je Zemlja idealna krogla in da z idealnim sekstantom merimo višino zvezde iz opazovališča 0 na nadmorski višini v (sl. 1). Kot med vodoravno ravnino skozi opazovališče in smerjo 0Σ proti vesoljskemu telesu Σ je višina h tega telesa. Če je opazovališče na morski gladini, je merjenje višine h preprosto. Če pa je opazovališče nad morsko gladino (npr. da merimo s palube ali stolpa večje ladje, z vrha svetilnika, letala), izmerimo višino h'. Pravo višino h dobimo tako, da od izmerjene odštejemo kot ϑ, torej $h = h' - \vartheta$. Kot ϑ je kot med vodoravno ravnino in obzorjem opazovališča, imenovan tudi *depresijski kot*. Če je r radij Zemlje, je $\vartheta = (2v/r)^{1/2}$ (sl. 1). Pri opazovanju s palube 10 m visoke ladje je $\vartheta = (2 \cdot 10\ \mathrm{m}/6{,}4 \cdot 10^6\ \mathrm{m})^{1/2} = 1{,}8 \cdot 10^{-3} = 6'$. Pri opazovanju z letala na višini 3,2 km nad Zemljo pa je kot večji: $\vartheta = 1{,}8^0$ in ustreza že dobrim trem zornim kotom Lune.



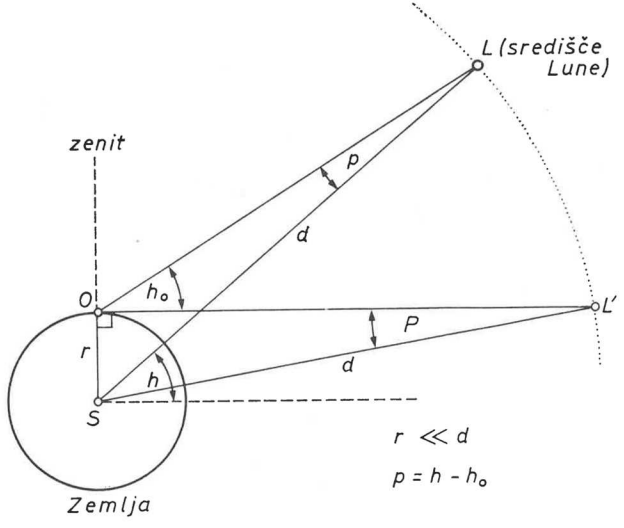
Sl. 1. Razdaljo obzorja $a = |0B|$ dobimo iz enačbe $(r + v)^2 = a^2 + r^2$ za $v \ll r$: $a = (2rv)^{1/2}$ [1]. Depresijski kot $\vartheta = a/r = (2v/r)^{1/2}$. Pri konstantnem r je torej ϑ sorazmeren z $v^{1/2}$; h — prava višina vesoljskega telesa, h' — izmerjena višina

Lom svetlobe v zemeljskem ozračju smo zanemarili. Zaradi loma opazujemo vesoljsko telo više, kot je v resnici [2]. Z upoštevanjem loma je prava višina vesoljskega telesa $h = h' - \vartheta - \varrho$. Pri tem je $\varrho = \varrho_0 \operatorname{ctg} h'$ *astronomska refrakcija*; $\varrho_0 = 1'$ [3].

Če z 10 m visokega stolpa nad morsko gladino izmerimo višino zvezde $h' = 36^0$, je prava višina $h = 36^0 - 6' - 1' \,.\, \operatorname{ctg} 36^0 = 36^0 - 6' - 1' = 35^0\ 53'$. Ta račun velja le za zvezde in približno za planete.

Pri Soncu ali Luni navadno merimo višino spodnjega roba [3]. Višino središča Lune ali Sonca dobimo tako, da prištejemo polovico Luninega ali Sončevega zornega kota (navidezni polmer) φ. Vrednost zornega kota za datum opazovanja preberemo iz astronomskih efemerid (npr. Nautical Almanac).

Če je vesoljsko telo daleč, lahko vzamemo Zemljo za točko, saj bi pri opazovanju zvezde iz središča Zemlje izmerili enako višino kot pri opazovanju s površja. Drugače je, če je telo blizu, kot npr. Luna (sl. 2). Vse meritve navadno preračunamo na zemeljsko središče [3].



Sl. 2. Zemlja in najbližje vesoljsko telo — Luna. Velja $r \ll d$. $P = r/d$ je ekvatorska horizontska paralaksa Lune, h_0 pa višina Luninega središča, popravljena za refrakcijo in depresijski kot. Iz trikotnika OSL sledi $\sin p = (r/d) \,.\, \cos h_0$. Ker so koti majhni, je $p = P \cos h_0$. Zaradi bližine je višina Luninega središča glede na središče Zemlje (geocentrična višina) za $P \cos h_0$ večja kakor za opazovalca na Zemlji. Pri zvezdah te razlike ni. Pri veliki natančnosti pa bi morali upoštevati paralakso in zorni kot tudi pri merjenju višin planetov [3]

Pri Luni, ki je najbližje vesoljsko telo, moramo torej upoštevati še *paralakso*. Kako jo upoštevamo, kaže sl. 2. Zaradi paralakse izmerimo manjšo višino Lune, kot bi jo izmerili pri opazovanju iz središča Zemlje. Da dobimo pravo višino h središča Lune glede na zemeljsko središče, moramo višini, ki jo izmerimo z idealnim sekstantom, dodati $p = P \cos h_0$. Pri tem je P *ekvatorska horizontska paralaksa* Lune v času opazovanja, h_0 pa višina Luninega središča, popravljena za refrakcijo in depresijski kot [3]. P preberemo iz efemerid. Torej velja $h = h' - \vartheta - \varrho + \varphi + p$.

Vzemimo, da zvečer določenega dne z idealnim sekstantom želimo izmeriti pravo višino Luninega središča. Merimo z 10 m visokega stebra tik ob morski obali. Za višino spodnjega roba Lune smo izmerili $46^0\ 20'$. Iz efemerid odberemo $P = 55'$ in $\varphi = 15'$. Računamo takole:

Izmerjena višina spodnjega roba Lune:		$46^0\ 20'$
depresijski kot:		$-\ 6'$
refrakcija ($1'\ .\ \text{ctg}\ 46^0\ 20'$):		$-\ 1'$
navidezni polmer:		$+\ 15'$
	h_0:	$46^0\ 28'$
paralaksa ($55'\ .\ \cos 46^0\ 28'$):		$+\ 38'$
prava višina središča Lune glede na zemeljsko središče:		$47^0\ 6'$

LITERATURA

[1] K. Bajec, *Kako daleč je do obzorja*, Presek **6** (1978/79) 4/5.

[2] F. Avsec, M. Prosén, *Astronomija*, DZS, Ljubljana 1975, str. 36.

[3] W. M. Smart, *Foundations of Astronomy*, Longmans, Green and Co, London, N. Y., Toronto 1953, str. 106, 116 in 152.

NOVE KNJIGE

STANTON D., WHITE D., Constructive Combinatorics, Undergraduate Texts in Mathematics, Springer Verlag, New York 1986, 158 + 26 str.

Knjiga vsebuje izbrana poglavja iz kombinatorike. Avtorja obravnavata kombinatoriko z algoritmičnega vidika, saj smatrata, da tako lahko na razumljiv način razložimo naravo kombinatoričnih principov, po drugi strani pa je algoritmično razmišljanje tudi močno orodje za dokazovanje v diskretni matematiki.

V uvodnem poglavju predstavita nekatere osnovne kombinatorične objekte: permutacije, podmnožice, razbitje naravnega števila, razbitje množice. Vse objekte tudi algoritmično konstruirata, v skladu z vrstnim redom generiranja v algoritmih mednje uvedeta linearno urejenost in izpeljeta algoritme, ki bijektivno priredijo danim objektom ustrezni indeks njihove urejenosti. Algoritmi so med tekstom pisani v simboličnem jeziku, tako da za njihovo razumenje ne potrebujemo programerskega znanja, medtem ko so v dodatku podani v programskem jeziku Pascal. Zatem vpeljeta na naraven način med vse predstavljene objekte iz prvega poglavja delno urejenost.

V tretjem poglavju preštevata kombinatorične objekte predvsem z metodo bijekcije, tj. dano družino objektov, ki jo hočemo prešteti, bijektivno preslikamo na množico, katero smo že prešteli. V zadnjem poglavju pa s tehniko involucij (permutacija, katere kvadrat je identiteta), oz. fiksnih točk involucij, avtorja dokažeta več pomembnih kombinatoričnih in tudi drugih izrekov. Naj omenim le princip vključitve-izključitve in Cayley-Hamiltonov izrek.

Kje iskati podrobnejše znanje o obravnavanih problemih izvemo na koncu vsakega poglavja. Predvsem v zadnjih dveh poglavjih srečamo nekatere probleme, ki se intenzivno proučujejo v zadnjem času in je tako knjiga dobrodošel pregled narejenega na omenjenih področjih. Ker zahteva nekaj predznanja osnov kombinatorike (osnovni principi, rodovne funkcije) in diskretnih struktur, je primerna predvsem za študente višjih letnikov ter podiplomcev računalniško-matematične usmeritve.

Sandi Klavžar

NOVE KNJIGE

PATERSON A. R., A first Course in Fluid Dynamics, Cambridge University Press 1983.

Vsebina: Predgovor. Matematični uvod. Fizikalni uvod. Opazovalčev uvod. Ohranitev mase in tokovne funkcije. Vrtinčenje. Hidrostatika. Termodinamika. Enačba gibanja. Rešitve Navier-Stokesovih enačb. Neviskozni tok. Potencialna teorija. Zvočni valovi v tekočinah. Vodni valovi. Nadzvočni tok. Stacionarni površinski valovi v kanalih. Kompleksni potencial. Konformno upodabljanje in letalska krila.

Pri vsej nasičenosti angleško govorečega knjižnega trga na prenekaterem področju, tako da je bralec nemalokrat zbegan, kaj naj izbere, je Patersonova knjiga zapolnila zevajočo vrzel. Če se namreč nad številom in tudi kakovostjo učbenikov in traktatov o hidrodinamiki od Lamba do Batchelorja ne moremo pritoževati, je od vedno manjkala na trgu začetnica. In za táko bi lahko z eno besedo označili Patersonovo knjigo, ki neprisiljeno in v pogovornem slogu uvede bralca v problematiko in matematična sredstva panoge; ki — namesto da bi ga pošiljala drugam ali vsaj k dodatkom lastne knjige — sproti izoblikuje matematična sredstva takrat, ko postanejo potrebna; ki navaja bralca tako med tekstom kot v nalogah na to, kako zgraditi in uporabljati modele, predvsem pa na to, kako nanje gledati (do kam so koristni, kje nas zavajajo in katere so njihove omejitve). Kako potrebno je slednje pri hidrodinamiki, nas lepo svarijo bleščeče matematične rešitve s pičlo uporabnostjo, od katerih kar mrgoli starejša literatura.

In pomanjkljivosti? Recenzent v (1) se spotika nad dejstvom, da knjiga ne vsebuje uporabe računalništva pri hidrodinamiki. Jaz bi dodal, da ne vsebuje še marsičesa. Na primer: nič ali skoro nič ni v njej t. i. geofizikalne hidrodinamike, pa tudi linearna teorija vodnih valov je precej nepopolna, nelinearne pa sploh ne vsebuje. Toda že tako ima knjiga čez 500 strani. In pri pisanju začetnice je vsaj tako važno, da veš, kaj smeš izpustiti iz nje, kot to, kaj moraš vnesti vanjo.

Še nekaj besed o nalogah. Teh je kar precej in na splošno niso ne prelahke ne pretežke. Razporejene pa so tako, da vsaka nastopi trikrat: prvič je ob koncu poglavja besedilo, drugič, na koncu vseh poglavij, je daljši namig in šele na koncu vseh koncev rešitev. Med vzorcem nalog, ki sem jih rešil, sem žal naletel, da ima, recimo vsaka deseta, če ne celo vsaka peta, napačen rezultat. Dobro bi bilo, da bi se avtor pri morebitni novi izdaji tega zavedel in popravil.

(1) SIAM Review **27** (1985) 2 *Drago Bajc*

STRNAD Janez, Na pot v kvantno elektrodinamiko. — DMFA SRS 1986. — Str. 176 — (Zbirka izbranih poglavij iz fizike; 22)

V najnovejšem delu Janez Strnad nadaljuje prizadevanja za boljši pouk in razumevanje kvantne fizike. Bralca želi po kolikor mogoče elementarni poti uvesti v nerelativistično kvantno elektrodinamiko. S tem se knjiga omeji predvsem na kvantno teorijo svetlobe, da bi »razčistili vprašanje: Kaj je foton«? Namenjena je predvsem učiteljem fizike in študentom izobraževalne smeri, a zagotovo bo zanimivo in vzpodbudno branje tudi za druge fizike.

Knjiga je razdeljena na štiri dele. Nekaj prvih strani osveži spomin na osnovne pojme klasične mehanike in na klasično obravnavo harmoničnega oscilatorja. Nato ponovi osnove kvantne mehanike v koordinatni reprezentaciji in z njo nekoliko podrobneje obdela harmonični oscilator kot pripravo na poznejšo kvantizacijo elektromagnetnega polja. Uvede tudi uničevalne in ustvarjalne operatorje in potem koherentna stanja, s katerimi je mogoče povezati klasično in kvantno mehaniko. Na zgledu harmoničnega oscilatorja pojasni še Heisenbergovo sliko in Diracov zapis vektorjev stanj in matričnih elementov. Tretji del ponovi osnove klasične elektrodinamike in obravnava razvoj elektromagnetnega polja v votlini po lastnih nihanjih. Trije pripravljalni deli uvedejo vse osnovne pojme, vendar pa so preveč zgoščeni, da bi lahko koristili bralcu, ki se s kvantno mehaniko še ni srečal.

Četrti del, ki obsega skoraj tri četrtine knjige, se loti kvantizacije elektromagnetnega polja. Kot je v navadi, izkoristi formalno podobnost med Hamiltonovo funkcijo harmoničnega oscilatorja in energijo elektromagnetnega valovanja. Tu zapiše tudi valovno funkcijo s količino polja, kar je nekoliko nenavadno. Foton uvede kot kvant energije enega elektromagnetnega lastnega nihanja in poudari, da ga ni mogoče pojmovati kot enostavno razširitev pojma delca. Foton je last vsega prostora, v katerem je elektromagnetno polje, in mu lahko pripišemo le energijo in gibalno količino, nikakor pa ne lege. Nato avtor preko koherentnega stanja pokaže zvezo s klasično elektrodinamiko. Obravnavo razširi še na več valov, uvede statistični operator in obravnava kaotično svetlobo in sevanje črnega telesa. Izračuna verjetnost za prehod atoma s sevanjem in pokaže pomanjkljivosti polklasičnega približka, ki ne more pojasniti spontanega sevanja. V nekoliko daljšem računu oceni verjetnost za ionizacijo vodikovega atoma s svetlobo. Sledita dokaj zahtevni obravnavi Casimirjeve sile in Lambovega premika. Oba pojava je mogoče pojasniti z ničelnimi fluktuacijami elektromagnetnega polja in imata tako povsem kvantno naravo. Tri poglavja so nato posvečena fotonskim korelacijam in štetju fotonov. V zaključnem poglavju avtor bralcu pojasni, da se prava elektrodinamika prične šele, ko kvantiziramo še polja delcev in upoštevamo zahteve relativistične mehanike.

Knjiga vsebuje veliko starejših in novejših citatov, ki napravijo branje posebej zanimivo. Kateri od citatov utegne sicer novinca zmesti, ker oporeka drugim, avtor pa jih ne komentira. Knjiga ni lahko branje, saj uvaja vrsto novih težavnih pojmov in se ne izogne nekaterim zapletenim računom. Zelo dobro je, da je nekaj primerov uporabe formalizma kvantne elektrodinamike izračunanih od začetka do konca. Avtor se je trudil, da bi izvajanja kolikor mogoče tesno naslonil na kvantno mehaniko iz naših uvodnih tečajev, to je predvsem na Schroedingerjevo koordinantno reprezentacijo. Zdi se mi, da je s tem celo nekoliko pretiraval, saj na primer valovna funkcija s količino polja nima kakšnega pametnega fizikalnega pomena, a je matematično dosti bolj zapletena od številske reprezentacije.

Delo bo zagotovo dragocen prispevek k slovenski fizikalni literaturi. Vprašanje valovne in delčne narave svetlobe je že desetletja eno od najtežavnejših vprašanj pri poučevanju kvantne fizike v uvodnih visokošolskih tečajih in v srednji šoli. Upam, da bo po njej seglo čim več učiteljev in drugih fizikov. Za vloženi trud bodo morda nagrajeni s tem, da bodo le zvedeli, kje je foton.

Martin Čopič

ONICESCU O., Principes de logique et de philosophie mathématique, Éditions de l' Académie de la République socialiste de Roumanie, Bucarest 1971, 229 str.

Avtor razpravlja o matematični logiki in filozofiji matematike, z vidika teh dveh pa tudi o raznih področjih matematike. Obravnava oblike matematične misli, aksiomatično zasnovo matematične logike, logiko verjetnostnega računa, vlogo neskončnosti in antinomije teorije množic, slučaj in verjetnost ter statistično obravnavo skupin, krize objektov v naravoslovju ter filozofijo informacije.

Avtor razlaga tako intuitivno kot tudi aksiomatično zgradbo matematičnih teorij; v teh ga še posebej zanima snovanje matematičnih objektov in njih realizacija v modelih. Med drugim je pokazan logični in matematični pristop h geometriji, k neskončnosti, slučajnosti ..., pa tudi k problemom mehanike in naravoslovja sploh. Upoštevaje zgodovino matematike, nam pisec prinaša še svoje osebne poglede na matematiko in na odnos med človekom in svetom. Tako je knjiga zanimiva za vsakogar, ki se želi poglobiti v osnove matematike, da bi potem bolj celovito dojemal njena posamezna področja.

Janez Rakovec

MURŠIČ Milan, Osnove tehniške mehanike, 2. del, Kinematike, Ljubljana, DMFA SRS, 1986. Cena 5000.— din (4000.— din)

Učbenik Kinematike je drugi del v zbirki učbenikov iz osnov tehniške mehanike in je namenjen predvsem študentom tehniških in tehnoloških fakultet, ki imajo na učnem programu tudi poglavja iz kinematike in kinetike.

Snov učbenika je razdeljena na štiri obširnejša poglavja. V uvodnem poglavju so podane osnovne veličine mehanike, definirani so pojmi prostora, mase in časa z omejitvami, ki so običajne in dopustne v tehniških aplikacijah. Nakazan je postopek reševanja realnega problema od izbire ustreznega modela, njegovega matematičnega zapisa z upoštevanjem principov mehanike do končnega, pravilnega razlaganja rezultatov. Zaradi potrebe v kasnejših poglavjih je avtor posvetil precej pozornosti nekaterim osnovam vektorske analize. Detajlno je prikazan časovni odvod vektorja konstantne in spremenljive dolžine, med zgledi pa so podane še Frenetove enačbe, s katerimi se študent tehnike danes pri matematičnih kurzih ne seznani.

Drugo poglavje je posvečeno kinematiki točke. Izpeljana sta vektorja hitrosti in pospeška v najbolj uporabljanih koordinatnih sistemih. Že prej nakazana formulacija kinematičnih problemov v prostoru, je detaljno prikazana na zgledih premočrtnega gibanja, pri katerem je pospešek funkcija časa, hitrosti ali poti. Poglavje zaključuje 18 raznolikih in dobro izbranih zgledov.

Tretje, najobširnejše poglavje je namenjeno kinematiki togega telesa. Po definiciji togega telesa in njegovih prostostnih stopenj so prikazani najprej končni premiki, njihova delitev in operacije z njimi, nato pa je po infinitezimalnih premikih določeno trenutno gibalno stanje telesa. Ta pot je običajno v učbenikih iz kinematike površno podana. Zelo izčrpno je obdelano ravninsko

gibanje, ki je osnova za analizo mehanizmov. Prikazan je pomen pomične in nepomiče poloide ter pola pospeškov. Avtor podaja vzporedno analitične in grafične rešitve. Razlago dopolnjujejo številne izvirne, precej bogate slike. Poglavje se zaključi z gibanjem togega telesa okoli stalne točke. Izpeljane so Eulerjeve kinematične enačbe v gibljivem in fiksnem koordinatnem sistemu. Žal, poglavja ne zaključujejo konkretni primeri, ki bi ilustrirali analizo zahtevnejših gibanj v tehniki.

Poslednje poglavje je uvod v analitično kinematiko in je posvečeno kinematiki sistemov ter njihovim prostostnim stopnjama. Vpeljane so generalizirane koordinate in z njimi izražena vektorja hitrosti in pospeška. Na koncu so podani še virtualni pomiki sistema.

Slovenci imamo v svojem jeziku natisnjene precej literature iz statike in elastomehanike. Zaman pa išče študent tehnike ali strokovnjak v praksi obširnejše razlage iz poglavij kinematike in kinetike. To praznino zapolnjuje predstavljeni učbenik Milana Muršiča in zato nedvomno predstavlja na tem področju najbolj kompletno delo. Želimo si, da bi ga čimprej dopolnil še napovedani učbenik iz kinetike .

Mladen Houška

VARADARAJAN V. S., Geometry of Quantum Theory. Second Edition. Springer Verlag, New York, Berlin, Heidelberg, Tokyo 1985. Str. XVIII + 412.

Knjiga govori o osnovah kvantne teorije, kakor so jih postavili P. A. M. Dirac, J. von Neumann, H. Weyl, E. P. Wigner indr. Preden se podrobneje seznanimo z njeno vsebino, se spomnimo, v čem se razločuje kvantna mehanika od klasične. Imejmo mehanski sistem in si oglejmo množico vseh izjav, ki so smiselne za ta sistem in se dajo vsaj v načelu s poskusi potrditi ali ovreči. Primer take izjave je, da ima energija sistema določeno vrednost ali da leži na predpisanem intervalu. Vse izjave sestavljajo logiko mehanskega sistema. Implikacija določa v tej logiki delno urejenost, negacija pa komplementiranost. Značilno za klasično mehaniko je to, da je logika sistema komplementirana distributivna mreža, tj. Booleova algebra. V kvantni mehniki pa velja načelo nedoločenosti: nekaterih količin, kot so npr. koordinata delca in pripadajoča komponenta gibalne količine, ni mogoče hkrati ostro meriti. Zato logika L kvantnomehanskega sistema ni Booleova algebra. Kljub temu pa je mreža in sicer ortokomplementirana, ker vsaki izjavi $a \in L$ pripada negacija $a' \in L$. Kakšna mreža pa je logika kvantnomehanskega sistema? Posplošitve distributivnih mrež so modulske mreže, v katerih velja le poseben primer distributivnostnega zakona. Zgledi za modulske mreže so projektivni prostori. Projektivni prostor najlaže opredelimo z množico vseh podprostorov danega vektorskega prostora. Delno urejenost določa v mreži podprostorov inkluzija. Vendar končnorazsežni projektivni prostori ne pridejo v poštev za logiko kvantnomehanskega sistema. V neskončnorazsežnem projektivnem prostoru pa ni mogoče definirati ortokomplementiranosti. Zato vzamemo Banachov prostor, logiko L pa naj sestavljajo vsi njegovi zaprti podprostori. (Žal ta mreža ni modulska.) Toda mreža zaprtih podprostorov Banachovega prostora je ortokomplementirana samo v primeru, ko je Banachov prostor v bistvu Hilbertov. To pove izrek, ki sta ga l. 1946 dokazala Kakutani in Mackey. Mrežo vseh zaprtih podprostorov neskončno razsežnega separabilnega Hilbertovega prostora imenujemo standardna logika. Vsak zaprt podprostor lahko

nadomestimo s pripadajočim projektorjem E. Ortogonalnemu komplementu pa pripada projektor $I - E$, kjer je I identični operator.

Imejmo kvantnomehanski sistem z logiko L. Kaj so observable (opazljivke) tega sistema, kaj so njegova stanja in simetrije? Observabla je funkcija, ki priredi vsaki Borelovi množici točk na številski premici natanko določen element logike L, disjunktnim množicam pa priredi ortogonalne elemente. Stanja sistema pa so mere definirane na mreži L. Torej je stanje funkcija p, ki priredi vsakemu elementu $a \in L$ nenegativno število $p(a)$. Simetrije sistema so avtomorfizmi množice stanj. Vsak avtomorfizem mreže L pa določa tudi avtomorfizem množice stanj.

Knjiga Varadarajana pripoveduje o tem, kako pri dani logiki izpeljemo osnovne zakone kvantne mehanike. Razdeljena je na devet poglavij: I. Booleove algebre na klasičnem faznem prostoru; II. Projektivne geometrije; III. Logika kvantnomehanskega sistema; IV. Logike pridružene Hilbertovim prostorom; V. Teorija mere in G-prostori; VI. Sistemi imprimitivnosti; VII. Množitelji; VIII. Kinematike in dinamike; IX. Relativistični prosti delci.

V prvih štirih poglavjih obravnava avtor osnovne lastnosti projektivnih geometrij, študira ortokomplementirane mreže in observable, stanja in simetrije na takih mrežah, načelo superpozicije itd. Najbolj zanimiva je seveda standardna logika. Brez težave ugotovimo, da lahko pri standardni logiki tolmačimo observable kot sebiadjungirane operatorje pripadajočega Hilbertovega prostora. Tudi stanja se tu izražajo na običajni način; posebej so čista stanja določena z enorazsežnimi podprostori. To pove izrek Gleasona: V standardni logiki je stanje preslikava p, ki priredi vsakemu projektorju E Hilbertovega prostora nenegativno število $p(E)$ in je $p(E + F) = p(E) + p(F)$, če sta E in F ortogonalna projektorja. Gleasonov izrek trdi, da obstaja tak pozitiven operator C s sledjo, da velja $p(E) = \mathrm{Tr}(CE)$ za vsak projektor E. Tu pomeni $\mathrm{Tr}(A)$ sled operatorja A. Avtomofizmi mreže L pa se v standardnem modelu izražajo z unitarnimi in in antiunitarnimi operatorji. Grupam simetrij kvantnomehanskega sistema ustrezajo grupe unitarnih operatorjev. Tako pridemo do problema upodabljanja grup. O tem govore peto, šesto in sedmo poglavje, ki so povsem matematične narave. Obravnavajo tiste dele teorije lokalno kompaktnih grup, njihovih upodobitev in harmonične analize na grupah, ki pridejo v poštev pri študiju kvantne mehanike. V predzadnjem poglavju izpelje avtor najprej abstraktno Schrödingerjevo enačbo. Dinamika sistema se namreč izraža z enoparametrično grupo unitarnih operatorjev. Generator te grupe se imenuje Hamiltonov operator H. Če je konfiguracijski prostor sistema evklidski prostor, so simetrije sistema unitarne upodobitve grupe togih premikov. Upodobitve podgrupe vzporednih premikov nam dajo gibalno količino, upodobitve rotacijske grupe pa vrtilno količino. Observable, ki določajo lego, gibalno in vrtilno količino delca, se izražajo z operatorji množenja in odvajanja na običajen način, če je Hilbertov prostor $L^2(R^3)$. Gibalna in vrtilna količina sta konstanti gibanja, tako da pripadajoči operatorji komutirajo s Hamiltonovim operatorjem H. Od tod se da izpeljati oblika za H: V Schrödingerjevi reprezentaciji je H pri prostem delcu sorazmeren Laplaceovemu operatorju. Upodobitve grupe togih premikov nam dajo tudi spin delca. Zadnje poglavje govori o relativističnem prostem delcu. Tu igrajo pomembno vlogo upodobitve homogene in nehomogene Lorentzove grupe. Med drugim dobimo Diracovo valovno enačbo za elektron.

Iz knjige zvemo, kako se dajo matematično izpeljati osnovni fizikalni zakoni kvantne mehanike, če privzamemo, da je logika sistema standardna. Odprto pa ostane vprašanje, zakaj je logika standardna. Pomisliti je treba, da je mreža zaprtih podprostorov neskončno razsežnega Hilbertovega prostora izredno abstraktna matematična konstrukcija.

Knjiga se zelo lepo bere. Vendar zahteva od bravca določeno znanje iz funkcionalne analize, teorije grup, predvsem Liejevih grup in njihovih upodobitev.

Ivan Vidav

DOMAČE VESTI

MEDNARODNI KONGRES MATEMATIKOV, BERKELEY 1986

Prvi mednarodni kongres matematikov je bil leta 1893 v Chicagu. Doslej se jih je zvrstilo že 21, od tega 10 po drugi svetovni vojni. Običajno je bil razmik med dvema zaporednima kongresoma 4 leta, so pa tudi izjeme: predzadnji v Varšavi je bil npr. prestavljen za eno leto naprej zaradi izrednih dogodkov na Poljskem v letu 1982.

The National Academy of Sciences U.S.A. je preko U. S. National Committee for Mathematics ponudila Mednarodni matematični uniji (IMU), da leta 1986 organizira naslednji mednarodni kongres matematikov. University of California je predlagala, da naj poteka kongres v Berkeleyu. Organizacijo in izvedbo so poverili the American Mathematical Society, največjemu matematičnemu združenju v Severni Ameriki.

Kongres se je pričel 3. avgusta s svečano otvoritvijo v Greek Theatre v Berkeleyu, na kateri so podelili Fieldsove medalje. Priznanje se imenuje po kanadskemu matematiku *Johnu C. Fieldsu*, ki je pred več kot 40 leti predlagal, da naj bi tudi v matematiki podeljevali priznanja, podobna Nobelovim nagradam na drugih področjih. (Uradno še danes ni znano, čemu Alfred Nobel tudi za matematike ni predvidel nagrad, čeprav obstajajo številne nedokumentirane govorice o njegovih razlogih za tako ravnanje.) Fields je tudi daroval začetna sredstva za taka priznanja in določil, da naj bodo nagrajenci

praviloma mlajši od 40 let. Prvi Fieldsovi medalji so podelili na kongresu v Oslu leta 1936 — dobila sta ju Finec *Lars Ahlfors* in Američan *Jessie Douglas*. Ahlfors je bil predsednik kongresa v Berkeleyu in imel je čast podeliti najnovejše 3 medalje. Dobili so jih 29-letni *Simon K. Donaldson* iz Oxforda, 32-letni *Gerhard Faltings* iz Wuppertala (sedaj v Princetonu) in 35-letni *Michael H. Freedman* iz San Diega.

Imena nagrajencev so dobro znana vsakomur, ki je zadnja 4 leta sledil najzanimivejšim rezultatom v sodobni teoretični matematiki. Faltings je bil nagrajen za svoje vrhunske rezultate v teoriji števil in algebraični geometriji — najbolj je v svetu odmeval njegov dokaz Mordellove domneve, ki je bila postavljena pred 60 leti in so jo neuspešno naskakovali številni znani matematiki. Freedman je našel izredno elegantno klasifikacijo enostavno povezanih topoloških 4-mnogoterosti in kot rezultat dokazal slovito Poincaréjevo domnevo (za dimenzijo 4). Kako nenavaden je svet gladkih 4-mnogoterosti, pa je pokazal Donaldson. Za študij 4-razsežnih mnogoterosti je iznašel popolnoma nove metode — osnovo zanje je našel v matematični fiziki, v teoriji Yang-Millsovih enačb. Najodmevnejša posledica njegovega briljantnega dela je rezultat, ki se ga ni nihče nadejal: evklidski prostor $\mathbb{R}^4$ ima *več* gladkih struktur, ki med seboj *niso* ekvivalentne (t. j. difeomorfne). Ta pojav ni mogoč v nobeni drugi dimenziji in ni še razvidno, kakšne posledice bo imelo Donaldsovo delo denimo v teoretični fiziki.

Letos so že drugič podelili tudi posebno priznanje za matematične raziskave v informacijskih znanostih in računalništvu — *Nevanlinnovo* nagrado. Prejel jo je *Leslie Valient* iz Cambridgea, ZDA za raziskave rešljivosti matematičnih problemov s pomočjo računalnika.

Kongres je trajal 9 dni, potekal pa je po naslednjem programu: vsako dopoldne sta bili dve enourni plenarni predavanji, popoldne pa se je okoli 3 tisoč udeležencev iz 70 držav razdelilo po sekcijah, kjer so poslušali 45-minutna povabljena predavanja in 10-minutne referate. Skupno je bilo predstavljenih 16 plenarnih predavanj, 145 povabljenih predavanj in okoli 500 referatov.

Vzporedno s kongresom so potekale tudi številne druge prireditve. Vodilne založniške hiše iz Evrope in Amerike so pripravile razstavo matematične literature in ponujale izreden popust pri nakupu. Svojo opremo so razstavili izdelovalci računalniških paketov, posebej še programov za sestavljanje besedil. Predvajali so več matematičnih filmov in video posnetkov. Udeleženci so organizirali večje število neformalnih seminarjev. Prišli so celo specialisti za posebne efekte iz Holywooda in predavali o računalniški animaciji na filmu — kot ilustracijo so predvajali znano trilogijo *Star Wars — The Empire Strikes Back — Return of the Jedi.*

Tudi družabnih prireditev je bilo veliko: od rodea v sloviti Cow Palace v San Franciscu do koncertov klasične in jazz glasbe. Za družinske člane udeležencev kongresa so pripravili več izletov v San Francisco in okolico, med drugim denimo na snemanje popularne TV oddaje na eni izmed lokalnih TV postaj.

Kongres je bil lepa priložnost, da se seznanimo z najnovejšimi dogajanji v matematiki in da srečamo nekatere vodilne raziskovalce na svetu.

Dušan Repovš

Društvo matematikov, fizikov in astronomov SR Slovenije prireja ob sodelovanju Oddelka za fiziko Fakultete za naravoslovje in tehnologijo, Instituta J. Stefan, Inštituta za matematiko, fiziko in mehaniko in Zavoda SR za šolstvo 29. in 30. januarja 1987, 12. seminar iz fizike

MEDICINA IN FIZIKA

Seminar je namenjen učiteljem matematike in fizike na srednjih in osnovnih šolah za strokovno izpopolnjevanje. Vabljeni so tudi drugi člani društva.

Četrtek, 29. 1. 1987

9.00 Začetek seminarja
Marjan Erjavec, Onkološki inštitut:
Radioaktivni izotopi v medicini

11.30 Janez Stepišnik, Oddelek za fiziko:
Slikanje z jedrsko magnetno resonanco v medicini

13.30 Jože Žakelj, Iskra Elektrooptika:
Laserji v medicini

Petek, 30. 1. 1987

8.00 Saša Svetina, Inštitut za biofiziko:
Biofizika rdeče krvne celice

10.00 Sergej Pahor, Oddelek za fiziko:
Človeško telo in fizika v srednji šoli

12.30 Marjan Pajntar, Bolnišnica za ginekologijo in porodništvo, Kranj:
Ultrazvok v medicini.

Vodstva šol prosimo, da prispevek za seminar 2000.— dinarjev nakažejo na žiro račun DMFA SRS, Ljubljana 50101-678-49168, lahko pa ga udeleženci plačajo na seminarju.

Vodja seminarja:
Janez Strnad