RAČUNALA NOVE DOBE, 2. del

Matematiko lahko definiramo kot predmet, pri katerem nikoli ne vemo, o čem govorimo, niti nikoli ne vemo, ali je tisto, kar pravimo, resnično.

Bertrand Russell

V prejšnji številki Preseka smo z analizo seštevanja in množenja naravnih, celih oziroma racionalnih števil vpeljali pojma *grupa* in *obseg*, ki imata pomembno vlogo v algebri. Ponovimo:

V grupi $(G, \circ)$ velja:

(G1) za vsaka elementa $a, b \in G$ je $a \circ b \in G$;

(G2) obstaja tak element $e \in G$, da za vsak element $g \in G$ velja $e \circ g = g \circ e = g$;

(G3) za vsak element $g \in G$ obstaja tak element $f \in G$, da je $g \circ f = f \circ g = e$;

(G4) za vse elemente $a, b, c \in G$ velja $(a \circ b) \circ c = a \circ (b \circ c)$.

V obsegu $(\mathcal{O}, +, *)$ pa velja:

(O1) par $(\mathcal{O}, +)$ je grupa z enoto 0;

(O2) par $(\mathcal{O} \backslash \{0\}, *)$ je grupa z enoto 1;

(O3) za vse elemente $a, b, c \in \mathcal{O}$ je $a * (b + c) = a * b + a * c$ in $(b + c) * a = b * a + c * a$.

V tem sestavku bomo odgovorili na vprašanja o najmanjših grupah in obsegih ter na še nekatera sorodna vprašanja, naš cilj pa so končni obsegi, t.j. končne strukture, v katerih bomo znali ne samo seštevati in množiti, pač pa tudi odštevati in deliti.

Gotovo ste hitro ugotovili, da mora imeti grupa zaradi aksioma (G2) vsaj en element, enoto e namreč, obseg pa vsaj dva, enoto za operacijo "+" in enoto za operacijo "$*$". Nadalje se ni težko prepričati, da en element v primeru grupe že zadošča, saj $e \circ e = e$ izpolnjuje vse aksiome (G1)–(G4). V primeru obsega z dvema elementoma enako velja za multiplikativno grupo: $1 * 1 = 1$ izpolni aksiom (O2).

Ne pozabite, da operaciji "+" in "$*$" ne predstavljata (nujno) običajnega seštevanja in množenja. V tem sestavku bomo spoznali kar nekaj takih obsegov. V vsakem obsegu je produkt poljubnega elementa a z aditivno enoto 0 enak 0, saj je $0 * a = (0 + 0) * a = 0 * a + 0 * a$ (upoštevali smo (G2) in (O3)). Če odštejemo $0 * a$, res dobimo $0 * a = 0$. Podobno dobimo, da je tudi $a * 0 = 0$. V primeru najmanjšega obsega zato velja $0 * 0 = 0$ in $0 * 1 = 0 = 1 * 0$, kjer je 1 multiplikativna enota.

Kako pa je z grupo, ki ima dva elementa, npr. enoto e in a? Poleg $e \circ e = e$ in $e \circ a = a = a \circ e$ mora zaradi (G3) in $e \neq a$ veljati še $a \circ a = e$ in že so izpolnjeni vsi aksiomi (G1)-(G4). Torej velja za obseg z dvema elementoma in pravkar odkrito aditivno grupo tudi aksiom (O1). Zlahka preverimo še (O3), torej smo že našli najmanjši obseg.

Vrnimo se k vprašanju, koliko informacij potrebujemo za določitev grupe kot matematičnega objekta. Na to vprašanje je leta 1854 odgovoril *Arthur Cayley*. Po analogiji s tabelo množenja je vpeljal tabelo za poljubno binarno operacijo, ki ji bomo rekli *komponiranje*. Elemente množice G, v kateri je definirano komponiranje, razporedimo v zgornjo vrstico tabele in v enakem vrstnem redu še v levi stolpec tabele (imenovali ju bomo *koordinatna vrstica in stolpec*). V polja tabele pa vpišemo ustrezne *kompozitume* (tabeli 6a in 6b).

$+$	0	1
0	0	1
1	1	0

(a)

$*$	0	1
0	0	0
1	0	1

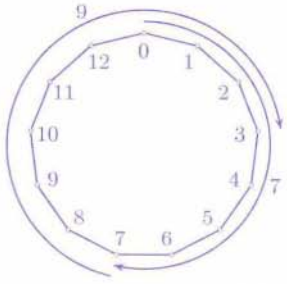
(b)

Tabela 6. Najmanjši obseg ima dva elementa, tabeli za njegovi operaciji pa sta (a) za seštevanje in (b) za množenje.

Gotovo ste opazili, da je $1+1=0$. V naslednjem razdelku bo postalo jasno, da ne gre za napako. Omeniti moramo le še, da pri iskanju grupe z enim in dvema elementoma sploh nismo imeli izbire pri določanju tabele, pri grupi s štirimi elementi pa obstajata že natanko dve različni grupi (ena ustreza grupi simetrij pravokotnika, drugo pa boste spoznali v naslednjem razdelku).

Praštevilski obseg $\mathbb{Z}_p$

Namesto s celimi števili bomo tokrat računali z ostanki pri deljenju s 13, t.j. z elementi iz množice $\mathbb{Z}_{13} = \{0, 1, \ldots, 12\}$. Računamo na naslednji način: števili seštejemo ali zmnožimo tako, da običajni rezultat nadomestimo z njegovim ostankom pri deljenju z *modulom* 13, npr. $7 +_{13} 9 = 7 + 9 \mod 13 = 3$ in $5 *_{13} 4 = 5 \cdot 4 \mod 13 = 7$, saj ima pri deljenju s 13 vsota 16 ostanek 3, produkt 20 pa ostanek 7 (tabela 7 in slika 1).



Slika 1. Prikaz računanja po modulu 13.

$+_{13}$	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12	0
2	2	3	4	5	6	7	8	9	10	11	12	0	1
3	3	4	5	6	7	8	9	10	11	12	0	1	2
4	4	5	6	7	8	9	10	11	12	0	1	2	3
5	5	6	7	8	9	10	11	12	0	1	2	3	4
6	6	7	8	9	10	11	12	0	1	2	3	4	5
7	7	8	9	10	11	12	0	1	2	3	4	5	6
8	8	9	10	11	12	0	1	2	3	4	5	6	7
9	9	10	11	12	0	1	2	3	4	5	6	7	8
10	10	11	12	0	1	2	3	4	5	6	7	8	9
11	11	12	0	1	2	3	4	5	6	7	8	9	10
12	12	0	1	2	3	4	5	6	7	8	9	10	11

(a)

$*_{13}$	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	[1]	2	3	4	5	6	7	8	9	10	11	12
2	0	2	4	6	8	10	12	[1]	3	5	7	9	11
3	0	3	6	9	12	2	5	8	11	[1]	4	7	10
4	0	4	8	12	3	7	11	2	6	10	[1]	5	9
5	0	5	10	2	7	12	4	9	[1]	6	11	3	8
6	0	6	12	5	11	4	10	3	9	2	8	[1]	7
7	0	7	[1]	8	2	9	3	10	4	11	5	12	6
8	0	8	3	11	6	[1]	9	4	12	7	2	10	5
9	0	9	5	[1]	10	6	2	11	7	3	12	8	4
10	0	10	7	4	[1]	11	8	5	2	12	9	6	3
11	0	11	9	7	5	3	[1]	12	10	8	6	4	2
12	0	12	11	10	9	8	7	6	5	4	3	2	[1]

(b)

Tabela 7. Seštevanje po modulu 13 (a), množenje po modulu 13 (b).

Če želimo sešteti ali zmnožiti več števil iz $\mathbb{Z}_{13}$, lahko pridemo do pravega rezultata tudi tako, da števila najprej seštejemo oziroma zmnožimo kot običajna cela števila in šele nato poiščemo ostanek pri deljenju s 13. To pomeni, da iz zakonov o združevanju celih števil za seštevanje in množenje (asociativnost) ter zakona o razčlenjevanju (distributivnost) sledi veljavnost zakonov o združevanju za seštevanje in množenje ter razčlenjevanju po modulu.

Pozoren bralec bo opazil, da se v vsakem stolpcu in v vsaki vrstici tabele za seštevanje nahajajo prav vsi elementi iz $\mathbb{Z}_{13}$. Podobno velja tudi za tabelo množenja, če odmislimo vse ničle. (Če bi 13 nadomestili s 14, bi videli, da tabela množenja po modulu 14 nima te lastnosti; le-ta je rezervirana samo za praštevila.) Torej lahko s pomočjo tabel 7(a) in 7(b) najdemo tudi razlike in kvociente. Če želimo izračunati $2 :_{13} 7$, iščemo odgovor na vprašanje, 7 krat koliko je 2. V tabeli 7(b) izberemo vrstico, ki ustreza številu 7, in ugotovimo, da se število 2 nahaja v stolpcu, ki pripada številu 4. Zato zaključimo, da je $2 :_{13} 7 = 4$. Do enakega zaključka bi prišli tudi, če bi številu 2 prišteli število 13 tolikokrat, da bi dobljena vsota postala deljiva s 7 in bi nato izračunali kvocient. Povejmo, da ne moremo izračunati $2 :_{14} 7$, torej $2 : 7$ v množici $\mathbb{Z}_{14}$. Zakaj ne?

S pomočjo tabel se ni težko prepričati, da je trojica $(\mathbb{Z}_{13}, +_{13}, *_{13})$ obseg. Prav tako hitro ugotovimo, da je $(\mathbb{Z}_n, +_n)$ grupa za poljubno naravno število n. Z razširjenim Evklidovim algoritmom (glej članka

M. Juvana, *O Evklidovem algoritmu*, Presek **21** (1993–94), str. 116–121, ter A. Jurišića, *Kako deliti skrivnost?*, Presek **29** (2001–02), str. 356–364), pa lahko enako pokažemo tudi za $(\mathbb{Z}_p \backslash \{0\}, *_p)$, kjer je p poljubno praštevilo. Tako pridemo do **praštevilskega obsega** $(\mathbb{Z}_p, +_p, *_p)$.

Tabele in grupe

Sedaj si oglejmo tabele nekoliko pobliže. Vprašali se bomo, kako lahko iz tabele ugotovimo, ali gre za grupo. Pri tem bomo opazovali naslednje lastnosti:

(T1) *V tabeli se lahko pojavijo samo tisti elementi, ki jih komponiramo.*

(T2) *Ena vrstica in en stolpec morata biti element za elementom enaka koordinatni vrstici in koordinatnemu stolpcu, množica enot v tabeli pa je simetrična glede na glavno diagonalo, t.j. diagonalo, ki izhaja iz levega zgornjega kota.*

(T3) *V vsaki vrstici in vsakem stolpcu se pojavi vsak element natanko enkrat.*

(T4) *V tabeli si izberimo enoto e in v njeni vrstici oziroma stolpcu še element r oziroma s. Potem je element, ki leži v isti vrstici kot s in istem stolpcu kot r, enak $s \circ r$,* (tabela 8(b)).

$\circ$		
	?	s
	r	e

(a)

$\circ$	x'	y
y'	$s \circ r$	s
x	r	e

(b)

Tabela 8.

Lastnost (T1) je ekvivalentna zaprtosti množice za komponiranje, medtem ko je lastnost (T2) ekvivalentna obstoju enote. Tablicam, ki zadovoljujejo lastnost (T3), pravimo *latinski kvadrati*. Lastnost (T3) je ekvivalentna zahtevi, da sta za poljubna elementa a in b enačbi $a \circ x = b$ in $x \circ a = b$ rešljivi, saj v vrstici oziroma stolpcu, ki ustreza elementu a, poiščemo element b, katerega stolpec oziroma vrstica ustreza elementu x. Če si za b izberemo enoto, potem nam ta lastnost zagotavlja obstoj inverznega elementa za vsak a. Prepričajmo se še, da velja lastnost (T4) v vsaki

grupi z enoto e (tabela 8(b)). Iz $x \circ y = e$, $x \circ x' = r$ in $y' \circ y = s$ namreč sledi $y \circ x = e$ in

$$y' \circ x' = (y' \circ e) \circ x' = y' \circ e \circ x' = (y' \circ (y \circ x)) \circ x' = (y' \circ y) \circ (x \circ x') = s \circ r.$$

Velja pa tudi obratno: pogoji (T1)–(T4) nam zagotavljajo, da tabela za komponiranje ustreza neki grupi.

Izrek. Tabela za komponiranje ustreza lastnostim (T1)–(T4) natanko takrat, ko je tabela neke grupe.

Dokaz. Prepričati se moramo le še, da iz (T1)–(T4) sledi asociativnost. Najprej izpeljemo asociativnost za elemente b^{-1}, b in c, t.j. $c = (b^{-1} \circ b) \circ c = b^{-1} \circ (b \circ c)$. Seveda lahko privzamemo $e \neq b$ in $c \neq b^{-1}$, saj je tedaj pogoj (G4) očitno izpolnjen. V tabeli izberemo vrstici e in b ter stolpca c in b^{-1}. Zapišemo ustrezne produkte, uporabimo (T4) in dobimo želeno relacijo (tabela 9(a)).

$\circ$	c	b^{-1}
$e = b^{-1} \circ b$	$c = b^{-1} \circ (b \circ c)$	b^{-1}
b	$b \circ c$	e

(a)

$\circ$	$b \circ c$	b
a	$a \circ (b \circ c) = (a \circ b) \circ c$	$a \circ b$
b^{-1}	$b^{-1} \circ (b \circ c) = c$	e

(b)

Tabela 9.

Sedaj pokažimo asociativnost še za poljubne elemente, t.j. $a \circ (b \circ c) = (a \circ b) \circ c$. Privzamemo $a \neq b^{-1}$ in $c \neq e$, kajti sicer sledi želena relacija iz pravkar obdelanega posebnega primera. Izberemo si vrstici a in b^{-1} ter stolpca $b \circ c$ in b ter uporabimo lastnost (T4) (tabela 9(b)).

Končni obseg GF(p^n)

Pokažimo, da tabeli 10(a) in 10(b) ustrezata grupnima operacijama in da je množica binarnih trojic $\{000, 001, 010, 011, 100, 101, 110, 111\}$ za ti operaciji obseg.

Zakon o združevanju (asociativnost) za seštevanje je pravzaprav očiten, saj seštevanje poteka tako, da seštevamo trojice po mestih (prvo, drugo in tretje) po modulu 2 (tabela 6(a)). Zato označimo to grupo z $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, +_2)$. Zakona o združevanju za množenje in zakona o razčlenjevanju (distributivnost) pa ni tako lahko neposredno preveriti. Če pa v ta namen uporabimo zgornji izrek, si lahko pomagamo z zakonom o zamenjavi, saj sta tabeli simetrični glede na glavno diagonalo.

+	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

(a)

*	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	111	101	011	001	100	110
011	000	011	101	110	111	100	010	001
100	000	100	011	111	010	110	001	101
101	000	101	001	100	110	011	111	010
110	000	110	100	010	001	111	101	011
111	000	111	110	001	101	010	011	100

(b)

Tabela 10. Seštevanje (a), množenje (b).

Za konec vključimo v našo zgodbo še polinome s stopnjo, manjšo od n, $n \in \mathbb{N}$, in s koeficienti iz obsega $(\mathbb{Z}_p, +_p, *_p)$, kjer je p praštevilo. Te polinome seštevamo na enak način kot števila v tabeli 10(a), le da tokrat seštevamo enakoležne koeficiente. Množimo jih tako, da običajni produkt zmanjšamo po modulu nekega polinoma stopnje n, ki ga ne moremo razcepiti v obsegu $(\mathbb{Z}_p, +_p, *_p)$. Tako zopet dobimo končni obseg. Matematikom je celo uspelo dokazati, da mora biti vsak končni obseg take oblike in da velja za množenje zakon o zamenjavi (Wedderburnov izrek), a to že presega okvir našega razmišljanja. Omenimo le še, da jih imenujemo **Galoisovi obsegi** in jih označimo z $\mathrm{GF}(p^n)$. Za $n = 1$ dobimo seveda praštevilski obseg.

Primer. Naj bo $n = 3$, $p = 2$ (tabeli 6(a) in 6(b)), za nerazcepni polinom pa si izberemo $x^3 + x^2 + 1$. Potem v zgornjih binarnih trojicah prvo mesto ustreza koeficientu ob x^3, drugo koeficientu ob x^2, tretje pa konstantnemu koeficientu.

Opomba. Osnova za Evklidov algoritem je lastnost, da lahko za vsak par naravnih števil a in b, $a > b$, najdemo natanko določeni števili q in r, da velja $a = qb + r$, kjer je ostanek r manjši od b. Za polinoma $a(x)$ in $b(x)$ nad končnim obsegom, $\mathrm{st}(a) > \mathrm{st}(b)$ (st je oznaka za stopnjo polinoma) pa velja $a(x) = q(x)b(x) + r(x)$, kjer je $\mathrm{st}(b) > \mathrm{st}(r)$. Za zgled pokažimo, kako z razširjenim Evklidovim algoritmom poiščemo obratni element polinoma $x^4 + x + 1$ v obsegu $GF(2^5)$ z nerazcepnim polinomom $x^5 + x^2 + 1$. Leva stran ustreza Evklidovemu algoritmu, desna pa razširjenemu delu:

$$x^5 + x^2 + 1 = x(x^4 + x + 1) + x + 1 \qquad x \cdot 1 + 0 = x$$

$$x^4 + x + 1 = (x^3 + x^2 + x + 1)(x + 1) + 1 \qquad (x^3 + x^2 + x + 1)x + 1 = x^4 + x^3 + x^2 + 1$$

Naloge

1. Isto grupo lahko srečamo v različnih preoblekah. Prepričaj se o tem za grupo $(\mathbb{Z}_4, +_4)$ in množico $\{1, -1, i, -i\}$, kjer je $i = \sqrt{-1}$, z običajnim množenjem. Potrebno je najti bijekcijo iz $\mathbb{Z}_4$ v $\{1, -1, i, -i\}$, ki preslika vsoto dveh elementov v produkt njunih slik. Taki preslikavi pravimo *izomorfizem*.

2. Znano je, da je multiplikativna grupa poljubnega končnega obsega *ciklična*, kar pomeni, da v grupi obstaja tak element, da so vsi elementi grupe njegove potence. Prepričaj se, da je ciklična grupa z n elementi izomorfna grupi $(\mathbb{Z}_n, +_n)$ (element 1 *generira* s svojimi večkratniki, kakor v aditivnem primeru pravimo potencam, vse elemente). To grupo označimo na kratko s C_n.
   Trditev preveri najprej na primeru (tabela 7(b) in 10(b)).

3. *Diederska grupa* D_n je grupa simetrij pravilnega n-kotnika. Dokaži, da v grupi D_3 ne velja zakon o zamenjavi (komutativnost) (grupo D_3 lahko predstavimo tudi kot grupo permutacij treh elementov $\mathcal{S}_3$).

4. Naslednja zanimiva grupa ima 8 elementov in ji pravimo *kvaternionka* (tabela 11). Poišči njeno tabelo množenja.

moč	ime grupe
1	C_1
2	C_2
3	C_3
4	C_4, $C_2 \times C_2$
5	C_5
6	C_6, D_3
7	C_7
8	C_8, $C_2 \times C_4$, $C_2 \times C_2 \times C_2$, D_8, Q_8
9	C_9, $C_3 \times C_3$
10	C_{10}, D_{10}

Tabela 11. *Moč* grupe je število njenih elementov. Zgornja tabela vsebuje vse grupe z največ desetimi elementi.

Za nadaljnje branje priporočamo: I. Grossman in W. Magnus, *Grupe in njihovi grafovi*, Školska knjiga Zagreb, 1975 in internet, npr. `http://members.tripod.com/ dogschool//`, za zrelejše bralce pa Vidav, *Algebra*, Mladinska knjiga, 1972.

Aleksandar Jurišić