MATEMATIKOS AKIRAČIAI

$\alpha + \omega$, 2001, Nr. 1, 53–56

Komutuojantys daugianariai

Giedrius Alkauskas

giedrius.alkauskas@maf.vu.lt

Kada dviejų daugianarių kompozicijos rezultatas nepriklauso nuo to, kurį daugianarį laikysime pirmu, kurį antru? Perskaitę šį straipsnį įsitikinsite, kad atsakyti nelengva, tačiau galima sukonstruoti įdomių pavyzdžių.

Kiekvienas mokinukas žino, kad sudedant arba dauginant skaičius jų eilė nesvarbi:

$$a + b = b + a, \qquad a \cdot b = b \cdot a. \tag{1}$$

Atidžiau pažiūrėjus, pasirodo, kad šios lygybės ne tokios jau ir akivaizdžios. Panagrinėkime pavyzdį, kai jos negalioja.

Tegu a reiškia šuolį iš mašinos, o b — mašinos sustabdymą. Tegu $a \cdot b$ reiškia veiksmų kompoziciją: pirma b, po to a. Analogiškai apibrėžkime ir $b \cdot a$. Dabar palyginkime rezultatus. Kompozicija $a \cdot b$ reiškia, kad pirma mašina sustojo, o po to iš jos iššokome. Jeigu tik mašina sustojo ne ant tilto, mums nieko neatsitiks. Paliekame skaitytojui pačiam įsivaizduoti veiksmo $b \cdot a$ padarinius. Šiaip ar taip, tikriausiai $a \cdot b \neq b \cdot a$.

Taigi (1) lygybės nėra nei visada teisingi gamtos dėsniai, nei logiškai įrodomi teiginiai. Tai tik tam tikros savybės, kurias vieni objektai gali turėti, o kiti ne.

Kelios savybės

O dabar pereikime prie tikrųjų mūsų straipsnelio herojų — daugianarių.

Nagrinėsime n-osios eilės daugianarius

$$P(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n,$$

kurių koeficientai a_i yra realieji skaičiai.

Tarkime, turime du tokius daugianarius $P(x)$ ir $Q(x)$ ir skaičių x_0. Iš pradžių pasinaudoję daugianariu $P(x)$, gausime skaičių $P(x_0)$, o po to pasinaudoję $Q(x)$, gausime skaičių $Q(P(x_0))$. Atlikę šias operacijas kita tvarka, gausime skaičių $P(Q(x_0))$. Ar abu šie skaičiai yra lygūs? Kartais jie lygūs, o kartais ne.

1 uždavinys. *Tegu $P(x) = ax + b$, $Q(x) = cx + d$. Įrodykite, kad, jei $b(c-1) \neq d(a-1)$, tai su visais x $P(Q(x)) \neq Q(P(x))$.*

Daugianarius, kurie su visais x tenkina lygybę $P(Q(x)) = Q(P(x))$, vadiname *komutuojančiaisiais*. Tokiu atveju žymėsime $P \sim Q$. Ar iš viso yra komutuojančių daugianarių? Akivaizdu, kad daugianaris $P(x) = x$ komutuoja su visais kitais daugianariais, o daugianaris $P(x) = x^2$ komutuoja su daugianariais $Q_k(x) = x^k$, $k = 1, 2, \ldots$.

2 uždavinys. *Įrodykite, kad daugianaris $P(x) = x^2$ komutuoja tik su išvardytaisiais daugianariais.*

Pastebėkime dar vieną įdomų faktą: su visais indeksais k, l

$$Q_k(Q_l(x)) = Q_k(x^l) = x^{kl} = Q_l(x^k) = Q_l(Q_k(x)),$$

taigi $Q_k(x)$ ir $Q_l(x)$ komutuoja tarpusavyje. Gavome begalinę šeimą poromis komutuojančių daugianarių. Iškelkime tokį klausimą: jei daugianaris P komutuoja su Q ir su R, ar Q ir R taip pat komutuoja? Atsakymą gauti, tiesą sakant, visai lengva. Daugianaris $P(x) = x$ komutuoja su visais daugianariais, tačiau juk yra ir nekomutuojančių daugianarių. Taigi bendruoju atveju atsakymas yra neigiamas. Tačiau pasirodo, kad nagrinėjant didesnio už vienetą laipsnio daugianarius, teiginys teisingas. Tai vienas įdomesnių faktų apie komutuojančius daugianarius.

Daugianario P laipsnį susitarsime žymėti $\deg P$. Šiame skyrelyje įrodysime tokią teoremą.

Teorema. *Tegu P, Q, R yra trys daugianariai, kurių laipsniai yra ne mažesni už 2. Jei daugianaris P komutuoja su Q ir su R, tai Q ir R taip pat komutuoja.*

Įrodymą pradėsime nuo pagalbinio teiginio.

1 lema. *Tegu $P(x)$ yra daugianaris, $\deg P \geqslant 2$. Tada kiekvienam $n \geqslant 2$ egzistuoja ne daugiau kaip vienas n-ojo laipsnio daugianaris Q, komutuojantis su P.*

Lemos įrodymas. Tegu toks daugianaris Q egzistuoja ir

$$P(x) = a_0x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m, \quad a_0 \neq 0, \ m \geqslant 2,$$
$$Q(x) = b_0x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n, \quad b_0 \neq 0, \ n \geqslant 2.$$

Kadangi daugianariai tarpusavyje komutuoja, tai $P(Q(x)) = Q(P(x))$, arba

$$\begin{aligned} &a_0Q(x)^m + a_1Q(x)^{m-1} + \cdots + a_{m-1}Q(x) + a_m = \\ &\quad = b_0P(x)^n + b_1P(x)^{n-1} + \cdots + b_{n-1}P(x) + b_n. \end{aligned} \tag{2}$$

Dabar sulyginkime koeficientus prie tų pačių x laipsnių (2) lygybės kairiojoje ir dešiniojoje pusėse:

$$\begin{aligned} &x^{mn}\colon\ a_0b_0^m = b_0a_0^n, \\ &x^{mn-1}\colon\ ma_0b_0^{m-1}b_1 = nb_0a_0^{n-1}a_1, \\ &x^{mn-2}\colon\ \ldots \end{aligned} \tag{3}$$

Iš pirmos lygybės vienareikšmiškai gauname b_0 (nes $m \geqslant 2$), iš antrosios — randame b_1 (nes $a_0b_0 \neq 0$). Nesunku įsitikinti (išrašykite dar keletą lygybių), kad kiekvienas koeficientas b_i vienareikšmiškai išreiškiamas koeficientais $a_0, a_1, \ldots, a_m$. Iš viso lygčių yra $mn+1$, o nežinomųjų — tik $n+1$, taigi gali atsitikti, kad sistema bus nesuderinta. Tokiu atveju komutuojantis su P daugianaris neegzistuos. Taigi lemos tvirtinimas teisingas: komutuojantis su P didesnio už vienetą laipsnio daugianaris arba yra vienintelis, arba jo iš viso nėra.

Dabar įrodykime teoremą.

Teoremos įrodymas. Tarkime, daugianariai P, Q, R tenkina teoremos sąlygą. Tada

$$P(Q(R(x))) = Q(P(R(x))) = Q(R(P(x))),$$

taigi $P(x)$ komutuoja su $Q(R(x))$. Analogiškai gauname, kad $P(x)$ komutuoja ir su $R(Q(x))$. Jeigu $\deg R = q$, $\deg Q = p$, tai abiejų su P komutuojančių daugianarių $R(Q(x))$ ir $Q(R(x))$ laipsniai yra lygūs pq. Kadangi $pq > 2$, tai pasirėmę lema gauname, kad daugianariai $R(Q(x))$ ir $Q(R(x))$ sutampa. Taigi Q ir R komutuoja. Teorema įrodyta.

Komutuojančių daugianarių klasės

Nagrinėkime daugianarių, kurių laipsnis ne mažesnis už 2, aibę. Joje sąryšis $\sim$ turi tokias savybes:

1) $P \sim P$ kiekvienam P (refleksiškumas);

2) jei $P \sim Q$, tai $Q \sim P$ (simetriškumas);

3) jei $P \sim Q$ ir $Q \sim R$, tai $P \sim R$ (tranzityvumas).

Pirmosios dvi savybės lengvai išplaukia tiesiog iš sąryšio $\sim$ apibrėžimo. Trečioji savybė išplaukia iš ankstesniame skyrelyje įrodytos teoremos ir antrosios savybės.

Sąryšis, tenkinantis 1)–3) savybes, vadinamas *ekvivalentumo* sąryšiu. Juo naudojantis, visus objektus (mūsų atveju — ne mažesnio kaip 2-ojo laipsnio daugianarius) galima suskaidyti į klases. Iš tikrųjų imkime kokį nors daugianarį P ir sudarykime komutuojančių su juo daugianarių (t. y. Q, kuriems $P \sim Q$) aibę. Į ją įeina pats P; bet kurie du jos elementai yra taip pat tarpusavyje komutuojantys daugianariai (3) savybė!). Taigi visus ne mažesnio kaip 2-ojo laipsnio daugianarius suskaidėme į klases. Šios klasės nesikerta. Iš tiesų, jei A ir B yra dvi tokios klasės, turinčios bendrą elementą R, t. y. $R \in A, R \in B$, tai su visais $P \in A$ ir $Q \in B$ teisingas sąryšis $R \sim P, R \sim Q$. Bet tada $P \sim Q$ ir P bei Q turi priklausyti tai pačiai klasei. Taigi A ir B turi sutapti.

Svarbiausias komutuojančių daugianarių teorijos uždavinys — tirti, kokie daugianariai šias klases sudaro. Mes jau turime vieną pavyzdį: daugianariai $Q_k(x) = x^k$, $k \geqslant 2$, sudaro vieną ekvivalentumo klasę.

Tegu $P(x)$ — bet koks, ne mažesnio kaip 2-ojo laipsnio daugianaris. Tada daugianariai $P(x), P(P(x)), P(P(P(x))), \ldots$ sudaro begalinę tarpusavyje komutuojančių daugianarių seką. Tačiau tvirtinti, kad jie sudaro visą ekvivalentumo klasę, mes negalime. Taip pat nelengva pasakyti, ar du skirtingus daugianarius $P(x)$, $Q(x)$ atitinkančios sekos

$$P(x), P(P(x)), P(P(P(x))), \ldots, \quad Q(x), Q(Q(x)), Q(Q(Q(x))), \ldots$$

neturi bendrų elementų. Akivaizdu, kad šios sekos turi bendrų elementų, jeigu P ir Q yra kokios nors sekos

$$R(x), R(R(x)), R(R(R(x))), \ldots$$

daugianariai.

Čebyšovo daugianariai

Šiame skyrelyje pasinaudosime tapatybe

$$\left(t^n + \frac{1}{t^n}\right)\left(t + \frac{1}{t}\right) = \left(t^{n+1} + \frac{1}{t^{n+1}}\right) + \left(t^{n-1} + \frac{1}{t^{n-1}}\right). \tag{4}$$

Teorema. *Kiekvienam $n \geqslant 1$ egzistuoja vienintelis n-ojo laipsnio daugianaris $P_n(x)$, su visais $t \neq 0$ tenkinantis sąlygą*

$$P_n\left(t + \frac{1}{t}\right) = t^n + \frac{1}{t^n}.$$

Įrodymas. Kai $n = 1$, daugianarį nesunku rasti: $P_1(x) = x$. Kadangi

$$\left(t + \frac{1}{t}\right)^2 = 2 + t^2 + \frac{1}{t^2}, \quad \text{tai} \quad P_2(x) = x^2 - 2.$$

Toliau pasinaudosime matematine indukcija. Tarkime, daugianariai $P_s(x)$ egzistuoja visiems $1 \leqslant s \leqslant n$.

Pasinaudosime (4) tapatybe perrašę ją taip:

$$t^{n+1} + \frac{1}{t^{n+1}} = P_n\Big(t + \frac{1}{t}\Big)\Big(t + \frac{1}{t}\Big) - P_{n-1}\Big(t + \frac{1}{t}\Big).$$

Iš šios lygybės matome, kad $P_{n+1}(x)$ vienareikšmiškai apibrėžiamas rekurenčiuoju sąryšiu

$$P_{n+1}(x) = P_n(x)x - P_{n-1}(x). \tag{5}$$

Iš (5) rekurenčiojo sąryšio nesunku rasti daugianarius $P_n(x)$ vieną po kito. Pavyzdžiui, $P_3(x) = x^3 - 3x$, $P_4(x) = x^4 - 4x + 2$ ir taip toliau.

Daugianariai $P_n(x)$ vadinami Čebyšovo daugianariais. Jie turi daug įdomių savybių. Pavyzdžiui, įrodysime, kad su visais m, n daugianariai $P_m(x)$ ir $P_n(x)$ komutuoja. Iš tiesų, kai $t \neq 0$, gauname

$$P_n\Big(P_m\Big(t + \frac{1}{t}\Big)\Big) = P_n\Big(t^m + \frac{1}{t^m}\Big) = t^{nm} + \frac{1}{t^{nm}} = P_m\Big(t^n + \frac{1}{t^n}\Big) = P_m\Big(P_n\Big(t + \frac{1}{t}\Big)\Big).$$

Kadangi reiškinys $x = t + \frac{1}{t}$ įgyja visas reikšmes x, $|x| > 2$, tai su jomis teisinga tapatybė $P_n(P_m(x)) = P_m(P_n(x))$. Tačiau iš tiesų ji teisinga su visais x, taigi daugianariai komutuoja. Todėl daugianariai $P_2(x), P_3(x), \ldots, P_n(x), \ldots$ sudaro vieną ekvivalentumo klasę.

Tapatybė, kuria pasinaudojome Čebyšovo daugianariams konstruoti, yra atskiras atvejis tokios tapatybės:

$$\Big(t^n + \frac{\xi^n}{t^n}\Big)\Big(t + \frac{\xi}{t}\Big) = \Big(t^{n+1} + \frac{\xi^{n+1}}{t^{n+1}}\Big) + \xi\Big(t^{n-1} + \frac{\xi^{n-1}}{t^{n-1}}\Big);$$

čia ξ yra fiksuotas skaičius. Panašiai kaip ir anksčiau, galime įrodyti, kad egzistuoja daugianariai $P_{n,\xi}(x)$, tenkinantys sąlygą

$$P_{n,\xi}\Big(t + \frac{\xi}{t}\Big) = t^n + \frac{\xi^n}{t^n}.$$

Reiškinį $t^{nm} + \frac{\xi^{nm}}{t^{nm}}$ galime užrašyti dviem būdais:

$$t^{nm} + \frac{\xi^{nm}}{t^{nm}} = P_{n,\xi^m}\Big(t^m + \frac{\xi^m}{t^m}\Big) = P_{n,\xi^m}\Big(P_{m,\xi}\Big(t + \frac{\xi}{t}\Big)\Big)$$

ir

$$t^{nm} + \frac{\xi^{nm}}{t^{nm}} = P_{m,\xi^n}\Big(t^n + \frac{\xi^n}{t^n}\Big) = P_{m,\xi^n}\Big(P_{n,\xi}\Big(t + \frac{\xi}{t}\Big)\Big).$$

Iš šios tapatybės gauname dar vieną, siejančią keturis daugianarius:

$$P_{n,\xi^m}(P_{m,\xi}(x)) = P_{m,\xi^n}(P_{n,\xi}(x)).$$

Pasirinkę ξ taip, kad būtų $\xi^m = \xi^n = \xi$, gautume dar vieną komutuojančių daugianarių seką. Kai $\xi = 1$, gauname tuos pačius Čebyšovo daugianarius. Matome, kad ξ turi tenkinti lygybes $\xi^{n-1} = \xi^{m-1} = 1$. Jei n ir m nelyginiai, tai šios lygybės tenkinamos su $\xi = -1$. Taigi gauname dar vieną begalinę komutuojančių daugianarių seką

$$P_{3,-1}(x), P_{5,-1}(x), \ldots, P_{2n+1,-1}(x), \ldots.$$

Daugiau komutuojančių daugianarių sekų gautume rinkdami kompleksinius skaičius ξ.