Polinom-e minden függvény?

CSÁKÁNY BÉLA*

A címben feltett kérdésre számos egyetemi hallgató kollégám nagyjából azonos módon reagált. Először pontosította a pongyolán kitűzött problémát, pl. így: "Valós (együtthatós) polinom(mal felírható)-e minden valós fügvény?" Ezután megadta a választ, ami — helyesen — mindig "nem" volt, csak az indokolások különböztek, tükrözve a válaszoló ismereteit és érdeklődését.

1. A valós függvények halmazának számossága nagyobb, mint a valós polinomok halmazáé.

2. A valós polinomok folytonos függvények, de nem minden valós függvény folytonos.

3. $\frac{1}{x^2+1}$ nem polinom, mert minden racionális törtfüggvény egyetlen módon írható fel egy polinom és elemi törtfüggvények összegeként.

A következőkben pontosabban és általánosabban fogalmazzuk meg a címben szereplő kérdést, és megmutatjuk, hogy a válasz bizonyos esetekben "igen" (!). Ehhez először a polinom fogalmát kell tisztáznunk.

A szokásnak megfelelően $f : M \to M$ a továbbiakban azt jelenti, hogy f az M halmaznak M-be való leképezése; ekkor $f : a \mapsto a'$ azt jelenti, hogy f az M halmaz tetszőleges a elemének a'-t felelteti meg; természetesen a' helyett írhatunk $f(a)$-t is. Pl. ha $\mathbf{R}$ a valós számok halmazát jelöli, $f : \mathbf{R} \to \mathbf{R}$, $f : a \mapsto a^2$ azt jelenti, hogy f a valós számok halmazán értelmezett négyzetreemelés (azaz $f(a) = a^2$ minden $a \in \mathbf{R}$ számra).

Az M értelmezési tartományú függvények közül a legegyszerűbb az **identikus függvény**; jelölje ezt x. További egyszerű függvények a **konstans függvények**; legyen $c : a \mapsto c$ (azaz minden konstans függvényt jelöljünk az értékével). Ha M-en eleve bizonyos műveletek (pl. összeadás, szorzás) vannak értelmezve, ezeket természetes módon elvégezhetjük az M-en értelmezett, M-be eső értékkészletű függvényeken is a következőképpen: az $f : M \to M$, $g : M \to M$ függvényekre legyen pl. $f + g : M \to M$, $f + g : a \mapsto f(a) + g(a)$. Ezt a függvények pontonkénti összeadásának, általában pedig a függvényeken így értelmezett műveleteket **pontonkénti műveleteknek** nevezzük. Így pl. a négyzetreemelés $\mathbf{R}$-en az identikus függvény önmagával való pontonkénti szorzata.

Mostmár könnyen észrevehetjük, hogy a közönséges — a meghatározottság kedvéért, mondjuk, valós — polinomok által megadott függvények pontosan

* Ez a cikk a tiszakécskei Móricz Zsigmond Gimnáziumban működő Rédei Kör 1990. november 19-i Rédei-emlékülésén elhangzott előadás részletesebb változata. Hálás vagyok Zsuffa Lajos tanár-kollégámnak e szakmai konferencia Rédei László emlékéhez méltó megszervezéséért és a meghívásért.

azok az $f : \mathbf{R} \to \mathbf{R}$ függvények, amelyek az $\mathbf{R}$-en értelmezett identikus függvényből és konstans függvényekből a pontonkénti összeadás és szorzás segítségével (pontosabban beszélve: ezek véges számú elvégzésével) előállíthatók. Valóban, nevezzük az így előálló függvényeket ($\mathbf{R}$ **feletti**) **polinom-függvényeknek.** Ekkor az előállításukhoz szükséges pontonkénti műveletek száma szerinti teljes indukcióval belátható, hogy az $\mathbf{R}$ feletti polinom - függvények mind felírhatók a hagyományos

$$(*) \qquad a_n x^n + \ldots + a_1 x + a_0 \quad (a_i \in \mathbf{R};\ i = 0, \ldots, n)$$

alakban; másrészt az $(\star)$ alakú polinom szemmelláthatóan egy $\mathbf{R}$ feletti polinom-függvény felírása.

Eszerint a valós polinomok — az (*) alakú jelsorozatok — a valós számtest feletti polinom-függvények jelei. Gyakran előfordul, hogy egy vizsgált dolognak és a jelölésére szolgáló dolognak a megnevezésére ugyanazt a szót használjuk (pl. permutáción egyaránt értünk bizonyos fajta leképezést és — az ilyen leképezések megadására alkalmas — jelsorozatot). Most is ezt fogjuk tenni: polinomról beszélve, ezen érthetünk polinom-függvényt is és az őt megadó jelsorozatot is. Ha lényeges, hogy melyikről van szó, ez kiderül a szövegkörnyezetből. (Tankönyvekben rendszerint szigorúan különbséget tesznek polinom és polinom-függvény között, amire a polinomok elméletének rendszeres felépítéséhez valóban szükség is van.)

Eddig **egyváltozós** polinomokról volt szó; rájöttünk, hogy ezekben az x változó az identikus függvény jele. Használunk azonban többváltozós polinomokat is; pl. az $s = a \cdot (x_1x_2 + x_1x_3 + x_2x_3)$ háromváltozós polinom a harmadfokú algebrai egyenlet gyökei és együtthatói közötti összefüggésben szerepel (ha x_1, x_2, x_3 az $ax^3 + bx^2 + cx + d = 0$ egyenlet gyökei, akkor polinomunk éppen a c együttható értékét adja meg). Mit jelentenek itt az x_1, x_2, x_3 változók? Identikus függvény csak egy van; azt nem jelenthetik. Az s polinom háromváltozós függvényt határoz meg, amelynek értékét az (r, s, t) helyen úgy számítjuk ki, hogy x_1 helyébe az r, x_2 helyébe az s, x_3 helyébe a t értéket írjuk, s a kijelölt műveleteket elvégezzük. Eszerint x_1 azt a függvényt jelenti, amely bármely elemhármashoz annak első elemét rendeli, x_2 és x_3 pedig hasonlóképpen a második ill. harmadik elemét. Projekciófüggvényeknek, röviden **projekcióknak** nevezzük őket, mivel térbeli Descartes-féle koordinátarendszerben az (r, s, t) pontnak pl. az első koordinátatengelyre (amelyet számegyenesnek tekintünk) való vetülete, más szóval projekciója éppen az r szám. Bármely n természetes szám esetén tekinthetjük az $x_1, \ldots, x_n$ n-változós projekciókat: x_i az az n-változós függvény, amely minden elem-n-eshez annak i-edik elemét rendeli. Az egyetlen egyváltozós projekció éppen az identikus függvény.

Idáig eljutva, nem lesz nehéz meggondolnunk, hogy bármely n-re az n-változós valós polinomok éppen azokat a valós függvényeket jelölik, amelyek az n-változós projekciókból és az n-változós konstans függvényekből

$(c : (a_1, \ldots, a_n) \mapsto c;\ a_1, \ldots, a_n,\ c \in \mathbb{R})$ a pontonkénti összeadás és szorzás véges számú alkalmazásával keletkeznek (ha f és g n-változós valós függvények — röviden: $f, g : \mathbb{R}^n \to \mathbb{R}$ — akkor pl. pontonkénti összegük $f + g : (a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n)$). Jegyezzük meg, hogy műveletek véges számú alkalmazásába azt a lehetőséget is beleértjük, hogy a műveleteket egyszer sem alkalmazzuk; ennek megfelelően a projekciók és a konstansok is polinomok.

Most jön a meglepő észrevétel: **polinomokat bármely halmazon bevezethetünk**, hiszen bármely halmazon van identikus függvény és vannak akárhány változós projekciófüggvények, ugyancsak vannak akárhány változós konstans függvények is; továbbá, ha halmazunkon még műveletek is vannak megadva, akkor a pontonkénti műveletek is elvégezhetők, s ezekkel a már rendelkezésünkre álló függvényekből újabbakat képezhetünk. Ha a valós polinomok speciális esetében tapasztaltakat akarjuk általánosítani, akkor a polinom következő definícióját fogadhatjuk el:

Tekintsünk egy M halmazt és az M-en értelmezett műveletek egy O halmazát (amely üres is lehet). Az (M, O) **algebrai struktúra polinomjain** azokat az M-en értelmezett függvényeket értjük, amelyek projekciókból és konstans függvényekből az O-beli műveletek végesszámú pontonkénti elvégzésével nyerhetők. (Ebben a mondatban négy helyen is kitehettük volna az "n-változós" jelzőt; így (M, O) **n-változós polinomjai** definíciójához jutottunk volna. Természetesen a pontonkénti műveleteket csak azonos változószámú függvényeken végezhetjük el!)

Látjuk, hogy ha halmazunkon nincsenek műveletek, akkor nincsenek más polinomok, mint a projekciók és a konstansok. Másrészt, jelölje O_M az M-en értelmezhető összes — akárhány változós — M-be eső értékkészletű függvények halmazát. Tekintsük az (M, O_M) algebrai struktúrát (azaz nevezzünk ki M-en minden lehetséges függvényt műveletnek); akkor az O_M-beli függvények mind polinomjai lesznek (M, O_M)-nek, hiszen az $f : M^n \to M$ m-változós függvény nyilvánvalóan előáll $f(x_1, \ldots, x_n)$ alakban, vagyis úgy, hogy az $x_1, \ldots, x_n$ n-változós projekciókon az f pontonkénti műveletet végezzük el.

Mivel egy M alaphalmazú algebrai struktúra polinomjai mind O_M-hez tartoznak, csak az O_M-beli függvényektől várható el, hogy mind egy M alaphalmazú algebrai struktúra polinomjai legyenek. A címbeli kérdés tehát korrektül, teljes általánosságban így hangzik: van-e olyan (M, O) algebrai struktúra, amelynek az O_M-hez tartozó függvények mind polinomjai? Az előző bekezdésben láttuk, hogy (M, O_M) eleget tesz ennek a követelménynek, tehát az általánosított kérdésre a válasz: "igen"! Ám ez a — valljuk meg, triviális — válasz aligha teszi elégedetté az olvasót, aki szeretne olyan természetes, lehetőleg már korábban ismert algebrai struktúrát is látni, amelyen minden függvény polinom. A következőkben ilyen példákkal ismerkedünk meg.

Rögzítsünk egy p prímszámot és tekintsük a $\mathbf{p} = \{0, 1, \ldots, p-1\}$ halmazon a modulo p összeadást és szorzást, azaz, ha $a, b \in \mathbf{p}$, legyen a és b modulo p összege az $a + b$ (közönséges) összeg p-vel való osztásának maradéka; hasonlóan értelmezzük a modulo p szorzást. Ismeretes, hogy a $(\mathbf{p}, \{+, \cdot\})$ algebrai struktúrában a kivonás és a nem 0-val való osztás is elvégezhető, s a műveletek rendelkeznek a számokon végzett műveletek néhány fontos tulajdonságával (asszociativitás, kommutativitás, disztributivitás). Ez az algebrai struktúra a p **elemű véges test**, szokásos jele $GF(p)$.* Nem nehéz felismernünk benne a mod p maradékosztálytestet. Megmutatjuk, hogy a $GF(p)$**-n értelmezhető függvények mind** $GF(p)$ **polinomjai.** Ezt a tényt Rédei László és Szele Tibor fedezték fel 1947-ben.

Legyen először $f : GF(p) \to GF(p)$ egyváltozós függvény. Ha $i = 0, 1, \ldots, (p-1)$-re van olyan χ_i polinomunk, hogy $\chi_i(i) = 1$, és $\chi_i(j) = 0$ $k \neq i$ esetén, úgy készen vagyunk, mert ekkor $f(x) = f(0) \cdot \chi_0(x) + \ldots + f(p-1) \cdot \chi_{p-1}(x)$, és így f polinom, mivel polinomokból és konstansokból $GF(p)$ műveletei — összeadás és szorzás — végesszámú alkalmazásával keletkezik (f felépítésének ezt az ötletét a klasszikus algebra Lagrange-féle interpolációs formulájából vettük át). Ám a kívánt polinomok valóban léteznek: $\chi_i(x) = 1 - (x - i)^{p-1}$, ugyanis ha $x = i$, akkor $\chi_i(x) = 1$; ha pedig $x = j \neq i$, akkor $(x - i)^{p-1} = (j - i)^{p-1} = 1$ (ez utóbbi egyenlőség éppen a kis Fermat-tétel!), ezért $\chi_i(x) = 0$.

Bizonyításunk azon múlt, hogy $GF(p)$ elemeinek **karakterisztikus függvényei** polinomoknak bizonyultak. Ez az észrevétel többváltozós függvényekre is használható. Az $(i_1, \ldots, i_n)$ elem-n-es karakterisztikus függvénye

$$\chi_{(i_1,\ldots,i_n)}(x_1, \ldots, x_n) = \begin{cases} 1, & \text{ha } x_1 = i_1, \ldots, x_n = i_n, \\ 0 & \text{máskülönben.} \end{cases}$$

Ellenőrizhetjük, hogy $\chi_{(i_1,\ldots,i_n)}(x_1, \ldots, x_n) = (1 - (x_1 - i_1)^{p-1}) \ldots (1 - (x_n - i_n)^{p-1})$. Ekkor pedig bármely $f : (GF(p))^n \to GF(p)$ n-változós függvény felírható

$$f(x_1, \ldots, x_n) = \sum_{(i_1,\ldots,i_n) \in (GF(p))^n} f(i_1, \ldots, i_n) \cdot \chi_{(i_1,\ldots,i_n)}(x_1, \ldots, x_n)$$

alakban (figyeljük meg, hogy a jobboldali p^n tagú összegnek bármely $x_1 = j_1, \ldots, x_n = j_n$ helyettesítés esetén egyetlen tagja különbözik 0-tól, és az a tag éppen $f(j_1, \ldots, j_n)$). A jobboldalon n-változós polinom áll, s ezzel a bizonyítás kész.

---

* GF a német Galois-Feld (Galois-mező) rövidítése; az algebrai egyenletek megoldhatóságának elméletét megalkotó E. Galois emlékét őrzi.

A $p > 2$ esetben a többváltozós függvényekre vonatkozó meggondolás megtakarítható, ha tudjuk Słupecki lengyel matematikus 1939-ben bizonyított tételét, amely szerint, ha egy legalább 3 elemű véges alaphalmazú (M, O) algebrai struktúrának **van lényeges művelete**, és az O_M-be tartozó **egyváltozós** függvények mind (M, O) polinomjai, akkor az O_m-be tartozó **összes** függvények (M, O) polinomjai. Słupecki az M-en értelmezett olyan műveletet nevezte lényegesnek, amely ténylegesen függ legalább két változójától és értékkészlete az egész M halmaz ($GF(p)$ mindkét művelete ilyen). Słupecki tételének bizonyítása nem kíván ugyan előismereteket, de nem is egyszerű; ezért itt mellőzzük.*

Az utóbbi évtizedekben számos, más szempontból is érdekes algebrai struktúráról derült ki, hogy az alaphalmazán értelmezhető s abba eső értékkészletű függvények mind polinomjai. Ezért az ilyen algebrai struktúrák külön elnevezést kaptak: **függvényteljesnek** nevezzük őket. Most két további példát mutatunk be függvényteljes algebrai struktúrára.

Fried Ervin és Alden F. Pixley amerikai matematikus 1977-ben kezdte vizsgálni a háromváltozós d **duális diszkriminátor-műveletet**, amely minden M halmazon definiálható a következőképpen: bármely $a, b, c \in M$ esetén

$$d(a,b,c) = \begin{cases} a, & \text{ha } a = b, \\ c & \text{máskülönben.} \end{cases}$$

Vegyük észre, hogy, ha d legalább két változója megegyezik, akkor a "többségben levő" változó lesz d értéke, míg csupa különböző változók esetén az utolsó változó (azaz d demokratikusan és udvariasan viselkedik). Fried és Pixley többek között azt is bebizonyították, hogy, **ha M legalább három elemű véges halmaz, akkor (M, d) függvényteljes**. Bemutatjuk ennek egy egyszerű bizonyítását.

Először megmutatjuk, hogy d lényeges művelet. Valóban, d értékkészlete M; továbbá a $d(a,b,a) = a$, $d(b,b,a) = b$, $d(b,a,a) = a$, $d(b,a,b) = b$ egyenlőségek mutatják, hogy d mindhárom változójától ténylegesen függ. Ezért Słupecki tétele alapján csak azt kell belátnunk, hogy M minden önmagába való leképezése polinomja (M, d)-nek.

Jelölje n az M halmaz elemeinek számát. Felhasználjuk azt a tényt, hogy M bármely önmagába való leképezése megkapható leképezés-szorzással M összes transzpozícióiból (azaz két elemet felcserélő, a többieket változatlanul hagyó leképezéseiből) és egyetlen olyan további leképezésből, amelynek

* A bizonyítás megtalálható a következő helyen: Diszkrét matematika a számítástudományban (szerk.: Sz. V. Jablonszkij és O. B. Lupanov), Műszaki Könyvkiadó, Budapest, 1980; 50-56. oldal. Függvényteljes algebrai struktúrákról általában S. Burris és H. P. Sankappanavar Bevezetés az univerzális algebrába című könyvében olvashatunk (Tankönyvkiadó, Budapest, 1988; 195-202. oldal).

értékkészlete $n-1$ elemből áll. Jegyezzük meg azt is, hogy ha az $\alpha : M \to M$ leképezést az f polinom, a $\beta : M \to M$ leképezést a g polinom állítja elő, akkor α és β szorzata ugyancsak előállítható polinommal, mégpedig a $gf : a \mapsto g(f(a))$ polinommal. Ezek szerint a bizonyításhoz elegendő lesz polinom-alakban felírnunk M

(a) tetszőleges transzpozícióját, és

(b) egyetlen olyan leképezését önmagába, melynek értékkészlete $n-1$ elemű.

(a) Tekintsük M egy τ transzpozícióját és jelölje $1, 2$ az M halmaz τ által felcserélt két elemét, $3, \ldots, n$ pedig a többi elemeit. Nem nehéz találni (M, d)-nek olyan polinomját, amely 1-et 2-vel felcseréli, M többi elemét pedig 1-be viszi át. Ilyen a $d(2, d(3, d(1, x, 3), 2), 1)$ polinom; jelölje ezt $g_2(x)$. Definiáljuk a $g_3(x), \ldots, g_n(x)$ polinomokat a

$$g_k(x) = d(k, x, g_{k-1}(x)) \quad (k = 3, \ldots, n)$$

szabállyal, s ellenőrizzük, hogy g_k 1-et 2-vel felcseréli, a $3, \ldots, k$ elemeket változatlanul hagyja, a $k+1, \ldots, n$ elemeket pedig 1-be viszi át. Ekkor g_n éppen a τ transzpozíció.

(b) Tekintsük azt a $\sigma : M \to M$ leképezést, melyet $\sigma(1) = 2$ és $i \neq 1$-re $\sigma(i) = i$ definiál. Ekkor $h_2(x) = d(2, x, g_2(x))$ megegyezik σ-val az $1, 2$ elemeken, M többi elemét pedig 1-be viszi át. Most vegyük a

$$h_j(x) = d(k, x, h_{k-1}(x)) \quad (k = 3, \ldots, n)$$

polinomokat. Mint az imént, ellenőrizhető $h_n = \sigma$, s a bizonyítás kész.

Harmadik példánk a bizonyára sokak által ismert **élet-játékkal** van kapcsolatban, melyet 1970-ben talált ki John H. Conway cambridge-i matematikus. A játék lényege a következő: a $t = 0$ időpontban egy síkbeli végtelen négyzetrács minden elemi négyzete vagy aktív, vagy passzív állapotban van. A négyzetek állapota időegységenként változik a következő szabályok szerint:

(1) Ha egy passzív négyzet nyolc szomszédja közül pontosan három aktív, akkor aktívvá változik; különben passzív marad.

(2) Ha egy aktív négyzet nyolc szomszédja közül kettő vagy három aktív, akkor aktív marad; különben passzívvá válik.

Ennek megfelelően az aktív állapotok alkotta kezdeti alakzat változik, fejlődik, s ezt igen érdekes megfigyelni, különösen, ha az (1), (2) szabályokat nem a megfigyelőnek kell fáradságos, könnyen elhibázható munkával alkalmazni, hanem személyi számítógép és megfelelő program állítja elő és jeleníti meg a képernyőn az alakzat fejlődését, "életét".

Jelölje 1 az aktív, 0 a passzív állapotot. Az állapotváltozás (1), (2) szabályai egy kilencváltozós c műveletet adnak meg a $\mathbf{2} = \{0, 1\}$ halmazon a következő módon: $a_1, \ldots, a_9 \in \mathbf{2}$ esetén legyen $c(a_1, \ldots, a_9)$ az élet-játék négyzetrácsa

bármely 3×3-as részrácsa középső négyzetének állapota a $t+1$ időpontban, ha a kilenc négyzet állapota a t időpontban a következő:

a_9	a_2	a_3
a_8	a_1	a_4
a_7	a_6	a_5

Például

$$c(0,1,0,0,1,1,0,0,0) = 1,\ c(0,0,0,1,0,0,0,0,1) = c(0,1,1,1,1,1,1,1,1) = 0$$

az (1) szabály szerint, és

$$c(1,1,1,0,0,0,0,0,0) = c(1,0,1,0,1,0,1,0,0) = 1,\ c(1,1,0,0,0,0,0,0,0) = 0$$

a (2) szabály szerint.

Tekintsük a $(\mathbf{2}, c)$ algebrai struktúra

$$c_a = c(0,0,0,x_1,x_1,x_1,x_2,x_2,x_2)$$

és

$$c_m = c(0,0,0,0,0,0,x_1,x_1,x_2)$$

kétváltozós polinomjait. Akkor $c_a(a_1,a_2)$ éppen a_1 és a_2 modulo 2 összege, $c_m(a_1,a_2)$ pedig a_1 és a_2 modulo 2 szorzata; ezért $(\mathbf{2}, c_a, c_m)$ — amelynek műveletei $(\mathbf{2}, c)$ polinomjai — nem más, mint $GF(2)$. Korábban láttuk azonban, hogy $GF(2)$ függvényteljes. Most a polinom és a függvényteljesség definíciójából azonnal következik, hogy $(\mathbf{2}, c)$ is függvényteljes.

A cikk elején említett 1. számú cáfolatot tovább gondolva beláthatjuk, hogy ha egy végtelen algebrai struktúrának nincs több művelete, mint eleme, akkor nem lehet függvényteljes. Ebből következik, hogy csak véges csoportok, gyűrűk és hálók lehetnek függvényteljesek. Ismeretes, hogy a csoportok közül pontosan a véges nemkommutatív egyszerű csoportok függvényteljesek (az algebrai struktúrát **egyszerűnek** mondjuk, ha minden művelettartó leképezése vagy kölcsönösen egyértelmű, vagy konstans).* Hasonló állítás érvényes a gyűrűkre: egy gyűrű akkor és csak akkor függvényteljes, ha véges, nem zérógyűrű

* Ezeket a csoportokat ma már teljesen ismerjük, leírásuk a huszadik századi algebra egyik csúcsteljesítménye; itt csak azt a tényt idézzük fel, hogy a legegyszerűbb (nemkommutatív) egyszerű csoportot öt elem összes páros permutációi alkotják.

(azaz vannak olyan elemei, melyek szorzata nem 0) és egyszerű. Végül, egynél több elemű háló nem lehet függvényteljes. Ezt — ellentétben a csoportok és gyűrűk függvényteljességére vonatkozó tételekkel — könnyű belátni: a háló részbenrendezett halmaz (is), s e részbenrendezésre nézve a hálóműveletek monotonok; úgyszintén monotonok a projekciók és a konstans függvények, ezért a polinomok, amelyek mindezekből képezett összetett függvények, ugyancsak monotonok. A nemmonoton függvények tehát nem lehetnek polinomok.

Csákány Béla
József Attila Tudományegyetem
Bolyai Intézet
Szeged, Aradi vértanuk tere 1.