KAPCSOLATOK POLINOMOKNAK ÉS HELYETTESÍTÉSI ÉRTÉKEIKNEK SZÁMELMÉLETI TULAJDONSÁGAI KÖZÖTT

LOVÁSZ LÁSZLÓ

I. Az egész együtthatós polinomok körében egyértelmű az irreducibilis felbontás, így e polinomok körében az egész számok elméletéhez hasonló számelmélet építhető ki. Kérdés, hogy az a homomorfizmus, melyet a „behelyettesítés" létesít e két gyűrű között, mennyire tartja meg a számelméleti tulajdonságokat. Ilyen jellegű kérdés természetesen igen sok felvethető, és igen sok közülük nagyon nehéz. Az a kérdés pl., hogy ha egy $f(x)$ polinomra minden egész a helyen $f(a)$ összetett, akkor milyen feltételek mellett lesz más polinomok szorzata, a számelmélet igen nevezetes megoldatlan problémája és csak lineáris polinomokra adja meg a választ Dirichlet nevezetes tétele.[1]

Igen egyszerűen megválaszolható probléma azonban a következő: Tegyük fel, hogy minden $a \geqq a_0$ egész helyen

$$f(a) | g(a).$$

Igaz-e, hogy $f(x) | g(x)$? A válasz az, hogy ha $f(x)$ együtthatóinak legnagyobb közös osztója relatív prím $(gr\, g)$!-hoz, akkor igaz. Osszuk el ugyanis $g(x)$-et $f(x)$-szel maradékosan:

$$g(x) = q(x) f(x) + r(x),$$

ahol $q(x)$, $r(x)$ racionális együtthatós polinomok. Jelölje c a $q(x)$-ben fellépő nevezők legkisebb közös többszörösét, akkor

$$\frac{cg(a)}{f(a)} - cq(a) = \frac{r(a)}{f(a)}$$

egész szám minden $a \geqq a_0$ helyen. Mivel másrészt ez 0-hoz tart ($a \to \infty$; $gr\, r < gr\, f$ miatt), kell, hogy elég nagy a-ra — és így a számláló polinom lévén, minden a-ra — eltűnjék. Tehát

$$q(a) = \frac{g(a)}{f(a)}$$

értéke mindenütt egész szám, és így mint ismeretes,[2]

$$q(x) = \frac{1}{m!} Q(x) \qquad (m = gr\, q < gr\, g)$$

[1] T. i., hogy ha egy lineáris polinom értéke mindenütt összetett szám, akkor együtthatói nem relatív prímek. Általában szükséges még feltenni, hogy a tekintett polinomnak ne legyen konstans osztója, de hogy ez elégséges-e, az nem ismeretes.

[2] Lásd pl. [6] 61—62. oldal 1. jegyzet.

ahol $Q(x)$ egész együtthatós. Legyen mármost $f(x)$ együtthatóinak legnagyobb közös osztója d, ekkor $\frac{f(x)}{d}$ primitív polinom és így Gauss lemmája szerint

$$\frac{\frac{g(x)}{f(x)}}{d} = \frac{d}{m!} Q(x)$$

egész együtthatós. Ez azonban $(d, m!) = 1$ miatt csak úgy lehet, ha $q(x) = \frac{1}{m!} Q(x)$ is egész együtthatós.[3]

II. Dolgozatunk fő célja az alábbi tétel bizonyítása, mely Brissetől és Jentzschtől származik:

TÉTEL: *Ha $f(x)$ egész együtthatós polinom, melynek értéke minden egész helyen egy egész szám k-adik hatványa, akkor $f(x)$ egy egész együtthatós polinom k-adik hatványa.*

E tétel lényegesen mélyebben fekvő az I. pontban bizonyítottaknál, és számos különböző bizonyítás ismeretes rá[4]. Az alábbiakban egy polinomalgebrai jellegű bizonyítást mutatunk be rá. E bizonyítás — értelemszerű módosításokkal — minden olyan prímfaktorizációs integritási tartomány felett érvényben maradna, melyben az I. pont tétele érvényes.

III. A tétel bizonyítása céljából emeljük ki $f(x)$-ből azt a legmagasabb fokú polinomosztóját, mely teljes k-adik hatvány:

$$f(x) = g(x)^k h(x).$$

Bontsuk fel $h(x)$-et irreducibilis tényezők szorzatára:

$$h(x) = h_1(x)^{k_1} \dots h_n(x)^{k_n}.$$

Itt nyilvánvaló an $k_i < k$ $(1 \leqq i \leqq n)$. Mivel a $h_i(x)$ polinomok Gauss lemmája szerint a racionális számok felett is irreducibilisek, nincs többszörös gyökük és két különböző $h_i(x)$-nek nincs közös gyöke. Ebből következik, hogy $h(x)$ gyökei legfeljebb $(k-1)$-szeres multiplicitásúak. Ha kimutatjuk, hogy másrészt legalább k-szoros multiplicitásúak, akkor $h(x)$ csak konstans lehet, éspedig csak egy másik konstans k-adik hatványa, ami a tételt bizonyítja.

$h(x)$-ről egyelőre annyit állapíthatunk meg, hogy értéke minden olyan egész helyen, ahol $g(x) \neq 0$, k-adik hatvány.

Azt akarjuk tehát bizonyítani, hogy ha egy m-ed fokú $h(x)$ polinom értéke

[3] A fenti bizonyítás tartalmaz algebrától idegen (azaz pl. primfaktorizációs gyűrűkben nem interpretálható) elemet, t. i. 0-hoz tartást. Ezt azonban némi bonyolódás árán elkerülhetjük. Legyen ui. $f(x)$ és $g(x)$ legnagyobb közös osztója $h(x)$, $f = h \cdot \varphi$, $g = h \cdot x$. Ekkor van olyan $p(x)$, $q(x)$ polinom és c egész szám, hogy $c \cdot h(x) = p(x)f(x) + q(x) \cdot g(x)$, amiből adódik, hogy $\varphi(a) | c$ minden egész a-ra. Ez nyilván csak úgy lehet, ha φ konstans. Innen a bizonyítás a fentiekhez hasonlóan folytatható. Az így módosított gondolatmenet adja a tétel érvényességét pl. minden olyan primfaktorizációs integritási tartományban, melyben véges sok egység van (itt „minden elég nagy számra" helyett „véges sok kivétellel minden elemre" írandó).

[4] Lásd pl. [1], [2], [4], [5]. A tétel messzemenő általánosításait tartalmazza pl. a [3] dolgozat

minden $a \geqq a_0$ helyen egy egész szám k-adik hatványa, akkor a polinom gyökei legalább k-szoros multiplicitásúak. Nyilvánvalóan elég ezt a

$$\varphi(x) = \frac{h(a_0 + xh(a_0)\, m!)}{h(a_0)}$$

polinomra igazolni, mely szintén egész együtthatós és melynek értékei $a \geqq 0$ esetén szintén k-adik hatványok. Ezenfelül, ha p m-nél nem nagyobb prímszám, akkor

$$\varphi(x) \equiv 1 \pmod{p}. \tag{1}$$

Ahhoz, hogy a $\varphi(x)$ polinom gyökei legalább k-szoros multiplicitásúak legyenek, szükséges és elégséges, hogy

$$[\varphi(x)]^{k-1} \mid [\varphi'(x)]^k \tag{2}$$

legyen, hiszen $\varphi(x)$-nek egy α multiplicitású gyöke $\varphi'(x)$-nek $\alpha - 1$ multiplicitással gyöke és így (2) azzal egyenértékű, hogy $\varphi(x)$ bármely gyökének α multiplicitására

$$(k-1)\alpha \leqq k(\alpha - 1),$$

azaz

$$k \leqq \alpha.$$

IV. (2) belátása céljából (1) alapján támaszkodhatunk az I. pontban bizonyítottakra, vagyis elég belátni, hogy minden $a \geqq 0$ egész helyen

$$[\varphi(a)]^{k-1} \mid [\varphi'(a)]^k \tag{3}$$

Ezt igazolandó írjuk fel a Taylor-formulát:

$$\varphi(a+x) = \varphi(a) + x\varphi'(a) + \ldots + x^m \frac{\varphi^{(m)}(a)}{m!}. \tag{4}$$

Legyen p $\varphi(a)$-nak egy prímosztója; $\varphi(a)$ k-adik hatvány volta miatt p $\varphi(a)$-nak $k\alpha$-adik hatványon osztója valamely pozitív α-val. Azt kell belátnunk, hogy p $\varphi'(a)$-nak legalább $(k-1)\alpha$-adik hatványon osztója.

Legyen p^{β_ν} a $\frac{\varphi^{(\nu)}(a)}{\nu!}$-ból kiemelhető legnagyobb p-hatvány ($\nu = 1, \ldots, m$). Ha (4)-ben x helyébe $p^\gamma y$-t helyettesítünk úgy, hogy

$$\beta_\nu + \gamma_\nu \geqq k(\alpha - 1) + 1 \tag{5}$$

legyen, akkor minden egész y-ra

$$p^{k(\alpha-1)+1} \mid \varphi(a + p^\gamma y)$$

tehát $\varphi(a+p^\gamma y)$ $y \geqq 0$ esetén k-adik hatvány lévén,

$$p^{k\alpha} \mid \varphi(a + p^\gamma y) \tag{6}$$

Mivel $p > m$, (6) csak úgy állhat fenn minden $y \geqq 0$-ra az I. pontban bizonyítottak szerint, ha y hatványai szerint rendezve $p^{k\alpha}$ osztója minden együtthatónak, azaz

$$\beta_\nu + \gamma_\nu \geqq k\alpha \tag{7}$$

Válasszuk most γ-t úgy, hogy (5) teljesüljön, de γ minimális legyen e tekintetben. Ekkor tehát van olyan $\mu \geqq 1$, hogy

$$\beta_\mu + (\gamma - 1)\mu \leqq k(\alpha - 1) \tag{8}$$

(7)-ben $\nu=\mu$-t helyettesítve és (8)-at levonva belőle

$$\mu \geqq k$$

és így (8) azt adja, hogy

$$\gamma \leqq \alpha$$

Ekkor azonban (7)-be $\nu=1$-et helyettesítve kapjuk, hogy

$$k\alpha \leqq \beta_1+\gamma \leqq \beta_1+\alpha$$

azaz

$$(k-1)\alpha \leqq \beta_1,$$

amit bizonyítani akartunk.

IRODALOM

[1] *Ch. Brisse:* Problème, Intermédiaire des Math., 1 (1894), 10. Megoldás: Uo. 2 (1895) 94. J. Franeltől.
[2] *R. Jentzsch:* Aufgabe, Archiv d. Math. u. Phys., Serie 3, 19 (1912) 361. Megoldás: Uo. 21 (1913) 368. W. Groschtól.
[3] *K. Dörge:* Zum Hilbertschen Irreduzibilitätssatz, Math. Annalen 96 (1926) 84—97.
[4] *G. Pólya—G. Szegő:* Aufgaben und Lehrsätze aus der Analysis, I—II., 2. Auflage, Springer-Verlag, 1954. 8. rész 114. és 190. feladat.
[5] *Fried E.* és *Surányi J.:* Egy polinomokra vonatkozó számelméleti problémáról, Mat. Lapok 11 (160) 75—78.
[6] *Kürschák J.—Hajós Gy.—Neukom Gy.— Surányi J.:* Matematikai versenytételek I. rész, 3. kiadás.

СВЯЗЬ МЕЖДУ ТЕОРЕТИКО-АРИФМЕТИЧЕСКИМИ СВОЙСТВАМИ МНОГОЧЛЕНОВ И ИХ ПОДСТАНОВОЧНЫХ ЗНАЧЕНИЙ

ЛАСЛО ЛОВАС

ON SOME CONNECTION BETWEEN ALGEBRAIC AND ARITHMETIC STRUCTURE OF POLYNOMIALS

L. LOVÁSZ