EGY POLINOM IRREDUCIBILITÁSÁRÓL

Írta: SERES IVÁN

Sokan foglalkoztak oly $F(P(x))$ polinomok irreducibilitásával, amelyekben az $F(z)$ irreducibilis polinom együtthatói racionális egész számok, a főegyütthatójuk 1 és a

$$z = P(x) = \prod_{k=1}^{m} (x - a_k) \quad \text{polinomban az} \quad a_1 < a_2 < \cdots < a_m$$

számok racionális egész számok. Mindezen szétbontásokat a racionális számtest, Γ fölött vizsgálták. Mi bebizonyítjuk a következő

TÉTELT: *Vegyük a 2^{n+1}-edik körosztási polinomot, az $F_{2^{n+1}}(z)$-t, ebbe helyettesítsük a következő szorzatot:*

$$P(x) = \prod_{k=1}^{m} (x^2 + a_k^2), \quad \textit{ahol} \quad o < |a_1| < |a_2| \cdots < |a_m|$$

racionális egész számok, a $G(x) = F_{2^{n+1}}(P(x))$ polinom irreducibilis a racionális számtest, a Γ fölött.

Bizonyítás: Tegyük fel, hogy a $G(x)$ polinom reducibilis a Γ számtest fölött;

$$G(x) = G_1(x)\, G_2(x),$$

ahol a $G_1(x)$ és $G_2(x)$ polinom összes együtthatói racionális egész számok.

Kis átrendezéssel a tényezők így írhatók:

$$G_1(x) = xH_1(x^2) + K_1(x^2),$$
$$G_2(x) = xH_2(x^2) + K_2(x^2),$$

ahol a $H_1(x^2)$, $H_2(x^2)$, $K_1(x^2)$, $K_2(x^2)$ polinomok racionális egész együtthatójúak. Szorozzuk össze a $G_1(x)$ polinomot a $G_2(x)$-szel:

$$G(x) = x^2 H_1(x^2)\, H_2(x^2) + K_1(x^2)\, K_2(x^2) +$$
$$+ x\big(H_1(x^2)\, K_2(x^2) + H_2(x^2)\, K_1(x^2)\big).$$

Az együtthatók összehasonlításával adódik, hogy

$$H_1(x^2)\, K_2(x^2) + H_2(x^2)\, K_2(x^2) = 0. \tag{1}$$

1. A $H_1(x^2)$, $H_2(x^2)$, $K_1(x^2)$, $K_2(x^2)$ polinomok egyike sem azonosan 0. Pl. $H_1(x^2) \equiv 0$ esetén (1)-ből a $H_2(x^2)\, K_1(x^2) \equiv 0$ azonosságot kapjuk. Ezen szorzatban $K_1(x^2) \not\equiv 0$, mert ellenkező esetben a $G_1(x)$ és $G(x)$ polinom $\equiv 0$ volna. Tehát $H_2(x^2) \equiv 0$, s így

$$G(x) = F_{2^{n+1}}\left(\prod_{k=1}^{m}(x^2 + a_k^2)\right) = K_1(x^2)\, K_2(x^2).$$

Ezen polinomokban $x^2 = y$-t írva az

$$F_{2^{n+1}}\left(\prod_{k=1}^{m}(y + a_k^2)\right) = K_1(y)\, K_2(y)$$

összefüggéshez jutunk. Ez [1] miatt csak úgy lehet, ha $K_1(y)$ vagy a $K_2(y)$ egyike konstans, de akkor a $G_1(x)$ vagy a $G_2(x)$ polinom egyike konstans. Tehát a polinomnak nem felbontása a $G_1(x)\, G_2(x)$ szorzat. Hasonló az okoskodás, ha a $H_2(x^2)$, $K_1(x^2)$, $K_2(x^2)$ polinomok egyikéről tesszük fel, hogy azok azonosan zérusok.

2. Az (1) egyenlet szerint

$$K_1(x^2) = -\frac{H_1(x^2)\, K_2(x^2)}{H_2(x^2)} \tag{2}$$

és

$$G(x) = x^2 H_1(x^2)\, H_2(x^2) - \frac{H_1(x^2)\, K_2^2(x^2)}{H_2(x^2)}. \tag{3}$$

Legyen $(H_1(x^2), H_2(x^2)) = E(x^2)$, ahol az euklideszi algoritmus miatt $E(x^2)$ az x-re nézve páros kitevőjű polinom, amelynek együtthatói racionális számok.

3. A $G(x)$ polinom még így is írható

$$G(x) = x^2 H_1(x^2)\, H_2(x^2) - \frac{H_1(x^2)}{E(x^2)}\,\frac{K_2^2(x^2)}{\dfrac{H_2(x^2)}{E(x^2)}}. \tag{4}$$

A $\dfrac{H_1(x^2)}{E(x^2)}$ és $\dfrac{H_2(x^2)}{E(x^2)}$ racionális együtthatójú polinomokról azt tudjuk, hogy egymáshoz relatív prímek. A (2) szerint

$$K_1(x^2) = -\frac{\dfrac{H_1(x^2)}{E(x^2)}\, K_2(x^2)}{\dfrac{H_2(x^2)}{E(x^2)}},$$

ezért $\dfrac{H_2(x^2)}{E(x^2)} \Big| K_2(x^2)$, továbbá természetesen fennáll a $\dfrac{H_2(x^2)}{E(x^2)} \Big| x H_2(x^2)$ összefüggés.

Így $G(x)$ osztható volna $\frac{H_2(x^2)}{E(x^2)}$-tel, ami csak akkor lehet [1] miatt, ha a $\frac{H_2(x^2)}{E(x^2)}$ polinom konstans, ekkor

$$\operatorname{Gr} H_2(x^2) = \operatorname{Gr} E(x^2).$$

A $\frac{K_2(x^2)}{\frac{H_2(x^2)}{E(x^2)}}$ kifejezés racionális együtthatójú algebrai polinom, így (4) szerint $\frac{H_1(x^2)}{E(x^2)}$-tel osztható volna a $G(x)$ polinom.

Ez, [1] miatt szintén csak akkor lehetséges, ha a $\frac{H_1(x^2)}{E(x^2)}$ polinom konstans.

Végül is

$$\operatorname{Gr} H_1(x^2) = \operatorname{Gr} H_2(x^2) = \operatorname{Gr} E(x^2)$$

és

$$\left.\begin{aligned} H_1(x^2) &= \delta_1 E(x^2) \\ H_2(x^2) &= \delta_2 E(x^2) \end{aligned}\right\} \text{ ahol a } \delta_1 \text{ és } \delta_2 \text{ racionális számok}$$

s így $H_1(x^2) = \delta_3 H_2(x^2)$ (a δ_3 is racionális szám). Ezt a (3) összefüggésnél figyelembe véve,

$$G(x) = F_{2n+1}\left(\prod_{k=1}^{m}(x^2 + a_k^2)\right) = \delta_3(x^2 H_2^2(x^2) - K_2^2(x^2)).$$

Mivel az $x^2 H_2^2(x^2) - K_2^2(x^2)$ polinom együtthatói racionális egész számok és a $G(x)$ valamint az $(xH_2(x^2) + K_2(x^2))(xH_2(x^2) - K_2(x^2))$ polinom főegyütthatóinak abszolút értéke 1, azért $\delta_3 = \pm 1$.

Így

$$\mp F_{2n+1}\left(\prod_{k=1}^{m}(x^2 + a_k^2)\right) = x^2 H_2^2(x^2) - K_2^2(x^2).$$

Az $x = 0$ helyen a következő összefüggést kapjuk:

$$\mp F_{2n+1}\left(\prod_{k=1}^{m} a_k^2\right) = \mp\left(\prod_{k=1}^{m} a_k^{2n+1} + 1\right) = K_2^2(0).$$

Ez ellentmondást ad, mert a jobboldalon négyzetszám állt, a baloldalon $\prod_{k=1}^{m} a_k \neq 0$ miatt pedig nem.

Köszönettel megemlítem KÖRNYEI IMRÉnek egy általános megjegyzését:

Ha az $f(x)$ racionális egész együtthatós, a Γ fölött irreducibilis polinom, amelynek főegyütthatója 1, az $f(x^2)$ polinom is irreducibilis marad, ha $f(0) \neq a^2$-tel (ahol a a racionális egész szám).

A bizonyítás ugyanúgy vihető végbe, mint a $G(x)$ polinom irreducibilitásának kimutatásánál.

IRODALOM

[1] I. Seres: Lösung und Verallgemeinerung eines I. Schurschen Irreduzibilitätsproblem für Polynome, *Acta Math. Acad. Sci. Hung.* **7** (1956) 151—157.

(Beérkezett: 1960. XII. 14.)

A Magyar Tudományos Akadémia
Matematikai Kutató Intézete