BIZONYOS POLINOMOK IRREDUCIBILITÁSA A KÖROSZTÁSI TESTEKBEN

Írta: SERES IVÁN

DORWART, H. L. és OYSTEIN ORE [1] vizsgálták bizonyos egész együtthatójú polinomok irreducibilitását, főleg kvadratikus számtestek fölött. A Szerző [2] bebizonyította, hogy ha $F_m(z)$ az m-edik körosztási polinom és ebbe a $z = P(x) = \prod_{k=1}^{n}(x-a_k)$ polinomot helyettesítjük, az új $F_m(P(x))$ polinom irreducibilis a racionális számok fölött, ahol az $a_1 < a_2 < \cdots < a_n$ számok racionális egészek, és a $P(x) - e^{\frac{2\pi i}{m}}$ polinom irreducibilis a fenti feltételek mellett, ha $n \geqq 5$ a $\mathfrak{K}_m$ test fölött. Hogy $n \leqq 4$-re a dolog hogyan áll, nem volt ismeretes. A jelen dolgozat bebizonyítja a következő

I. tételt: *Jelentsen az* $a_1 < a_2 < \cdots < a_n$ *racionális egész számokat,* $F_m(z)$ *az* m*-edik körosztási polinomot. A* $G(x) = F_m(P(x))\left(m > 2;\ P(x) = \prod_{k=1}^{n}(x-a_k)\right)$ *polinom akkor és csak akkor reducibilis a racionális számtest fölött, ha* $n = 3$, *az* $a_1 < a_2 < a_3$ *három szomszédos racionális egész szám és* $F_m(z) = z^4 - z^2 + 1$ *a 12. körosztási polinom.*

BIZONYÍTÁS: CAPELLI tétele szerint [3] a $G(x)$ polinom akkor és csak akkor reducibilis a racionális számok fölött, ha a $\prod_{k=1}^{n}(x-a_k) - e^{\frac{2\pi i}{m}}$ polinom reducibilis az m-edik körosztási test, $\mathfrak{K}_m$ fölött. ($\mathfrak{K}_0$ jelentse a racionális számok testét, a rövidség kedvéért legyen $e^{\frac{2\pi i}{m}} = \zeta$. Jegyezzük meg a későbbiek miatt azt, hogy a $\prod_{k=1}^{n}(x-a_k) - e^{\frac{2\pi l i}{m}}$, $((l, m) = 1)$ polinom helyett a $\prod_{k=1}^{n}(x-a_k) - e^{\frac{2\pi i}{m}}$ polinommal foglalkozunk, ami csak egyszerűsíti a vizsgálódást. CAPELLI tétele szerint ezt szabad tennünk.)

Tegyük fel, hogy a $P(x) - \zeta$ polinom reducibilis a $\mathfrak{K}_m$ fölött: $P(x) - \zeta = g(x)h(x)$, ahol a $g(x)$ és a $h(x)$ polinom főegyütthatója 1. Legyen a $g(x)$ polinom irreducibilis és fokszáma egyik legkisebb a $P(x) - \zeta$ polinom tényezői között.

Szükségünk lesz a következő segédtételekre:

1. SEGÉDTÉTEL. (L. KRONECKERnek a körosztási test egységeire vonatkozó tétele [4].) *Minden ω egység az m-edik körosztási testből, $\mathfrak{K}_m$-ből így írható: $\omega = \varepsilon\eta$, ahol ε valós egység, η egységgyök, [az m-edik, esetleg a $2m$-edik vagy a $4m$-edik].*

2. SEGÉDTÉTEL. *Vegyen fel egy $\mathfrak{K}_m$-beli egészegyütthatós polinom, $g(x)$ az $x = a_k$ és $x = a_l$ racionális egész számokon egységeket a $\mathfrak{K}_m$-ből. Az 1. segédtétel szerint a két egység*

$$g(a_k) = \varepsilon_k \eta_k \quad \text{és} \quad g(a_l) = \varepsilon_l \eta_l$$

alakú, ahol ε_k és ε_l valós egységek, η_k és η_l egységgyökök.

Az esetben, ha

a) $|a_k - a_l| > 2$, *az* $\eta_k = \pm \eta_l$, *ha*

b) $|a_k - a_l| = 2$, *az* $\eta_k = i^\alpha \eta_l$, *ahol* $\alpha = 1$ *vagy* 3.

A 2. segédtétel bizonyítása:

$$a_k - a_l \mid g(a_k) - g(a_l) = \varepsilon_k \eta_k - \varepsilon_l \eta_l .$$

A jobboldalt az $\varepsilon_k^{-1}\eta_l^{-1}$ egységgel szorozva,

$$a_k - a_l \mid \eta_k \eta_l^{-1} - \varepsilon_l \varepsilon_k^{-1} .$$

A konjugált komplexre térve át,

$$a_k - a_l \mid \eta_k^{-1} \eta_l - \varepsilon_l \varepsilon_k^{-1} .$$

A két utóbbi összefüggésből adódik, hogy

$$a_k - a_l \mid \eta_k^2 \eta_l^{-2} - 1 . \tag{1}$$

Ez igaz, ha az osztandó helyett annak konjugáltjait írjuk, és ezért az (1)-ben az osztó és osztandónak a $\mathfrak{K}_0$-ra vonatkozó normáira helyes a következő:

$$N(a_k - a_l) \mid N(\eta_k^2 \eta_l^{-2} - 1).$$

(A két norma nyilván racionális egész szám.)

a) Ha $|a_k - a_l| > 2$, akkor

$$|N(a_k - a_l)| > N(2) \geqq |N(\eta_k^2 \eta_l^{-2} - 1)| .$$

Ez csak akkor nem vezet ellenmondásra, ha

$$\eta_k = \pm \eta_l .$$

b) Ha $|a_k - a_l| = 2$, akkor (2) szerint

$$|N(a_k - a_l)| = N(2) \mid N(\eta_k^2 \eta_l^{-2} - 1).$$

Az $\eta_k^2\eta_l^{-2}-1$ és minden konjugáltjának abszolút értéke $\leqq 2$ miatt

$$N(2)=|N(\eta_k^2\eta_l^{-2}-1)|.$$

Ez csak akkor következhetik be, ha az $\eta_k^2\eta_l^{-2}-1$-re, illetve annak bármely konjugáltjára fennáll a következő összefüggés:

$$|\eta_k^2\eta_l^{-2}-1|=2.$$

Ez, mivel $|\eta_k^2\eta_l^{-2}|+|-1|=2$, azt mondja, hogy az $\eta_k^2\eta_l^{-2}$ és a -1 vektor egy egyenesbe esik a GAUSS-féle koordináta rendszerben.

Ebből

$$\eta_k^2\eta_l^{-2}=-1, \tag{2}$$

vagyis igaz a 2b segédtétel.

Az I. tétel bizonyítása:

Az n = 4 eset.

1. Legyen adva $a_1<a_2<a_3<a_4$; $a_4-a_1\geqq 4$. Ha a $\prod_{k=1}^{4}(x-a_k)-e^{\frac{2\pi i}{m}}$ polinomnak a $\mathfrak{K}_m$ fölött egyik (legkisebb fokú) tényezője a $g(x)$ polinom, akkor $g(a_k)=\varepsilon_k\eta_k$ $(k=1, 2, 3, 4)$ egység. Ezen egységek között van legalább három, amely egy egyenesbe esik a GAUSS-féle koordináta rendszerben.

Ennek bizonyítására gondoljuk meg, hogy $a_4-a_1>2$ és a $2a$ segédtétel miatt

$$\eta_4=\pm\eta_1. \tag{3}$$

a) Ha $a_2-a_1=1$, akkor $a_4-a_2>2$ s így a 2a segédtétel miatt

$$\eta_4=\pm\eta_2,$$

b) ha $a_2-a_1=2$, akkor $a_3-a_1>2$ és a 2a segédtétel miatt

$$\eta_1=\pm\eta_3, \tag{4}$$

c) ha $a_2-a_1>2$, akkor a 2a segédtétel miatt

$$\eta_1=\pm\eta_2=\pm\eta_3=\pm\eta_4.$$

Mindenesetre az η_1, η_4, η_r egy egyenesbe esik, ahol $r=2$ az a) és c) esetben, és $r=3$ a b) esetben. A $g(x)$ (foka $\leqq 2$) az interpolációs formulával előállítható:

$$g(x)=\sum_{\substack{v=1\\ v=r\\ v=4}}\frac{R(x)\,g(a_v)}{R'(a_v)(x-a_v)},$$

ahol $R(x)=(x-a_1)(x-a_r)(x-a_4)$.

Az a), b), és c)-ben kapott eredményeket felhasználva,

$$g(x) = \eta_1 \sum_{\substack{v=1 \\ v=r \\ v=4}} \frac{R(x)(\pm \varepsilon_v)}{R'(a_v)(x-a_v)} = \eta_1 L_1(x),$$

ahol az $L_1(x)$ valós egészegyütthatójú polinom a $\mathfrak{K}_m$ fölött. Mivel a $g(x)$ polinom főegyütthatója 1, ezért az η_1 egységgyök $= \pm 1$, tehát a $g(x)$ polinom minden együtthatója valós algebrai szám. Osszuk el a $P(x)-\zeta$ polinomot a $g(x)$ valós polinommal:

$$P(x)-\zeta = Q(x)g(x)+T(x), \tag{A}$$

ahol a $Q(x)$ polinom a hányados és a $T(x)$ polinom a maradék. Ez nulla kell hogy legyen. Hasonlóképpen osszuk el a $P(x)$ polinomot a $g(x)$ polinommal:

$$P(x) = Q_1(x)g(x)+T_1(x), \tag{B}$$

ahol a $Q_1(x)$ polinom a hányados, a $T_1(x)$ polinom a maradék. Ezek valós együtthatójúak.

Az (A) és (B) egyenletekből

$$T_1(x)-\zeta-T(x) \equiv 0 \qquad (\mathrm{mod}\, g(x)).$$

De a $\mathrm{Grad}\,(T_1(x)-\zeta) \leqq \mathrm{Grad}\, g(x)$; $\mathrm{Grad}\,(T(x)) < \mathrm{Grad}\,(g(x))$; $\mathrm{Grad}\, g(x) > 0$ miatt $T_1(x)-\zeta = T(x)$.

Ez utóbbi egyenlet ellenmondást ad, ha a $T(x) \equiv 0$. Ugyanis a $T_1(x)$ valós polinom, de a $T_1(x)-\zeta$ már nem valós.

2. *Legyen* $a_4-a_1=3$; $a_1=0$, $a_2=1$, $a_3=2$, $a_4=3$ *és* $g(x)=x^2+Ax+B$; $h(x)=x^2+Cx+D$. (A taglalás megkönyítése végett vegyük az $a_1<a_2<a_3<a_4$ számokat minél kisebb abszolút értékű racionális egész számnak. Ez módunkban áll, mert az x változót a valós tengelyen megfelelőképpen eltoljuk.)

Érvényes a következő összefüggés:

$$g(1)-g(2)+\frac{g(3)-g(0)}{3} = 0.$$

Erről a négy alapművelet győz meg bennünket.

Az 1. segédtétel szerint $\varepsilon_2\eta_2-\varepsilon_3\eta_3+\frac{\varepsilon_4\eta_4-\varepsilon_1\eta_1}{3}=0$. $a_4-a_1=3$ miatt fennáll (3) és ezért $\eta_4 = \pm\eta_1$. A 2b segédtétel felhasználásával:

$$a_3-a_1 = 2,$$

ezért

$$\eta_3 = i^{\alpha_1}\eta_1. \tag{5}$$

Másrészt

$$a_4 - a_2 = 2,$$

ezért

$$\eta_4 = i^{\alpha}\eta_2,$$

a (3) figyelembevételével

(6) $$\eta_2 = i^{\alpha_2}\eta_1.$$

A (3), (5), (6) összefüggést felhasználva és η_1-gyel rövidítve:

(7) $$\varepsilon_2 i^{\alpha_2} - (\pm\varepsilon_3) i^{\alpha_1} + \frac{1}{3}(\pm\varepsilon_4 - \varepsilon_1) = 0.$$

A 2b segédtétel szerint α_1 és α_2 csak páratlan lehet, így (7) valós része,

$$\frac{\pm\varepsilon_4 - \varepsilon_1}{3} = 0.$$

Szorozzunk vissza az η_1-gyel és használjuk fel a (3) és a (4) összefüggéseket. Ekkor

$$\varepsilon_4\eta_4 - \varepsilon_1\eta_1 = g(3) - g(0) = 0;$$

vagyis $3^2 + 3A + B - B = 0$, és így

$$A = -3.$$

Hasonló az eset a $h(x)$ polinomnál. Ott $C = -3$. Így

$$x(x-1)(x-2)(x-3) - e^{\frac{2\pi i}{m}} = g(x)h(x) = (x^2 - 3x + B)(x^2 - 3x + D).$$

A műveletek elvégzése után az együtthatók összehasonlításával a

(8) $$B + D = 2 \quad \text{és a} \quad B \cdot D = -e^{\frac{2\pi i}{m}} = -\zeta$$

egyenlethez jutunk, amiből

(9) $$B = 1 \pm \sqrt{1+\zeta} \quad \text{és} \quad D = 1 \mp \sqrt{1+\zeta}.$$

B és D egész szám, a szorzatuk (8) szerint egységet ad. Az egyik egység $1 + \sqrt{1+\zeta}$ alakú. Ez KRONECKER tétele miatt nem lehetséges, mert

$$\arc \sqrt{1+\zeta} = \frac{2\pi}{2m} \cdot \frac{1}{2},$$

$$\arc (1 + \sqrt{1+\zeta}) < \frac{2\pi}{4m};$$

ilyen egység a $\mathfrak{K}_m$-ben nincs. Ezzel az $n = 4$ eset el van intézve.

Az n = 3 eset.

Legyenek adva az $a_1 < a_2 < a_3$ racionális egész számok. A

$$\prod_{k=1}^{3}(x-a_k)-e^{\frac{2\pi i}{m}}=P(x)-\zeta$$

polinom legyen két egész együtthatós polinom szorzatával, $g(x)h(x)$-szel egyenlő (a $\mathfrak{K}_m$ fölött). [A jelölés hasonlít az $n=4$ esetben tárgyaltakéhoz.]

Legyen a $g(x)$ polinom elsőfokú

$$g(x)=x+A;\quad h(x)=x^2+Bx+C.$$

1. $g(x)$-et tekintve, az $a_3-a_1>2$ egyenlőtlenség nem lehetséges. Ugyanis az 1. segédtétel szerint

$$g(a_1)=\varepsilon_1\eta_{i_1},\quad g(a_2)=\varepsilon_2\eta_{i_2},\quad g(a_3)=\varepsilon_3\eta_{i_3}.$$

A 2a segédtétel szerint, $a_3-a_1>2$ miatt

$$\eta_{i_3}=\pm\eta_{i_1}.$$

Az interpolációs formula az $x=a_1$ és $x=a_3$-ra a $g(x)$ polinomot $\eta_{i_1}L_3(x)$ alakban adja meg, ahol az $L_3(x)$ polinom valós. Ilyen osztója a $P(x)-\zeta$ polinomnak nincs. (L. az $n=4$ esetet.)

2. Legyen $a_3-a_1=2$.

Legyen $a_1=-1$, $a_2=0$, $a_3=1$; $g(-1)=\varepsilon_1\eta_{i_1}$, $g(1)=\varepsilon_3\eta_{i_3}$. Ez esetben a 2b segédtétel szerint

$$\eta_{i_3}=i^{\alpha}\eta_{i_1},$$

továbbá

$$g(-1)=-1+A;\quad g(1)=1+A.$$

A fenti egyenletekből

(10)
$$\left.\begin{aligned} A&=\frac{\varepsilon_1+\varepsilon_3 i^{\alpha}}{2}\eta_{i_1}\\ -\eta_{i_1}^{-1}&=\frac{\varepsilon_1-\varepsilon_3 i^{\alpha}}{2}\end{aligned}\right\}$$ Az első egyenletben szereplő tört kifejezés és $-\eta^{-1}$ egymáshoz konjugált komplex számok.

A 2b segédtétel szerint α páratlan, tehát (10)-ből

$$A=-\eta_{i_1}^2\quad\text{és így}\quad g(x)=x-\eta_{i_1}^2.$$

A

$$P(x)-\zeta=(x+1)x(x-1)-e^{\frac{2\pi i}{m}}=(x-\eta_{i_1}^2)(x^2+Bx+C).$$

A műveletek elvégzése után együttható összehasonlítással kapjuk a

$$(11)\qquad \left.\begin{aligned} -\eta_{i1}^2+B&=0\\ -B\eta_{i1}+C&=-1\\ -C\eta_{i1}^2\quad&=-e^{\frac{2\pi i}{m}}\end{aligned}\right\}$$

egyenletrendszert, amiből a B és a C eliminálásával a

$$(12)\qquad -\eta_{i1}^6+\eta_{i1}^2+e^{\frac{2\pi i}{m}}=0$$

egyenletet. Ebből azt olvashatjuk le, hogy a $-\eta_{i1}^6, \eta_{i1}^2, e^{\frac{2\pi i}{m}}$ egységnyi hosszúságú vektorok egymással $\pm\frac{2\pi}{3}$ szöget zárnak be,

$$(13)\qquad \eta_{i1}^2=e^{\frac{2\pi i}{m}}e^{\pm\frac{2\pi i}{3}}.$$

Ennek köbreemelésével nyerjük:

$$(14)\qquad -\eta_{i1}^6=-e^{\frac{6\pi i}{m}}$$

(13) és (14) eredményeit a (12) egyenletbe helyettesítve:

$$-e^{\frac{6\pi i}{m}}+e^{\frac{2\pi i}{m}}e^{\frac{2\pi i}{3}}+e^{\frac{2\pi i}{m}}=0;\quad e^{\frac{2\pi i}{m}}\neq 0,$$

ezért osszuk el vele az utóbbi egyenletet:

$$e^{\frac{4\pi i}{m}}=1+e^{\pm\frac{2\pi i}{3}}=\begin{cases}1-\frac{1}{2}+i\frac{\sqrt{3}}{2}=e^{\frac{2\pi i}{6}}, & \text{illetve}\\ 1-\frac{1}{2}-i\frac{\sqrt{3}}{2}=e^{\frac{10\pi i}{6}}.\end{cases}$$

Vagyis $e^{\frac{2\pi i}{m}}=\pm e^{\frac{2\pi i}{12}}$, illetve $e^{\frac{2\pi i}{m}}=\pm e^{\frac{10\pi i}{12}}$. Ezek a számok mind primitív *12-edik* egységgyökök. E miatt $m=12$.

Vegyük ezek közül egyelőre az $e^{\frac{2\pi i}{12}}$ egységgyököt és helyettesítsük azt — a $g(x)$ megszerkesztése miatt — a (13) egyenletbe. Ekkor $\eta_{i1}^2=e^{\frac{10\pi i}{12}}$ (illetve $\eta_{i1}^2=e^{\frac{6\pi i}{12}}=-i$) $g(x)=x-e^{\frac{10\pi i}{12}}$ (illetve $g(x)=x+i$; ez utóbbi, mint arról egyszerű osztással meggyőződhetünk, nem osztója a $P(x)-\zeta=$ $=(x+1)\,x(x-1)-e^{\frac{2\pi i}{12}}$ polinomnak.) Azt kaptuk tehát, hogy $g(x)=x-e^{\frac{10\pi i}{12}}$. A (11) egyenletrendszerből $\eta_{i1}^2=e^{\frac{10\pi i}{12}}$ segítésével nyerjük a B és a C koefficienseket és a $h(x)=x^2+e^{\frac{10\pi i}{12}}x+e^{\frac{16\pi i}{12}}$ polinomot.

Végül is $g(x)\cdot h(x)=\left(x-e^{\frac{10\pi i}{12}}\right)\left(x^2+e^{\frac{10\pi i}{12}}x+e^{\frac{16\pi i}{12}}\right)=x^3-x-e^{\frac{2\pi i}{12}}=$ $=P(x)-\zeta$. Minthogy a $P(x)-\zeta=x^3-x-e^{\frac{2\pi i}{12}}$ reducibilis a $\mathfrak{K}_m$ fölött, azért CAPELLI tétele miatt a $\mathfrak{K}_0$ fölött az $F_{12}(P(x))=P^4(x)-P^2(x)+1$ polinom is reducibilis, vagyis $F_{12}(P(x))=x^{12}-4x^{10}+6x^8-5x^6+3x^4-x^2+1$, [Ez utóbbi polinom található meg H. L. DORWART és OYSTEIN ORE említett dolgozatában.] $F_{12}(P(x))=(x^4-x^2+1)(x^8-3x^6+2x^4+1)=\text{Norm}\,g(x)\,\text{Norm}\,h(x)$.

Általánosabb megoldást kapunk, ha x helyébe $x+a$-t írunk, ahol a racionális egész szám.

GALOIS tételével a $\mathfrak{K}_{12}$ fölött még más irreducibilis polinomot is találunk, ha az $\left(e^{\frac{2\pi i}{12}}:e^{\frac{10\pi i}{12}}\right)$, vagy az $\left(e^{\frac{2\pi i}{12}}:e^{\frac{14\pi i}{12}}\right)$, végül az $\left(e^{\frac{2\pi i}{12}}:e^{\frac{22\pi i}{12}}\right)$ szubsztitúciót alkalmazzuk. Így kapjuk a következő, $\mathfrak{K}_{12}[x]$-ben reducibilis polinomokat

$$x^3-x-e^{\frac{10\pi i}{12}}=\left(x-e^{\frac{2\pi i}{12}}\right)\left(x^2+e^{\frac{2\pi i}{12}}x+e^{\frac{8\pi i}{12}}\right),$$

$$x^3-x-e^{\frac{14\pi i}{12}}=\left(x-e^{\frac{22\pi i}{12}}\right)\left(x^2+e^{\frac{22\pi i}{12}}x+e^{\frac{16\pi i}{12}}\right),$$

$$x^3-x-e^{\frac{22\pi i}{12}}=\left(x-e^{\frac{14\pi i}{12}}\right)\left(x^2+e^{\frac{14\pi i}{12}}x+e^{\frac{8\pi i}{12}}\right).$$

Általánosabb megoldást kapunk, ha x helyébe $x+b$-t helyettesítünk, ahol b racionális egész szám.

Az n = 2 eset.

Ha az $(x-a_1)(x-a_2)-e^{\frac{2\pi i}{m}}$ felbomlik a $\mathfrak{K}_m$ fölött, akkor két elsőfokú faktor szorzatára bomolhat fel:

(15) $$g(x)=x+A;\quad h(x)=x+B.$$

Az 1. segédtétel szerint

$$g(a_1)=\varepsilon_1\eta_1,\quad g(a_2)=\varepsilon_2\eta_2.$$

1. Ha $a_2-a_1>2$, akkor a 2a segédtétel szerint $\eta_1=\pm\eta_2$ és ez, mint sokszor láttuk, ellenmondásra vezet az interpolációs formula segítségével.

2. Legyen $a_2-a_1=2$ és $a_1=-1$, $a_2=1$, ekkor a 2b segédtétel szerint $\eta_2=i^\alpha\eta_1$, ahol az α páratlan.

$$g(a_1)=-1+A=\varepsilon_1\eta_1,$$

$$g(a_2)=1+A=\varepsilon_2\eta_2=\varepsilon_2 i^\alpha.$$

Ezen egyenletrendszerből:

$$A=\frac{\varepsilon_1+i^\alpha\varepsilon_2}{2}\eta_1,\qquad -\eta_1^{-1}=\frac{\varepsilon_1-i^\alpha\varepsilon_2}{2}.$$

Ez utóbbi konjugált komplex az előző tört-kifejezéshez, tehát

$$A=-\eta_1^2, \quad \text{és (15) szerint} \quad g(x)=x-\eta_1^2.$$

Hasonlóképpen

$$B=-\eta_3^2, \quad \text{ahol } \eta_3 \text{ egységgyök és (15) szerint } h(x)=x-\eta_3^2; \quad \text{ebből}$$

$$(x-a_1)(x-a_2)-e^{\frac{2\pi i}{m}}=x^2-1-e^{\frac{2\pi i}{m}}=x^2-(\eta_1^2+\eta_3^2)x+\eta_1^2\eta_3^2.$$

Az együtthatók összehasonlításával:

$$\eta_1^2+\eta_3^2=0,$$

$$\eta_1^2\eta_3^2=-1-e^{\frac{2\pi i}{m}}.$$

Ezekből

$$\eta_1=\sqrt[4]{1+e^{\frac{2\pi i}{m}}},$$

de

$$\operatorname{arc}\eta_1=\frac{2\pi}{8m}+s\frac{2\pi}{4}=\frac{2\pi(1+2ms)}{8m},$$

ahol

$$s=0, \quad \text{vagy} \quad 1, \quad \text{vagy} \quad 2, \quad \text{vagy} \quad 3.$$

A $g(a_1)$ nem lehet egység. Ugyanis az 1. segédtétel miatt a hozzátartozó η szög a $\frac{2\pi}{4m}$-nek egész számú többszöröse és nem a $\frac{2\pi}{8m}$-nek páratlan számú többszöröse.

3. $a_2-a_1=1$.

Legyen $a_1=-1$, $a_2=0$; $P-\zeta=x^2+x-e^{\frac{2\pi i}{m}}$. Ez utóbbi polinomot gyöktényezőire bontva, az

$$\left(x+\frac{1+\sqrt{1+4e^{\frac{2\pi i}{m}}}}{2}\right)\left(x+\frac{1-\sqrt{1+4e^{\frac{2\pi i}{m}}}}{2}\right). \tag{16}$$

szorzatot kapjuk.

Miután az $x^2+x-e^{\frac{2\pi i}{m}}$-et a $\mathfrak{K}_m$ fölött reducibilisnek tesszük fel, legyen (16) szerint a $g(x)$ polinom az első, a $h(x)$ polinom a második gyöktényezője, az $x^2+x-e^{\frac{2\pi i}{m}}$ polinomnak. A $g(x)$ és a $h(x)$ polinom konstans tagjai egységek a $\mathfrak{K}_m$-ben.

Az 1. segédtétel miatt pl.

$$\frac{1\cdot+\sqrt{1+4e^{\frac{2\pi i}{m}}}}{2}=\varepsilon\eta. \tag{17}$$

Állítjuk, hogy

$$\operatorname{arc}\eta=\frac{2\pi}{4m}.$$

Ugyanis $\operatorname{arc}\left(1+4e^{\frac{2\pi i}{m}}\right)<\frac{2\pi}{m}$, mert ha 4 helyett egy nagy pozitív K számot írnánk, az $1+Ke^{\frac{2\pi i}{m}}$ közel párhuzamos lenne az $e^{\frac{2\pi i}{m}}$-mel. Ezt az egyszerű rajz is mutatja, tehát

$$\operatorname{arc}\sqrt{1+4e^{\frac{2\pi i}{m}}}<\frac{2\pi}{2m}.$$

Az $\operatorname{arc}\frac{1+\sqrt{1+4e^{\frac{2\pi i}{m}}}}{2}$-ről is csak azt mondhatjuk, hogy $<\frac{2\pi}{2m}$. De ekkor az 1. segédtétel szerint $\operatorname{arc}\eta=\frac{2\pi}{4m}$ lehet csupán. A (17)-ből $\varepsilon\eta=\varepsilon e^{\frac{2\pi i}{4m}}$ és így $g(x)=x+\varepsilon\eta^{\frac{2\pi i}{4m}}$.

A $h(x)$ polinom konstans tagja így írható:

$$1-\frac{1+\sqrt{1+4e^{\frac{2\pi i}{m}}}}{2}=1-\varepsilon e^{\frac{2\pi i}{4m}}.$$

A másik polinom:

$$h(x)=x+1-\varepsilon e^{\frac{2\pi i}{4m}}.$$

Az $(x-a_1)(x-a_2)-\zeta=x^2+x-e^{\frac{2\pi i}{m}}$ polinom és a $g(x)h(x)=\left(x+\varepsilon e^{\frac{2\pi i}{4m}}\right)\cdot\left(x+1-\varepsilon e^{\frac{2\pi i}{4m}}\right)$ polinom konstans tagjait összehasonlítva,

$$\varepsilon^2 e^{\frac{2\pi i}{m}}-\varepsilon e^{\frac{2\pi i}{4m}}+e^{\frac{2\pi i}{m}}=0.$$

Végül az $\varepsilon^2-\varepsilon e^{-\frac{2\pi i}{4m}}+e^{\frac{2\pi i}{2m}}=0$ egyenlethez jutottunk. Ebből

$$\varepsilon=\frac{e^{-\frac{2\pi i}{4m}}\pm\sqrt{e^{-\frac{4\pi i}{4m}}-4e^{\frac{4\pi i}{4m}}}}{2}.$$

(Ez valós szám!) Ez csak úgy lehet, ha $e^{\frac{2\pi i}{4m}}$-nek a konjugált komplexe

$$e^{\frac{2\pi i}{m}} = \pm\sqrt{e^{-\frac{4\pi i}{4m}} \cdot 4e^{\frac{4\pi i}{4m}}}$$

gyökkifejezéssel. Mindkét oldalt négyzetre emelve,

$$e^{\frac{4\pi i}{4m}} = e^{-\frac{4\pi i}{4m}} - 4e^{\frac{4\pi i}{4m}}.$$

Ez nem lehetséges, mert így a $2i \sin\frac{\pi}{m} = 4e^{\frac{4\pi i}{4m}}$ egyenlethez jutunk. (A baloldalon tiszta-képzetes szám van. A jobboldalon levő szám csak akkor lehet tiszta-képzetes szám, ha $m = 2$, ekkor azonban a következő helytelen egyenlőséget kapjuk: $2i \sin\frac{\pi}{2} = 4i$.)

Az n = 1 eset.

Ezt nem kell vizsgálni, mert az $F_m(x)$ polinom irreducibilis a $\mathfrak{K}_0$ fölött, az $F_m(x+a)$ polinom is irreducibilis a $\mathfrak{K}_0$ fölött, feltéve, hogy az a racionális egész szám.

Az eddigi eredményekből nyertük a

II. tételt: *Az m-edik körosztási polinom, $F_m(z)$ a $\mathfrak{K}_m$ körosztási test fölött lineáris tényezőkre bomlik. Helyettesítsük egy ilyen tényezőnél $z - e^{\frac{2k\pi i}{m}}$ $((k, m) = 1)$-nél a z helyébe a $z = P(x) = \prod_{k=1}^{n}(x - a_k)$ polinomot, ahol az a_k $(k = 1, 2, \ldots, n)$ racionális egészek. Ezek a polinomok majdnem mind irreducibilisek a $\mathfrak{K}_m$ fölött. Kivétel: ha az $F_m(z)$ a 12. körosztási polinom valamelyik gyöktényezője és $a_2 = a_1 + 1$, $a_3 = a_1 + 2$ (három egymásután következő racionális egész szám).*

IRODALOM

[1] Dorwart, H. L.—Oystein Ore: Criteria for the irreducibility of polynomials. *Annals of Math.* II. s., **34**, (1933), 81—94.

[2] Seres, I.: Lösung und Verallgemeinerung eines Schur'schen Irreduzibilitätsproblems für Polynome. *Acta Math. Hung.*, **7**, (1956), 151—156.

[3] Tschebotaröw—Schwerdtfeger: *Grundzüge der Galois'schen Theorie, Groningen—Djakarta* (1950), 288.

[4] L. Kronecker's Werke: *Über komplexe Einheiten*, Berlin (1895), 109—118.

(Beérkezett: 1959. IV. 12.)

A Magyar Tudományos Akadémia
Matematikai Kutató Intézete