I. SCHUR EGY SEJTÉSÉNEK IGAZOLÁSA

SERES IVÁN

Bemutatta Turán Pál r. tag az 1955. november 25-én tartott felolvasó ülésen

Bevezetés

I. SCHUR az Archiv der Mathematik und Physik XIII. kötetében a következő feladatot tűzte ki [1]: „Mutassuk meg, hogy ha $a_1, a_2, \ldots, a_n$ egymástól különböző racionális egész számok, akkor az

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_n)-1$$

polinom irreducibilis a racionális számtest fölött."

W. FLÜGEL a feladatot megoldotta [2] és kimutatta, hogy az

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_n)+1$$

polinom is, néhány kivételtől eltekintve, irreducibilis a racionális számtest, Γ fölött [3].

I. SCHUR az Archiv der Mathematik und Physik-nak ugyanebben a kötetében az a_k-kra vonatkozó fenti feltétel mellett feladatul tűzte ki annak kimutatását, hogy az

$$f(x) = (x-a_1)^2(x-a_2)^2\cdots(x-a_n)^2+1$$

polinom irreducibilis a $\Gamma[x]$ polinomgyűrűben [4]. Ennek megoldása megtalálható G. PÓLYA—G. SZEGŐ „Aufgaben und Lehrsätze aus der Analysis" II. kötetében [5].

A. BRAUER, R. BRAUER és H. HOPF [6] kimutatták, hogy az

$$f_4(x) = \prod_{k=1}^{n}(x-a_k)^4+1 \quad \text{és} \quad f_8(x) = \prod_{k=1}^{n}(x-a_k)^8+1$$

polinomok az a_k-ra adott fenti feltételek mellett irreducibilisek a $\Gamma[x]$-ben.

Jelen dolgozatomban négy tételt bizonyítok.

1. tétel: Az $F(x) = \prod_{k=1}^{M}(x-a_k)^{2^n}+1$ *irreducibilis a* $\Gamma[x]$*-ben, ha az* a_k*-k egymástól különböző racionális egész számok, n pozitív egész szám és* $M \geqq 1$.

(Ezen állítást I. SCHUR egyik sejtésének nevezik. A. és R. BRAUER „Über Irreduzibilitätskriterien von I. Schur und G. PÓLYA" című cikkükben [7] közlik, hogy I. SCHUR sejtette az $F(x)$ polinom irreducibilitását a fenti

feltételek mellett. A tétel, miként ők megjegyzik, bizonyítva még nincs, legfeljebb csak $n = 0, 1, 2, 3$-ra).

I. SCHUR fenti problémájának két általánosítását igazolom.

2. tétel: Legyenek az $a_1, \ldots a_M$ *egymástól különböző racionális egész számok és* $f_m(x)$ *az m-edik körosztási polinom. Az* $f_m(P(x))$ *polinom irreducibilis* $\Gamma[x]$*-ben, ha a* $P(x) = \prod_{k=1}^{M} (x - a_k)$ *polinom foka,* $M \geqq 5$. *Néhány kivétellel akkor is kimutatható az* $f_m(P(x))$ *polinom irreducibilitása a* $\Gamma[x]$*-ben, ha* $M < 5$.

3. tétel: Legyenek $a_1, a_2, \ldots a_M$ *egymástól különböző racionális egész számok és* $Q(x)$ *racionális egész együtthatós polinom, melynek főegyütthatója* 1, *továbbá jelentse* $f_m(x)$ *az m-edik körosztási polinomot* $m > 2$*-re és* $R(x)$ *a* $Q(x) \prod_{k=1}^{M} (x - a_k)$ *polinomot. Azt bizonyítom, hogy az* $f_m(R(x))$ *polinom irreducibilis a* $\Gamma[x]$*-ben, feltéve, hogy* $M \geqq 6$ *és a* $Q(x)$ *polinom foka kisebb* $P(x) = \prod_{k=1}^{M} (x - a_k)$ *polinom fokánál.*

4. tétel: Bizonyítás közben még azt az eredményt is nyerjük, hogy a

$$\psi(x) = Q(x) \prod_{k=1}^{M} (x - a_k) - \zeta \qquad \left(\zeta = e^{\frac{2\pi i}{m}}\right)$$

polinom irreducibilis a $\Gamma(\zeta)$ *test fölött, ha* $Q(x)$, $a_1, \ldots, a_M$, M *és* m *a 3.-ban felsorolt követelményeknek tesz eleget.*

Az eredményeket a körosztási testek egységei speciális tulajdonságainak felhasználásával, L. KRONECKER erre vonatkozó alapvető tételeinek segítségével fogjuk bizonyítani [8].

Segédtételek

Szükségünk van néhány segédtételre:

1. segédtétel: Jelentse $f_m(x)$ *az m-edik* $(m > 2)$ *körosztási polinomot, és legyen* $R(x)$ *racionális együtthatójú polinom. A* $\Phi_m(x) = f_m(R(x))$ *polinom akkor és csak akkor irreducibilis a racionális számtest,* Γ *fölött, ha a* $\psi(x) = R(x) - e^{\frac{2\pi i}{m}} = R(x) - \zeta$ *polinom is irreducibilis a* $\Gamma(\zeta)$ *fölött.*

Bizonyítás:

1. Tegyük fel először, hogy a $\psi(x)$ polinom irreducibilis a $\Gamma(\zeta)[x]$ polinom-gyűrűben, ellenben ugyanekkor a $\Phi_m(x)$ polinom felbomlik a $\Gamma[x]$-ben két polinom szorzatára: $\Phi_m(x) = G(x) \cdot H(x)$.

Nyilván $\psi(x) \mid \Phi_m(x)$, és, mivel $\psi(x)$ polinom irreducibilis a $\Gamma(\zeta)$ fölött, azért $\psi(x)$ osztja $G(x)$ és $H(x)$ valamelyikét; például vehetjük, hogy $\psi(x) \mid G(x)$. A $\psi(x)$ polinom minden konjugáltjával is osztható a $G(x)$ polinom. A $\psi(x)$ polinom konjugáltjai az $R(x)-\zeta^s$ polinomok, $((s, m)=1)$, szintén irreducibilisek, egymástól különbözőek; ha N a norma jele $\Gamma(\zeta)$-ra vonatkozólag, úgy

$$N(\psi(x)) \mid G(x); \quad \operatorname{gr} N(\psi(x)) = \varphi(m) \operatorname{gr} \psi(x).$$

A $\Phi_m(x)$ polinom foka szintén ennyi:

$$\operatorname{gr} \Phi_m(x) \leqq \operatorname{gr} G(x).$$

Ezek miatt $\Phi_m(x)$ irreducibilis.

2. Annak bizonyítása, hogy ha a $\psi(x)$ polinom $\Gamma(\zeta)[x]$-ben reducibilis, akkor a $\Phi_m(x)$ is reducibilis a $\Gamma[x]$-ben, igen egyszerű. Legyen

$$\psi(x) = \tau(x) \cdot \omega(x),$$

ahol

$$\tau(x), \omega(x) \in \Gamma(\zeta)[x], \operatorname{gr} \tau(x) > 0, \operatorname{gr} \omega(x) > 0$$

és legyen $\Phi_m(x)$ irreducibilis $\Gamma[x]$-ben. Mármost

$$N(\psi(x)) = \Phi_m(x) = N(\tau(x)) \cdot N(\omega(x)),$$

ami lehetetlen, mert

$$\operatorname{gr} N(\tau(x)) > 0, \operatorname{gr} N(\omega(x)) > 0$$

és a $\Phi_m(x)$ polinom $\Gamma[x]$-ben irreducibilis.

Ezzel az I. segédtétel igazolva van.

A teljesség kedvéért jegyezzük meg, hogy feltehető, hogy

$$\psi(x) = Q(x) \prod_{k=1}^{M} (x-a_k) - \zeta$$

polinom $\Gamma(\zeta)$ fölött reducibilis

$$\psi(x) = \tau(x) \cdot \omega(x),$$

ahol $\tau(x), \omega(x) \in \Gamma(\zeta)[x]$ és mindkét polinom főegyüttható 1. (Ezt később megcáfoljuk.)

A II. segédtétel előkészítésére hangsúlyozzuk a következőket: $\tau(a_k)$ számok algebrai egészek a $\Gamma(\zeta)$-ből $(k = 1, \ldots, M)$, mert $\tau(x)$ együtthatói egészek és a_k-k racionális egészek; továbbá, mivel $\tau(a_k) \mid \zeta$, ezért a $\tau(a_k)$ számok egységek a $\Gamma(\zeta)$-ból $(k = 1, \ldots, M)$.

II. segédtétel: A $\tau(x)$ polinom együtthatói legyenek a $\Gamma(\zeta)$ körosztási test egész számai. Ha az a_k és a_l racionális egészekre a $\tau(x)$ polinom egységeket vesz fel helyettesítési értékül, akkor $|a_k - a_l| > 2$ esetén a $\tau(a_k)$ és $\tau(a_l)$ egységek a komplex számsíkon ugyanarra a 0-n keresztülmenő egyenesre esnek.

Bizonyítás: L. KRONECKER egy tétele szerint [8] $\Gamma(\zeta)$ egységei így írhatók:

$$\vartheta = \eta_i^{\alpha}\,\varepsilon,$$

ahol ε valós egység a $\Gamma(\zeta)$-ból, továbbá

$\eta_i = \zeta = e^{\frac{2\pi i}{m}}$, ha m prímszámhatvány,

$\eta_i = e^{\frac{2\pi i}{2m}}$, ha m páros szám és nem prímszámhatvány,

$\eta_i = e^{\frac{2\pi i}{4m}}$, ha m páratlan szám és nem prímszámhatvány.

Legyen

$$\tau(a_k) = \eta_i^{\alpha_k}\varepsilon_k,\ \tau(a_l) = \eta_i^{\alpha_l}\varepsilon_l.$$

Az $(a_k - a_l) | (\tau(a_k) - \tau(a_l))$ oszthatóság miatt

$$(a_k - a_l) | (\eta_i^{\alpha_k}\varepsilon_k - \eta_i^{\alpha_l}\varepsilon_l);$$

elosztva az osztandót az $\eta_i^{\alpha_l}\varepsilon_k$ egységgel:

$$(a_k - a_l) \left| \left(\eta_i^{\alpha_k - \alpha_l} - \frac{\varepsilon_l}{\varepsilon_k} \right) \right.$$

A konjugált komplexre kapjuk:

$$(a_k - a_l) \left| \left(\eta_i^{-\alpha_k + \alpha_l} - \frac{\varepsilon_l}{\varepsilon_k} \right) \right.$$

A két utóbbi osztandóinak különbségét véve kapjuk:

$$(a_k - a_l) | \left(\eta_i^{\alpha_k - \alpha_l} - \eta_i^{-\alpha_k + \alpha_l} \right).$$

Ez utóbbi nem állhat fenn, ha

$$N\left(\eta_i^{\alpha_k - \alpha_l} - \eta_i^{-\alpha_k + \alpha_l} \right) \neq 0.$$

Ugyanis $N(a_k - a_l) | > 2^{\varphi(m_1)}$, ahol m_1 az η_i-nak megfelelően m-et, $2m$-et, illetve $4m$-et jelent; viszont

$$|N(\eta_i^{\alpha_k - \alpha_l} - \eta_i^{-\alpha_k + \alpha_l})| = \left| N\left(2i \sin \frac{\alpha_k - \alpha_l}{m_1} 2\pi \right) \right| \leq 2^{\varphi(m_1)}.$$

Márpedig ha $N(\eta_i^{\alpha_k - \alpha_l} - \eta_i^{-\alpha_k + \alpha_l}) = 0$, akkor $\frac{\alpha_k - \alpha_l}{m_1} 2\pi$ a 2π-nek racionális egész számú többszöröse. Tehát $\tau(a_k)$ és $\tau(a_l)$ a kívánt tulajdonsággal rendelkeznek, és

$$\tau(a_l) = \pm \eta_i^{\alpha_k}\varepsilon_l,$$

qu. e. d.

III. segédtétel: *Legyenek* $a_1 < a_2 < \cdots < a_M$ *racionális egész számok,* $M \geq 6$ *és* $\tau(x)$ *a* $\Gamma(\zeta)[x]$*-ből vett egész együtthatós polinom. Ha* $\tau(a_k)$ $(k = 1, \ldots, M)$ *a* $\Gamma(\zeta)$*-ba tartozó egységek, akkor mindegyikük ugyanarra a* 0*-n keresztülmenő egyenesre esik.*

Bizonyítás: Fennállnak a következő relációk:

$$2 < a_4 - a_1 < a_5 - a_1 < \cdots < a_M - a_1$$

és

$$2 < a_M - a_3 < a_M - a_2.$$

A II. segédtétel szerint $\tau(a_1), \tau(a_4), \ldots, \tau(a_M)$ ugyanarra a 0-n átmenő egyenesre esik és ugyanerre esik $\tau(a_M)$-mel együtt $\tau(a_2), \tau(a_3)$ is. Qu. e. d.

A tételek bizonyítása

Ezen segédtételekkel bebizonyítható a

3. tétel. Bizonyítás: Feltesszük, hogy $\Phi_m(x)$ polinom reducibilis a racionális számtest fölött:

$$\Phi_m(x) = G(x) \cdot H(x), \quad (G(x), H(x) \in \Gamma[x]).$$

A $G(x)$ és $H(x)$ polinomok főegyütthatója legyen 1. A $\psi(x) = Q(x) \prod_{k=1}^{M} (x - a_k) - \zeta$ polinomnak az I. segédtétel szerint szintén reducibilisnak kell a $\Gamma(\zeta)$ fölött lennie. $\psi(x)$ polinomot bontsuk a $\Gamma(\zeta)$ fölött irreducibilis tényezők szorzatára:

$$\psi(x) = \tau_1(x) \cdots \tau_r(x).$$

A $\tau_i(x)$ $(i = 1, \ldots, r)$ polinomok főegyütthatói legyenek 1-gyel egyenlők. Szükséges, hogy az egyik, pl. a $\tau_1(x)$ polinom foka, $s \leqq \frac{M + \operatorname{gr} Q(x)}{2} < M$ legyen.

A $\tau_1(a_k)$ $(k = 1, \ldots, M)$ egységek a III. segédtétel szerint így írhatók:

$$\tau_1(a_k) = \pm \eta_1^{\alpha_1} \varepsilon_k \quad (k = 1, \ldots, M),$$

ahol $\eta_1 = e^{\frac{2\pi i}{m_1}}$; ε_k valós egység a $\Gamma(e^{\frac{2\pi i}{m}})$ testből.

Alkalmazva LAGRANGE interpolációs formuláját

$$\tau_1(x) = \eta_1^{\alpha_1} \sum_{k=1}^{s+1} \frac{P_1(x)\ (\pm \varepsilon_k)}{P_1'(a_k)\,(x - a_k)} = \eta_1^{\alpha_1} L(x),$$

ahol $P_1(x) = \prod_{l=1}^{s+1} (x - a_l)$ és $L(x)$ valós együtthatós polinom a $\Gamma(\zeta)[x]$-ből.

A $\tau_1(x)$ polinom főegyütthatója 1, ezért $\eta_1^{\alpha_1} = \pm 1$ valós egységgyöknek adódik. Tehát a $\tau_1(x)$ polinom is valós.

$\tau_1(x) | \psi(x)$ miatt $\tau_1(x) | \overline{\psi(x)}$, ahol a $\overline{\psi(x)}$ polinom a $\psi(x)$ polinomnak konjugált komplex polinomja.

Ez nem lehetséges, mert

$$\tau_1(x) \nmid (\psi(x) - \overline{\psi}(x)) = \zeta - \zeta^{-1}.$$

Az ellentmondás megszűnik, ha $\Phi_m(x)$ irreducibilis a Γ fölött.

Ezzel a 3. tételt igazoltuk.

A most bizonyított tétel alkalmazható a 2. tétel igazolására.

A 2. tétel bizonyítása: Az $M \geqq 6$ esetben a 3. tétel szerint a tétel igaz. (Természetesen $Q(x) = 1$). $M \leqq 5$-re minden esetet külön vizsgálunk.

$M = 5$. *Az* $f_m P(x)$ *polinom irreducibilis a* Γ *fölött.*

Az I. segédtétel szerint csak a $\psi(x) = \prod_{k=1}^{5} (x - a_k) - \zeta$ polinomnak a $\Gamma(\zeta)$ fölötti irreducibilitását kell igazolnunk. Ha $\psi(x)$ polinom reducibilis $\Gamma(\zeta)$ fölött, akkor van oly $\tau(x)$ polinom-osztója, amely irreducibilis a $\Gamma(\zeta)$ fölött, foka $\leqq 2$ és főegyüttható 1.

$2 < a_4 - a_1$, $2 < a_5 - a_1$ következtében a II. segédtétel szerint a $\tau(a_1)$, $\tau(a_4)$, $\tau(a_5)$ egységek ugyanazon a 0-n átmenő egyenesen vannak. A $\tau(x)$ polinom valós együtthatójú. Hasonlóképpen mint a 3. tételnél, itt is belátható, hogy $\psi(x)$ irreducibilis a $\Gamma(\zeta)$ fölött.

Ha $M = 4$, *illetve* $M = 3$ *és az* $a_k = a_1 + k - 1 (k = 1, \ldots, M)$ *nem teljesül, a* $\psi(x) = \prod_{k=1}^{M} (x - a_k) - \zeta$ *polinom irreducibilis a* $\Gamma(\zeta)$ *fölött és* $\Phi_m(x)$ *irreducibilis a* Γ *fölött.*

$M = 4$. Ugyanis, ha $\psi(x)$ reducibilis a $\Gamma(\zeta)$ fölött, akkor egyik irreducibilis tényezőjének, a $\tau(x)$ polinomnak foka: $s \leqq 2$ kell, hogy legyen (a főegyüttható legyen ismét 1)

$$a_4 - a_1 > 2 \text{ és } \begin{array}{l} \text{vagy } a_3 - a_1 > 2, \\ \text{vagy } a_4 - a_2 > 2. \end{array}$$

Mindkét esetben $\tau(x)$ három helyen vesz fel helyettesítési értékül olyan egységet, melyek ugyanazon a 0-n átmenő egyenesre esnek, ami ellentmondás.

$M = 3$. Ha a $\psi(x)$ polinom a $\Gamma(\zeta)$ fölött reducibilis volna, akkor léteznék $\psi(x)$ polinomnak oly $\tau(x)$ irreducibilis tényezője, amelynek foka: $s = 1$, főegyüttható szintén 1. A feltétel szerint $a_3 - a_1 > 2$ így $\tau(a_1)$, $\tau(a_3)$ ugyanarra a 0-n keresztülmenő egyenesre esnek. Az ellentmondásra ugyanúgy jutunk, mint az előbb.

Ha $M = 2$, *akkor a* $\Phi_m(x)$ *polinom irreducibilis a* $\Gamma(\zeta)$ *fölött, feltéve, hogy* $|a_2 - a_1| > 2$.

Ha $\psi(x)$ reducibilis, akkor kell, hogy legyen egy lineáris tényezője 1 főegyüttható val. Hasonlóan jutunk ellentmondásra, mint az $M = 4$ esetben.

Kiegészítés

Avégből, hogy I. SCHUR problémáját maradék nélkül igazoljuk, nézzük meg a $\Phi_m(x) = f_m(P(x))$ polinom irreducibilitásának taglalásánál kimaradt eseteket, természetesen a Schur-féle problémában szereplő

$$F(x) = \prod_{k=1}^{M} (x - a_k)^{2^n} + 1$$

polinomra vonatkozólag.

Előzőleg egy segédtételt bizonyítunk:

4. segédtétel: Az $F(x) = \prod_{k=1}^{M} (x - a_k)^{2^n} + 1$ *polinom racionális egész* a_k*-k* ($k = 1, \ldots, M$) *mellett irreducibilis a racionális számtest fölött, ha létezik oly egész együtthatós* mod 2 *— irreducibilis* $\psi(x)$ *polinom, hogy*

$$K(x) = \prod_{k}^{M}{}_{1} (x - a_k) + 1 \equiv [\psi(x)]^r \pmod 2$$

és r pozitív egész.

Bizonyítás: Tegyük fel, hogy $F(x)$ reducibilis a I' fölött.

Érvényes a következő kongruencia:

$$F(x) \equiv \left[\prod_{k=1}^{M} (x - a_k) + 1\right]^{2^n} \pmod 2.$$

Ennek helyességéről ismételt négyzetreemelésekkel győződhetünk meg.

Ha feltesszük, hogy

$$K(x) = \prod_{k=1}^{M} (x - a_k) + 1 \equiv \psi(x)^r \pmod 2,$$

akkor

$$F(x) \equiv G(x) \cdot H(x) \equiv [\psi(x)]^{2^n \cdot r} \pmod 2.$$

Mivel $\psi(x)$ mod 2 irreducibilis, azért

$$G(x) \equiv \psi^\alpha(x) \pmod 2 \text{ és } H(x) \equiv \psi^\beta(x) \pmod 2.$$

Az $\alpha > 0$, $\beta > 0$, mivel $G(x)$ polinom foka és $H(x)$ polinom foka pozitív, még az esetben is, ha a két polinom együtthatóit mod 2 vesszük.

A kongruenciák helyett a következő egyenlőtlenséget írhatjuk:

$$G(x) = \psi^\alpha(x) + 2A(x) *$$

ill.

$$H(x) = \psi^\beta(x) + 2B(x),$$

ahol

$$gr A(x) < gr \psi^\alpha(x) \quad \text{és} \quad gr B(x) < gr \psi^\beta(x).$$

* Az alábbiakban szereplő polinomok együtthatói racionális egészek.

A $G(x)\cdot H(x)$-et tekintsük mod 4:

(1) $F(x)=G(x)\cdot H(x)\equiv\psi^{\alpha+\beta}(x)+2\psi^{\beta}(x)A(x)+2\psi^{\alpha}(x)B(x)\pmod 4$;

másrészt

$$\prod_{k=1}^{M}(x-a_k)=\psi^{r}(x)-1+2K_1(x),$$

és így ismételt négyzetreemelésekkel adódik:

(2) $F(x)=[\psi^{r}(x)-1+2K_1(x)]^{2^n}+1\equiv[\psi(x)]^{r\cdot 2^n}+2[\psi(x)]^{r\cdot 2^{n-1}}+2\pmod 4$.

Az (1) és (2) alatti kongruenciákat összehasonlítva, rendezés és 2-vel való osztás után kapjuk a

$$[\psi(x)]^{\beta}A(x)+[\psi(x)]^{\alpha}B(x)-[\psi(x)]^{r\cdot 2^{n-1}}\equiv 1\pmod 2$$

kongruenciát.

Ez nem állhat fenn, mert α, β, $r\cdot 2^{n-1}$ pozitív egészek és így a baloldal osztható a $\psi(x)$ polinommal, a jobboldal viszont nem. Ezzel az ellentmondással a segédtétel be van bizonyítva.

Ezek után vizsgáljuk meg még azon eseteket, amelyeket I. SCHUR szóban forgó problémájánál kihagytunk:

Ha $M=4$ és $a_k=a_1+k-1\,(k=1,\ldots,M)$, akkor

$$a_1\equiv a_3\pmod 2,\quad a_2\equiv a_4\equiv a_1+1\pmod 2$$

miatt adódik:

$$K(x)=(x-a_1)(x-a_2)(x-a_3)(x-a_4)+1=[(x-a_1)(x-a_1-1)+1]^2\pmod 2.$$

Minthogy a $\psi(x)=(x-a_1)(x-a_1-1)+1$ polinom mod 2 nyilván irreducibilis, ezért $F(x)$ a IV. segédtétel szerint irreducibilis a Γ fölött.

Ha $M=3$ és $a_k=a_1+k-1$, akkor

$$K(x)\equiv(x-a_1)^2(x-a_1-1)+1\pmod 2.$$

$\psi(x)\equiv K(x)$ mod 2— irreducibilis, ezért $F(x)$ irreducibilis a Γ fölött.

Ha $M=2$ és $|a_1-a_2|\leq 2$, akkor vagy

$$a_1\equiv a_2\pmod 2\text{ és }K(x)\equiv(x-a_1)^2+1\equiv(x-a_1+1)^2\pmod 2$$
$$\psi(x)\quad x-a_1+1,$$

vagy $a_2\equiv a_1+1\pmod 2$ és

$$K(x)=(x-a_1)(x-a_1-1)+1=\psi(x).$$

Mindkét esetben $\psi(x)$ mod 2— irreducibilis, ezért $F(x)$ irreducibilis a Γ fölött. Ezzel I. SCHUR szóban forgó sejtése teljesen igazolva van.

Megjegyzés: Ahhoz, hogy az $F(x)=\prod_{k=1}^{M}(x-a_k)^{2^n}+1$ polinom az $a_k\,(k=1,\ldots,M)$ racionális egészek megadása esetén $n>0$-ra irreducibilis

legyen a Γ fölött, nem szükséges, hogy a $K(x) \prod_{k=1}^{M} (x-a_k)+1$ polinom valamely mod 2— irreducibilis polinom pozitív egész kitevőjű hatványával mod 2 kongruens legyen. Példa erre az $F(x)=[x(x-4)(x-8)]^{2^n}+1$ polinom. Ez a polinom az 1. tétel szerint irreducibilis a Γ fölött, viszont nem teljesíti a IV. segédtétel követelményeit, mert

$$K(x) \equiv x^3+1 \pmod 2$$

és ez mod 2 reducibilis.

IRODALOM

[1]. A $P(x)-1 \prod_{k=1}^{n} (x-a_k)-1$ polinom irreducibilitási kérdésének felvetése. *Archiv der Math. u. Phys.* XIII. (1908), 367.

[2]. A $P(x)-1$ polinom irreducibilitásának bizonyítása. *Archiv. der Math. u. Phys.* XV. (1909), 271.

[3] W. Flügel a $P(x)+1$ polinom irreducibilitásáról. *Archiv. der Math. u. Phys.* XV. (1909), 272.

[4] A $[P(x)]^2+1$ polinom irreducibilitásának kérdése. *Archiv der Math. u. Phys.* XV. (1909), 259.

[5] A $[P(x)]^2+1$ polinom irreducibilitásának bizonyítása. G. Pólya—G. Szegő: Aufgaben und Lehrsätze aus der Analysis, II. *Berlin, Springer* (1925), 347.

[6] A $[P(x)]^4+1$ és $[P(x)]^8+1$ polinomok irreducibilitásának bizonyítása. *A. Brauer—R. Brauer—H. Hopf:* Über Irreduzibilität einiger speziellen Klassen von Polynomen. *Jahresbericht der Deutschen Math. Ver.* XXXV. (1926), 99—112.

[7] „Über Irreduzibilitätskriterien von I. Schur und G. Pólya." *Mathematische Zeitschrift* XL (1935), 204.

[8] L. Kronecker: Über complexe Einheiten. Crelle, *Journal für die reine und angew. Math.* LVI. 188.