ALGEBRA ÉS SZÁMELMÉLET 4

5. Előadás

Emlékeztető:

$T[x]$, T test: pl.: $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Q}[x]$

Ezekre:
- a maradékos osztás elvégezhető
- maradékos osztásból → euklideszi algoritmus
- kitüntetett közös osztó létezik
- irreducibilis polinomok prímtulajdonságúak
- az irreducibilisekre történő felbontás egyértelmű (lényegében)
- SZAT (számelmélet alaptétele)

Mi a helyzet $\mathbb{Z}[x]$-ben? (Ott pl. ∄ mar. osztás!)

Oszthatóság: $f, g \in \mathbb{Z}[x]$: $f \mid g \iff \exists h \in \mathbb{Z}[x]$
$g = f \cdot h$

Egység: mindennek osztója $\iff$ invertálható elem
$\iff \pm 1$

Triviális felbontás: valamelyik tényező egység

Irreducibilis polinom: csak triviális felbontása létezik (és $\neq 0$, $\neq$ egység)

Vigyázat! Test fölött: $f = g \cdot h$ triviális felbontás
$\Updownarrow$
g konstans v. h konstans

(Mivel itt a nem nulla konstansok az egységek)

Így test fölött: $f = g \cdot h$ nem triviális fölbontás

$\Updownarrow$

g és h alacsonyabb fokú, mint f

Ugyanakkor: – $\mathbb{Z}[x]$-ben most: $2x + 4 = 2\cdot(x+2)$ nem triviális fölbontás, noha $gr(x+2) = gr(2x+4)$
– $\mathbb{Z}[x]$-ben a $\mathbb{Z}$-beli prímek fölbonthatatlanok

Látni fogjuk: $\mathbb{Z}[x]$ szerkezete két részből tevődik össze: $\mathbb{Z}$ szerkezetéből és $\mathbb{Q}[x]$ szerkezetéből.

Cél: SZAT bizonyítása $\mathbb{Z}[x]$-ben.

Fontos alapfogalom volt $\mathbb{Z}[x]$-ben:

Def.: $f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$ primitív, ha $(a_0, \dots, a_n) = 1$, azaz az együtthatók rel. prímek.

$\uparrow$ leg. közös osztó

Észrevétel: 1) $f \in \mathbb{Z}[x] \Rightarrow \exists\, a \in \mathbb{Z},\ g \in \mathbb{Z}[x]$:

$f(x) = a \cdot g(x)$, g primitív

2) $f \in \mathbb{Q}[x] \Rightarrow \exists\, q \in \mathbb{Q},\ g \in \mathbb{Z}[x]$:

$f(x) = q \cdot g(x)$, g primitív

Sőt, ez a fölbontás lényegében egyértelmű (q, $g(x)$ csak egységszorzóban térhetnek el)

Megj.: Egyértelműség a 4. feladatsoron.

$\boxed{\text{AS24}}$

1. Gauss-lemma   Primitív polinomok szorzata primitív.

<u>Biz.</u> mod p osztódás:

$f \in \mathbb{Z}[x] \mapsto \bar{f} \in \mathbb{Z}_p[x]$, ahol az együtthatók maradékait vesszük

Ez egy szorzattartó megfeleltetés: $\overline{f\cdot g} = \bar{f}\cdot\bar{g}$

Ha f, g primitív $\Rightarrow$ $\forall p$-re: $\bar{f}, \bar{g} \neq 0$

$$\Rightarrow \overline{f\cdot g} = \bar{f}\cdot\bar{g} \neq 0 \Rightarrow f\cdot g \text{ primitív.}$$

(hiszen $\mathbb{Z}[x]$ nullosztómentes)

<u>Tankönyvben</u>: ez az 1. G.-lemma következménye.

Az ottani Gauss-lemma:

<u>1. Gauss-lemma (p-változat)</u> p prím $\mathbb{Z}$-ben $\Rightarrow$ p prímtulajdonságú $\mathbb{Z}[x]$-ben, azaz:

$$p \mid f\cdot g \Rightarrow p \mid f \text{ vagy } p \mid g.$$

<u>Biz.</u> Az előző tételből, ill. annak biz.-ából:

$$p \mid f\cdot g \Rightarrow \overline{f\cdot g} = 0 \quad \mathbb{Z}_p[x]\text{-ben}$$

$$\Rightarrow \bar{f} = 0 \text{ v. } \bar{g} = 0 \quad \mathbb{Z}_p[x]\text{-ben}$$

$$\Rightarrow p \mid f \text{ vagy } p \mid g.$$

<u>Hf.</u> Hogyan következik az 1. Gauss-lemma a p-s változatból?

Gauss-lemma 2. következménye

Legyen $f, h \in \mathbb{Z}[x]$, f primitív.

T. föl: $f \mid h$ $\mathbb{Q}[x]$-ben (azaz $\exists g \in \mathbb{Q}[x]$: $h = f \cdot g$)

Ekkor $f \mid h$ $\mathbb{Z}[x]$-ben is (mert a fenti $g \in \mathbb{Z}[x]$).

<u>Biz.</u> (Megj. Hasonló jellegű állítást megfogalmazhatunk pl.: $\mathbb{Q}[x] \subset \mathbb{R}[x]$, v. $\mathbb{R}[x] \subseteq \mathbb{C}[x]$ vonatkozásában

$f, h \in \mathbb{Q}[x]$, $f \mid h$ $\mathbb{R}[x]$-ben $\Rightarrow$ $f \mid h$ $\mathbb{Q}[x]$-ben is

Az ottani bizonyítás a maradékos osztás létezésén és egyértelműségén múlik.)

Tegyük föl tehát, hogy $f \cdot g = h$, $g \in \mathbb{Q}[x]$.

Ekkor: $g = \left(\frac{s}{t}\right) \cdot g_0$, $s, t \in \mathbb{Z}$, g_0 primitív, $(s,t) = 1$.

Tehát: $h = f \cdot g = f \cdot \left(\frac{s}{t}\right) \cdot g_0 \Longrightarrow$

$$\underset{\mathbb{Z}[x]}{\underset{\cap}{t \cdot h}} = s \cdot \underbrace{f \cdot g_0}_{\text{primitív az 1. G. lemma miatt}}$$

Ha $p \mid t$, $p \in \mathbb{Z}$ prímszám $\Longrightarrow$

$p \mid s$ v. $p \mid f$ v. $p \mid g_0$ (p prímtulajdonsága, G. lemma p-vel. miatt).

Ez viszont nem lehetséges: $(t, s) = 1$, f, g_0 prim

Ez azt jelenti, hogy t egység (± 1) $\Rightarrow$

$$\underset{\overset{\cap}{\mathbb{Z}}}{g = \left(\frac{s}{t}\right)} \cdot g_0 \quad \text{miatt,} \quad g \in \mathbb{Z}[x].$$

$\square$

2. Gauss-lemma: $0 \neq f \in \mathbb{Z}[x]$, $f = g \cdot h$ $\mathbb{Q}[x]$-ben

$\Rightarrow$ $\exists\, g_0, h_0 \in \mathbb{Z}[x]$, hogy:

a) $f = g_0 \cdot h_0$

b) g_0 a g nec. számszorosa

h_0 a h nec. számszorosa

Megj: Ez a lemma tehát egy nem triviális

$\mathbb{Q}[x]$-beli fölbontásból nem triviális

$\mathbb{Z}[x]$-beli fölbontást csinál $(f \in \mathbb{Z}[x])$.

Biz. Legyen $g = r \cdot g_1$, $r \in \mathbb{Q}$, g_1 primitív

$h = s \cdot h_1$, $s \in \mathbb{Q}$, h_1 primitív

Ilyenek léteznek, ezt láttuk.

Ekkor:

$$f = (r \cdot g_1) \cdot (s \cdot h_1) = \underset{\overset{\cap}{\mathbb{Q}}}{(r \cdot s)} \cdot \underbrace{g_1 \cdot h_1}_{\text{primitív (1. G. lemma)}} \in \mathbb{Z}[x].$$

Mivel $g_1 \cdot h_1$ primitív, ezért $(r \cdot s) \in \mathbb{Z}$ (hiszen $f \in \mathbb{Z}[x]$).

(Itt hivatkozhattunk volna a 2. következményre is.)

Ekkor: $f = \underbrace{(r \cdot s \cdot g_1)}_{g_0 \in \mathbb{Z}[x]} \cdot \underbrace{h_1}_{h_0 \in \mathbb{Z}[x]}$

És a feltételből adódik: g_0 a g-nek, h_0 a h-nak

nem. számszorosa. □

Készen állunk arra, hogy leírjuk a $\mathbb{Z}[x]$-beli irreducibilis polinomokat. Láttuk már pl., hogy $p \in \mathbb{Z}$ prím $\Rightarrow$ p irreducibilis $\mathbb{Z}[x]$-ben.

De most teljes leírást adunk.

<u>Tétel</u>: Legyen $f \in \mathbb{Z}[x]$.

f irreducibilis $\mathbb{Z}[x]$-ben $\iff$ 1) $f = p \in \mathbb{Z}$ prímszám

<u>vagy</u>

2) f primitív, nem konstans, és f irreducibilis $\mathbb{Q}[x]$-ben.

<u>Biz.</u> $\Leftarrow$ 1) p nyilván felbonthatatlan: a felbontásában csak konstansok szerepelhetnek, de ezek csak triviális felbontások

2) Legyen most f nem konstans primitív polinom, ami irr. $\mathbb{Q}$ fölött.

Ha $f = g \cdot h$, és itt $g, h \in \mathbb{Z}[x]$ $\Rightarrow$

a $\mathbb{Q}[x]$-beli irreducibilitás miatt ez triv. fölb.

$\Rightarrow$ g v. h konstans. $(\Rightarrow \in \mathbb{Z})$

$\Rightarrow$ g v. h egység, mivel f primitív.

$\Rightarrow$ T. fel: $f \in \mathbb{Z}[x]$ irreducibilis $\mathbb{Z}[x]$-ben.

Ekkor: $f = n \cdot f_0$, $n \in \mathbb{Z}$, f_0 primitív $\in \mathbb{Z}[x]$.

Az irreducibilitás miatt ez a fölbontás triviális

$\Rightarrow$ n egység $(\Rightarrow f = \pm f_0$ primitív$)$

vagy

f_0 egység $(\Rightarrow f = \pm n$ konstans, és így prímszám$)$

Azt kell már csak, hogy ha f primitív, akkor $\mathbb{Q}[x]$-ben is fölbonthatatlan.

Ha $f = g \cdot h$ $\mathbb{Q}[x]$-ben nem triviális fölbontás

$\Rightarrow$ g, h foka kisebb, mint f foka

A 2. Gauss lemma miatt: $f = g_0 \cdot h_0$, ahol $g_0, h_0 \in \mathbb{Z}[x]$, és $\operatorname{gr} g_0 = \operatorname{gr} g$, $\operatorname{gr} h_0 = \operatorname{gr} h$.

Ez viszont egy nem triviális felbontást adna $\mathbb{Z}[x]$-ben, ami ellentmondana f irreducibilitásának.

Ezzel a tételt beláttuk.

$\mathbb{Z}[x]$-beli SZAT-hoz már csak egy dolog kell:

<u>Áll.</u> $f \in \mathbb{Z}[x]$ irreducibilis $\Rightarrow$ prímtulajdonságú $\mathbb{Z}[x]$-ben.

<u>Biz.</u>: Láttuk: $f = p \in \mathbb{Z}$ prím vagy f primitív, irred. $\mathbb{Q}[x]$-ben.

Ha $f = p$ $\rightsquigarrow$ az 1. Gauss-lemma β verzió mondja ki, hogy f prímtulajdonságú!

Ha f primitív, irred. $\mathbb{Q}[x]$-ben:

T. fel: $f \mid g \cdot h$, $g, h \in \mathbb{Z}[x]$, oszthatóság $\mathbb{Z}[x]$-ben $\Rightarrow$ $\mathbb{Q}[x]$-ben is.

De f irred. $\mathbb{Q}[x]$-ben $\rightsquigarrow$ prímtulajdonságú $\mathbb{Q}[x]$-ben

$\Rightarrow$ $f \mid g$ v. $f \mid h$ $\mathbb{Q}[x]$-ben

$\Rightarrow$ Az 1. G. lemma 2. következménye miatt az oszthatóság fennáll $\mathbb{Z}[x]$-ben is. $\square$

<u>Tétel:</u> $\mathbb{Z}[x]$-ben érvényes a számelmélet alaptétele:

$\forall f \in \mathbb{Z}[x]$, $f \neq 0$, $f \neq$ egység polinomra

$\exists f = f_1 \cdots f_k$ felbontása, ahol $f_i \in \mathbb{Z}[x]$ irr., és ez a felbontás lényegében (sorrendtől és egységszorzótól eltekintve) egyértelmű.

<u>Biz:</u> Az egyértelműség a jól ismert módon következik abból, hogy $\forall$ irr. polinom prímtulajdonságú (lásd $\mathbb{Z}$, $T[x]$ esetét).

Csak a felbonthatóságot kell igazolnunk.

$f = n \cdot f_0$, ahol $n \in \mathbb{Z}$, f_0 primitív.

$n = p_1 p_2 \cdots p_k$ a $\mathbb{Z}$-beli SZAT-ból;

prímek $\quad$ p_i-k irr.-ek $\mathbb{Z}[x]$-ben is.

$f_0 = f_1 \cdot f_2 \cdots f_t$ $\quad$ $\mathbb{Q}[x]$-beli felbontás irr.-ekre

felbonthatatlanok ($\rightsquigarrow$ nem konstansok)

$\Downarrow$ 2. Gauss-lemma, (több lépésben, indukcióval)

$f_0 = f_1' f_2' \cdots f_t'$ $\quad$ $\mathbb{Z}[x]$-beli felbontás, ahol

$$f_i' = c \cdot f_i, \quad c \in \mathbb{Q}.$$

De akkor f_i' is felbonthatatlan $\mathbb{Q}[x]$-ben, és nyilván primitív (mert f_0 is primitív) $\Rightarrow f_i' \in \mathbb{Z}[x]$ irr. $\square$

<u>Megjegyzés:</u> Az előző folyamatot ($\mathbb{Z}[x] \rightsquigarrow \mathbb{Z}$, $\rightsquigarrow \mathbb{Q}[x]$) általában is megcsinálhatjuk:

Ha R kommutatív, nullosztómentes egységelemes gyűrű („szokásos" gyűrű), és legyen Q az R hányadosteste:

Ha R alaptételes, akkor:

$R[x]$ alaptétele $\rightsquigarrow$ R számelmélete

$\rightsquigarrow$ $Q[x]$ alaptétele

<u>Tétel</u> (biz. nélkül) R szokásos gyűrű alaptételes $\Longrightarrow$ $R[x]$ is alaptételes.

<u>Következmény</u>: $T[x_1, x_2, \dots x_n]$ alaptételes $\forall n$-re.

<u>Biz.</u>: Indukcióval: $T[x_1]$ alaptételes $\rightsquigarrow$ $T[x_1, x_2]$ alaptételes

$T[x_1, \dots x_{n-1}]$ alaptételes $\rightsquigarrow$ $T[x_1, \dots x_n]$ alaptételes.

Láttuk: $\mathbb{Z}[x]$ alaptételét $\mathbb{Q}[x]$ alaptételéből kaptuk meg. De van lehetőség a másik irányba is: $\mathbb{Z}[x]$ visszavezetése $\mathbb{Q}[x]$ alaptételére.

Schönemann – Eisenstein-kritérium

$f \in \mathbb{Z}[x]$, nem konstans, $f = a_0 + a_1 x + \dots + a_n \cdot x^n$.
Tegyük fel, hogy $\exists\, p \in \mathbb{Z}$ prímszám, melyre:

a) $p \nmid a_n$

b) $p \mid a_0, \dots, a_{n-1}$

c) $p^2 \nmid a_0$

Ekkor f irreducibilis $\mathbb{Q}[x]$-ben.

Biz.: Vegyük az 1. Gauss-lemmából ismert mod p módszert: $f \rightsquigarrow \bar{f}$.

T. fel: f nem irreducibilis $\mathbb{Q}[x]$-ben $\Rightarrow$

$f = g \cdot h$, ahol $g, h \in \mathbb{Q}[x]$ alacsonyabb fokúak, mint f.

$\overset{\text{2. Gauss lemma}}{\Longrightarrow}$ $f = g_0 \cdot h_0$, ahol $g_0, h_0 \in \mathbb{Z}[x]$, és g_0, h_0 is alacsonyabb fokúak.

Vegyük az együtthatókat mod p:

$\bar{f} = \overline{g_0 \cdot h_0} = \bar{g}_0 \cdot \bar{h}_0$ $\mathbb{Z}_p[x]$-ben.

(Tudjuk: $f \rightsquigarrow \bar{f}$ szorzattartó).

A feltételek miatt:

$\mathrm{gr}\, f = \mathrm{gr}\, \bar{f}_g$ hiszen $p \nmid a_n$.

Másrészt: $\bar{f} = c \cdot X^n$ (ahol $n = \mathrm{gr}\, f$), $c \in \mathbb{Z}_p$, $c \neq 0$

Mivel $\mathbb{Z}_p[x]$ alaptételes, $c \cdot X^n$ osztói csak $c' \cdot x^k$ alakúak lehetnek, ahol $c' \in \mathbb{Z}_p$ nem nulla konstans.

Ez azt jelenti: $\bar{g}_0 = c_1 x^k$

$\bar{h}_0 = c_2 \cdot x^l$ $\quad k + l = n$, $1 \leq k, l < n$

De ez azt jelenti, hogy $g_0, h_0 \in \mathbb{Z}[x]$ konstans tagjai oszthatók p-vel (hiszen $\bar{g}_0$, $\bar{h}_0$-ban eltűnnek)

$\Longrightarrow$ $f = g_0 \cdot h_0$ konstans tagja osztható p^2-tel $\lightning$.

Tehát f irreducibilis $\mathbb{Q}[x]$-ben.

Megjegyzés: 1) f irreducibilitása $\mathbb{Z}[x]$-ben nem következik a feltételekből (pl.: $2x + 6$-ra $p = 3$ jó, de $2x + 6 = 2(x + 3)$).

2) A Sch.-E. krit. nem megfordítható!!!

Pl.: $x^2 + 1$ nem teljesíti a feltételeket, de mégis irreducibilis $\mathbb{Q}[x]$-ben.

Körosztási polinomok

Egy fontos polinomosztállyal ismerkedünk meg.

Emlékeztető: 1) $z \in \mathbb{C}$ <u>n-edik egységgyök</u>, ha $z^n = 1$. Trig. alakban: $z = \cos\left(k \cdot \frac{2\pi}{n}\right) + i \sin\left(k \frac{2\pi}{n}\right)$.

2) z <u>primitív n-edik egységgyök</u>, ha n-edik egységgyök, és nem k-adik egységgyök semilyen $k < n$-re sem. (Csoportelméletben: z rendje n a $\mathbb{C}$ szorzási csoportjában)

Ilyenkor: z primitív n-edik egységgyök $\rightsquigarrow$ $\forall$ n-edik egységgyök z-nek hatványa.

Trig. alakból: $z = \cos\left(k \frac{2\pi}{n}\right) + i \sin\left(k \frac{2\pi}{n}\right)$ primitív, ha $(k, n) = 1$, azaz k és n relatív prímek.

Ebből következik: n-edik egységgyökök száma: n

prim. n-edik egységgyökök száma: $\varphi(n)$

Euler-függvény

$\varphi(n) = \{k \in \mathbb{Z} \mid 1 \leq k \leq n, (k, n) = 1\}$.

Pl.: Prim. egységgyökök: $n = 1$: $z = 1$

$n = 2$: $z = -1$

$n = 3$: $z_1 = -\frac{1}{2} + i \frac{\sqrt{3}}{2}$

$z_2 = -\frac{1}{2} - i \frac{\sqrt{3}}{2}$

$n = 4$: $z_1 = i$ és $z_2 = -i$.

Def. $\Phi_n(x) \in \mathbb{C}[x]$ az a monolt polinom, melynek (egyszeres) gyökei a komplex primitív n-edik egységgyökök:

$$\Phi_n(x) = (x-\varepsilon_1)(x-\varepsilon_2)\cdot\ldots\cdot(x-\varepsilon_{\varphi(n)})$$

az összes primitív n-edik egységgyök.

Példa: $\Phi_1(x) = x-1$

$\Phi_2(x) = x+1$

$\Phi_4(x) = (x-i)(x+i) = x^2+1$

$\Phi_3(x) = \left(x+\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)\left(x+\frac{1}{2}+i\frac{\sqrt{3}}{2}\right) = x^2+x+1$

Végül érve: $\Phi_n(x) \in \mathbb{C}[x]$, ε_i-k általában „nagyon nem valósak", de $\Phi_n(x)$ – a fenti példákban – valós, sőt racionális együtthatós, sőt: egész együtthatós!

Tétel: $\Phi_n(x) \in \mathbb{Z}[x]$, monolt $\forall n$-re.

Biz. előtt egy lemma a $\Phi_n(x)$ rekurzív előállításához.

Lemma: $n \geq 1$-re: $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$

Biz.: $x^n - 1 = (x - z_1) \dots (x - z_n)$, ahol

z_i-k az ~~[illegible]~~ n-edik egységgyökök.

Közöttük vannak szerepelnek a primitív d-edik egységgyökök $\forall\, d \mid n$-re:

$$\{z_1, \dots z_n\} = \{z \in \mathbb{C} \mid o(z) \mid n\} = \{z \in \mathbb{C} \mid o(z) = d \mid n\}$$

multiplikatív rend

$$= \{z \in \mathbb{C} \mid o(z) = d_1\} \cup \{z \in \mathbb{C} \mid o(z) = d_2\} \cup \dots$$

$d_1, d_2, \dots d_k$ az n (pozitív) osztói

Ez pontosan azt jelenti, hogy:

$$x^n - 1 = \Phi_{d_1}(x)\, \Phi_{d_2}(x) \dots \Phi_{d_k}(x),$$ ahol

$d_1, \dots d_k$ az n összes osztója,

hiszen: $$\Phi_{d_i}(x) = \prod_{o(\xi_j) = d_i} (x - \xi_j)$$

Köv.: $$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x)}$$

Ez a képlet lehetőséget ad Φ_n rekurzív számolására

<u>A tétel bizonyítása:</u> indukcióval n-re.

$\Phi_1(x) = x-1$ – igaz az állítás.

$$\Phi_n(x) = \frac{x^n-1}{\prod\limits_{\substack{d\mid n\\ d\neq n}} \Phi_d(x)}$$; itt indukcióval: $\Phi_d(x)$ normált, egész együtthatós

$\rightsquigarrow$ $\mathbb{C}[x]$-ben: $\underbrace{\prod\limits_{\substack{d\mid n\\ d\neq n}} \Phi_d(x)}_{\text{indukcióval: } \in \mathbb{Z}[x], \text{ normált}} \;\Big|\; x^n-1$ világos

$\rightsquigarrow$ $\mathbb{Z}[x]$-ben is tudunk maradékosan osztani, mivel 1 a főegyüttható.

$\rightsquigarrow$ a hányadospolinom $\in \mathbb{Z}[x]$, normált.

<u>Példa:</u> $$\Phi_6(x) = \frac{x^6-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)} =$$

$$= x^2 - x + 1$$

<u>Tétel:</u> $\Phi_n(x)$ irreducibilis $\mathbb{Z}[x]$-ben és $\mathbb{Q}[x]$-ben.

Nem bizonyítjuk, csak az $n=p$ prím esetet.

(Vegyük észre, hogy $\Phi_n(x)$ normált $\Rightarrow$ primitív $\Rightarrow$ $\mathbb{Z}[x]$-beli és $\mathbb{Q}[x]$-beli irreducibilitás ekvivalens)

<u>Igazoljuk:</u> $\Phi_p(x)$ irreducibilis $\mathbb{Z}[x]$-ben és $\mathbb{Q}[x]$-ben (p prím).

<u>Biz.</u> <u>Segéd-állítás:</u> $f(x) \in \mathbb{Z}[x]$, $g(x) = f(x+c) \in \mathbb{Z}[x]$, ahol $c \in \mathbb{Z}$ tetszőleges. (Vegyük észre: $\mathrm{gr}\, f = \mathrm{gr}\, g$.)

Ekkor: f irr. $\Leftrightarrow$ g irr.

<u>Biz</u> Elég az egyik irányt bizonyítani, mert

$$g(x) = f(x+c) \rightsquigarrow f(x) = g(x-c)$$

szintén behelyettesítéssel kapható.

T. fel: $f(x) = f_1(x) \cdot f_2(x)$ nem triviális faktorizáció

$$\rightsquigarrow f(x+c) = f_1(x+c) \cdot f_2(x+c)$$
$$\quad\;\; g(x) \;\;=\;\; g_1(x) \;\cdot\; g_2(x)$$

Ha tehát f nem irred. $\Rightarrow$ g sem irred. $\square$

(Viszont: másodfokú behelyettesítéssel már elronthatjuk az irreducibilitást:

$$f(x) = x; \qquad g(x) = f(x^2-1) = x^2-1 = (x-1)(x+1))$$

Tekintsük most, $\Phi_p(x) = \dfrac{x^p-1}{x-1} = x^{p-1} + \dots + x + 1$

A rekurzió képletben $d \mid p$, $d \neq p$ $\rightsquigarrow d = 1$.

Megmutatjuk, hogy a $\Psi(x)=\Phi_p(x+1)$ polinomra teljesülnek a Sch.-Eisenstein-krit. feltételei.

Ugyanis: $\Phi_p(x+1) = \dfrac{(x+1)^p-1}{(x+1)-1} = \dfrac{x^p+\binom{p}{1}x^{p-1}+\dots+\binom{p}{p-1}x+1-1}{x} =$

$$= x^{p-1}+\binom{p}{1}x^{p-2}+\dots+\binom{p}{p-1}$$

De itt $p \mid \binom{p}{i}$ $\quad \forall\, 1\le i\le p-1$-re,

és $p^2 \nmid \binom{p}{p-1}$, $\quad p^2 \nmid \underset{\substack{\uparrow \\ \text{főegyüttható}}}{1}$

$\Longrightarrow$ $\Psi(x)=\Phi_p(x+1)$ irreducibilis $\mathbb{Q}[x]$-ben (és $\mathbb{Z}[x]$-ben is a modultság miatt)

$\underset{\substack{\uparrow \\ \text{s.állítás}}}{\Longrightarrow}$ $\Phi_p(x)$ is irreducibilis $\mathbb{Q}[x]$-ben és $\mathbb{Z}[x]$-ben.

<ins>Megjegyzés</ins>: A fenti módszert nevezik <ins>„eltolt S-E-kritériumnak"</ins> is.