3. Egy- és többváltozós polinomok

3.1 Többváltozós polinomok

3.1.1 Definíció: legyen R egységelemes kommutatív gyűrű. Ekkor $R[x_1,x_2,\dots,x_n]$ az $x_1,x_2,\dots,x_n$ változók R feletti polinomjainak halmaza, azaz $\{\sum c_{a_1,a_2,\dots,a_n}\cdot x_1^{a_1}x_2^{a_2}\cdot\dots\cdot x_n^{a_n}\,|\,n\in\mathbb{N},a_i\in\mathbb{N},c_{(\dots)}\in R\setminus\{0\}\}$, ahol megköveteljük, hogy az összeg véges sok tagból álljon és különböző tagjaiban a kitevők legalább egy helyen különbözzenek. Egy tag foka legyen a benne szereplő kitevők $(a_1,\dots,a_n)$ összege, egy polinom foka pedig a benne szereplő tagok fokainak maximuma. Az azonosan 0 polinom fokát ismét nem, vagy $(-\infty)$-nek definiáljuk.

Ezek a „logikus" műveletekre egységelemes gyűrűt alkotnak, hiszen $R[x_1,x_2]$ tekinthető az x_2 változó $R[x_1]$ egységelemes gyűrű feletti polinomgyűrűjének, így maga is egységelemes gyűrű stb. $R[x_1,\dots,x_n]$ pontosan akkor kommutatív és/vagy nullosztómentes, ha R az.

3.1.2 Állítás: akárcsak az egyváltozós polinomoknál, **(1)** $deg(p\pm q)\le\mathbf{max}(deg\,p,deg\,q)$ és $deg\,p\neq deg\,q$ esetén egyenlőség áll fenn. Továbbá **(2)** $deg(pq)\le deg(p)+deg(q)$ és nullosztómentes gyűrűben egyenlőség áll fenn (az első triviális, a második kiszámolható – a nemsokára bevezetendő fogalmakkal látható, hogy p ill. q legmagasabb fokú tagjai közül a lexikografikusan legnagyobbak szorzata nem esik ki).

3.1.3 Definíció: $p\in R[x_1,\dots,x_n]$ homogén, ha minden tagja azonos fokú, pl. $x_1^2x_2+x_2^2x_3+x_3^2x_1$. Az n-változós homogén másodfokú polinomokat kvadratikus alaknak hívjuk.

Egy n változós k-adfokú p polinom mindig felírható $p=\sum_{k=0}^{deg\,p}p_k$ alakban, ahol p_k ugyanezen n változó homogén k-adfokú polinomja.

3.1.4 Definíció: egy n-változós polinom szimmetrikus, ha a változók bármilyen permutációja önmagába viszi át: $\forall\sigma\in S_n\colon p\circ\sigma=p$, azaz $p(x_{1\sigma},x_{2\sigma},\dots,x_{n\sigma})=p(x_1,x_2,\dots,x_n)$. Az n-változós szimmetrikus polinomok részgyűrűt alkotnak az n-változós polinomok között. n változó elemi szimmetrikus polinomjai: $\sigma_k=\sum_{1\le i(1)<\dots<i(k)\le n}(x_{i(1)}x_{i(2)}\dots x_{i(k)})$, ahol $1\le k<n$. Például $\sigma_1=x_1+x_2+\dots+x_n$, $\sigma_n=x_1x_2\dots x_n$.

3.1.5 Megjegyzés: legyenek a $p(x)=x^n+a_1x^{n-1}+\dots+a_{n-1}x+a_n$ polinom gyökei $\alpha_1,\dots,\alpha_n$. Ekkor a gyökök és együtthatók közötti összefüggés a $(-1)^ia_i=\sigma_i(\alpha_1,\dots,\alpha_n)$ alakba írható.

3.1.6 Definíció: $p(x_1,\dots,x_n)$ két tagja közül az legyen lexikografikusan nagyobb, amelyikben az első, a két tagban különböző kitevőn szereplő változó kitevője nagyobb (az együtthatótól tekintsünk el):

$$x_1^{a_1}x_2^{a_2}\dots x_n^{a_n}\succ x_1^{b_1}x_2^{b_2}\dots x_n^{b_n}\Leftrightarrow\exists k\in\{1\dots n\}\colon a_1=b_1,\dots,a_{k-1}=b_{k-1},a_k>b_k$$

$\succ$ antireflexív, antiszimmetrikus és tranzitív lesz, továbbá bármely két különböző elem összehasonlítható, azaz $\succ$ rendezés p tagjain. p vezető tagja alatt a lexikografikusan legnagyobbat értjük (ez értelmes, mert véges között lesz legnagyobb). Persze $R[x_1,\dots,x_n]$ két különböző polinomjának tagjait is összehasonlíthatjuk. Legyen $p\succ q$, ha p vezető tagja lexikografikusan nagyobb q vezető tagjánál. Így részbenrendezést kapunk $R[x_1,\dots,x_n]$ felett, melyet lexikografikus rendezésnek nevezünk.

3.1.7 Állítás: ha R nullosztómentes, akkor két $R[x_1\dots x_n]$-beli polinom szorzatának vezető tagja a két tényező vezető tagjának szorzata lesz. (Egyszerű számolás.)

3.1.8 Állítás: egy $p(x_1,\dots,x_n)$ szimmetrikus polinom $\xi=x_1^{a_1}x_2^{a_2}\dots x_n^{a_n}$ vezető tagjában $a_1\ge a_2\ge\dots\ge a_n$.

Bizonyítás: $\nexists\ i<k,a_i<a_k$, ekkor $\sigma=(ik)\in S_n$-re

$$\xi(\sigma(x_1\dots x_n))=x_{1\sigma}^{a_1}x_{2\sigma}^{a_2}\dots x_{n\sigma}^{a_n}=(x_1^{a_1}\dots x_{i-1}^{a_{i-1}})\cdot x_i^{a_k}\cdot\dots\cdot x_k^{a_i}\cdot\dots\succ(x_1^{a_1}\dots x_{i-1}^{a_{i-1}})\cdot x_i^{a_i}\cdot\dots=\xi(x_1\dots x_n)$$

Mivel p szimmetrikus, a $\xi\circ\sigma$ tag is szerepel benne, így ξ nem lehet vezető tag, $\lightning$.

Tekintsünk most egy $q(y_1,\dots,y_n)\in R[y_1,\dots,y_n]$ $q\in R[y_1,\dots,y_m]$ polinomot. Megtehetjük, hogy az y_i változó helyére rendre a $p_i\in R_\chi=R[x_1\dots x_n]$ polinomokat helyettesítjük be, hiszen $R\le R_\chi$ miatt $R[y_1,\dots,y_n]\le R_\chi[y_1,\dots,y_n]$, tehát q tekinthető R_χ feletti polinomnak is. Ekkor a $q(p_1,\dots,p_m)$ behelyettesítési érték egy R_χ-beli polinom lesz. Sőt,

definiálhatjuk az $R[p_1,\dots,p_m]\le R_\chi$ gyűrűt is, ez legyen $\{q(p_1,\dots,p_m)\,|\,q(y_1,\dots,y_n)\in R[y_1,\dots,y_n]\}$, tehát azon R_χ-beli polinomok halmaza, melyek előállnak a p_i-k polinomjaként. A következő tétel azt mondja, hogy $R[\sigma_1,\dots,\sigma_m]$ éppen az R_χ-beli szimmetrikus polinomok halmaza és minden szimmetrikus polinom egyértelműen áll elő $R[\sigma_1,\dots,\sigma_m]$ elemeként.

3.1.9 Szimmetrikus polinomok alaptétele: **(1)** $\forall q(y_1,\dots,y_n)\in R[y_1,\dots,y_n]$-re $p(x_1\dots x_n)=q(\sigma_1\dots\sigma_n)$ szimmetrikus polinomja $x_1\dots x_n$-nek, továbbá **(2)** minden $p\in R[x_1\dots x_n]$ szimmetrikus polinom előáll ilyen alakban és az előállítás egyértelmű.

Bizonyítás: **(1)** nyilvánvaló.

(2): Legyen $p\in R[x_1\dots x_n]$ szimmetrikus, $\chi=\{x_1,\dots,x_n\}$, $S=\{\sigma_1,\dots,\sigma_n\}$. Vegyük az összes lehetséges $\xi(\chi)=\prod_{i=1}^n x_i^{a_{\xi,i}}$ tagot, amelynek foka legfeljebb $\deg p$. Állítsuk őket lexikografikus sorrendbe és indexeljük meg őket ezen sorrend szerint. (A legkisebb tag indexe legyen 1. Az indexelés megoldható, mert csak véges sok ilyen tag van.) Ezután nevezzük $(x_1,\dots,x_n)$ tetszőleges, p-nél nem magasabb fokú r polinomja indexének a legnagyobb indexű tagjának indexét. Az azonosan nulla polinom indexe legyen 0.

Legyen q vezető tagja $c_0\cdot x_1^{a_1}x_2^{a_2}\dots x_n^{a_n}$. Legyen ekkor $\delta_0=\sigma_1^{a_1-a_2}\cdot\sigma_2^{a_2-a_3}\cdot\dots\cdot\sigma_n^{a_n}$. Ennek a legnagyobb indexű tagja azonos p vezető tagjával és $\deg\delta_0\le\deg p$, azaz $q_1=p-c_0\cdot\delta_0$ indexét definiáltuk és ez alacsonyabb p indexénél, mert a vezető tag kiesik. Vegyük p_1-hez hasonló módon δ_1-et stb. Mivel az index mindig csökken, idővel $p_k-c_k\delta_k=0$ lesz. Ekkor $q=\sum_{i=0}^k c_i\delta_i$ éppen a keresett felírás.

Most már csak azt kell belátnunk, hogy ez a felírás egyértelmű. Ez ekvivalens azzal, hogy az azonosan 0 polinom csak triviálisan áll elő $q(S)$ alakban. Legyen $q\ne0$ és lássuk be, hogy $q(\sigma_1,\dots,\sigma_n)\ne0$.

Egy $\zeta=c\cdot\sigma_1^{\alpha_1}\cdot\sigma_2^{\alpha_2}\cdot\dots\cdot\sigma_n^{\alpha_n}$ szorzat vezető tagjában x_k kitevője $\sum_{i=0}^k\alpha_i$. Eszerint $q(S)$ két különböző tagjának vezető tagja (χ polinomjaként tekintve) lexikografikusan összehasonlítható, mert valamely x_k kitevőjében különböznek. $q(S)$-nek legalább egy tagja van, így van lexikografikusan legnagyobb vezető taggal rendelkező $\zeta^*=c^*\cdot\sigma_1^{\alpha_1^*}\cdot\sigma_2^{\alpha_2^*}\cdot\dots\cdot\sigma_n^{\alpha_n^*}$ tagja. Ennek vezető tagját $q(S)$ többi tagja nem ejtheti ki, így $q(S)\ne0$.

3.1.10 Definíció: egy n-változós p polinom (permutáció)csoportja S_n azon részhalmaza, amelyre $p\circ\sigma=p$. (Ez valóban csoport.) Például $\prod_{i\le j}(x_j-x_i)$ csoportja A_n (épp ezzel definiáltuk A_n-t).

3.1.11 Definíció: n változó k-adik hatványösszege $s_k(x_1\dots x_n)=\sum_{i=1}^n x_i^k$.

3.1.12 Tétel (Newton–Waring formulák): ha $1\le k\le n$, akkor $s_k-s_{k-1}\sigma_1+s_{k-2}\sigma_2-\dots+(-1)^{k-1}s_1\sigma_{k-1}+(-1)^k\cdot k\cdot\sigma_k=0$, ha pedig $k>n$, akkor $s_k-s_{k-1}\sigma_1+s_{k-2}\sigma_2-\dots+(-1)^{n-1}s_{k-n+1}\sigma_{n-1}(-1)^n s_{k-n}\sigma_n=0$.

Ezt $k<n$-re be is látjuk.

Bizonyítás: tekintsük $p(x)=(x-x_1)(x-x_2)\dots(x-x_n)=\sum_{i=0}^n(-1)^i\sigma_i\cdot x^{n-i}$-t mint az x változó $R[x_1,\dots,x_n]$ feletti polinomját és legyen $a_i=(-1)^i\sigma_i$. Ennek a deriváltja egyrészt $\sum_{i=1}^n(n-i)\cdot a_i x^{n-i-1}$, másrészt a szorzat deriváltjának képlete szerint $\sum_{m=1}^n\left[(x-x_m)'\cdot\prod_{i\ne j}(x-x_i)\right]=\sum_{m=1}^n\frac{p(x)}{x-x_m}$. Beszorzással ellenőrizhető, hogy

$$(x-x_m)\left[x^{n-1}+x^{n-2}(a_1+x_m)+\dots+x\cdot(a_{n-1}+a_{n-2}x_m+\dots+a_1x_m^{n-2})+(a_n+a_{n-1}x_m+\dots+a_1x_m^{n-1})\right]=p(x)-p(x_m).$$

Mivel $p(x_m)$ $R[x_1,\dots,x_n]$ nulleleme (az azonosan nulla polinom), a fenti szorzat éppen $p(x)$, így a zárójelben $\frac{p(x)}{x-x_m}$ van. A derivált két alakja ugyanazt a polinomot adja, azaz minden $1\le k<(n-1)$-re x^{n-k-1} együtthatója ugyanaz bennük:

$$0=\left(\sum_{m=1}^n(a_{k-1}x_m+\dots+a_1x_m^{k-1}+x_m^k)\right)-(n-k)\cdot a_k=k\cdot a_k+\left(\sum_{i=1}^{k-1}a_{k-i}s_i\right)+s_k=s_k-s_{k-1}\sigma_1+s_{k-2}\sigma_2-\dots+(-1)^{k-1}\cdot s_1\sigma_{k-1}+(-1)^k\cdot k\cdot\sigma_k.$$

Ezt akartuk belátni.

3.2 Diszkrimináns, rezultáns

3.2.1 Definíció: vegyük egy $p\in K[x]$ polinomra $\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2$-t. Ez a gyökök homogén szimmetrikus polinomja és pontosan akkor 0, ha van többszörös gyök. Mivel nem nulla skalárral való szorzás ezen a tulajdonságon nem változtat, ugyanez igaz $a_0^{2n-2}\cdot\prod(\alpha_i-\alpha_j)^2$-re is. Ezt p diszkriminánsának hívjuk és $D(p)$-vel jelöljük.

3.2.2 Definíció: $p(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ és $q(x)=b_0x^k+b_1x^{k-1}+\ldots+b_{k-1}x+b_k$ K feletti polinomok rezultánsa legyen $R(p,q)=a_0^k\cdot q(\alpha_1)\cdot q(\alpha_1)\cdot\ldots\cdot q(\alpha_n)$. Ez pontosan akkor lesz 0, ha a két polinomnak van közös gyöke. A rezultáns képletébe beírva $q(x)=b_0\cdot\prod_{j=1}^k(x-\beta_j)$-t azt kapjuk, hogy $R(p,q)=a_0^kb_0^n\cdot\prod_{i=1}^n\prod_{j=1}^k(\alpha_i-\beta_j)$. Erről az alakról az is könnyen leolvasható, hogy $R(p,q)=(-1)^{nk}\cdot R(q,p)$.

3.2.3 Állítás: $R(p,q)$ annak az $\mathbf{A}\in M_{n+k}(K)$ mátrixnak a determinánsa, melynek első, második … k-adik sorában $(a_0,a_1,\ldots,a_{n-1},a_n)$ van 0-val, 1-el … $(k-1)$-el eltolva, a maradék n sorban pedig $(b_0,b_1,\ldots,b_{k-1},b_k)$ van 0-val, 1-el … $(n-1)$-el eltolva. A mátrix többi eleme 0 (Sylvester-féle alak).

Bizonyítás: n szerinti teljes indukcióval. Ha $n=0$, akkor $\mathbf{A}$ egy $k\times k$-as mátrix, amelynek átlójában a_0 van, mindenütt másutt 0, azaz $\det(\mathbf{A})=a_0^k=R(p,q)$, hiszen a rezultáns ekkor egy üres szorzat a_0^k-szorosa, az üres szorzat pedig definíció szerint 1.

Tegyük fel, hogy az állítás minden alacsonyabb fokú p^* esetén teljesül és lássuk be, hogy ekkor p-re is teljesül. Legyen $p^*=a_0\cdot\prod_{i=1}^{n-1}(x-\alpha_i)=a_0\cdot\sum_{i=1}^{n-1}a_i^*x^{n-1-i}$.

Ekkor $R(p,q)=a_0^k\cdot\prod_{i=1}^n q(\alpha_i)=q(\alpha_n)\cdot a_0^k\cdot\prod_{i=1}^{n-1}q(\alpha_i)=R(p^*,q)\cdot q(\alpha_n)$. Jelöljük α_n-t α-val. Tekintsük most az $\mathbf{A}$ mátrixot. Mivel $p(x)=p^*(x)\cdot(x-\alpha)$, ennek első k sora a következő lesz:

$$\begin{pmatrix} a_0^* & a_1^*-a_0^*\alpha & a_2^*-a_1^*\alpha & \ldots & a_{n-1}^*-a_{n-2}^*\alpha & -a_{n-1}^*\alpha & 0 & \ldots & 0 & 0\\ 0 & a_0^* & a_1^*-a_0^*\alpha & a_2^*-a_1^*\alpha & \ldots & a_{n-1}^*-a_{n-2}^*\alpha & -a_{n-1}^*\alpha & 0 & \ddots & 0\\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots\\ 0 & \ddots & 0 & a_0^* & a_1^*-a_0^*\alpha & a_2^*-a_1^*\alpha & \ldots & a_{n-1}^*-a_{n-2}^*\alpha & -a_{n-1}^*\alpha & 0\\ 0 & 0 & \ldots & 0 & a_0^* & a_1^*-a_0^*\alpha & a_2^*-a_1^*\alpha & \ldots & a_{n-1}^*-a_{n-2}^*\alpha & -a_{n-1}^*\alpha \end{pmatrix}$$

Adjuk hozzá az első oszlop α-szorosát a másodikhoz, majd a második oszlop α-szorosát a harmadikhoz stb., végül az utolsó előtti oszlop α-szorosát az utolsóhoz. Az első k sor így azonos lesz annak a mátrixnak az első k sorával, amelyet p^*-ból kaptunk, csak van még a végén egy 0 oszlop. Az alsó n sor viszont kissé „elromlott”:

$$\begin{pmatrix} b_0 & b_0\alpha+b_1 & b_0\alpha^2+b_1\alpha+b_2 & \ldots & b_0\alpha^{k-1}+b_1\alpha^{k-2}+\ldots+b_{k-1} & q(\alpha) & \alpha\cdot q(\alpha) & \ldots & \alpha^{n-2}\cdot g(\alpha) & \alpha^{n-1}\cdot q(\alpha)\\ 0 & b_0 & b_0\alpha+b_1 & b_0\alpha^2+b_1\alpha+b_2 & \ldots & b_0\alpha^{k-1}+\ldots+b_{k-1} & q(\alpha) & \ddots & \ddots & \alpha^{n-2}\cdot q(\alpha)\\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots\\ 0 & \ddots & 0 & b_0 & b_0\alpha+b_1 & b_0\alpha^2+b_1\alpha+b_2 & \ldots & b_0\alpha^{k-1}+\ldots+b_{k-1} & q(\alpha) & \alpha\cdot q(\alpha)\\ 0 & 0 & \ldots & 0 & b_0 & b_0\alpha+b_1 & b_0\alpha^2+b_1\alpha+b_2 & \ldots & b_0\alpha^{k-1}+\ldots+b_{k-1} & q(\alpha) \end{pmatrix}$$

Vonjuk le a második (az eredeti mátrixban $(k+2)$-dik) sor α-szorosát az első sorból, majd a harmadik α-szorosát a másodikból stb., végül az utolsó sor α-szorosát az előzőből. Így ez a rész is majdnem ugyanaz lesz, mint $R(p^*,q)$ determinánsának megfelelő része, csak minden sor végére jött egy 0 és lett még egy sor, aminek a végén $q(\alpha)$ van. Az utolsó oszlopban csak ez az elem nem 0. Ezen oszlop szerint kifejtve $\det(\mathbf{A})$-t és felhasználva, hogy a fellépő aldeterminánsz az indukciós feltevés szerint $R(p^*,q)$:

$$\det(\mathbf{A})=a_{n+k,n+k}\cdot\det(\mathbf{A}_{n+k,n+k})=q(\alpha)\cdot R(p^*,q)=R(p,q).$$

Ezzel az állítást beláttuk.

3.2.4 Állítás: $R(p,p')=a_0\cdot D(p)\cdot(-1)^{\frac{1}{2}n(n-1)}$.

Bizonyítás: $p'(x)=a_0\cdot\sum_{k=1}^n\prod_{i\neq k}(x-\alpha_i)$. $x=\alpha_k$ esetén ennek az összegnek csak a k-adik tagja nem nulla, így $p'(\alpha_k)=a_0\cdot\prod_{i\neq k}(\alpha_k-\alpha_i)$. Ez alapján

$$R(p,p')=a_0^{n-1}\cdot\prod_{k=1}^n p'(\alpha_k)=a_0^{n-1}\cdot\prod_{k=1}^n\left(a_0\cdot\prod_{i\neq k}(\alpha_k-\alpha_i)\right)=a_0^{2n-1}\cdot(-1)^{\frac{1}{2}n(n-1)}\cdot\prod_{i<j}(\alpha_i-\alpha_j)^2,$$

kész vagyunk. Az előző állítás segítségével a diszkriminánst is megkaphatjuk determináns alakban:

$$D(p)=\frac{(-1)^{\frac{1}{2}n(n-1)}}{a_0}\cdot R(p,p')=(-1)^{\frac{1}{2}n(n-1)}\cdot\det\begin{pmatrix} 1 & a_1 & \cdots & a_{n-1} & a_n & 0 & \cdots & 0 & 0\\ 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n & 0 & \ddots & 0\\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots\\ 0 & \ldots & 0 & a_0 & a_1 & \ldots & a_{n-1} & a_n & 0\\ 0 & 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n\\ n & (n-1)a_1 & \cdots & 2a_{n-2} & a_{n-1} & 0 & 0 & \cdots & 0\\ 0 & na_0 & (n-1)a_1 & \cdots & 2a_{n-2} & a_{n-1} & 0 & \ddots & 0\\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots\\ 0 & \ddots & 0 & na_0 & (n-1)a_1 & \ldots & 2a_{n-2} & a_{n-1} & 0\\ 0 & 0 & \ldots & 0 & na_0 & (n-1)a_1 & \ldots & 2a_{n-2} & a_{n-1} \end{pmatrix}\begin{matrix}\\\\\\\\\\\} n-1 \text{ sor}\\\\\\\\\\\} n \text{ sor}\end{matrix}$$

A rezultánst igen jól lehet használni magasabb fokú egyenletrendszerek megoldására. Legyen az egyenletrendszerünk $p(x,y)=0, q(x,y)=0$, ahol ezek $K[x,y]$-beli polinomok. Tekintsük most a két polinomot mint x polinomjait $K[y]$ felett. Legyen ezen két polinom rezultánsa $r(y)\in K[y]$. Azon $y=\beta$ értékek mellett van megoldás, melyeknél p_y-nak és q_y-nak mint x polinomjának lesz közös gyöke. Ez majdnem ekvivalens azzal, hogy $r(\beta)=0$. Azért nem egészen, mert ha mind $p_y(x)$, mind $q_y(x)$ főegyüttható-polinomjának gyöke α, akkor a rezultáns első oszlopában csupa 0 lesz, így a determináns mindenképp 0 és semmit nem mond a közös gyök létezéséről. Ha legalább az egyiknek nem gyöke, akkor már ekvivalens a két feltétel, azaz elég megkeresnünk $r(y)$ gyökeit és azokra megkeresni a megfelelő x értékeket (persze egyhez lehet több is, de mindhez lesz legalább egy). Így a feladatot visszavezettük egy egyváltozós polinom gyökeinek megkeresésére.

3.3 Komplex test feletti polinomok gyökeinek megkeresése

3.3.1 Elsőfokú polinom megoldása: $ax+b=0\ (a\neq 0)$. Megoldása $x=-\frac{b}{a}$.

3.3.2 Másodfokú polinom megoldása: $ax^2+bx+c=0\ (a\neq 0)$.

Osszunk le a főegyütthatóval (ezt a jövőben automatikusan megtesszük): $x^2+px+q=0$. Ezután bontsuk egy elsőfokú polinom négyzete és egy komplex szám összegére: $(x+\frac{p}{2})^2+q-(\frac{p}{2})^2=0 \Leftrightarrow (x+\frac{p}{2})^2=(\frac{p}{2})^2-q$. Tudjuk, hogy egy z komplex számnak pontosan két négyzetgyöke van, melyeket $\pm\sqrt{z}$-vel jelölünk (a nullának csak egy van, de ez lényegtelen). Eszerint a megoldáshalmaz a következő: $\{-\frac{p}{2}-\sqrt{(\frac{p}{2})^2-q}, -\frac{p}{2}+\sqrt{(\frac{p}{2})^2-q}\}$, az eredeti együtthatókkal $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$.

3.3.3 Harmadfokú polinom megoldása: $x^3+ax^2+bx+c=(x+\frac{a}{3})^3+\left(b-\frac{a^2}{3}\right)(x+\frac{a}{3})+\left(c-\frac{ab}{3}+\frac{2a^3}{27}\right)$. Ezen átalakításból látszik, hogy elég az $x^3+px+q=0$ alakú egyenleteket megoldanunk.

Keressük a megoldásokat $u+v$ alakban. Tudjuk, hogy $(u+v)^3=u^3+v^3+3uv(u+v)$, azaz $(u+v)^3-3uv(u+v)-(u^3+v^3)=0$. Ebben az a jó, hogy ha találunk egy u,v párost, amire $p=-3uv$ és $q=-(u^3+v^3)$, akkor azok jó megoldást adnak. Ha valamely u,v párosra ez fennáll, akkor ezekre $u^3v^3=-(\frac{p}{3})^3$. Ebből és a másik feltételből következik, hogy u^3, v^3 a $z^2+qz-(\frac{p}{3})^3=0$ egyenlet gyökei, azaz $-\frac{q}{2}\pm\sqrt{(\frac{q}{2})^2+(\frac{p}{3})^3}$. Eszerint

$$u=\sqrt[3]{-\tfrac{q}{2}+\sqrt{(\tfrac{q}{2})^2+(\tfrac{p}{3})^3}}\ ;\ v=\sqrt[3]{-\tfrac{q}{2}-\sqrt{(\tfrac{q}{2})^2+(\tfrac{p}{3})^3}}$$

A köbgyöknek 3 értéke lehet, ez tehát összesen 9 megoldást adna, de ezek csak a gyengébb $u^3v^3=-(\frac{p}{3})^3$ feltételt elégítik ki. Az erősebb $p=-3uv$ feltételhez minden egyes u értékhez pontosan egy megfelelő v érték tartozik. Válasszunk ki egy teljesen jó u,v párost. Ekkor a megoldások: $x_1=u+v$; $x_2=\varepsilon_3\cdot u+\varepsilon_3^2\cdot v=-\frac{1}{2}(u+v)+\frac{i\cdot\sqrt{3}}{2}(u-v)$; $x_3=\varepsilon_3^2\cdot u+\varepsilon_3\cdot v=-\frac{1}{2}(u+v)-\frac{i\cdot\sqrt{3}}{2}(u-v)$. Mivel találtunk három gyököt, megtaláltuk az összeset. Ha esetleg több megoldás egybeesik, akkor is, mert pont jó multiplicitással fognak szerepelni, de ezt most nem bizonyítjuk.

Sajnos van egy apró probléma a fenti képlettel. Ha ugyanis egy olyan harmadfokú polinom gyökeit számoljuk ki vele, amelynek három valós gyöke van, akkor azokat a gyököket felettébb visszataszító alakban, komplex számok köbgyökeinek összegeként kapjuk meg. Vizsgáljunk most meg közelebbről egy valós együtthatós x^2+px+q polinomot. Legyen $d=(\frac{q}{2})^2+(\frac{p}{3})^3$. Ha $d>0$, akkor a különböző gyökvonások jól definiáltak a valós számok felett, így nyugodtan írhatunk $u=\sqrt[3]{-\frac{q}{2}+\sqrt{d}}$; $v=\sqrt[3]{-\frac{q}{2}-\sqrt{d}}$-t és a gyökök $x_1=u+v\in\mathbb{R}$; $x_{2,3}=-\frac{1}{2}(u+v)\pm\frac{i\cdot\sqrt{3}}{2}(u-v)\notin\mathbb{R}$ mert $u\neq v \Rightarrow (u-v)\neq 0$. Ha $d=0$, akkor $u=v \Rightarrow x_2=x_3=-\frac{1}{2}(u+v)\in\mathbb{R}$, azaz a két valós gyök egyike kétszeres gyök. (Mellesleg az egyszeres gyök $-\sqrt[3]{4q}$, a másik $-\sqrt[3]{\frac{q}{2}}$. Ha q és d is 0, azaz p is 0, akkor a 0 háromszoros gyök. Ha $d<0$, akkor

$$u^3=-\tfrac{q}{2}+i\cdot\sqrt{-(\tfrac{q}{2})^2-(\tfrac{p}{3})^3} \Rightarrow \left|u^3\right|=\sqrt{\mathbf{Re}^2(u^3)+\mathbf{Im}^2(u^3)}=\sqrt{(\tfrac{q}{2})^2-(\tfrac{q}{2})^2-(\tfrac{p}{3})^3} \Rightarrow r=\left|u\right|=\sqrt{-\tfrac{p}{3}}$$

Mivel $uv=-\frac{p}{3}$, u és v egymás konjugáltjai. Ha $u=a+bi$, akkor a gyökök $x_1=2a$ és $x_{2,3}=-a\pm b\sqrt{3}$. Ha u trigonometrikus alakja $r\cdot(\cos\varphi+i\cdot\sin\varphi)$, akkor a gyökök $x_1=2r\cdot\cos\varphi$, $x_{2,3}=2r\cdot(\cos\varphi\pm 120^\circ)$ alakba írhatóak.

3.3.4 Negyedfokú polinom megoldása: $x^4+px^2+qx+r=0$.

A megoldásokat $x=u+v+w$ alakban keressük. Felhasználva, hogy $[(u+v+w)^2-(u^2+v^2+w^2)]^2=4(uv+vw+wu)^2$, az alábbi egyenlőséghez jutunk:

$$(u+v+w)^4-(u+v+w)^2\cdot 2(u^2+v^2+w^2)+(u^2+v^2+w^2)^2=4(u^2v^2+v^2w^2+w^2u^2)+8uvw(u+v+w)$$
$$x^4-2\sigma_1(u^2,v^2,w^2)\cdot x^2+\sigma_1^2=4\sigma_2+8uvw\cdot x$$
$$x^4-2\sigma_1\cdot x^2-8uvw\cdot x+\sigma_1^2-4\sigma_2=0$$

Elég tehát találnunk olyan u,v,w számokat, melyekre $\sigma_1(u^2,v^2,w^2)=-\frac{p}{2}$, $\sigma_2=\frac{p^2-4r}{16}$, $uvw=-\frac{q}{8}$. A legutolsó feltételt gyengítve azt kapjuk, hogy $\sigma_3=u^2v^2w^2=\frac{q^2}{64}$. Így pont akkor teljesülnek a feltételek, ha u^2,v^2,w^2 a

$$z^3+z^2\cdot\frac{p}{2}+z\cdot\frac{p^2-4r}{16}-\frac{q^2}{64}=0$$

egyenlet – a harmadfokú rezolvens – három gyöke. Az így kapott értékek mindegyikének két-két négyzetgyöke lesz, azaz összesen 8 megoldáshármast kapunk, melyeknek azonban a fele hamis gyök, mert az egyik felében $uvw=\frac{q}{8}$ lesz $-\frac{q}{8}$ helyett. Ha a rezolvens gyökeit z_1,z_2,z_3-al jelölve $\sqrt{z_1},\sqrt{z_2},\sqrt{z_3}$ jó megoldást adnak, akkor a megoldások: $x_1=\sqrt{z_1}+\sqrt{z_2}+\sqrt{z_3}$, $x_2=\sqrt{z_1}-\sqrt{z_2}-\sqrt{z_3}$, $x_3=-\sqrt{z_1}+\sqrt{z_2}-\sqrt{z_3}$, $x_4=-\sqrt{z_1}-\sqrt{z_2}+\sqrt{z_3}$.

3.4 Valós együtthatós polinomok gyökei

Legyen $p(x)=x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n\in\mathbb{R}[x]$.

3.4.1 Állítás: ha $|x|>\sum_{i=1}^n|a_i|$ és $|x|\geq 1$, akkor x nem gyöke p-nek.

Bizonyítás: $\nexists$ egy ilyen x mégis gyök. Ekkor $|x^n|=|p(x)-x^n|=|\sum_{i=1}^n a_i\cdot x^{n-i}|\leq\sum_{i=1}^n|a_i|\cdot|x^{n-i}|\leq\sum_{i=1}^n|a_i|\cdot|x^{n-1}|$. Az x-re tett feltevés szerint ez kisebb, mint $|x|\cdot|x^{n-1}|=|x^n|$, összefoglalva $|x^n|<|x^n|$ $\lightning$. Ez a becslés komplex együtthatós polinom komplex gyökeire is fennáll.

3.4.2 Állítás: ha egy valós x-re $x\geq 1+\sqrt[r]{|a_k|}$ $x\geq 1+\sqrt[r]{|a_k|}$, akkor $p(x)>0$, ahol r az első negatív együttható indexe, a_k pedig a legnagyobb abszolútértékű negatív együttható.

Bizonyítás: tegyük fel, hogy $x\geq 1+\sqrt[r]{|a_k|}$. Ekkor $x^{r-1}(x-1)>(x-1)^r\geq|a_k|\Rightarrow x^n(x-1)>|a_k|\cdot x^{n-r+1}$. Eszerint $x^n>|a_k|\cdot\frac{x^{n-r+1}-1}{x-1}=\sum_{i=r}^n(-a_k)\cdot x^{n-i}\geq-(\sum_{i=r}^n a_ix^{n-i})$, így

$$p(x)=x^n+\sum_{i=1}^n a_ix^{n-i}\geq x^n-(-\sum_{i=r}^n a_ix^{n-i})>0.$$

Ekkor x nem lehet gyöke p-nek.

3.4.3 Lemma: legyen x_0 a p valós együtthatós polinom r-szeres gyöke ($r\geq 1$). Ekkor van olyan kis h pozitív valós szám, amelyre $p(x)$ és $p'(x)$ előjele az (x_0-h,x_0) illetve (x_0,x_0+h) nyílt intervallumokon állandó és a két előjel a második intervallumon azonos, az elsőn nem. (Azaz x_0 előtt $p(x)$ és $p'(x)$ előjele különböző, utána azonos.)

Bizonyítás: a derivált definíciójából kiszámolható, hogy $p(x+d)=p(x)+p'(x)\cdot d+\frac{1}{2}p''(x)\cdot d^2+\ldots+\frac{1}{n!}p^{(n)}(x)\cdot d^n$. Mivel x_0 r-szeres gyök, $p(x_0+d)$-t így felírva mint d polinomját, az első r együttható ($d^0,d^1,\ldots,d^{r-1}$ együtthatói) 0 lesz, a következő: $s_r=\frac{1}{r!}p^{(r)}(x_0)$ viszont nem. Azaz $p(x_0+d)=\sum_{i=r}^n\frac{1}{i!}p^{(i)}(x_0)\cdot d^i$ és hasonlóan $p'(x_0+d)=\sum_{i=r}^n\frac{1}{(i-1)!}p^{(i)}(x_0)\cdot d^{i-1}$. Ha d abszolútértéke elég kicsi, akkor ezen összegek előjelét az első tag előjele dönti el, mert a többi tag elhanyagolható lesz hozzá képest. Tehát valamely kis pozitív h-ra $0<|d|<h$ esetén $p(x_0+d)$ ill. $p'(x_0+d)$ előjele azonos $s_r\cdot d^r$ ill. $s_r\cdot d^{r-1}$ előjelével, tehát x_0 előtt ($d<0$) valóban különbözőek, utána ($d>0$) pedig azonosak.

3.4.4 Definíció: egy $p(x)\in\mathbb{R}[x]$ polinom Sturm-lánca az alábbi, polinomokból álló sorozat: $p_0=p,p_1=p'$, a további elemeket maradékos osztással kapjuk meg: $p_k(x)=q_k(x)\cdot p_{k+1}(x)-p_{k+2}(x)$ mindaddig, amíg van maradék. Ha $p_{m+1}(x)$ az azonosan 0 polinom lenne, akkor a láncot p_m-nél befejezzük. A polinomokat gyakran olyan pozitív konstanssal megszorozva adjuk meg, hogy a főegyütthatója ± 1 legyen. (A Sturm-lánc polinomjainak igazán csak a különböző behelyettesítési értékekhez tartozó előjelei számítanak, így ez megengedhető.) Mivel ez majdnem az euklideszi algoritmus polinomjait adja, két szomszédos p_k közös gyökei mindnek gyökei, speciálisan p-nek és p'-nek is, azaz többszörös gyöke p-nek.

3.4.5 Definíció: egy rögzített $p(x)\in\mathbb{R}[x]$ polinomra és x_0 valós számra – ami nem gyöke p-nek – $\omega(x_0)$ legyen az előjelváltások száma az $p_0(x_0),p_1(x_0),\ldots,p_m(x_0)$ sorozatban. Ez jól definiált érték lesz. (A két szélső érték nem lesz 0, mert x_0 nem volt gyöke p-nek, azaz nem gyöke p_m-nek sem, ami p és p' legnagyobb közös osztója. A közbülső nullák nem zavarnak minket: pl. $(1,0,-1)$ egy, $(1,0,0,1)$ nulla előjelváltást ér.)

3.4.6 Definíció: egy polinom értéke a végtelenben a következő: páros fokúra mindkét végtelenben a főegyütthatóval egyező előjelű végtelen, páratlan fokúra plusz végtelenben ugyanez, mínusz végtelenben az

ellentettje. A konstans polinomok persze a végtelenben is a konstanst vegyék fel. (Ez így együtt aránylag logikus definíció.) Ez alapján tudjuk értelmezhető $\omega(\pm\infty)$ is.

3.4.7 Sturm-tétel: egy $p(x)\in\mathbb{R}[x]$ polinomra és $(a,b)\in\mathbb{R}\cup\{-\infty,+\infty\}; a<b$ számokra – melyek nem gyökei – a valós gyökök száma (multiplicitás nélkül) az $[a,b]$ zárt intervallumon $\omega(a)-\omega(b)$.

Bizonyítás: az előjelváltások száma csak olyan pontnál változhat, ahol valamelyik p_k előjele változik, ez pedig csak p_k gyökeinél történhet meg. (Ez némi magyarázatra szorul. Legyenek egy p valós együtthatós polinom valós gyökei $r_1,r_2,\dots,r_k$, komplex gyökei – melyek, mint tudjuk, konjugált párokból állnak – $z_1,\bar{z}_1,\dots,z_m,\bar{z}_m$. Ekkor $p(x)=a_0\cdot\prod(x-r_i)\cdot\prod[(x-z_i)(x-\bar{z}_i)]=a_0\cdot\prod(x-r_i)\cdot\prod[(x-\mathbf{Re}\,z_i)^2+\mathbf{Im}^2 z_i]$. A második szorzat minden valós x-re pozitív, azaz p előjelét az első szorzat és a_0 előjele határozza meg, tehát a polinom behelyettesítési értékének előjele valóban csak a gyököknél változhat.)

Vizsgáljuk meg először azokat az α értékeket, melyek valamely p_k-nak gyökei, de p-nek legfeljebb egyszeres gyökei. A Sturm-lánc definíciójánál mondottak miatt α-ban sem p_{k-1}, sem p_{k+1} nem lesz 0, azaz kicsivel előtte ill. utána sem. $p_{k-1}(\alpha)=q_{k-1}(\alpha)p_k(\alpha)-p_{k+1}(\alpha)=0-p_{k+1}(\alpha)$ miatt ezek előjele α közelében különböző. Azaz bármi legyen is $p_k(x)$ előjele α környezetében, $p_{k-1}(x),p_k(x),p_{k+1}(x)$ között pontosan egy előjelváltás van $\Rightarrow$ az előjelváltások száma ezen elemek között nem változik α-ban. Az sem zavar minket, ha α esetleg több p_k-nak is gyöke, mert ezek nem lehetnek szomszédosak, azaz az előjelek megváltozásai nem zavarják egymást. Két olyan polinom között, melyeknek α nem gyöke, nem történik semmi.

Ha α egyszeres gyöke p-nek, akkor – mint nemrég beláttuk – α-nál egy előjelváltás „elvész" p és p' között. Marad még az az eset, amikor α r-szeres ($r\geq 2$) gyöke p-nek. Ekkor minden p_k-nak legalább $(r-1)$-szeres gyöke. Legyen $p_i(x)=(x-\alpha)^{r-1}\cdot q_i(x)$. Azt állítjuk, hogy a $q_1(x),\dots,q_m(x)$ sorozat előjelváltásainak száma nem változik α-ban. Ez azért igaz, mert α q_0-nak egyszeres gyöke, q_1-nek nem gyöke és a további elemeket úgy kapjuk q_0,q_1-ből, mint egy Sturm-lánc elemeit. A q_1 és q_m közötti előjelváltásokra tehát ugyanazt elmondhatjuk, amit arra az esetre elmondtunk, amikor α egyszeres gyöke volt p-nek. Ha $(r-1)$ páratlan, akkor $p_i(x)=(x-\alpha)^{r-1}\cdot q_i(x)$-ben α előtt $p_1(x),\dots,p_m(x)$ előjele a megfelelő q-sorozat előjeleinek ellentettje, páratlan $(r-1)$-re α után vagy páros $(r-1)$-re α közelében a két sorozat előjelei megegyeznek. Az előjelváltások száma α közelében tehát ugyanaz az $p_1(x),\dots,p_m(x)$ és a $q_1(x),\dots,q_m(x)$ sorozatban, azaz nem változik α-ban. p_0 és p_1 között többszörös gyöknél is elvész egy előjelváltás.

Összefoglalva: p gyökeinél az előjelváltások száma eggyel csökken, máshol nem változik. Ezzel az állítást beláttuk.

3.4.8 Állítás: ha $f(x)=\sum_{k=0}^{n}a_k x^{n-k}\in\mathbb{Z}[x]$ és valamely p,q relatív prímekre $f(\frac{p}{q})=0$, akkor $q\,|\,a_0$ és $p\,|\,a_n$.

Bizonyítás: a feltételek szerint $a_0p^n+a_1p^{n-1}q+\dots+a_{n-1}pq^{n-1}+a_nq^n=0$ osztható p-vel és q-val is. Az első tagon kívül minden tag osztható q-val, tehát az első tag is osztható q-val, azaz $q\,|\,a_0p^n$. Ha p és q relatív prímek, akkor ebből következik, hogy $q\,|\,a_0$. Az állítás másik fele ugyanígy jön ki.

3.4.9 Következmény: egy 1 főegyütthatójú egész együtthatós polinom minden racionális gyöke egész.

3.4.10 Definíció: $\alpha\in\mathbb{C}$ algebrai, ha van olyan egész együtthatós polinom, aminek gyöke. Az algebrai számok testet alkotnak, amelyet $\mathbb{A}$-val jelölünk. Ennek megszámlálható sok eleme van, mert csak megszámlálható sok egész együtthatós polinom van. α algebrai egész akkor, ha van olyan egy főegyütthatós egész együtthatós polinom, aminek gyöke. Az algebrai egészek halmaza Ω. A nem algebrai számokat transzcendensnek hívjuk.

3.4.11 Definíció: az $f(x)\in\mathbb{Z}[x]$ polinom primitív, ha összes együtthatójának legnagyobb közös osztója 1.

3.4.12 Állítás: két primitív polinom – $f(x)=\sum_{k=0}^{n}a_k x^{n-k}$ és $g(x)=\sum_{l=0}^{m}b_l x^{m-l}$ – szorzata is primitív.

Bizonyítás: $\nexists$ valamely p prím a szorzat – $h(x)=\sum_{i=0}^{n+m}c_i x^{n+m-i}$ – minden együtthatóját osztja, de g-nek és h-nak is van olyan együtthatója, amit nem oszt. Legyenek a legkisebb indexű ilyen együtthatók a_s és b_t. Ekkor $p\,|\,c_{s+t}=\sum_{k+l=s+t}a_kb_l$. Ebben az összegben minden tagban van s-nél kisebb indexű a_k vagy t-nél kisebb indexű b_l, kivéve a_sb_t-t. Eszerint az összes többi tag osztható p-vel és az összeg is, tehát a kimaradó a_sb_t is. Ha p prím osztja két egész szám szorzatát, akkor valamelyiket osztania kell, amit kizártunk. Ellentmondásra jutottunk, tehát h köteles primitív lenni.

3.4.13 Állítás: az f primitív polinomot megszorozva a $\frac{p}{q}\in\mathbb{Q}$ számmal pontosan akkor lesz primitív, ha $\frac{p}{q}=\pm 1$.

Bizonyítás: feltehetjük, hogy $(p,q)=1, q>0$. Ha q nem 1, akkor van olyan prímosztója, ami nem osztja f egyik a_k együtthatóját és akkor $\frac{p}{q}\cdot a_k$ nem lesz egész. Ha $q=1$ és p nem ± 1, akkor p osztani fogja az együtthatókat és nem lesznek relatív prímek. Az nyilvánvaló, hogy minden $\mathbb{Q}[x]$-beli polinom megszorozható olyan $\frac{p}{q}\in\mathbb{Q}$-val, hogy primitív legyen. A most belátott állítás szerint ez a szám az előjeltől eltekintve egyértelmű.

3.4.14 Állítás: ha $f(x)\in\mathbb{Z}[x]$ felbomlik két alacsonyabb fokú racionális együtthatós polinom szorzatára (felbomlik $\mathbb{Q}[x]$-ben), akkor felbomlik két egész alacsonyabb fokú együtthatós polinom szorzatára is (felbomlik $\mathbb{Z}[x]$-ben).

Bizonyítás: osszuk le f-et együtthatói legnagyobb közös osztójával. Ez továbbra is felbomlik $\mathbb{Q}[x]$-ben. Ha belátjuk, hogy felbomlik $\mathbb{Z}[x]$-ben is, akkor már kész is vagyunk. Elég tehát primitív polinomokra belátnunk az állítást. Legyen $\mathbb{Q}[x]$-ben $f=g\cdot h$. Szorozzuk meg g-t és h-t úgy racionális számokkal, hogy primitív polinomokat kapjunk. Ezek szorzata is primitív és f skalárszorosa. Az előző állítás szerint ez a skalár csak ± 1 lehet, tehát f vagy $-f$ felbontását kaptuk $\mathbb{Z}[x]$-ben, így a keresett felbontás létezik.

3.4.15 Schönemann-Eisenstein kritérium: ha az $f(x)=\sum_{i=0}^{n} a_i x^{n-i}\in\mathbb{Z}[x]$ polinomra van olyan p prím, hogy $p\nmid a_0; p\mid a_1,\dots,a_n; p^2\nmid a_n$, akkor f irreducibilis (nem bomlik fel) $\mathbb{Z}[x]$-ben.

Bizonyítás: $\nexists$ f felbomlik $(\sum_{i=0}^{k} b_i x^{k-i})(\sum_{i=0}^{m} c_i x^{m-i})$ alakban. Ekkor $a_n=b_k c_m$ miatt b_k, c_m közül pontosan az egyik osztható p-vel, például c_m. Ekkor a $p\mid a_{n-1}=(b_{k-1}c_m)+b_k c_{m-1}$ összegnél a zárójelben lévő tagok oszthatóak p-vel, az utolsó szorzatban pedig b_k nem osztható p-vel. Akkor viszont c_{m-1} osztható p-vel. Ezt folytatva $p\mid a_{n-2}=(b_{k-2}c_m+b_{k-1}c_{m-1})+b_k c_{m-2}$ miatt c_{m-2} is osztható p-vel stb., végül $p\mid a_m=(\dots+b_{k-2}c_2+b_{k-1}c_1)+b_k c_0$ miatt c_0 is osztható p-vel. Ekkor viszont $a_0=b_0 c_0$ is osztható p-vel, $\lightning$.

Persze ugyanez a helyzet, ha a tétel feltételei között a_0 és a_n szerepét megcseréljük.

Következmény: x^n-p irreducibilis.

3.4.16 Következmény: a p-edik körosztási polinom, $\Phi_p(x)=\frac{x^{p-1}-1}{x-1}=x^{p-2}+x^{p-3}+\dots+x+1$ felbonthatatlan ($p\in\mathbb{Z}^+$ prím). Ugyanis $f(y)=\Phi_p(y+1)=\frac{(y+1)^p-1}{y}=y^{p-1}+\binom{p}{1}\cdot y^{p-2}+\dots+\binom{p}{p-2}\cdot y+\binom{p}{p-1}$ irreducibilis lesz, tehát $\Phi_p(x)$ is az.