Appendix

Az f egész együtthatós polinomot $\mathbb{Z}$ (illetve $\mathbb{Q}$) felett *felbonthatatlannak* nevezzük, ha nem írható fel két alacsonyabb fokszámú egész (illetve racionális) együtthatós polinom szorzataként.

Tétel. *Tetszőleges egész együtthatós polinom pontosan akkor felbonthatatlan $\mathbb{Z}$ felett, ha $\mathbb{Q}$ felett is az.*

A bizonyítás során többször hivatkozunk egy f polinom együtthatóinak legnagyobb közös osztójára, ezt $\operatorname{cont}(f)$ jelöli.

Lemma (Gauss). *Ha $\operatorname{cont}(f) = \operatorname{cont}(g) = 1$, akkor $\operatorname{cont}(fg) = 1$.*

Bizonyítás: Tegyük fel, hogy $\operatorname{cont}(f) = \operatorname{cont}(g) = 1$, de $\operatorname{cont}(fg) = d \neq \pm 1$. Legyen p a d egy prímosztója, a_r és b_s pedig az $f = \sum a_i x^i$ és $g = \sum b_i x^i$ p polinomok legkisebb indexű p-vel nem osztható együtthatói. Mennyi az fg polinom x^{r+s} tagjának együtthatója? Az fg polinom összes többi együtthatójával együtt ez is osztható p-vel. Másrészt viszont ez a szám azoknak az $a_i b_i$ szorzatoknak az összege, amelyekre $i + j = r + s$. E szorzatok között azonban szerepel $a_r b_s$ is, amely nem osztható p-vel, elvégre vagy $i < r$, vagy $j < s$, ez pedig ellentmondás. □

Rátérünk a tétel bizonyítására:

Feltehetjük, hogy $\operatorname{cont}(f) = 1$. Az $f = \varphi_1 \varphi_2$ felbontás alapján, amelyben φ_1 és φ_2 racionális együtthatós polinomok, meg kell konstruálnunk egy $f = f_1 f_2$ felbontást, amelyben f_1 és f_2 egész együtthatós polinomok. Írjuk fel a φ_i polinomokat $\varphi_i = \frac{a_i}{b_i} f_i$ alakban, ahol $a_i, b_i \in \mathbb{Z}$, az f_i-k pedig olyan egész együtthatós polinomok, amelyekre $\operatorname{cont}(f_i) = 1$. Ekkor $b_1 b_2 f = a_1 a_2 f_1 f_2$, amiből $\operatorname{cont}(b_1 b_2 f) = \operatorname{cont}(a_1 a_2 f_1 f_2)$. A Gauss-lemma alapján $\operatorname{cont}(f_1 f_2) = 1$, így $a_1 a_2 = \pm b_1 b_2$, $f = \pm f_1 f_2$ tehát éppen egy megfelelő felbontás. □

A1. Tétel. *Tegyük fel, hogy az f és g egész együtthatós polinomoknak van közös gyökük, f pedig olyan felbonthatatlan polinom, amelynek főegyütthatója 1. Ekkor g/f is egész együtthatós polinom.*

BIZONYÍTÁS: Az euklideszi algoritmus alapján (amelynek során mindig a maradékkal osztunk):

$$g = a_1 f + b_1, \;\; f = a_2 b_1 + b_2, \;\; b_1 = a_3 b_2 + b_3, \ldots, \;\; b_{n-2} = a_{n-1} b_n.$$

Könnyen igazolható, hogy ekkor b_n az f és g legnagyobb közös osztója. Valamennyi a_i és b_i polinom együtthatói racionális számok. Az f és g polinomok $\mathbb{Q}$ feletti legnagyobb közös osztója emiatt megegyezik $\mathbb{C}$ feletti legnagyobb közös osztójukkal. Mivel azonban $\mathbb{C}$ felett az f és g polinomoknak létezik nemtriviális közös osztója, f-nek és g-nek $\mathbb{Q}$ felett is van nemtriviális közös osztója, jelölje ez utóbbit r. Mivel f felbonthatatlan, 1 főegyütthatójú polinom, azt kapjuk, hogy $r = \pm f$. □

A2. TÉTEL (EISENSTEIN-KRITÉRIUM). *Legyen*

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

egész együtthatós polinom, p pedig olyan prímszám, amely a_n-nek nem, de az $a_0, \ldots, a_{n-1}$ együtthatók mindegyikének osztója, tegyük fel továbbá, hogy a_0 nem osztható p^2-tel. Ekkor az f polinom $\mathbb{Z}$ felett felbonthatatlan.

BIZONYÍTÁS: Tegyük fel, hogy $f = gh = \left(\sum b_k x^k\right)\left(\sum c_l x^l\right)$, ahol g és h egyike sem konstans. A $b_0 c_0 = a_0$ szám osztható p-vel, így ilyen b_0 és c_0 egyike szintén osztható p-vel. Ha például b_0 osztható p-vel, akkor c_0 nem, máskülönben ugyanis $a_0 = b_0 c_0$ osztható lenne p^2-tel. Ha valamennyi b_i szám osztható p-vel, akkor a_n is osztható lenne p-vel, van tehát olyan i, amelyre $0 < i \leq \deg g < n$, és b_i nem osztható p-vel.

Legyen i a legkisebb olyan index, amelyre b_i nem osztható p-vel. Ekkor feltevésünk szerint egyrészt a_i osztható p-vel, másrészt $a_i = b_i c_0 + b_{i-1} c_1 + \ldots + b_0 c_i$, és $b_i c_0$ kivételével az összeg valamennyi tagja osztható p-vel; ellentmondás. □

KÖVETKEZMÉNY. *Ha p prímszám, akkor az $f(x) = x^{p-1} + \ldots + x + 1$ polinom felbonthatatlan $\mathbb{Z}$ felett.*

BIZONYÍTÁS: Alkalmazzuk az Eisenstein-kritériumot a

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{1} x^{p-2} + \ldots + \binom{p}{p-1}$$

polinomra. □

A3. TÉTEL. *Legyenek az $x_1, \ldots, x_n$ pontokban adottak az*

$$y_1, \;\; y_1^{(1)}, \ldots, \; y_1^{(\alpha_1 - 1)}, \ldots, \; y_n, \;\; y_n^{(1)}, \ldots, \; y_n^{(\alpha_n - 1)}$$

számok; tegyük fel, hogy $m = \alpha_1 + \ldots + \alpha_n - 1$. Ekkor létezik olyan, legfeljebb m-ed fokú $H_m(x)$ polinom, amelyre $H_m(x_j) = y_j$ és $H_m^{(i)}(x_j) = y_j^{(i)}$.

BIZONYÍTÁS: Legyen $k = \max(\alpha_1, \dots, \alpha_n)$. A $k = 1$ esetben hivatkozhatunk a *Lagrange-féle*

$$L_n(x) = \sum_{j=1}^{n} \frac{(x - x_1) \dots (x - x_{j-1})(x - x_{j+1}) \dots (x - x_n)}{(x_j - x_1) \dots (x_j - x_{j-1})(x_j - x_{j+1}) \dots (x_j - x_n)} y_j.$$

interpolációs polinomra. Legyen $\omega_n(x) = (x - x_1) \dots (x - x_n)$. Tetszőleges, legfeljebb $(m - n)$-ed fokú H_{m-n} polinomnak feleltessük meg a $H_m(x) = L_n(x) + \omega_n(x) H_{m-n}(x)$ polinomot. Világos, hogy tetszőleges H_{m-n} esetén $H_m(x_j) = y_j$; emellett

$$H'_m(x) = L'_n(x) + \omega'_n(x) H_{m-n}(x) + \omega_n(x) H'_{m-n}(x),$$

amiből $H'_m(x_j) = L'_n(x_j) + \omega'_n(x_j) H_{m-n}(x_j)$. Mivel $\omega'_n(x_j) \neq 0$, így azokban a pontokban, amelyekben $H'_m(x_j)$ értékei adottak, meghatározhatjuk a $H_{m-n}(x_j)$ értékeket is. Fennáll továbbá a

$$H''_m(x_j) = L''_n(x_j) + \omega''_n(x_j) H_{m-n}(x_j) + 2\omega'_n(x_j) H'_{m-n}(x_j)$$

összefüggés is, így azokban a pontokban, amelyekben a $H''_m(x_j)$ értékek adottak, meghatározhatjuk a $H'_{m-n}(x_j)$ értékeket is stb. A probléma tehát annak a legfeljebb $(m - n)$-ed fokú $H_{m-n}(x)$ polinomnak a megadására redukálódik, amelyre $i = 0, \dots, \alpha_j - 2$ esetén $H^{(i)}_{m-n}(x_j) = z^{(i)}_j$ (ha $\alpha_j = 1$, akkor H_{m-n} értékeire és az x_j-beli deriváltakra semmiféle kikötés nincs). Világos ezenfelül, hogy $m - n = \sum(\alpha_j - 1) - 1$, így $k - 1$ hasonló lépés megtétele után már csak a Lagrange-féle interpolációs polinomot kell felírnunk. □

A4. A Hilbert-féle „Nullstellensatz" következő speciális esete is elegendő lesz a céljainkra.

TÉTEL. *Legyenek $f_1, \dots, f_r$ olyan n-változós komplex együtthatós polinomok, amelyeknek egyetlen közös gyöke sincs. Ekkor vannak olyan $g_1, \dots, g_r$ polinomok, amelyekre $f_1 g_1 + \dots + f_r g_r = 1$.*

BIZONYÍTÁS: Legyen $I(f_1, \dots, f_r)$ a $\mathbb{C}[x_1, \dots, x_n] = K$ polinomgyűrűnek az $f_1, \dots, f_r$ polinomok által generált ideálja. Tegyük fel, hogy nem léteznek olyan $g_1, \dots, g_r$ polinomok, amelyekre $f_1 g_1 + \dots + f_r g_r = 1$. Ekkor $I(f_1, \dots, f_r) \neq K$. Legyen I az $I(f_1, \dots, f_r)$ ideált tartalmazó maximális nemtriviális ideál. Könnyen igazolható, hogy K/I test. Valóban, ha $f \notin I$, akkor $I + Kf$ olyan ideál, amely – „valódi módon" – tartalmazza I-t, és mint ilyen, megegyezik K-val. Léteznek tehát olyan $g \in K$ és $h \in I$ polinomok, amelyekre $1 = h + fg$. A $\overline{g} \in K/I$ ekvivalenciaosztály ekkor az $\overline{f} \in K/I$ ekvivalenciaosztály inverze.

Bebizonyítjuk, hogy $A = K/I$ megegyezik $\mathbb{C}$-vel.

Legyen α_i az x_i elemnek a

$$p : \mathbb{C}[x_1, \dots, x_n] \longrightarrow \mathbb{C}[x_1, \dots, x_n]/I = A.$$

természetes projekció szerinti képe. Ekkor

$$A = \left\{ \sum z_{i_1 \dots i_n} \alpha_1^{i_1} \dots \alpha_n^{i_n} : z_{i_1 \dots i_n} \in \mathbb{C} \right\} = \mathbb{C}[\alpha_1, \dots, \alpha_n].$$

Legyen továbbá $A_0 = \mathbb{C}$ és $A_s = \mathbb{C}[\alpha_1, \dots, \alpha_s]$. Ekkor

$$A_{s+1} = \left\{ \sum a_i \alpha_{s+1}^i : a_i \in A_s \right\} = A_s[\alpha_{s+1}];$$

s szerinti indukcióval igazoljuk, hogy létezik $f : A_s \longrightarrow \mathbb{C}$ gyűrűhomomorfizmus (amelynél 1 képe 1). Az $s = 0$ esetben az állítás nyilvánvaló. Lásuk, miként kaphatjuk meg a $g : A_{s+1} \longrightarrow \mathbb{C}$ homomorfizmust az $f : A_s \longrightarrow \mathbb{C}$ homomorfizmus alapján. Két esetet különböztetünk meg.

(a) Az $x = \alpha_{s+1}$ elem transzcendens A_s felett. Ekkor tetszőleges $\xi \in \mathbb{C}$ esetén definiálhatunk egy g homomorfizmust, amelyre $g(a_n x^n + \ldots + a_0) = f(a_n)\xi^n + \ldots + f(a_0)$. A $\xi = 0$ esetben olyan g-t kapunk, amelyre $g(1) = 1$.

(b) Az $x = \alpha_{s+1}$ elem A_s felett algebrai, van tehát olyan $b_i \in A_s$, amellyel $b_m x^m + b_{m-1} x^{m-1} + \ldots + b_0 = 0$. Ekkor minden olyan $\xi \in \mathbb{C}$ esetén, amelyre $f(b_m)\xi^m + \ldots + f(b_0) = 0$, létezik egy meghatározott $g\left(\sum a_k x^k\right) = \sum f(a_k)\xi^k$ homomorfizmus, amelynél 1 képe 1.

Megkaptunk tehát egy $h : A \longrightarrow \mathbb{C}$ homomorfizmust, amelyre $h(1) = 1$. A $h^{-1}(0)$ nyilván egy ideál, mivel pedig az A testben nincsenek nemtriviális ideálok, h egy monomorfizmus. $A_0 = \mathbb{C} \subset A$, a h monomorfizmus A_0-ra való leszűkítése pedig az identikus leképezés, így h izomorfizmus.

Feltehetjük tehát, hogy $\alpha_i \in \mathbb{C}$. A p projekció ekkor az $f_i(x_1, \dots, x_n) \in K$ polinomhoz az $f_i(\alpha_1, \dots, \alpha_n) \in \mathbb{C}$ komplex számot rendeli. $f_1, \dots, f_r \in I$ miatt ekkor $p(f_i) = 0 \in \mathbb{C}$, így $f_i(\alpha_1, \dots, \alpha_n) = 0$, ami ellentmondás. □

A5. Tétel. *Legyenek $f_i(x_1, \dots, x_n) = x_i^{m_i} + P_i(x_1, \dots, x_n)$ olyan polinomok, $(i = 1, \dots, n)$, amelyekre $\deg P_i < m_i$, legyen továbbá $I(f_1, \dots, f_n)$ az $f_1, \dots, f_n$ polinomok által generált ideál.*

(a) *Legyen $P(x_1, \dots, x_n)$ nemnulla, $\sum a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$ alakú polinom, ahol minden $k = 1, \dots, n$ esetén $i_k < m_k$. Ekkor $P \notin I(f_1, \dots, f_n)$.*

(b) *A komplex számok halmazán az $x_i^{m_i} + P_i(x_1, \dots, x_n) = 0$ $(i = 1, \dots, n)$ egyenletrendszer mindig megoldható, a megoldások száma pedig véges.*

Bizonyítás: (a) Ha $x_i^{m_i t_i + q_i}$ helyébe az $(f_i - P_i)^{t_i} x^{q_i}$ polinomot írjuk, ahol $0 \le t_i$ és $0 \le q_i < m_i$, akkor kiderül, hogy $Q(x_1, \dots, x_n)$ felírható

$$Q(x_1, \dots, x_n) = Q^*(x_1, \dots, x_n, f_1, \dots, f_n) = \sum a_{js} x_1^{j_1} \dots x_n^{j_n} f_1^{s_1} \dots f_n^{s_n},$$

alakban, ahol $j_1 < m_1, \dots, j_n < m_n$. Bebizonyítjuk, hogy az ilyen Q^* reprezentáció egyértelmű. Elegendő ehhez azt igazolni, hogy az $f_i = x_i^{m_i} + P_i(x_1, \dots, x_n)$ polinomokat bármelyik nemnulla $Q^*(x_1, \dots, x_n, f_1, \dots, f_n)$ polinomba helyettesítve egy nemnulla $\tilde{Q}(x_1, \dots, x_n)$ polinomot kapunk. A Q^* polinom tagjai közül válasszuk ki azt, amelyre az

$$(s_1 m_1 + j_1) + \ldots + (s_n m_n + j_n) = m$$

összeg maximális. Ekkor nyilván $\deg \tilde{Q} \leq m$. Határozzuk meg a $\tilde{Q}$ polinom $x_1^{s_1 m_1 + j_1} \dots x_n^{s_n m_n + j_n}$ tagjának együtthatóját. Mivel az

$$(s_1 m_1 + j_1) + \ldots + (s_n m_n + j_n)$$

összeg maximális, a szóban forgó kifejezés csak az $x_1^{j_1} \dots x_n^{j_n} f_1^{s_1} \dots f_n^{s_n}$ monomból származhat. Ezek együtthatója tehát megegyezik: $\deg \tilde{Q} = m$.

Nyilvánvaló, hogy $Q(x_1, \dots, x_n) \in I(f_1, \dots, f_n)$ pontosan akkor, ha

$$Q^*(x_1, \dots, x_n, f_1, \dots, f_n)$$

olyan monomok összege, amelyekre $s_1 + \ldots + s_n \geq 1$. Ezenfelül, ha

$$P(x_1, \dots, x_n) = \sum a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n},$$

ahol $i_k < m_k$, akkor

$$P^*(x_1, \dots, x_n, f_1, \dots, f_n) = P(x_1, \dots, x_n).$$

Így tehát $P \notin I(f_1, \dots, f_n)$.

(b) Ha az $f_1, \dots, f_n$ polinomoknak nincs közös gyöke, akkor a Hilbert-féle *Nullstellensatz* szerint az $I(f_1, \dots, f_n)$ ideál megegyezik a teljes polinomgyűrűvel, és így $P \in I(f_1, \dots, f_n)$, ami ellentmond az imént bizonyított (a) állításnak. A megadott egyenletrendszer tehát megoldható; legyen $\xi = (\xi_1, \dots, \xi_n)$ egy megoldás. Ekkor $\xi_i^{m_i} = -P_i(\xi_1, \dots, \xi_n)$, ahol $\deg P_i < m_i$, minek következtében a $Q(\xi_1, \dots \xi_n)$ polinom felírható $Q(\xi_1, \dots, \xi_n) = \sum a_{i_1 \dots i_n} \xi_1^{i_1} \dots \xi_n^{i_n}$ alakban, ahol $i_k < m_k$, az $a_{i_1 \dots i_n}$ együtthatók pedig valamennyi megoldás esetén ugyanazok. Legyen $m = m_1 \cdot \ldots \cdot m_n$. Az $1, \xi_i, \dots, \xi_i^m$ polinomok – mivel kifejezhetők a $\xi_1^{i_1} \dots \xi_n^{i_n}$ alappolinomok lineáris kombinációjaként (ahol $i_k < m_k$) – lineárisan összefüggő rendszert alkotnak, vagyis $b_0 + b_1 \xi_i + \ldots + b_m \xi_i^m = 0$, ahol a $b_0, \dots, b_m$ számok nem mindegyike 0, ezek a számok ráadásul valamennyi megoldásra ugyanazok (és nem függenek i-től). A $b_0 + b_1 x + \ldots + b_m x^m = 0$ egyenletnek így nyilvánvalóan csak véges számú megoldása lehet. □