5. POLINOMOK PRÍMFAKTORIZÁCIÓJA, TÖBBSZÖRÖS FAKTOROK

5.1.Tétel. *Legyen $K \subseteq \mathbb{C}$ egy számtest, ekkor bármely konstanstól különböző $f(x) \in K[x]$ polinom felbontható K felett irreducibilis $K[x]$-beli polinomok szorzatára: ha $\deg(f(x)) \geq 1$, akkor léteznek olyan K felett irreducibilis $p_i(x) \in K[x]$, $1 \leq i \leq k$ polinomok, amelyekre:*

$$f(x) = p_1(x)p_2(x)...p_k(x).$$

Az $f(x)$-nek ez a felbontása a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelmű. Ha a K felett irreducibilis $q_j(x) \in K[x]$, $1 \leq j \leq l$ polinomokra

$$f(x) = q_1(x)q_2(x)...q_l(x),$$

akkor létezik olyan $\pi : \{1, 2, ..., l\} \longrightarrow \{1, 2, ..., k\}$ bijektív megfeleltetés az index halmazok között, amelyre a $q_j(x) \sim p_{\pi(j)}(x)$, $j \in \{1, 2, ..., l\}$ asszociált viszonyok teljesülnek (így $l = k$).

Bizonyítás. A felbontás létezését az $n = \deg(f(x))$ egészre vonatkozó teljes indukcióval igazoljuk. Ha $n = 1$, akkor az $f(x) = p_1(x)$ a kívánt felbontást jelenti, hiszen a 4.A.Definíció szerint $f(x)$ irreducibilis K felett. Az indukcióhoz feltételezzük, hogy tetszőleges $1 \leq \deg(f(x)) \leq n$ tulajdonságú $K[x]$-beli polinom felbontható K felett irreducibilis ($K[x]$-beli) polinomok szorzatára.
Tekintsünk most egy $\deg(g(x)) = n + 1$ fokszámú $g(x) \in K[x]$ polinomot. Ha $g(x)$ irreducibilis K felett, akkor $g(x) = p_1(x)$ a kívánt felbontást jelenti. Amennyiben $g(x)$ reducibilis K felett, akkor $g(x) = u(x)v(x)$ olyan $u(x), v(x) \in K[x]$ polinomokkal, amelyekre $\deg(u(x)) \geq 1$ és $\deg(v(x)) \geq 1$. Mivel

$$\deg(u(x)) + \deg(v(x)) = \deg(g(x)) = n + 1,$$

ezért $1 \leq \deg(u(x)) \leq n$ és $1 \leq \deg(v(x)) \leq n$. Az indukciós feltevésünk szerint $u(x)$ is és $v(x)$ is felbontható K felett irreducibilis ($K[x]$-beli) polinomok szorzatára, ami $g(x)$-nek a kívánt felbontását is biztosítja.
Az egyértelműséget szintén az $n = \deg(f(x))$ egészre vonatkozó teljes indukcióval igazoljuk. Ha $n = 1$, akkor a K felett irreducibilis $p_i(x) \in K[x]$, $1 \leq i \leq k$ polinomokra az

$$f(x) = p_1(x)p_2(x)...p_k(x)$$

egyenlőségből

$$\deg(p_1(x)) + \deg(p_2(x)) + ... + \deg(p_k(x)) = \deg(f(x)) = 1$$

következik, ami $\deg(p_i(x)) \geq 1$ egyenlőtlenségek ($1 \leq i \leq k$) miatt csak a $k = 1$ esetben teljesülhet. Tehát $f(x) = p_1(x)$ és hasonlóan kapjuk azt is, hogy $f(x) = q_1(x)$.
Az indukcióhoz feltételezzük, hogy tetszőleges $1 \leq \deg(f(x)) \leq n$ tulajdonságú $K[x]$-beli polinomnak a K felett irreducibilis ($K[x]$-beli) polinomok szorzatára való felbontása a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelmű. Tekintsük most egy

$$\deg(g(x)) = n + 1 \text{ fokszámú } g(x) \in K[x]$$

polinomnak a K felett irreducibilis $p_i(x), q_j(x) \in K[x]$, $1 \leq i \leq k$, $1 \leq j \leq l$ polinomok szorzataként való

$$g(x) = p_1(x)p_2(x)...p_k(x) = q_1(x)q_2(x)...q_l(x)$$

kétféle felírását. Ekkor $p_k(x)$ irreducibilitása K felett és a $p_k(x) \mid g(x) = q_1(x)q_2(x)...q_l(x)$ oszthatóság a 4.5.Állítás 5.része alapján azt eredményezi, hogy $p_k(x) \mid q_t(x)$ teljesül valamilyen $1 \leq t \leq l$ indexre. Mivel a $q_t(x)$ irreducibilis K felett, ezért a 4.5.Állítás 1.része alapján csak triviális osztói léteznek: $p_k(x) \sim 1$ vagy $p_k(x) \sim q_t(x)$. A $p_k(x) \sim 1$ asszociált viszony nem teljesülhet, mert $\deg(p_k(x)) \geq 1$. Tehát $p_k(x) \sim q_t(x)$, ami a 3.5.Állítás 3.része szerint azt jelenti, hogy $q_t(x) = cp_k(x)$ valamilyen $0 \neq c \in \mathbb{C}$ komplex számra. Így előbb a

$$p_1(x)p_2(x)...p_k(x) = q_1(x)...q_t(x)...q_l(x) = q_1(x)...q_{t-1}(x)(cp_k(x))q_{t+1}(x)...q_l(x),$$

majd innen $p_k(x)$-el való egyszerűsítés után (lásd a 3.1.Állítás 4.részét) a

$$h(x) = p_1(x)p_2(x)...p_{k-1}(x) = (cq_1(x))q_2(x)...q_{t-1}(x)q_{t+1}(x)...q_l(x)$$

egyenlőséghez jutunk. A $p_k(x), q_t(x) \in K[x]$ tartalmazásokból nyilvánvalóan következik, hogy $c \in K$, ami a 4.5.Állítás 6.része szerint $cq_1(x)$ irreducibilitását biztosítja K felett. Végeredményben a $h(x) \in K[x]$ polinom kétféle K felett irreducibilis tényezőkre való felbontását kaptuk. Az indukciós feltevésünket $1 \leq \deg(h(x)) \leq n$ miatt (ez $h(x)p_k(x) = g(x)$, illetve $\deg(h(x)) + \deg(p_k(x)) = \deg(g(x)) = n+1$ következménye) alkalmazhatjuk a $h(x)$ kétféle felbontására. Tehát létezik olyan $\tau : \{1, ..., t-1, t+1, ..., l\} \longrightarrow \{1, ..., k-1\}$ bijektív megfeleltetés az index halmazok között, amelyre a

$$cq_1(x) \sim p_{\tau(1)}(x) \text{ és } q_j(x) \sim p_{\tau(j)}(x)\ ,\ j \in \{2, ..., t-1, t+1, ..., l\}$$

asszociált viszonyok teljesülnek. Nyilvánvaló, hogy a

$$\pi(t) = k \text{ és a } j \in \{1, ..., t-1, t+1, ..., l\} \text{ esetben a } \pi(j) = \tau(j)$$

módon értelmezett bijektív $\{1, ..., l\} \longrightarrow \{1, ..., k\}$ megfeleltetésre teljesülnek a $q_j(x) \sim p_{\pi(j)}(x)$, $j \in \{1, ..., l\}$ asszociált viszonyok, hiszen

$$q_1(x) \sim cq_1(x) \sim p_{\tau(1)}(x) = p_{\pi(1)}(x) \text{ és } q_t(x) \sim p_k(x) = p_{\pi(t)}(x).$$

□□□

5.2.Állítás. *Legyen $K \subseteq \mathbb{C}$ egy számtest és tekintsük az $f(x), g(x) \in K[x]$ konstanstól különböző polinomok felbontását K felett irreducibilis $K[x]$-beli polinomok szorzatára:*

$$f(x) = p_1(x)p_2(x)...p_k(x) \text{ és } g(x) = q_1(x)q_2(x)...q_l(x),$$

ahol $p_i(x), q_j(x) \in K[x]$, $1 \leq i \leq k$, $1 \leq j \leq l$ irreducibilis polinomok. A $g(x) \mid f(x)$ oszthatóság pontosan akkor teljesül, ha létezik olyan $\alpha : \{1, 2, ..., l\} \longrightarrow \{1, 2, ..., k\}$ injektív leképezés az index halmazok között, amelyre a $q_j(x) \sim p_{\alpha(j)}(x)$, $j \in \{1, 2, ..., l\}$ asszociált viszonyok teljesülnek (így $l \leq k$).

Bizonyítás. A $g(x) \mid f(x)$ oszthatóság olyan $q(x) \in \mathbb{C}[x]$ polinom létezését jelenti, amelyre $f(x) = g(x)q(x)$. Az $f(x), g(x) \in K[x]$ tartalmazások és a 3.5.Állítás 1.része alapján $q(x) \in K[x]$ is teljesül. Ha tekintjük a $q(x) \in K[x]$ polinom

$$q(x) = q_{l+1}(x)q_{l+2}(x)...q_{l+m}(x)$$

felbontását a K felett irreducibilis $q_{l+t}(x) \in K[x]$, $1 \leq t \leq m$ polinomok szorzatára, akkor megkapjuk $f(x)$-nek egy másik felbontását K felett irreducibilis tényezők szorzatára:

$$f(x) = g(x)q(x) = q_1(x)q_2(x)...q_l(x)q_{l+1}(x)q_{l+2}(x)...q_{l+m}(x).$$

Az 5.1.Tétel olyan $\pi : \{1, 2, ..., l, l+1, ..., l+m\} \longrightarrow \{1, 2, ..., k\}$ bijektív megfeleltetést szolgáltat az index halmazok között, amelyre a $q_j(x) \sim p_{\pi(j)}(x)$, $j \in \{1, 2, ..., l, l+1, ..., l+m\}$ asszociált viszonyok teljesülnek. A π-nek a megszorítása az $\{1, 2, ..., l\}$ halmazra a kívánt injektív leképezést biztosítja:

$$\alpha = \pi \restriction \{1, 2, ..., l\} : \{1, 2, ..., l\} \longrightarrow \{1, 2, ..., k\}.$$

Amennyiben létezik a tételben leírt tulajdonságú $\alpha : \{1, 2, ..., l\} \longrightarrow \{1, 2, ..., k\}$ injektív leképezés, akkor a $q_j(x) \mid p_{\alpha(j)}(x)$, $j \in \{1, 2, ..., l\}$ oszthatóságok is teljesülnek, ahonnan előbb

$$g(x) = q_1(x)q_2(x)...q_l(x) \mid p_{\alpha(1)}(x)p_{\alpha(2)}(x)...p_{\alpha(l)}(x),$$

majd

$$p_{\alpha(1)}(x)p_{\alpha(2)}(x)...p_{\alpha(l)}(x) \mid f(x)$$

figyelembe vételével $g(x) \mid f(x)$ adódik.

$\square\square\square$

5.3.Állítás. *Legyen $K \subseteq \mathbb{C}$ egy számtest, ekkor bármely konstanstól különböző*

$$f(x) = a_0 + a_1x + ... + a_nx^n \in K[x]$$

(itt $n \geq 1$ és $a_n \neq 0$) polinomhoz léteznek olyan 1 főegyütthatóval rendelkező K felett irreducibilis $r_i(x) \in K[x]$, $1 \leq i \leq k$ polinomok, amelyekre:

$$f(x) = a_nr_1(x)r_2(x)...r_k(x).$$

Az $f(x)$-nek ez a felbontása a tényezők sorrendjétől eltekintve egyértelmű, azaz ha egy $c \in \mathbb{C}$ konstansra és az 1 főegyütthatóval rendelkező K felett irreducibilis $q_j(x) \in K[x]$, $1 \leq j \leq l$ polinomokra

$$f(x) = cq_1(x)q_2(x)...q_l(x),$$

akkor $c = a_n$ és létezik olyan $\pi : \{1, 2, ..., l\} \longrightarrow \{1, 2, ..., k\}$ bijektív megfeleltetés az index halmazok között, amelyre a $q_j(x) = r_{\pi(j)}(x)$, $j \in \{1, 2, ..., l\}$ egyenlőségek teljesülnek.

Bizonyítás. Tekintsük az 5.1.Tételben megadott

$$f(x) = p_1(x)p_2(x)...p_k(x)$$

felbontást a K felett irreducibilis $p_i(x) \in K[x]$, $1 \leq i \leq k$ polinomokkal, ekkor

$$f(x) = a_nf^*(x) \text{ és } f^*(x) = p_1^*(x)p_2^*(x)...p_k^*(x),$$

ahonnan az $r_i(x) = p_i^*(x) \in K[x]$, $1 \leq i \leq k$ választással a kívánt

$$f(x) = a_nf^*(x) = a_np_1^*(x)p_2^*(x)...p_k^*(x) = a_nr_1(x)r_2(x)...r_k(x)$$

szorzat felbontáshoz jutunk. Valóban, a 4.5.Állítás 6.részére való tekintettel minden

$$r_i(x) = p_i^*(x) \sim p_i(x)\ ,\ 1 \le i \le k$$

polinom irreducibilis a K felett és nyilvánvaló, hogy mindegyik főegyütthatója 1. Amennyiben a $c \in \mathbb{C}$ számra és az 1 főegyütthatóval rendelkező K felett irreducibilis $q_j(x) \in K[x]$, $1 \le j \le l$ polinomokra

$$f(x) = cq_1(x)q_2(x)...q_l(x),$$

akkor az egyenlőség két oldalán a főegyütthatók egyezősége az $a_n = c$ következménnyel jár. Az $f(x)$ kétféle felbontásának összehasonlítása az a_n-el való egyszerűsítés után az

$$r_1(x)r_2(x)...r_k(x) = q_1(x)q_2(x)...q_l(x)$$

egyenlőséghez vezet. Az 5.1.Tétel ismét alkalmazható és egy olyan

$$\pi : \{1, 2, ..., l\} \longrightarrow \{1, 2, ..., k\}$$

bijektív megfeleltetést biztosít az index halmazok között, amelyre a $q_j(x) \sim r_{\pi(j)}(x)$ asszociált viszonyok teljesülnek minden $j \in \{1, 2, ..., l\}$ indexre. Mivel a $q_j(x)$ és $r_{\pi(j)}(x) = p^*_{\pi(j)}(x)$ mindegyikének a főegyütthatója 1, ezért $q_j(x) = r_{\pi(j)}(x)$.

$\Box\Box\Box$

5.A.Definíció. Legyen $K \subseteq C$ egy számtest, ekkor a konstanstól különböző

$$f(x) = a_0 + a_1x + ... + a_nx^n \in K[x]$$

(itt $n \ge 1$ és $a_n \ne 0$) polinomnak az 5.3.Állításban megadott (a tényezők sorrendjétől eltekintve egyértelmű)

$$f(x) = a_nr_1(x)r_2(x)...r_k(x)$$

szorzat felbontását (az 1 főegyütthatóval rendelkező K felett irreducibilis $r_i(x) \in K[x]$ polinomokkal) nevezzük az $f(x)$ **polinom K feletti prímtényezős felbontásának**.
A tényezők $r_1(x), r_2(x), ..., r_k(x)$ felsorolásában nem feltétlenül egymástól különböző polinomok szerepelnek, ezért célszerű az előbbi felsorolás tagjait ismétlődés nélkül egy

$$p_1(x), p_2(x), ..., p_t(x)$$

sorozatban megadni és minden egyes $p_i(x)$, $1 \le i \le t$ polinom esetében megadni azt a $k_i \ge 1$ egész számot, amely $p_i(x)$ előfordulásainak a számát jelenti az $r_1(x), r_2(x), ..., r_k(x)$ sorozatban. Tehát

$$\{r_1(x), r_2(x), ..., r_k(x)\} = \{p_1(x), p_2(x), ..., p_t(x)\},$$

ahol az $1 \le i < j \le t$ indexekre $p_i(x) \ne p_j(x)$. Így az $f(x)$ polinom prímtényezős felbontása az

$$f(x) = a_n(p_1(x))^{k_1}(p_2(x))^{k_2}...(p_t(x))^{k_t}$$

alakban írható.

Ha egy $q(x) \in K[x]$ polinom irreducibilis K felett, akkor a

$$q(x) \in \{p_1(x), p_2(x), ..., p_t(x)\}$$

esetben $q(x) = p_i(x)$ és ilyenkor azt mondjuk, hogy $q(x)$ **kitevője az** $f(x)$**-ben** a $k_i \geq 1$ egész szám (vagy azt, hogy a $q(x)$ polinom k_i**-szeres faktora** $f(x)$**-nek**). Amennyiben

$$q(x) \notin \{p_1(x), p_2(x), ..., p_t(x)\},$$

akkor azt mondjuk, hogy $q(x)$ **kitevője az** $f(x)$**-ben** zérus, a $q(x)$ ilyenkor is használható az $f(x)$ előállításában:

$$f(x) = a_n(p_1(x))^{k_1}(p_2(x))^{k_2}...(p_t(x))^{k_t}(q(x))^0,$$

ilyenkor **redundáns prímtényezős alakról** beszélünk.
A 4.7.Tétel szerint egy $f(x) \in \mathbb{C}[x]$ polinom $\mathbb{C}$ feletti prímtényezős felbontásában minden tényező elsőfokú, ezért (az 1 főegyütthatóra való tekintettel) $p_i(x) = x - \alpha_i$ valamilyen $\alpha_i \in \mathbb{C}$ számmal. Tehát

$$f(x) = a_n(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2}...(x - \alpha_t)^{k_t}.$$

és ezt nevezzük az $f(x)$ **gyöktényezős felbontásának** ($\mathbb{C}$ felett). Nyilvánvaló, hogy

$$\alpha_1, \alpha_2, ..., \alpha_t \in \mathbb{C}$$

az $f(x)$ polinom összes gyökeinek egy ismétlődés nélküli felsorolása. A gyöktényezős felbontásban a k_i egész számot nevezzük az α_i **gyök multiplicitásának**.♡

5.4.Állítás. *Legyen $K \subseteq \mathbb{C}$ egy számtest és tekintsük a konstanstól különböző*

$$f(x) = a_0 + a_1x + ... + a_nx^n \text{ és } g(x) = b_0 + b_1x + ... + b_mx^m$$

$K[x]$-beli polinomok (itt $a_n \neq 0 \neq b_m$) K feletti (redundáns) prímtényezős felbontásait

$$f(x) = a_n(p_1(x))^{k_1}(p_2(x))^{k_2}...(p_t(x))^{k_t} \text{ és } g(x) = b_m(p_1(x))^{l_1}(p_2(x))^{l_2}...(p_t(x))^{l_t},$$

ahol $p_i(x) \in K[x]$, $1 \leq i \leq t$ irreducibilis polinomok 1 főegyütthatóval (a k_i és l_i kitevők egyike lehet zérus). A $g(x) \mid f(x)$ oszthatóság pontosan akkor teljesül, ha $l_i \leq k_i$ minden $1 \leq i \leq t$ indexre.

Bizonyítás. Ha $l_i \leq k_i$ minden $1 \leq i \leq t$ indexre, akkor a $(p_i(x))^{l_i} \mid (p_i(x))^{k_i}$, $1 \leq i \leq t$ oszthatóságok nyilvánvalóan teljesülnek. Így szorzással azonnal adódik a kívánt $g(x) \mid f(x)$ oszthatóság (itt az a_n és b_m együtthatók szerepe lényegtelen).
Ha $g(x) \mid f(x)$, akkor az $l_i \leq k_i$ egyenlőtlenségeket az 5.3.Állítás egyszerű következményeként kapjuk, úgy mint az 5.2.Állítást az 5.1.Tételből.

□□□

5.5.Következmény. *Legyen $K \subseteq \mathbb{C}$ egy számtest és tekintsük a konstanstól különböző*

$$f(x) = a_0 + a_1x + ... + a_nx^n \text{ és } g(x) = b_0 + b_1x + ... + b_mx^m$$

$K[x]$-beli polinomok (itt $a_n \neq 0 \neq b_m$) K feletti (redundáns) prímtényezős felbontásait

$$f(x) = a_n(p_1(x))^{k_1}(p_2(x))^{k_2}...(p_t(x))^{k_t} \text{ és } g(x) = b_m(p_1(x))^{l_1}(p_2(x))^{l_2}...(p_t(x))^{l_t},$$

ahol $p_i(x) \in K[x]$, $1 \leq i \leq t$ irreducibilis polinomok 1 főegyütthatóval (a k_i és l_i kitevők egyike lehet zérus). Ekkor

$$\text{lnko}(f(x), g(x)) = (p_1(x))^{m_1}(p_2(x))^{m_2}...(p_t(x))^{m_t},$$

ahol $m_i = \min\{k_i, l_i\}$.

□□□

5.B.Definíció. Egy $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{C}[x]$ polinom **derivált polinomját** az alábbi

$$f'(x) = a_1 + 2a_2x + ... + ka_kx^{k-1} + ... + na_nx^{n-1}$$

módon értelmezzük. Nyilvánvaló, hogy $f'(x) \in \mathbb{C}[x]$ és a $\deg(f(x)) = n \geq 1$ esetben $\deg(f'(x)) = n - 1$. Ha $f(x)$ konstans ($\deg(f(x)) \leq 0$), akkor $f'(x) = 0$ a zérus polinom.♡

5.6.Állítás. *Legyen $K \subseteq \mathbb{C}$ egy számtest, $\alpha \in \mathbb{C}$ és tekintsük az $f(x), g(x) \in \mathbb{C}[x]$ polinomokat, ekkor az alábbiak teljesülnek.*

1. *Ha $f(x) \in K[x]$, akkor $f'(x) \in K[x]$.*
2. *$(f(x) \pm g(x))' = f'(x) \pm g'(x)$.*
3. *$(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.*
4. *Tetszőleges $k \geq 1$ egész kitevőre $\left((f(x))^k\right)' = k(f(x))^{k-1}f'(x)$.*
5. *Ha $f(\alpha) = g(\alpha)$ és $f^{(k)}(\alpha) = g^{(k)}(\alpha)$ minden $1 \leq k \leq n$ egészre, akkor $f(x) = g(x)$. Itt $n = \deg(f(x))$ és $f^{(k)}(x)$ az $f(x)$ polinom k-szoros derivált polinomját jelöli.*
6. $$f(x) = f(\alpha) + \frac{f'(\alpha)}{1!}(x-\alpha) + ... + \frac{f^{(k)}(\alpha)}{k!}(x-\alpha)^k + ... + \frac{f^{(n)}(\alpha)}{n!}(x-\alpha)^n,$$
   ahol $n = \deg(f(x))$ (és $f^{(k)}(x)$ az $f(x)$ polinom k-szoros deriváltja).

Az 5.6.Állítás részeit könnyen igazolhatjuk közvetlenül a derivált polinom definíciója alapján, de az analízisből is jól ismertek a fenti deriválási szabályok.

5.7.Tétel. *Legyen $K \subseteq \mathbb{C}$ egy számtest és tekintsük a konstanstól különböző $0 \neq a_n \in K$ főegyütthatóval rendelkező $f(x) \in K[x]$ polinom K feletti*

$$f(x) = a_n(p_1(x))^{k_1}(p_2(x))^{k_2}...(p_t(x))^{k_t}$$

prímtényezős felbontását, ahol $p_i(x) \in K[x]$, $1 \leq i \leq t$ irreducibilis polinomok 1 főegyütthatóval. Ekkor

$$\text{lnko}(f(x), f'(x)) = (p_1(x))^{k_1-1}(p_2(x))^{k_2-1}...(p_t(x))^{k_t-1}.$$

Bizonyítás. A $K[x]$-beli $d(x) = \text{lnko}(f(x), f'(x))$ polinom főegyütthatója 1 és $d(x) \mid f(x)$, ezért az 5.4.Állítás szerint a $d(x)$ (redundáns) prímtényezős felbontása a K felett

$$d(x) = (p_1(x))^{l_1}(p_2(x))^{l_2}...(p_t(x))^{l_t}$$

alakban írható, ahol $0 \leq l_i \leq k_i$ minden $1 \leq i \leq t$ egészre.
Most $f(x) = (p_i(x))^{k_i}q(x)$, ahol a

$$q(x) = a_n(p_1(x))^{k_1}...(p_{i-1}(x))^{k_{i-1}}(p_{i+1}(x))^{k_{i+1}}...(p_t(x))^{k_t}$$

polinomra az 5.5.Következmény szerint

$$\text{lnko}(p_i(x), q(x)) = 1$$

teljesül. Az 5.6.Állítás 3.része szerint

$$f'(x) = k_i(p_i(x))^{k_i-1}p_i'(x)q(x) + (p_i(x))^{k_i}q'(x) = (p_i(x))^{k_i-1}\left(k_ip_i'(x)q(x) + p_i(x)q'(x)\right),$$

ami azt jelenti, hogy a $(p_i(x))^{k_i-1} \mid f'(x)$ oszthatóság (és $(p_i(x))^{k_i-1} \mid f(x)$ is) teljesül.
Ha $(p_i(x))^{k_i} \mid f'(x)$ teljesülne, akkor valamilyen $u(x) \in \mathbb{C}[x]$ polinomra

$$(p_i(x))^{k_i}u(x) = f'(x) = (p_i(x))^{k_i-1}\left(k_ip_i'(x)q(x) + p_i(x)q'(x)\right),$$

ahonnan $(p_i(x))^{k_i-1}$-el való egyszerűsítés után

$$p_i(x)u(x) = k_ip_i'(x)q(x) + p_i(x)q'(x),$$

illetve

$$p_i(x)(u(x) - q'(x)) = k_ip_i'(x)q(x)$$

adódik. Tehát $p_i(x) \mid k_ip_i'(x)q(x)$ a $k_ip_i'(x), q(x) \in K[x]$ és a K felett irreducibilis $p_i(x)$ polinomra, így a 4.5.Állítás 5.része a $p_i(x) \mid k_ip_i'(x)$ vagy a $p_i(x) \mid q(x)$ oszthatóságok egyikét biztosítja. Az első $\deg(k_ip_i'(x)) = \deg(p_i(x)) - 1$ miatt, a második $\text{lnko}(p_i(x), q(x)) = 1$ miatt nem teljesülhet.
Tehát a legnagyobb közös osztó definíciója miatt $(p_i(x))^{k_i-1} \mid d(x)$ és $(p_i(x))^{k_i} \nmid f'(x)$ miatt $(p_i(x))^{k_i} \nmid d(x)$. Az 5.4.Állítást újra használva kapjuk, hogy a

$$(p_i(x))^{k_i-1} \mid (p_1(x))^{l_1}(p_2(x))^{l_2}...(p_t(x))^{l_t} = d(x)$$

oszthatóság pontosan akkor teljesül, ha $k_i - 1 \leq l_i$. Mivel $(p_i(x))^{k_i} \nmid d(x)$ miatt $l_i \leq k_i - 1$, ezért $l_i = k_i - 1$.

$\square\square\square$

5.8.Következmény. *Legyen $K \subseteq \mathbb{C}$ egy számtest és tekintsük a konstanstól különböző $0 \neq a_n \in K$ főegyütthatóval rendelkező K felett irreducibilis $p(x) \in K[x]$ polinom*

$$p(x) = a_n(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2}...(x - \alpha_t)^{k_t}$$

gyöktényezős felbontását, ahol $\alpha_1, \alpha_2, ..., \alpha_t \in \mathbb{C}$ az $f(x)$ polinom összes gyökeinek egy ismétlődés nélküli felsorolása. Ekkor minden gyök multiplicitása 1:

$$k_1 = k_2 = ... = k_t = 1.$$

Bizonyítás. Mivel $p'(x) \in K[x]$ és $p(x)$ irreducibilis K felett, továbbá $\deg(p'(x)) < \deg(p(x))$ miatt $p(x) \nmid p'(x)$, ezért a 4.5.Állítás 2.része alapján $\text{lnko}(p(x), p'(x)) = 1$. Az előbbi 5.7.Tételt a $K = \mathbb{C}$ esetben alaklamazva kapjuk a kívánt egyenlőséget:

$$\text{lnko}(p(x), p'(x)) = (x-\alpha_1)^{k_1-1}(x-\alpha_2)^{k_2-1}...(x-\alpha_t)^{k_t-1} = 1 \Longleftrightarrow k_1 = k_2 = ... = k_t = 1.$$

□□□

5.C.Definíció. Egy $K \subseteq \mathbb{C}$ számtest feletti **racionális törteken** (vagy **törtfüggvényeken**) az $(f(x), g(x))$ alakban írható rendezett párokat értjük, ahol $f(x), g(x) \in K[x]$ polinomok és $g(x)$ nem a zérus polinom: $g(x) \neq 0$. A racionális törtek közötti

$$(f_1(x), g_1(x)) \simeq (f_2(x), g_2(x))$$

relációt a szorzat polinomok $f_1(x)g_2(x) = f_2(x)g_1(x)$ egyenlőségével értelmezzük. Könnyen látható, hogy $\simeq$ egy ekvivalencia reláció, amelynek az $(f(x), g(x))$ racionális törtet tartalmazó ekvivalencia osztályát az $\frac{f(x)}{g(x)}$ tört jelöli:

$$\frac{f_1(x)}{g_1(x)} = \frac{f_2(x)}{g_2(x)} \Longleftrightarrow f_1(x)g_2(x) = f_2(x)g_1(x).$$

Az ekvivalencia osztályokon az alábbiak szerint bevezetjük az összeadás (kivonás) és a szorzás műveletét:

$$\frac{f_1(x)}{g_1(x)} \pm \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)g_2(x) \pm f_2(x)g_1(x)}{g_1(x)g_2(x)} \ , \ \frac{f_1(x)}{g_1(x)} \cdot \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)f_2(x)}{g_1(x)g_2(x)}.$$

Könnyen igazolható, hogy a fenti műveletek megadása szabályos, azaz a műveletek eredményeként kapott osztály nem függ az ekvivalencia osztályokat képviselő $(f_1(x), g_1(x))$ és $(f_2(x), g_2(x))$ reprezentánsoktól. Ha $K(x)$ jelöli a racionális törtek $\frac{f(x)}{g(x)}$ ekvivalencia osztályainak halmazát, akkor a $K(x)$-en az előbbiek során értelmezett összeadás és szorzás rendelkezik a jól ismert asszociatív, kommutatív és disztributív tulajdonságokkal. Sőt a zérustól (ez most a $\frac{0}{1}$ osztály) különböző elemeknek a szorzásra nézve is létezik inverze: ha $\frac{f(x)}{g(x)} \neq \frac{0}{1}$, azaz ha $f(x) \neq 0$, akkor

$$\frac{f(x)}{g(x)} \cdot \frac{g(x)}{f(x)} = \frac{1}{1},$$

ahol $\frac{1}{1}$ a $K(x)$-beli szorzásra nézve egységelem. A $K(x)$ elemeit (ezek ekvivalencia osztályok) is szokás racionális törteknek nevezni. A $K[x] \subseteq K(x)$ tartalmazás nyilvánvaló, ha az $f(x) \in K[x]$ polinomot „azonosítjuk” az $\frac{f(x)}{1} \in K(x)$ ekvivalencia osztállyal (racionális törtel), amelyeket **racionális egész függvényeknek** is nevezünk.
Az $\frac{u(x)}{(p(x))^m}$ alakú **racionális törtet eleminek** nevezzük, ha a $p(x) \in K[x]$ polinom irreducibilis a K felett és az $u(x) \in K[x]$ polinom fokszámára $\deg(u(x)) \leq \deg(p(x)) - 1$ teljesül.♡

5.9.Tétel. *Legyen $K \subseteq \mathbb{C}$ egy számtest, tekintsük a konstanstól különböző és $0 \neq a_n \in K$ főegyütthatóval rendelkező $g(x) \in K[x]$ polinom K feletti*

$$g(x) = a_n(p_1(x))^{k_1}(p_2(x))^{k_2}...(p_t(x))^{k_t}$$

prímtényezős felbontását, ahol $p_i(x) \in K[x]$, $1 \le i \le t$ *irreducibilis polinomok 1 főegyütthatóval. Ekkor tetszőleges* $\frac{f(x)}{g(x)} \in K(x)$ *racionális tört megkapható egy racionális egész függvénynek és bizonyos* $\frac{u(x)}{(p_i(x))^m}$ *alakú elemi törtek összegeként.*

Bizonyítás. A $t \ge 1$ egészre vonatkozó teljes indukciót alkalmazunk. Ha $t = 1$, akkor legyen $v_0(x) \in K[x]$ és $u_0(x) \in K[x]$ az $\frac{1}{a_n}f(x)$ polinomnak a $p_1(x)$-el való maradékos osztásánál fellépő osztási hányados és maradék, ekkor

$$\frac{1}{a_n}f(x) = p_1(x)v_0(x) + u_0(x)$$

és $\deg(u_0(x)) \le \deg(p_1(x)) - 1$. Ha $v_1(x) \in K[x]$ és $u_1(x) \in K[x]$ a $v_0(x)$ polinomnak a $p_1(x)$-el való maradékos osztásánál fellépő osztási hányados és maradék, akkor

$$\frac{1}{a_n}f(x) = p_1(x)v_0(x) + u_0(x) = p_1(x)(p_1(x)v_1(x) + u_1(x)) + u_0(x) = (p_1(x))^2 v_1(x) + p_1(x)u_1(x) + u_0(x),$$

ahol $\deg(u_1(x)) \le \deg(p_1(x)) - 1$. A maradékos osztásokat folytatva (az elsőként fellépő $v_l(x) = 0$ zérus osztási hányadosig, amikor is $u_l(x) = v_{l-1}(x)$) jutunk el az $\frac{1}{a_n}f(x)$ polinomonak a $p_1(x)$ hatványaival való

$$\frac{1}{a_n}f(x) = u_l(x)(p_1(x))^l + u_{l-1}(x)(p_1(x))^{l-1} + ... + u_1(x)p_1(x) + u_0(x).$$

alakú felírásához, ahol $\deg(u_j(x)) \le \deg(p_1(x)) - 1$ minden $0 \le j \le l$ indexre. Most

$$\frac{f(x)}{g(x)} = \frac{\frac{1}{a_n}f(x)}{(p_1(x))^{k_1}} = \frac{u_l(x)(p_1(x))^l + u_{l-1}(x)(p_1(x))^{l-1} + ... + u_1(x)p_1(x) + u_0(x)}{(p_1(x))^{k_1}} =$$

$$= \frac{u_l(x)(p_1(x))^l}{(p_1(x))^{k_1}} + \frac{u_{l-1}(x)(p_1(x))^{l-1}}{(p_1(x))^{k_1}} + ... + \frac{u_0(x)}{(p_1(x))^{k_1}},$$

ahol a $j \ge k_1$ esetben

$$\frac{u_j(x)(p_1(x))^j}{(p_1(x))^{k_1}} = \frac{u_j(x)(p_1(x))^{j-k_1}}{1}$$

racionális egész függvény és a $j < k_1$ esetben

$$\frac{u_j(x)(p_1(x))^j}{(p_1(x))^{k_1}} = \frac{u_j(x)}{(p_1(x))^{k_1-j}}$$

elemi tört. Mivel racionális egészek összege újra racionális egész, ezért a $t = 1$ eset igazolását befejeztük.

Ha $t \ge 2$, akkor a $K[x]$-beli $b(x) = a_n(p_1(x))^{k_1}(p_2(x))^{k_2}...(p_{t-1}(x))^{k_{t-1}}$ és $c(x) = (p_t(x))^{k_t}$ polinomokra $g(x) = b(x)c(x)$ és az 5.5.Következmény szerint $\mathrm{lnko}(b(x), c(x)) = 1$. A 3.6.Tétel és az azt követő megjegyzés szerint léteznek olyan $v(x) \in K[x]$ és $w(x) \in K[x]$ polinomok, amelyekre

$$b(x)v(x) + c(x)w(x) = 1.$$

Így

$$\frac{f(x)}{g(x)} = \frac{f(x)(b(x)v(x) + c(x)w(x))}{b(x)c(x)} = \frac{f(x)v(x)}{c(x)} + \frac{f(x)w(x)}{b(x)},$$

ahol mindkét összeadandóra alkalmazva az indukciós feltevést megkapjuk az $\frac{f(x)}{g(x)}$ előállítását egy racionális egész és $\frac{u(x)}{(p_i(x))^m}$ alakú elemi törtek összegeként. Valóban, az $\frac{f(x)w(x)}{b(x)}$ nevezőjében szereplő polinom prímtényezős felbontásának $t-1$ különböző prímtényezője van, ezért $\frac{f(x)w(x)}{b(x)}$ megkapható egy racionális egész és olyan $\frac{u(x)}{(p_i(x))^m}$ alakú elemi törtek összegeként, ahol $1 \leq i \leq t-1$. Az $\frac{f(x)v(x)}{c(x)}$ nevezője egyetlen prímtényezőt tartalmaz $c(x) = (p_t(x))^{k_t}$, a $t = 1$ esetnél már láttuk, hogy $\frac{f(x)v(x)}{c(x)}$ megkapható egy racionális egész és $\frac{u(x)}{(p_t(x))^m}$ alakú elemi törtek összegeként.

□□□