4. IRREDUCIBILIS POLINOMOK

4.A.Definíció. Legyen $R \subseteq \mathbb{C}$ egy számgyűrű, ekkor a $p(x) \in R[x]$ polinomról azt mondjuk, hogy az R (**számgyűrű**) **felett reducibilis** (vagy azt, hogy $R[x]$**-ben reducibilis**), ha léteznek olyan $u(x) \in R[x]$ és $v(x) \in R[x]$ polinomok, amelyekre $\deg(u(x)) \geq 1$, $\deg(v(x)) \geq 1$ és $p(x) = u(x)v(x)$. Tehát egy reducibilis polinom legalább másodfokú. Ha a $p(x) \in R[x]$ konstanstól különböző polinom nem reducibilis az R felett, akkor azt mondjuk, hogy **irreducibilis** az R (**számgyűrű**) **felett** (vagy azt, hogy **irreducibilis** $R[x]$**-ben**). A konstans polinom nem reducibilis, de nem tekintjük irreducibilisnek sem. Minden elsőfokú polinom irreducibilis (bármilyen számgyűrű feltt).♡

4.1.Tétel (Schönemann-Eizenstein kritérium). *Legyen $q \geq 2$ olyan prímszám, amely osztója az egész együtthatós $p(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} + a_nx^n \in \mathbb{Z}[x]$ polinom $a_0, a_1, ..., a_{n-1} \in \mathbb{Z}$ együtthatóinak, továbbá q nem osztója az a_n és q^2 nem osztója az a_0 együtthatónak: $q \mid a_k$ minden $0 \leq k \leq n-1$ indexre, továbbá $q \nmid a_n$ és $q^2 \nmid a_0$. Ekkor a $p(x)$ polinom irreducibilis a $\mathbb{Z}$ számgyűrű felett.*

Bizonyítás. Amennyiben az

$$u(x) = b_0 + b_1x + ... + b_rx^r \in \mathbb{Z}[x] \text{ és } v(x) = c_0 + c_1x + ... + c_sx^s \in \mathbb{Z}[x]$$

polinomokra $\deg(u(x)) = r \geq 1$, $\deg(v(x)) = s \geq 1$ és $p(x) = u(x)v(x)$, akkor $n = r + s$, $a_n = b_rc_s$ és $a_0 = b_0c_0$. Mivel $q \nmid a_n$, ezért $q \nmid b_r$ és $q \nmid c_s$. A $q \mid a_0$ oszthatóság és $q^2 \nmid a_0$ miatt vagy $q \mid b_0$ és $q \nmid c_0$, vagy $q \mid c_0$ és $q \nmid b_0$ teljesül.
Az $u(x)$ és $v(x)$ egyenrangú szerepére való tekintettel elegendő az elsőként említett $q \mid b_0$ és $q \nmid c_0$ esettel foglalkozni. Tekintsük azt az $0 \leq i \leq r-1$ indexet, amelyre

$$q \mid b_0, q \mid b_1, ..., q \mid b_i \text{ és } q \nmid b_{i+1}$$

($q \mid b_0$ és $q \nmid b_r$ miatt ilyen i létezik). Az

$$a_{i+1} = b_0c_{i+1} + b_1c_i + ... + b_ic_1 + b_{i+1}c_0$$

egyenlőségből kapjuk, hogy

$$b_{i+1}c_0 = a_{i+1} - b_0c_{i+1} - b_1c_i - ... - b_ic_1,$$

ahonnan tekintettel a $q \mid b_0, q \mid b_1, ..., q \mid b_i$ és $q \mid a_{i+1}$ oszthatóságokra (az utóbbi $i+1 \leq r = n-s \leq n-1$ miatt igaz) a $q \mid b_{i+1}c_0$ eredményhez jutunk, ellentmondásban azzal, hogy $q \nmid b_{i+1}$ és $q \nmid c_0$.

□□□

4.B.Definíció. Az **egész együtthatós** $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x]$ **polinomról** azt mondjuk, hogy **primitív**, ha nem létezik olyan $d \geq 2$ egész szám, amelyik az a_k, $0 \leq k \leq n$ együtthatók mindegyikének osztója, azaz ha

$$\text{lnko}(a_0, a_1, ..., a_n) = 1.♡$$

4.2.Tétel (Gauss lemma). *Az $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x]$ és*

$g(x) = b_0 + b_1x + ... + b_mx^m \in \mathbb{Z}[x]$ *primitív polinomok* $f(x)g(x)$ *szorzata is primitív polinom.*

Bizonyítás. Az $f(x)$ primitív, ezért tetszőleges $q \geq 2$ prímszám esetén létezik olyan $0 \leq i \leq n$ index, amelyre

$$q \mid a_0, q \mid a_1, ..., q \mid a_{i-1} \text{ és } q \nmid a_i$$

(az $i = 0$ esetben ez $q \nmid a_0$ teljesülését jelenti). Mivel $g(x)$ is primitív, ezért létezik olyan $0 \leq j \leq m$ index, amelyre

$$q \mid b_0, q \mid b_1, ..., q \mid b_{j-1} \text{ és } q \nmid b_j$$

(a $j = 0$ esetben ez $q \nmid b_0$ teljesülését jelenti).
Nyilvánvaló, hogy az $f(x)g(x) = u_0 + u_1x + ... + u_{i+j}x^{i+j} + ... + u_{n+m}x^{n+m}$ szorzat polinom

$$u_{i+j} = a_0b_{i+j} + ... + a_{i-1}b_{j+1} + a_ib_j + a_{i+1}b_{j-1} + ... + a_{i+j}b_0$$

együtthatója nem osztható q-val. Valóban,

$$q \mid a_0b_{i+j} + ... + a_{i-1}b_{j+1} \text{ és } q \mid a_{i+1}b_{j-1} + ... + a_{i+j}b_0,$$

továbbá $q \nmid a_i$ és $q \nmid b_j$ miatt $q \nmid a_ib_j$ (itt felhasználtuk, hogy q prímszám). Tehát nem létezik olyan $q \geq 2$ prímszám, amely minden u_k, $0 \leq k \leq n + m$ együtthatónak osztója. Így azt kaptuk, hogy az $f(x)g(x)$ szorzat polinom is primitív.

□□□

4.3.Állítás. *Bármely zérustól különböző racionális együtthatós* $f(x) = r_0 + r_1x + ... + r_nx^n \in \mathbb{Q}[x]$ *polinom egyértelműen írható* $f(x) = \frac{a}{b}\widehat{f}(x)$ *alakban, ahol* $\widehat{f}(x) \in \mathbb{Z}[x]$ *primitív polinom, továbbá az* $a \geq 1$ *és* $b \geq 1$ *egész számok relatív prímek:* $\text{lnko}(a, b) = 1$.

Bizonyítás. Az $r_0, r_1, ..., r_n \in \mathbb{Q}$ racionális számokat felírhatjuk egész számok hányadosaként úgy, hogy egy alkalmas $t \geq 1$ egész számot használunk közös nevezőnek:

$$r_0 = \frac{u_0}{t}, r_1 = \frac{u_1}{t}, ..., r_n = \frac{u_n}{t}.$$

Legyen $d = \text{lnko}(u_0, u_1, ..., u_n) \geq 1$, ekkor

$$u_0 = dv_0, u_1 = dv_1, ..., u_n = dv_n$$

olyan $v_0, v_1, ..., v_n \in \mathbb{Z}$ egész számokkal, amelyekre

$$\text{lnko}(v_0, v_1, ..., v_n) = 1.$$

Így

$$f(x) = r_0 + r_1x + ... + r_nx^n = \frac{d}{t}(v_0 + v_1x + ... + v_nx^n) = \frac{a}{b}\widehat{f}(x),$$

ahol $\widehat{f}(x) = v_0 + v_1x + ... + v_nx^n \in \mathbb{Z}[x]$ primitív polinom és $d = sa$, $t = sb$ az $s = \text{lnko}(d, t) \geq 1$ legnagyobb közös osztóval, valamint az $a \geq 1$ és $b \geq 1$ relatív prím egészekkel ($\text{lnko}(a, b) = 1$). Amennyiben $f(x) = \frac{a'}{b'}g(x)$ teljesül az $a' \geq 1$ és $b' \geq 1$ relatív prím egészekre ($\text{lnko}(a', b') = 1$) és a $g(x) \in \mathbb{Z}[x]$ primitív polinomra, akkor az $\frac{a'}{b'}g(x) = \frac{a}{b}\widehat{f}(x)$ egyenlőségből $a'bg(x) = ab'\widehat{f}(x)$

következik. Ha $a'b \neq ab'$, akkor $a'b \geq 1$ és $ab' \geq 1$ miatt létezik olyan $q \geq 2$ prímszám, amely különböző kitevővel szerepel az $a'b$ és az ab' számok prímtényezős felbontásában. Ha ez a kitevő az $a'b$-ben nagyobb, akkor az $a'bg(x)$ és az $ab'\widehat{f}(x)$ polinomok együtthatóinak egyenlősége azt eredményezi, hogy az $\widehat{f}(x)$ polinom minden együtthatójának osztója q. Fordítva, ha ez a kitevő az ab'-ben nagyobb, akkor az együtthatók előbbi egyenlősége azt eredményezi, hogy a $g(x)$ polinom minden együtthatójának osztója q. Mindkét esetben ellentmondásba kerülünk azzal, hogy $\widehat{f}(x)$ és $g(x)$ primitívek. Tehát $a'b = ab'$, ahonnan $g(x) = \widehat{f}(x)$ és $\frac{a'}{b'} = \frac{a}{b}$ következik. Az utóbbi egyenlőség az $\text{lnko}(a, b) = 1$ és $\text{lnko}(a', b') = 1$ tulajdonságokkal rendelkező $a \geq 1$, $b \geq 1$, $a' \geq 1$, $b' \geq 1$ egészekre csak akkor teljesül, ha $a = a'$ és $b = b'$.

□□□

4.4.Tétel. *Ha az egész együtthatós $f(x) \in \mathbb{Z}[x]$ polinom reducibilis a $\mathbb{Q}$ számtest felett, akkor reducibilis a $\mathbb{Z}$ számgyűrű felett is. Másképpen fogalmazva: ha az egész együtthatós $g(x) \in \mathbb{Z}[x]$ polinom irreducibilis a $\mathbb{Z}$ számgyűrű felett, akkor irreducibilis a $\mathbb{Q}$ számtest felett is.*

Bizonyítás. Az $f(x)$ reducibilitása a $\mathbb{Q}$ felett azt jelenti, hogy $f(x) = u(x)v(x)$ teljesül olyan $u(x) \in \mathbb{Q}[x]$ és $v(x) \in \mathbb{Q}[x]$ polinomokra, amelyekre $\deg(u(x)) \geq 1$, $\deg(v(x)) \geq 1$. Tekintsük most a 4.3.Állításban megadott alakját a fenti polinomoknak:

$$f(x) = \frac{a}{b}\widehat{f}(x)\ ,\ u(x) = \frac{a'}{b'}\widehat{u}(x)\ ,\ v(x) = \frac{a''}{b''}\widehat{v}(x).$$

Mivel $f(x) \in \mathbb{Z}[x]$ egész együtthatós, ezért könnyen látható, hogy $b = 1$. Az eddigiek alapján

$$f(x) = \frac{a}{1}\widehat{f}(x) = \frac{a'a''}{b'b''}\widehat{u}(x)\widehat{v}(x) = \frac{r}{s}\widehat{u}(x)\widehat{v}(x),$$

ahol az $\frac{r}{s}$ tört $\frac{a'a''}{b'b''}$-nek az egyszerűsített alakja ($\frac{a'a''}{b'b''} = \frac{r}{s}$, $\text{lnko}(r, s) = 1$, $r \geq 1$, $s \geq 1$), továbbá a 4.2.Tétel szerint az $\widehat{u}(x)\widehat{v}(x)$ szorzat polinom primitív. Így a racionális együtthatós polinomok 4.3.Állításban megadott alakjának egyértelműsége miatt kapjuk, hogy

$$\widehat{f}(x) = \widehat{u}(x)\widehat{v}(x) \text{ és } r = a\ ,\ s = 1.$$

Az $\frac{a'a''}{b'b''} = r$ tört az $\text{lnko}(a', b') = 1$ és $\text{lnko}(a'', b'') = 1$ tulajdonságokkal rendelkező $a' \geq 1$,$b' \geq 1$, $a'' \geq 1$, $b'' \geq 1$ egészekkel csak úgy lehet egész szám, ha $\frac{a'}{b''}$ és $\frac{a''}{b'}$ egész számok. Tehát

$$f(x) = \frac{a'a''}{b'b''}\widehat{u}(x)\widehat{v}(x) = \left(\frac{a'}{b''}\widehat{u}(x)\right)\left(\frac{a''}{b'}\widehat{v}(x)\right),$$

ami $\frac{a'}{b''}\widehat{u}(x) \in \mathbb{Z}[x]$ és $\frac{a''}{b'}\widehat{v}(x) \in \mathbb{Z}[x]$ miatt $f(x)$ reducibilitását jelenti a $\mathbb{Z}$ számgyűrű felett.

□□□

4.5.Állítás. *Legyen $p(x) \in K[x]$ irreducibilis polinom a $K \subseteq \mathbb{C}$ számtest felett, ekkor az alábbiak teljesülnek.*

1. *$p(x)$-nek csak triviális osztói léteznek $K[x]$-ben: $h(x) \in K[x]$ és $h(x) \mid p(x)$ esetén $h(x) \sim 1$ vagy $h(x) \sim p(x)$.*

2. *Tetszőleges* $h(x) \in K[x]$ *polinomra vagy* $\text{lnko}(p(x), h(x)) = 1$, *vagy* $\text{lnko}(p(x), h(x)) = p^*(x)$.

3. *Tetszőleges* $h(x) \in K[x]$ *polinomra vagy* $\text{lnko}(p(x), h(x)) = 1$, *vagy* $p(x) \mid h(x)$.

4. *Amennyiben egy* $h(x) \in K[x]$ *polinomnak és* $p(x)$*-nek létezik közös gyöke, akkor* $p(x) \mid h(x)$.

5. *Ha a* $p(x) \mid f_1(x)f_2(x)...f_r(x)$ *oszthatóság teljesül az* $f_1(x), f_2(x), ..., f_r(x) \in K[x]$ *polinomokra, akkor* $p(x) \mid f_i(x)$ *valamelyik* $1 \leq i \leq r$ *indexre.*

6. *Ha egy* $h(x) \in K[x]$ *polinomra* $h(x) \sim p(x)$, *akkor* $h(x)$ *is irreducibilis a* K *számtest felett.*

Bizonyítás.

1. A $h(x) \mid p(x)$ oszthatóság azt jelenti, hogy $p(x) = h(x)q(x)$ valamilyen $q(x) \in \mathbb{C}[x]$ polinomra. A 3.5.Állítás 1.része szerint ilyenkor $q(x) \in K[x]$ is teljesül, ami $p(x)$-nek a K feletti irreducibilitására való tekintettel azt eredményezi, hogy a fokszámokra $\deg(h(x)) = 0$ vagy $\deg(q(x)) = 0$ teljesül. A $\deg(h(x)) = 0$ esetben $h(x) = c \neq 0$ konstans polinom, azaz $h(x) \sim 1$. A $\deg(q(x)) = 0$ esetben $\deg(p(x)) = \deg(h(x)) + \deg(q(x))$ miatt $\deg(h(x)) = \deg(p(x))$, ahonnan a 3.5.Állítás 4.része (és $h(x) \mid p(x)$) alapján $h(x) \sim p(x)$ következik.

2. Legyen $d(x) = \text{lnko}(p(x), h(x))$, ekkor $d(x) \in K[x]$ és $d(x) \mid p(x)$. Így a már igazolt 1.részt használva kapjuk, hogy a $d(x) \sim 1$ vagy a $d(x) \sim p(x)$ asszociált viszonyok valamelyike teljesül. Mivel $d(x)$ főegyüttható 1, ezért $d(x) = 1$ vagy $d(x) = p^*(x)$.

3. A már igazolt 2.rész szerint, ha $\text{lnko}(p(x), h(x)) \neq 1$, akkor $\text{lnko}(p(x), h(x)) = p^*(x)$. Az $\text{lnko}(p(x), h(x)) = p^*(x)$ esetben $p^*(x) \mid h(x)$, ahonnan $p(x) \mid p^*(x)$ miatt kapjuk a kívánt $p(x) \mid h(x)$ oszthatóságot.

4. Az $\text{lnko}(p(x), h(x)) = 1$ egyenlőség most nem teljesülhet, hiszen az 1 konstans polinomnak nincs gyöke és a 3.5.Állítás 9.része szerint a $p(x)$ és $h(x)$ polinomok bármely közös gyöke a legnagyobb közös osztójuknak is gyöke. Tehát a már igazolt 3.rész alapján a $p(x) \mid h(x)$ oszthatóság teljesül.

5. Nyilvánvalóan elegendő az $r = 2$ esettel foglalkozni: $p(x) \mid f_1(x)f_2(x)$. A már igazolt 3.rész szerint vagy $p(x) \mid f_2(x)$, vagy $\text{lnko}(p(x), f_2(x)) = 1$. Az utóbbi esetben a 3.8.Tétel 3.része a $p(x) \mid f_1(x)$ oszthatóságot garantálja.

6. Amennyiben $h(x)$ reducibilis K felett, akkor léteznek olyan $u(x) \in K[x]$ és $v(x) \in K[x]$ polinomok, amelyekre $\deg(u(x)) \geq 1$, $\deg(v(x)) \geq 1$ és $h(x) = u(x)v(x)$. Mivel a $h(x) \sim p(x)$ asszociáltság miatt $p(x) = ch(x)$ teljesül valamilyen $c \in \mathbb{C}$ számra (lásd a 3.5.Állítás 3.részét), ezért a $p(x) = ch(x) = (cu(x))v(x)$ felbontáshoz jutunk. A $p(x), h(x) \in K[x]$ tartalmazások miatt $c \in K$. Így $cu(x) \in K[x]$ és $\deg(cu(x)) = \deg(u(x)) \geq 1$ miatt ellentmondásba kerülünk $p(x)$ irreducibilitásával.

□□□

4.6.Tétel (az „algebra alaptétele"). *Tetszőleges* $\deg(f(x)) \geq 1$ *tulajdonságú* $f(x) \in \mathbb{C}[x]$ *polinomnak létezik gyöke* $\mathbb{C}$*-ben, azaz van olyan* $\alpha \in \mathbb{C}$ *komplex szám, amelyre* $f(\alpha) = 0$.

Megjegyzés. Az Algebra Alaptételének több bizonyítása ismert, itt ezek egyikét sem közöljük. Mindegyik bizonyítás analízisbeli eredményekre támaszkodik, még a leginkább algebrainak tekinthető bizonyításban is szükség van arra a folytonos valós függvényekkel kapcsolatos észrevételre, hogy egy páratlan fokszámú valós együtthatós polinomnak létezik valós gyöke.

4.7.Tétel. *A* $p(x) \in \mathbb{C}[x]$ *polinom pontosan akkor irreducibilis a* $\mathbb{C}$ *számtest felett, ha* $\deg(p(x)) = 1$.

Bizonyítás. Ha $\deg(p(x)) = 1$, akkor már a 4.A.Definícióban megjegyeztük, hogy $p(x)$ irreducibilis. Ha $\deg(p(x)) \geq 2$, akkor a 4.6.Tétel szerint létezik a $p(x)$ polinomnak valamilyen $\alpha \in \mathbb{C}$ gyöke: $p(\alpha) = 0$. A 3.4.Állítást (Bezout tételét) alkalmazva kapjuk az $x - \alpha \mid p(x)$ oszthatóságot, tehát $p(x) = (x-\alpha)q(x)$ az $x-\alpha \in \mathbb{C}[x]$ és valamilyen $q(x) \in \mathbb{C}[x]$ polinomra. Most $\deg(p(x)) = \deg(x - \alpha) + \deg(q(x))$, ahonnan $\deg(q(x)) \geq 1$ adódik, ami azt jelenti, hogy $p(x)$ reducibilis a $\mathbb{C}$ számtest felett.

□□□

4.8.Tétel. *A* $p(x) \in \mathbb{R}[x]$ *polinom pontosan akkor irreducibilis az* $\mathbb{R}$ *számtest felett, ha* $\deg(p(x)) = 1$ *vagy* $\deg(p(x)) = 2$ *és* $p(x)$*-nek nincs valós (*$\mathbb{R}$*-beli) gyöke.*

Bizonyítás. Ha $\deg(p(x)) = 1$, akkor már a 4.A.Definícióban megjegyeztük, hogy $p(x)$ irreducibilis. Ha $\deg(p(x)) = 2$ és $p(x)$-nek nincs valós ($\mathbb{R}$-beli) gyöke, akkor a $p(x) = u(x)v(x)$ egyenlőség a $\deg(u(x)) \geq 1$ és $\deg(v(x)) \geq 1$ tulajdonságú $u(x), v(x) \in \mathbb{R}[x]$ polinomokra $\deg(p(x)) = \deg(u(x)) + \deg(v(x))$ miatt csak úgy teljesülhet, ha $\deg(u(x)) = \deg(v(x)) = 1$. Az $u(x) \in \mathbb{R}[x]$ elsőfokú polinomnak van valós ($\mathbb{R}$-beli) gyöke, ami nyilvánvalóan gyöke $p(x)$-nek is. A kapott ellentmondást az okozta, hogy a $p(x)$-ről feltételeztük, hogy reducibilis az $\mathbb{R}$ számtest felett.
Ha $\deg(p(x)) \geq 2$ és $p(x)$-nek létezik valós $\alpha \in \mathbb{R}$ gyöke, akkor a 3.4.Állítást (Bezout tételét) alkalmazva kapjuk az $x - \alpha \mid p(x)$ oszthatóságot, tehát $p(x) = (x - \alpha)q(x)$ az $x - \alpha \in \mathbb{R}[x]$ és valamilyen $q(x) \in \mathbb{C}[x]$ polinomra. Mivel $p(x) \in \mathbb{R}[x]$, ezért a 3.5.Állítás 1.része szerint ilyenkor $q(x) \in \mathbb{R}[x]$ is teljesül. Most $\deg(p(x)) = \deg(x - \alpha) + \deg(q(x))$, ahonnan $\deg(q(x)) \geq 1$ adódik, ami azt jelenti, hogy $p(x)$ reducibilis az $\mathbb{R}$ számtest felett.
Ha $\deg(p(x)) \geq 3$ és $p(x)$-nek nem létezik valós gyöke, akkor a 4.6.Tétel szerint létezik komplex $\alpha \in \mathbb{C}$ gyöke: $p(\alpha) = 0$. Mivel $\alpha \notin \mathbb{R}$, ezért $\overline{\alpha} \neq \alpha$ (itt $\overline{\alpha} \in \mathbb{C}$ az α konjugáltját jelöli). A $p(x) = c_0 + c_1x + ... + c_nx^n$ polinomnak $\overline{\alpha}$ is gyöke, hiszen a $c_k \in \mathbb{R}$, $0 \leq k \leq n$ együtthatókra $\overline{c}_k = c_k$, továbbá a konjugálásnak az 1.2.Állítás 4.részében leírt tulajdonságait felhasználva kapjuk, hogy $(\overline{\alpha})^k = \overline{\alpha^k}$ és

$$p(\overline{\alpha}) = c_0 + c_1\overline{\alpha} + ... + c_n(\overline{\alpha})^n = \overline{c}_0 + \overline{c}_1\overline{\alpha} + ... + \overline{c}_n\overline{\alpha^n} =$$

$$= \overline{c}_0 + \overline{c_1\alpha} + ... + \overline{c_n\alpha^n} = \overline{c_0 + c_1\alpha + ... + c_n\alpha^n} = \overline{p(\alpha)} = \overline{0} = 0.$$

Ismét a 3.4.Állítást (Bezout tételét) alkalmazva kapjuk az $(x-\alpha)(x-\overline{\alpha}) \mid p(x)$ oszthatóságot, tehát $p(x) = (x-\alpha)(x-\overline{\alpha})q(x)$ teljesül valamilyen $q(x) \in \mathbb{C}[x]$ polinomra. Mivel az

$$(x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha + \overline{\alpha}) + \alpha\overline{\alpha}$$

polinom együtthatói valós számok ($\alpha + \overline{\alpha}, \alpha\overline{\alpha} \in \mathbb{R}$), ezért $(x-\alpha)(x-\overline{\alpha}) \in \mathbb{R}[x]$. A $p(x) \in \mathbb{R}[x]$ tartalmazásra és a 3.5.Állítás 1.részére való tekintettel $q(x) \in \mathbb{R}[x]$ is teljesül. Most $\deg(p(x)) = \deg((x-\alpha)(x-\overline{\alpha})) + \deg(q(x))$, ahonnan $\deg(p(x)) \geq 3$ figyelembe vételével $\deg(q(x)) \geq 1$ adódik. Tehát $p(x)$ reducibilis az $\mathbb{R}$ számtest felett.

□□□