

1. Véges testek

Véges test elemszáma

6.7.2. Következmény

Minden véges test elemszáma *prímhatvány*.

Bizonyítás

Legyen T karakterisztikája p , prímteste P , és $|T : P| = n$.

Ekkor T elemei egyértelműen írhatók $\lambda_1 b_1 + \dots + \lambda_n b_n$ alakban, ahol b_1, \dots, b_n bázis T -ben P fölött, és $\lambda_1, \dots, \lambda_n \in P$. Mindegyik λ_i skalár $|P| = p$ -féle lehet, így $|T| = p^n$. \square

Megjegyzés

A $\lambda_1 b_1 + \dots + \lambda_n b_n \mapsto (\lambda_1, \dots, \lambda_n)$ megfeleltetés nyilván *összegtartó*. Ezért T additív csoportja izomorf a $\mathbb{Z}_p^+ \times \dots \times \mathbb{Z}_p^+$ n -tényezős direkt szorzattal.

Véges test multiplikatív csoportja

4.3.22. Tétel

Minden véges test multiplikatív csoportja *ciklikus*.

Bizonyítás

Legyen T elemszáma $k + 1$, azaz $|T^\times| = |T - \{0\}| = k$. Az $x^d - 1$ polinomnak legfeljebb d gyöke van T -ben. Így ha $g \in T^\times$ rendje d , akkor e gyökök éppen g hatványai. Speciálisan minden d rendű elem g -nek hatványa! A $\langle g \rangle$ ciklikus részcsoporthoz $\varphi(d)$ darab d rendű elem van. Vagyis a d rendű elemek száma T^\times -ben $\varphi(d)$ vagy 0. Ha $d \nmid k$, akkor nincs d rendű elem Lagrange tétele miatt. Az $x^k - 1 = \prod_{d|k} \Phi_d(x)$ -ben a fokokat véve $\sum_{d|k} \varphi(d) = k$. Ez csak úgy lehet, ha minden $d \mid k$ -ra van d rendű elem! Speciálisan van k rendű elem, azaz T^\times ciklikus. \square

Véges test egyértelműsége

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig legfeljebb egy darab q elemű test létezik.

Bizonyítás

Legyen K egy q elemű test, prímteste $P \cong \mathbb{Z}_p$. Nyilván K^\times elemszáma $q - 1$. Lagrange tétele miatt így $g \neq 0$ esetén $g^{q-1} = 1$. Ezért K minden eleme gyöke $x^q - x \in P[x]$ -nek. Mivel K összes eleme generálja K -t, ezért K az $x^q - x$ felbontási teste P fölött. A felbontási test egyértelmű (6.4.9. Következmény), és így bármely két q elemű test izomorf. \square

Megjegyzés: $q = p$ esetén a kis Fermat-tételt kaptuk: $x^p \equiv x \pmod{p}$.

Többszörös gyökök és a derivált

3.6.1. Definíció

Ha R szokásos gyűrű, akkor $f(x) = a_0 + \dots + a_n x^n \in R[x]$ (formális) *deriváltja* $f'(x) = a_1 + 2a_2 x + \dots + na_n x^{n-1}$.

HF: Érvényesek a deriválás szokásos azonosságai.

3.6.3. Állítás

Ha $f \in R[x]$ -nek $b \in R$ legalább k -szoros gyöke ($k \geq 1$), akkor b az f' deriválnak legalább $k - 1$ -szeres gyöke.

Bizonyítás

$$f(x) = (x - b)^k g(x) \implies f'(x) = (x - b)^{k-1} [kg(x) + (x - b)g'(x)].$$

Megjegyezzük, hogy ha b pontosan k -szoros gyöke f -nek, akkor pontosan $k - 1$ -szeres gyöke f' -nek, kivéve ha $kg(b) = 0$. \square

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímszámra izomorfa erejéig pontosan egy darab q elemű test létezik. Jele \mathbb{F}_q .

Bizonyítás

Legyen K az $x^q - x$ felbontási teste \mathbb{Z}_p fölött (ez létezik a 6.4.5. Következmény miatt). Jelölje L az $x^q - x$ gyökeinek halmazát K -ban. Ez résztest, mert $(a + b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a K -ban (hiszen $x \rightarrow x^q$ a Frobenius-endomorfizmus k -adik hatványa). Az L elemszáma q , mert $x^q - x$ -nek nincs többszörös gyöke. Ha ugyanis lenne, akkor az gyöke lenne a deriváltjának is. De $x^q - x \in \mathbb{Z}_p[x]$ deriváltja $qx^{q-1} - 1 = -1$, hiszen $p \mid q$. A -1 konstans polinomnak pedig nincs gyöke K -ban. \square

Véges test résztestei

6.7.8. Tétel

Ha $K \leq L$ véges testek, akkor ez a bővítés normális. A $q = p^n$ elemű \mathbb{F}_q testnek minden $k \mid n$ esetén egyetlen \mathbb{F}_{p^k} -val izomorf részteste van, más részteste pedig nincs. Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

Bizonyítás

Ha $L = \mathbb{F}_q$, akkor L az $x^q - x$ felbontási teste K fölött is. A szorzástétel miatt $k = |K : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$ -nek. Láttuk, hogy K elemei pontosan az $x^{p^k} - x$ gyökei. Ezért K az egyetlen p^k elemű résztest.

Megfordítva, $k \mid n$ esetén $p^k - 1 \mid p^n - 1 = |\mathbb{F}_q^\times|$. Mivel L^\times ciklikus, $x^{p^k - 1} - 1$ -nek $p^k - 1$ gyöke van L -ben. Ezek a nullával együtt p^k elemű résztestet alkotnak. \square

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik \mathbb{Z}_p fölött irreducibilis n -edfokú f polinom. Minden ilyen f polinomnak \mathbb{F}_{p^n} a felbontási teste, és $f(x) \mid x^{p^n} - x$.

Bizonyítás

Mivel $\mathbb{F}_{p^n}^\times$ ciklikus, van $p^n - 1$ rendű α eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.

Ezért az irreducibilis m_α foka $|\mathbb{F}_{p^n} : \mathbb{Z}_p| = n$.

Ha $f \in \mathbb{Z}_p[x]$ egy n -edfokú, irreducibilis polinom, akkor bővítsünk ennek egy β gyökével: $K = \mathbb{Z}_p(\beta)$ és $|K| = p^n$. Mivel $\mathbb{Z}_p \leq K$ normális, a K az f felbontási teste \mathbb{Z}_p fölött. A β közös gyöke f -nek és $x^{p^n} - x$ -nek, így $f(x) \mid x^{p^n} - x$ (hiszen f a β minimálpolinomja \mathbb{Z}_p fölött). \square

A nyolcelemeű test példája

\mathbb{Z}_2 fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$. Ezek irreducibilisek \mathbb{Z}_2 fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az \mathbb{F}_8 elemei az $x^8 - x$ polinom összes gyökei. Az egyetlen valódi résztest a prímtest: $\{0, 1\}$. A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$. A $\psi : z \mapsto z^2$ Frobenius-endorfizmus bijektív, mert magja $\{0\}$. Ez permutálja $x^3 + x + 1$ és $x^3 + x^2 + 1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$ és $E = 1 + (x^3+x+1)$; ekkor $\{O, E\}$ a prímtest. $A = x + (x^3+x+1)$ gyöke $Ex^3 + Ex + E$ -nek. A másik két gyök $A^2 = x^2 + (x^3+x+1)$ és $A^4 = x^2 + x + (x^3+x+1)$. A maradék három elem $Ex^3 + Ex^2 + E$ -nek lesz gyöke, ezek $A + E$, $A^2 + E$, $A^2 + A + E$.

Primitív polinomok

6.7.11. Definíció

Ha K véges test, akkor egy irreducibilis $f \in K[x]$ *primitív polinom*, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját.

(NEM azonos fogalom a $\mathbb{Z}[x]$ -beli primitív polinommal!)

9.3.9. Példa: Legyen $K = \mathbb{F}_{16}$, elemei $x^{16} - x$ gyökei. $|K : \mathbb{Z}_2| = 4$, az egyetlen valódi résztest \mathbb{F}_4 , ez $x^4 - x$ gyökeiből áll. Ezért a harmadrendű elemek között minimálpolinomja $x^2 + x + 1$. Ha $g \notin \mathbb{F}_4$, akkor $\mathbb{Z}_2(g) = K$, és ezért $\text{gr}(m_g) = 4$.

Ha g ötödrendű, akkor $x^5 - 1$ -nek is gyöke, így minimálpolinomja $x^4 + x^3 + x^2 + x + 1$, melynek többi gyöke g^2 , g^4 és g^8 .

A másik két negyedfokú irreducibilis gyökei a 15 rendű elemek, ezek primitív polinomok: $x^4 + x + 1$ és $x^4 + x^3 + 1$.

2. Algebrák test fölött

Az algebra fogalma

5.10.3. Definíció

A *algebra* a T test fölött, ha egyszerre gyűrű, vektortér T fölött, és $\lambda(ab) = (\lambda a)b = a(\lambda b)$ minden $a, b \in A$ és $\lambda \in T$ esetén.

Legyen R egységelemes gyűrű, T részteste R -nek, és $1_R = 1_T$. Az R akkor algebra T fölött, ha $\lambda r = r\lambda$ ($\forall \lambda \in T, \forall r \in R$). (A T egy elemével, mint skalárral való szorzás az R -beli szorzás.)

Példák

- A $T[x_1, \dots, x_n]$ polinomgyűrű a T test fölött.
- Ha $K \leq L$ testbővítés, akkor L a K fölött.
- A T test fölötti $n \times n$ -es mátrixok.
- A T test fölötti V vektortér lineáris transzformációi.
- A kvaterniók ferdeteste \mathbb{R} fölött.

Algebra elemének minimálpolinomja

5.10.6. Definíció

Ha A algebra a T test fölött, $f(x) = a_0 + a_1x + \dots + a_nx^n \in T[x]$ és $b \in A$, akkor $f(b) = a_01_A + a_1b + \dots + a_nb^n$ (behelyettesítés).

Tehát f konstans tagját A egységelemével szorozzuk.

5.10.7. Gyakorlat: $f(a) + g(a) = (f + g)(a)$ és $(fg)(a) = f(a)g(a)$.

5.10.8, 5.10.11. Definíció

Az $f \in T[x]$ *jó polinomja* $b \in A$ -nak, ha $f(b) = 0$. Ezek egy I ideált alkotnak, ami az $f \mapsto f(b)$ homomorfizmus magja. Ha $I = \{0\}$, akkor b *transzcendens*, különben *algebrai*. Ekkor I normált generátoreleme a $b \in A$ *minimálpolinomja*, jele m_b .

Az m_b létezik, mert $T[x]$ euklideszi, és így főideálgyűrű. Nyilván $f(b) = 0 \iff m_b \mid f$, vagyis a jó polinomok a minimálpolinom többszörösei.

A minimálpolinom irreducibilitása

5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

Valóban: ha $\dim_T(A) = n$, akkor $1, b, \dots, b^n$ már összefügg:

$\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$, ekkor f nem 0, és b gyöke f -nek. □

5.10.12. Tétel

Legyen A nullosztómentes algebra és $b \in A$ algebrai elem. Ekkor b minimálpolinomja irreducibilis T fölött.

Ha $f \in T[x]$ normált, irreducibilis és $f(b) = 0$, akkor $f = m_b$.

Valóban: ha $m_b = gh$, akkor $0 = m_b(b) = g(b)h(b)$. Ezért vagy $g(b) = 0$ (így $m_b \mid g$ miatt h egység), vagy $h(b) = 0$ és g egység.

Megfordítva: ha $f(b) = 0$, akkor $m_b \mid f$, de mindkettő irreducibilis és normált, ezért egyenlők. \square

3. A számfogalom lezárása

Frobenius tétele

5.11.6. Tétel, NB

Ha A véges dimenziós, nullosztómentes, nem nulla algebra \mathbb{R} fölött, akkor A vagy a valós számtesttel, vagy a komplex számtesttel, vagy a kvaterniók ferdetestével izomorf.

Vagyis a számkört nem lehet már tovább bővíteni, ha a nullosztómentességet és az asszociativitást megtartjuk.

A Frobenius-tétel feltételei szükségesek (5.11.1. Gyakorlat)

- Ha nem \mathbb{R} fölött vagyunk: \mathbb{Q} véges bővítései mind nullosztómentesek és véges dimenziósak (pl. $\mathbb{Q}(\sqrt[3]{2})$).
- $\mathbb{R}[x]$ nullosztómentes, \mathbb{R} fölötti, de nem véges dimenziós. Sőt, \mathbb{R} egyszerű transzcendens bővítése még test is.
- $\mathbb{R}^{3 \times 3}$ véges dimenziós, \mathbb{R} fölötti, de nem nullosztómentes.

A polinomok azonossági tétele

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!

Magyarázat: $x^2 + 1 = (x + i)(x - i)$ a „gyöktényezős alak”. Ide $j \in \mathbb{K}$ -t helyettesítve a bal oldal nulla lesz, de a jobb oldal nem:

$$(j + i)(j - i) = j^2 + ij - ji - i^2 = ij - ji = 2k \neq 0.$$

Az a gond, hogy i és j nem felcserélhetők. Nem tudjuk így kihasználni, hogy \mathbb{K} nullosztómentes.

5.11.5. Következmény

Az $x^2 + 1$ polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1, vagyis a $qi + rj + sk$ alakú kvaterniók, ahol $q^2 + r^2 + s^2 = 1$.

Valóban, ha $N(z) = 1$ és $\bar{z} = -z$, akkor $z^2 = -z\bar{z} = -N(z) = -1$.

Megfordítva: ha $z^2 = -1$, akkor $1 = N(z^2) = N(z)^2$, így $N(z) = 1$. Ezért $1 = z\bar{z} = -z^2$. Innen $z \neq 0$ miatt $\bar{z} = -z$. \square

4. A kvaterniók alkalmazásai

Kvaterniók és térvektorok

Tiszta kvaternió: $v = xi + yj + zk$ (valós része nulla). Azonosítsuk ezzel az $(x, y, z)^T \in \mathbb{R}^3$ vektort. Legyen $z = r + v$ ($r \in \mathbb{R}$).

- Ha $N(z) = 1$, akkor $z^{-1} = \bar{z}$. Ha z tiszta is, akkor $z^{-1} = -z$.
- Ha v és w tiszta kvaterniók, akkor $vw = v \times w - \langle v, w \rangle$ (vektoriális, illetve skaláris szorzat), mert $i^2 = j^2 = k^2 = -1$, továbbá $ij = i \times j$, $ji = j \times i$, $jk = j \times k$, stb.
- Így ha $v \perp w$, akkor $vw = v \times w = -w \times v = -wv$, ahonnan $w^{-1}vw = -v$, és $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \bar{z}$. Balról zw -vel szorozva $zw\bar{z} = z^2w$.
- Tehát ha $N(z) = 1$ és $v \perp w$, akkor $zww^{-1} = z^2w$.
Speciálisan ha $z = \cos \alpha + v \sin \alpha$, ahol $N(v) = 1$, akkor $v^2 = -1$ (mert v tiszta), $z^2 = \cos(2\alpha) + v \sin(2\alpha)$, és így $zww^{-1} = \cos(2\alpha)w + \sin(2\alpha)vw = \cos(2\alpha)w + \sin(2\alpha)(v \times w)$.
Ha $N(w)$ is 1, akkor v, w és $v \times w$ ONB a térben. \square

Kvaterniók és forgatások

Tétel

A térbeli, origón átmenő egyenesek körüli forgatások a(z 1 normájú) kvaterniókkal való konjugálások. Pontosabban:

ha v egységvektor, akkor a $z = \cos \alpha + v \sin \alpha$ -val való konjugálás 2α szögű forgatás a v irányú egyenes körül.

Bizonyítás

Legyen w egy v -re merőleges egységvektor. Írjuk föl a z -vel való konjugálás mátrixát a $v, w, vw = v \times w$ ONB-ben. Nyilván $zvwz^{-1} = v$ (hiszen $zv = vz$), és az iménti képletek alapján

$zww^{-1} = \cos(2\alpha)w + \sin(2\alpha)(vw)$. A kettőt összeszorozva $z(vw)z^{-1} = (zvwz^{-1})(zww^{-1}) = \cos(2\alpha)(vw) + \sin(2\alpha)v(vw)$, ahol $v(vw) = v^2w = -w$ (már láttuk, hogy $v^2 = -1$).

Ezért a megfelelő forgatás mátrixát kapjuk. \square

Euler-mátrix

Az előző bizonyításban kapott mátrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\alpha) & -\sin(2\alpha) \\ 0 & \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}$$

Az i, j, k bázisban, $z = r + xi + yj + zk$ esetén (*Euler-mátrix*):

$$\begin{pmatrix} r^2 + x^2 - y^2 - z^2 & -2rz + 2xy & 2ry + 2xz \\ 2rz + 2xy & r^2 - x^2 + y^2 - z^2 & -2rx + 2yz \\ -2ry + 2xz & 2rx + 2yz & r^2 - x^2 - y^2 + z^2 \end{pmatrix}$$

Előnyök:

Csak négy paraméter; numerikusan stabil; effektív.

Forgástengely folytonos változtatása (3D játékok grafikája).

Navigáció, aerodinamika, molekuláris dinamika, röntgenkristallográfia.

Számelméleti alkalmazások.

5. Csoportelméleti vonatkozások

A kvaterniók mint transzformációk

A kvaterniók vektortér \mathbb{C} fölött (a skalárral szorzás balszorzás).

FIGYELEM: ez *NEM* algebra \mathbb{C} fölött, mert $i(j1) \neq j(i1)$.

Legyen A_z a $z \in \mathbb{K}$ -val való jobbszorzás \mathbb{K} -n: $A_z(x) = xz$. Ez összegetartó.

Skalárszorostartó is az asszociativitás miatt: $A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$

(ahol $\lambda \in \mathbb{C}$ és $x \in \mathbb{K}$). Továbbá $A_{z_1 z_2}(x) = x(z_1 z_2) = (x z_1) z_2 = A_{z_2} A_{z_1}(x)$.

Azaz a $\psi : z \mapsto A_z$ leképezésre $\psi(z_1 z_2) = \psi(z_2) \psi(z_1)$.

Kellemetlen: megfordul a szorzás sorrendje. Megoldás: legyen $\psi(z) = A_{\bar{z}}$.

Erre $\psi(z_1 z_2) = \psi(z_1) \psi(z_2)$, hiszen $\overline{z_1 z_2} = \bar{z}_2 \bar{z}_1$.

Továbbá $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$, azaz ψ gyűrűhomomorfizmus.

Végül ψ injektív: ha $\psi(z) = 0$, akkor $0 = \psi(z)(1) = 1\bar{z}$, így $z = 0$.

Tehát a \mathbb{K} gyűrű izomorf $\text{Hom}(\mathbb{C}^2)$ egy részgyűrűjével.

Ha $z = p + qi + rj + sk$, akkor $\psi(z)$ mátrixa az $(1, j)$ bázisban $\begin{pmatrix} v & w \\ -\bar{w} & \bar{v} \end{pmatrix}$ ahol $v = p + qi$ és $w = r + si$ (így vezettük be \mathbb{K} -t).

A speciális unitér csoport

Ha $0 \neq v, w \in \mathbb{C}^2$ hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami v -t w -be viszi.

Bizonyítás

Tegyük föl, hogy van kettő: $B(v) = C(v)$. Legyen $D = B^{-1}C$, ekkor $D(v) = v$.

Ha u egy v -re merőleges egységvektor, akkor $D(u) \perp D(v) = v$, és így $D(u) \parallel u$.

A (v, u) bázisban $\det(D)$ -t felírva $D(u) = u$, azaz D az identitás, és így $B = C$.

Legyen $b_1 = v/\|v\|$, $c_1 = w/\|w\|$, és $(b_1, b_2), (c_1, c_2)$ ONB.

Előírhatósági tétel: van B , melyre $B(b_1) = c_1$ és $B(b_2) = \varepsilon c_2$.

Alkalmas $|\varepsilon| = 1$ -re B unitér, 1 determinánsú és $B(v) = w$. □

Jelölje $\text{SU}(2)$ a 2×2 -es, komplex elemű, 1 determinánsú *unitér* mátrixok csoportját a szorzásra (4.1.26. Definiáció).

Elnevezés: $\text{SU}(2)$ *regulárisan* hat az egységvektorok halmazán.

Az egységkvaterniók csoportja

Tétel

Az 1 normájú kvaterniók multiplikatív csoportja izomorf $SU(2)$ -vel.

Bizonyítás

Ha $z \in \mathbb{K}$, akkor láttuk, hogy $\psi(z) = A_{\bar{z}}$ mátrixa $\begin{pmatrix} v & w \\ -\bar{w} & \bar{v} \end{pmatrix}$, melynek determi-

nánása $N(z)$ és adjungáltja A_z mátrixa.

Ha $N(z) = 1$, akkor tehát $\psi(z)$ unitér és determinánása 1.

Megfordítás: Tegyük föl, hogy A unitér, 1 determinánúsú \mathbb{K} -n.

Legyen $z = \overline{A(1)}$, ekkor $A(1) = \bar{z} = 1\bar{z} = A_{\bar{z}}(1)$.

Ezért az imént bizonyított állítás miatt $A = A_{\bar{z}}$. \square

Az $SU(2)$ -t $Spin(3)$ csoportnak nevezik a kvantumfizikában. Fermionok (pl. neutron) leírására használják.

Miért kétszereződik a szög?

Tétel

$SU(2)/\{1, -1\} \cong SO(3)$ (a térbeli forgatások csoportja).

Bizonyítás

Legyen $z = \cos \alpha + v \sin \alpha$, ahol v egységvektor.

Láttuk: $F_z : w \rightarrow zwz^{-1}$ a v irányú egyenes körüli 2α szögű forgatás.

Nyilván $\varphi : z \rightarrow F_z$ homomorfizmus, melynek magja $\{1, -1\}$. \square

Algebrai magyarázat: a $zwz^{-1} = z^2w$ képlet, ha $v \perp w$.

Geometriai magyarázat: a $z \mapsto F_z$ homomorfizmus magja kételemű. Ezért $SU(2)$ az $SO(3)$ minden elemét kétszer „fedí le”.

Tekintsük az $f : \alpha \rightarrow z$ függvényt, miközben v fix, pl. $v = i$. Ha $0 \leq \alpha \leq 2\pi$, akkor $f(\alpha)$ végighalad a komplex egységkörön. De $\varphi(f(\alpha))$ kétszer halad körbe, már π -nél az identitás, és ezért kétszeres „sebességgel” halad.