1. A hatványok száma

Komplex szám rendje

A -1-nek két darab egész kitevőjű hatványa van: -1 és 1.

Az i-nek 4 van: i, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.
Innentől kezdve ismétlődik: $i^5 = i$, $i^6 = i^2 = -1$, stb.
Négyesével periodikus, csak a kitevő négyes maradéka számít.
Képletben: ha $n = 4q + r$, akkor $i^n = i^r$ (mert $i^{4q} = (i^4)^q = 1$).

Hasonlóan $-i$ hatványai $-i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1$.
Ezek is négyesével ismétlődnek (és ugyanazok, mint az előbb).

Definíció (K1.5.7)
A $0 \neq z \in \mathbb{C}$ *rendje* az egész kitevős hatványainak a száma.
Ez pozitív egész, vagy a ∞ szimbólum. Jele: $o(z)$.

Tehát $o(-1) = 2, \quad o(i) = 4, \quad o(-i) = 4$.

Szám rendje mod m

Az 9 hatványai mod 28: 9, $9^2 = 81 \equiv 25$ (28), $9^3 = 9 \cdot 25 \equiv 1$ (28).
Innentől ismétlődik: $9^4 \equiv 9 \cdot 9^3 \equiv 9$ (28), $9^5 \equiv 9 \cdot 9 \equiv 25$ (26), stb.
Hármasával periodikus, csak a kitevő hármas maradéka számít.
Képletben: ha $n = 3q + r$, akkor $9^n \equiv 9^r$ (28) (mert $9^{3q} = (9^3)^q \equiv 1$ (28)).

Viszont 2 nagyobb hatványai már nem adnak 2-t mod 28
mert mind oszthatók 4-gyel.

Definíció (FGy3.2.1)
Ha $(a, m) = 1$, akkor *a rendje mod m* az egész kitevős, páronként mod m inkongruens hatványainak a száma. Ez pozitív egész. Jele: $o_m(a)$.

Tehát $o_{28}(9) = 3, \quad o_{28}(2)$ nem értelmes.

Csoportelem rendje

A nem nulla komplex számok csoportja a szorzásra $\mathbb{C}^\times$.
A $\mathbb{Z}_m$ gyűrű m-hez relatív prím elemeinek csoportja a szorzásra $\mathbb{Z}_m^\times$.

K4.3.9. Definíció, K4.3.10. Gyakorlat
Egy g csoportelem *rendje* a különböző hatványainak száma.
Jele: $o(g)$. Ez pozitív egész, vagy a ∞ szimbólum.

Ha a művelet jele $+$, akkor hatvány helyett többszörösről beszélünk.

Példák
$\mathbb{C}^\times$-ben $\pm i$ rendje 4.
$\mathbb{Z}_{28}^\times$-ben 9 rendje 3.
$G = \mathbb{Z}_6^+$. Ekkor $o(4) = 3$, mert többszörösei 4, $8 \equiv 2$, $12 \equiv 0$.
$G = \mathbb{R}^+$. Ekkor 3 rendje végtelen: 3, 6, 9, ...
Az $\mathbb{R}^+$ csoportban csak a 0 véges rendű, a 0 rendje 1.

A jó kitevők létezése

Definíció (K1.5.6, 4.3.9)
Az n egész szám *jó kitevője* a g csoportelemnek, ha $z^n = 1$ (a csoport egységeleme).

Például i és $-i$ jó kitevői $\mathbb{C}^\times$-ben a néggyel osztható egész számok.

Tétel (K1.5.8)
Legyen $g \in G$ egy csoportelem. Ha g-nek van két egyenlő hatványa, akkor van pozitív jó kitevője.

Bizonyítás
Tegyük föl, hogy $g^k = g^\ell$, de $k \neq \ell$. Ekkor $g^{k-\ell} = g^{\ell-k} = 1$. Mivel a $k-\ell$ és $\ell-k$ jó kitevők egyike pozitív, ezért g-nek van *pozitív* jó kitevője is. □

A jó kitevők tulajdonságai

Lemma (K1.5.8, 4.3.9)
Legyen d a g *legkisebb pozitív* jó kitevője.
Ekkor a jó kitevők pontosan a d többszörösei.

Bizonyítás
Legyen n jó kitevő. Osszuk el n-et maradékosan d-vel:
$n = dq + r$, ahol $0 \leq r < d$. Ekkor $1 = g^n = g^{dq+r} = (g^d)^q g^r = 1^q g^r = g^r$. Tehát r is jó kitevő. A d a *legkisebb pozitív* jó kitevő. Mivel $r < d$, ezért r nem lehet pozitív. Tehát $r = 0$. De akkor $n = dq + r = dq$, azaz n többszöröse d-nek.
Megfordítva, ha n többszöröse d-nek, azaz $n = dq$,
akkor $g^n = g^{dq} = (g^d)^q = 1^q = 1$, azaz n jó kitevő. □

A hatványok periodikusan ismétlődnek

Tétel (K1.5.8, 4.3.10, FGy3.2.2)
Legyen $0 \neq g \in \mathbb{C}$ *legkisebb pozitív* jó kitevője d. Ekkor g rendje d, és g hatványai d hosszú periódusban ismétlődnek.

Bizonyítás:
Beláttuk: a jó kitevők pontosan a d többszörösei.
$g^k = g^\ell \iff g^{k-\ell} = 1 \iff d \mid k - \ell$.
Ezért $1 = g^0 = g^d, g^1, \ldots, g^{d-1}$ páronként különböző. Ezek g összes hatványai, mert ha n tetszőleges egész, akkor $n = dq + r$, ahol $0 \leq r < d$, és $d \mid n - r$ miatt $g^n = g^r$. (Így g^n csak az n-nek a d-vel való osztási maradékától függ.)
Tehát g különböző hatványainak a száma d. Azaz g rendje d, és a hatványok periódikusan ismétlődnek. □

Permutáció rendjének leolvasása

Állítás (K4.3.12)
Az $f = (x_1, \ldots, x_k)$ *ciklus rendje* k, vagyis *a hossza*. Permutáció rendje a diszjunkt ciklushosszak legkisebb közös többszöröse.

Példa: $(23)(15)(45)(42)(13) = (12)(354)$ rendje $[2, 3] = 6$.
FONTOS: a ciklusok diszjunktak kell, hogy legyenek!

Bizonyítás
Ha $\ell < k$, akkor f^ℓ az x_1-et $x_{\ell+1} \neq x_1$-be viszi, így $f^\ell \neq id$. De $f^k = id$, mert a ciklus minden eleme egyszer „körbemegy". Legyen $g = g_1 \ldots g_m$, ahol $g_1, \ldots, g_m$ diszjunkt ciklusok. Ekkor $g^\ell = id \iff g_j^\ell = id$ minden j-re, mert ezek a ciklusok diszjunkt halmazokat mozgatnak. De $g_j^\ell = id \iff g_j$ rendje (vagyis a hossza) osztója ℓ-nek. Tehát g jó kitevői a g_j ciklusok hosszainak közös többszörösei. □

2. Hatvány rendjének képlete

A bolhás feladat

Egy bolha ugrál körbe egy szabályos n-szög csúcsain úgy, hogy minden ugrásnál k csúcsnyit jut előre. Hány ugrás után jut vissza a kiindulóponthoz? Hány kört tesz meg ezalatt? Hány csúcsot érint összesen?

Legyen $n = 6$, a csúcsokat számozzuk így: $0, 1, 2, 3, 4, 5$.

k	bejárás	ugrásszám	körszám	csúcsszám
1	0-1-2-3-4-5-0	6	1	6
2	0-2-4-0	3	1	3
3	0-3-0	2	1	2
4	0-4-2-0	3	2	3
5	0-5-4-3-2-1-0	6	5	6
k		$n/(n,k)$	$k/(n,k)$	$n/(n,k)$

A bolhás feladat megoldása

Megoldás (K1.5.9)
A bolha k-asával ugrál: m ugrás után a km-edik csúcson lesz. Ez akkor a kiindulópont, ha $n \mid km$. A legkisebb ilyen m kell.

$$n \mid km \iff \frac{n}{(n,k)} \,\Big|\, \frac{k}{(n,k)} m$$

Mivel $n/(n,k)$ és $k/(n,k)$ relatív prímek, ez akkor igaz, ha

$$\frac{n}{(n,k)} \,\Big|\, m.$$

A *legkisebb* ilyen m maga az $n/(n,k)$. Így a bolha $n/(n,k)$ ugrást tesz meg, amikor először visszaér.

HF: ennyi csúcsot is érint.
Ezalatt k-szor ennyi „távolságot" tesz meg, ami $kn/(n,k)$. A kör hossza n, ezért a megtett körök száma a megtett távolság n-edrésze, vagyis $k/(n,k)$. □

Hatvány rendjének képlete

Tétel (K1.5.10, 4.3.10)

Ha g rendje véges és k egész, akkor $o(g^k) = \dfrac{o(g)}{(o(g),k)}$.

Bizonyítás
Legyen g rendje n, írjuk g hatványait egy n-szög csúcsaira. Amikor g^k-t hatványozzuk, akkor k-asával ugrálunk körbe a csúcsokon, a $z^0 = 1$-ből kiindulva. A bolhás feladat miatt először az $n/(n,k)$-adik lépésben kapunk 1-et. Vagyis g^k-nak az $n/(n,k)$-adik hatványa lesz először 1. □

Illusztráció: $o(i) = 4$. Ezért $o(i^3) = \dfrac{4}{(4,3)} = 4$.

A rend meghatározása komplex számokra

Állítás (K1.5.11)
A $0 \neq z \in \mathbb{C}$ rendje pontosan akkor véges (azaz z akkor egységgyök),
ha hossza 1,
és szöge a 2π *racionális* többszöröse.
Legyen a szög $(p/q)2\pi$. Egyszerűsítsük ezt a törtet: $p/q = k/n$.
Így $(k,n) = 1$, ekkor $z = \varepsilon_k = \cos(\frac{k}{n} \cdot 2\pi) + i\sin(\frac{k}{n} \cdot 2\pi)$ rendje n.

Bizonyítás
Ha $z^n = 1$, akkor $z = \cos(2k\pi/n) + i\sin(2k\pi/n)$ alkalmas k-ra. Láttuk, hogy $\varepsilon_1 = \cos(2\pi/n) + i\sin(2\pi/n)$-nek a k-adik hatványa ε_k, ezért ε_1 hatványai pontosan az n-edik egységgyökök. Így ε_1-nek n darab hatványa van, azaz rendje $o(\varepsilon_1) = n$. A hatvány rendjének képlete miatt $o(\varepsilon_k) = o(\varepsilon_1^k) = n/(n,k)$. Mivel $(n,k) = 1$, ezért $o(\varepsilon_k) = n$. □

Példa a rend meghatározására

Állítás
Ha $(n,k) = 1$, akkor $\varepsilon_k = \cos(2k\pi/n) + i\sin(2k\pi/n)$ rendje n.

Példa (K1.5.15)
Mennyi lesz $z = \cos 336^\circ + i\sin 336^\circ$ rendje?

Megoldás
$\cos 336° + i \sin 336°$ hossza 1, szöge $336 \cdot 1°$, ami $336/360 \cdot 2\pi$. $336/360$ racionális szám, így z egységgyök. Egyszerűsítve:

$$\frac{336}{360} = \frac{14}{15}.$$

Tehát $z = \cos(14 \cdot 2\pi/15) + i \sin(14 \cdot 2\pi/15)$. Mivel $(14, 15) = 1$, ezért z rendje a fenti állítás miatt 15. □

A rend tulajdonságainak összefoglalása

Összefoglalás (K1.5.8, K1.5.11)
Legyen z nem nulla komplex szám.

- A z *egységgyök*, ha $z^m = 1$ alkalmas $m > 0$ egészre.
- Ha z nem egységgyök, akkor bármely két egész kitevőjű hatványa különböző. Ilyenkor z rendje ∞.
- Ha z egységgyök, akkor a hatványai periodikusan ismétlődnek. A periódus hossza z *rendje*, $o(z)$. A rend a hatványok száma.
- $z^k = z^\ell \iff o(z) \mid k - \ell$. Így $z^n = 1 \iff o(z) \mid n$.
- A z *jó kitevői* azok az n egészek, melyekre $z^n = 1$.
- A z rendje a legkisebb pozitív jó kitevője. A jó kitevők pontosan a rend többszörösei.
- A z akkor egységgyök, ha hossza 1, szöge 2π-nek *racionális* többszöröse; $o(z)$ ezen egyszerűsíthetetlen tört nevezője.

3. Összefoglaló

A 25. előadáshoz tartozó vizsgaanyag

Fogalmak
Komplex szám rendje (K1.5.7).
Szám rendje mod m (FGy3.2.1).
Csoportelem rendje, jó kitevője (K1.5.6, 4.3.9).

Tételek
Csoportelem hatványainak egyenlősége (K1.5.8),
a rend és a jó kitevők kapcsolata (K1.5.8, 4.3.9, Fgy3.2.2).
Permutáció rendje a ciklusfelbontásból (K4.3.12).
A hatvány rendjének képlete (K1.5.10, 4,3,10).
A rend leolvasása a trigonometrikus alakból (K1.5.11).