1. Komplex szám rendje

A rend fogalma

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.

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

A jó kitevők létezése

Definíció (K1.5.6)
Az n egész szám *jó kitevője* a z komplex számnak, ha $z^n = 1$.

Például i és $-i$ jó kitevői a néggyel osztható egész számok.

Tétel (K1.5.8)
Legyen $0 \neq z \in \mathbb{C}$. Ha z nem egységgyök, akkor bármely két, egész kitevőjű hatványa különböző.

Bizonyítás
Tegyük föl, hogy $z^k = z^\ell$, de $k \neq \ell$. Ekkor $z^{k-\ell} = z^{\ell-k} = 1$.

Mivel a $k - \ell$ és $\ell - k$ jó kitevők egyike pozitív, ezért z-nek van *pozitív* jó kitevője is.

A jó kitevők tulajdonságai

Lemma (K1.5.8)
Legyen d a z *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 $1 = z^n = z^{dq+r} = (z^d)^q z^r = 1^q z^r = z^r$. 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 $z^n = z^{dq} = (z^d)^q = 1^q = 1$, azaz n jó kitevő.

A hatványok periódikusan ismétlődnek

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

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

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)

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

Bizonyítás

Legyen z rendje n, írjuk z hatványait egy n-szög csúcsaira. Amikor z^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 z^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

Állítás (K1.5.11)

A $z \neq 0$ 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 $\varepsilon_k = \cos(\frac{k}{n} \cdot 2\pi) + i\sin(\frac{k}{n} \cdot 2\pi)$ 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
$\cos 336^\circ + i \sin 336^\circ$ hossza 1, szöge $336 \cdot 1^\circ$, ami $336/360 \cdot 2\pi$. Mivel $336/360$ racionális szám, 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 periódikusan 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. Primitív egységgyökök

Primitív n-edik egységgyökök

Definíció (K1.5.12)
Az ε szám *primitív n-edik egységgyök*, ha rendje n.

Tétel (K1.5.13)
Az $\varepsilon \neq 0$ számra az alábbi három állítás ekvivalens.

(1) Az ε hatványai pontosan az n-edik egységgyökök.

(2) Az ε rendje n.

(3) $\varepsilon = \cos(2k\pi/n) + i \sin(2k\pi/n)$, ahol $(k, n) = 1$.

Emlékeztető
Ha $(n,k)=1$, akkor $\varepsilon_k=\cos(2k\pi/n)+i\sin(2k\pi/n)$ rendje n. Ha $(n,k)\neq 1$, akkor ε_k rendje n-nél kisebb, mert a k/n törtet még egyszerűsíteni kell. Így (2) $\iff$ (3).

A primitív n-edik egységgyökök jellemzése

Bizonyítandó:
Az $\varepsilon\neq 0$ számra ekvivalens:

(1) Az ε hatványai pontosan az n-edik egységgyökök.

(2) Az ε rendje n.

Bizonyítás
(1) $\implies$ (2) Ha ε hatványai pontosan az n-edik egységgyökök, akkor n darab hatványa van, így rendje n.
(2) $\implies$ (1) Ha ε rendje n, akkor n-edik hatványa 1, és ezért n-edik egységgyök. Így minden hatványa is az: $\varepsilon^n=1 \implies (\varepsilon^k)^n=(\varepsilon^n)^k=1^k=1$. Rendje n, tehát n hatványa van. Így minden n-edik egységgyököt megkapunk.

A primitív n-edik egységgyökök száma

Legyen n pozitív egész. Ekkor a $\varphi(n)$ *Euler-függvény* a $0,1,\dots,n-1$ számok közül az n-hez relatív prímek száma.

Számelméleti tétel
Ha n kanonikus alakja $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}$, ahol $\alpha_i\neq 0$, akkor

$$\varphi(n)=\left(p_1^{\alpha_1}-p_1^{\alpha_1-1}\right)\dots\left(p_k^{\alpha_k}-p_k^{\alpha_k-1}\right).$$

Állítás (K1.5.13)
A primitív n-edik egységgyökök száma $\varphi(n)$.

Bizonyítás
A primitív n-edik egységgyökök: $\varepsilon_k=\cos(2k\pi/n)+i\sin(2k\pi/n)$, ahol $(k,n)=1$.
Láttuk: $\varepsilon_k=\varepsilon_\ell \iff n\mid k-\ell$.

Példák primitív n-edik egységgyökökre

Példa
A *negyedik* primitív egységgyökök $i^1=i$ és $i^3=-i$, mert 1 és 3 relatív prímek 4-hez, de 0 és 2 nem. $\varphi(4)=2$.

Példa
A *hatodik* primitív egységgyökök

$$\cos(2\pi/6) + i\sin(2\pi/6) = \frac{1}{2} + i\frac{\sqrt{3}}{2} \quad \text{és}$$
$$\cos(5\cdot 2\pi/6) + i\sin(5\cdot 2\pi/6) = \frac{1}{2} - i\frac{\sqrt{3}}{2}\,,$$

mert 1 és 5 relatív prímek 6-hoz, de 0, 2, 3, 4 nem. $\varphi(6) = 2$.

Ezzel elvégeztük a Kiss-könyv 1.5. Szakaszát.

4. A körosztási polinom

A körosztási polinom

Definíció (K3.9.1)
Ha $n \geq 1$ egész, akkor Φ_n az *n-edik körosztási polinom.* Ennek egyszeres gyökei a primitív n-edik egységgyökök:

$$\Phi_n(x) = (x - \xi_1)\dots(x - \xi_{\varphi(n)}),$$

ahol $\xi_1, \dots, \xi_{\varphi(n)}$ az összes primitív n-edik egységgyök, vagyis az összes olyan komplex szám, melynek rendje n.

$\Phi_1(x) = x - 1.$ $\quad \Phi_2(x) = x - (-1) = x + 1.$
$\Phi_4(x) = (x - i)\big(x - (-i)\big) = (x - i)(x + i) = x^2 + 1.$

$$\Phi_3(x) = \left(x - \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)\right)\left(x - \left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\right) = x^2 + x + 1.$$

$$\Phi_6(x) = \left(x - \left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)\right)\left(x - \left(\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\right) = x^2 - x + 1.$$

A körosztási polinom kiszámítása

Tétel (K3.9.5, K3.9.7)
Ha $n \geq 1$, akkor $\prod_{d|n} \Phi_d(x) = x^n - 1$. Ezért mindegyik körosztási polinom egész együtthatós.

Példa (K3.9.11): Legyen p prím, ekkor $\Phi_1(x)\Phi_p(x) = x^p - 1$. Így

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + x^2 + \ldots + x^{p-1}\,.$$

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = \frac{x^6 - 1}{(x+1)(x^3 - 1)} = x^2 - x + 1\,.$$

HF: Számítsuk ki rekurzívan $\Phi_4(x)$-et és $\Phi_{12}(x)$-et.

Tétel (K3.9.9, nehéz)
Mindegyik *körosztási polinom irreducibilis* $\mathbb{Q}$ és $\mathbb{Z}$ fölött.

Hasznos képlet: K3.9.15. feladat.

5. Gyűrűk és testek

Hasonló tételek

Láttuk:
Legyen T a $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ egyike. Ekkor $T[x]$-ben

(1) ki lehet emelni a gyöktényezőket;

(2) érvényes a polinomok azonossági tétele;

(3) elvégezhető az interpoláció, a maradékos osztás;

(4) ugyanaz a gyökök és irreducibilitás kapcsolata;

és így tovább. *Nagyon hasonlóan viselkednek.* Oka: a négy alapművelet a szokásos szabályok szerint elvégezhető, és *ennyi elég az állítások bizonyításához.*
$\mathbb{Z}$ hasonló, de nem lehet minden nem nulla számmal osztani.

Nem érdemes ugyanazt a bizonyítást külön elmondani $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ esetén.
Hátha *más fontos számkör* is van, ahol a négy alapművelet elvégezhető, és így a fenti tételek érvényesek.

Gyűrűk és testek

Definíció-kísérlet
Az R *gyűrű*, ha az összeadás kivonás, szorzás *a szokásos szabályok szerint* elvégezhető. A T *test*, ha ezen felül még minden nem nulla számmal lehet osztani.

Példák (K2.2.35)

(1) A polinomok, azaz $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{C}[x, y]$: *gyűrű.*

(2) Analízisben tárgyalt függvények: *gyűrű.*

(3) Az $a + bi$ alakú számok ($a, b \in \mathbb{Z}$): *gyűrű.*

(4) Az $a + bi$ alakú számok ($a, b \in \mathbb{Q}$): *test.*

(5) Az $a + b\sqrt{2}$ alakú számok ($a, b \in \mathbb{Z}$): *gyűrű.*

(6) Az $a + b\sqrt{2}$ alakú számok ($a, b \in \mathbb{Q}$): *test.*

(7) Páratlan nevezőjű törtek: *gyűrű.*

Számolás maradékokkal

Definíció (K1.1.4)
Ha $n \geq 1$ egész, akkor legyen $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Összeadás: $a +_n b$ az $a + b$ maradéka n-nel osztva. Szorzás: $a *_n b$ az ab maradéka n-nel osztva.

Példa (K, 4. oldal)

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$*_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Ezek a *modulo* 5 *műveleti táblázatok. Ez gyűrű, sőt test!*

A szokásos tulajdonságok
Definiálni kell, hogy mik a „szokásos" tulajdonságok.

Definíció (K2.2.1)
Művelet egy R halmazon: bármely $a, b \in R$-hez $a * b \in R$.
Asszociativitás: $(a * b) * c = a * (b * c)$ bármely a, b, c-re. (Ilyenkor a sokténye zős szorzatot is akárhogy zárójelezhetjük.)
Kommutativitás: $a * b = b * a$ bármely a, b-re. (Ilyenkor sok tényezőt is akárhogy cserélgethetünk.)

Példák
A $\mathbb{C}$-beli összeadás és szorzás asszociatív és kommutatív. A $+_n$ és $*_n$ műveletek asszociatívak és kommutatívak. A halmazelméleti *unió* és *metszet* is asszociatív és kommutatív. Függvények *kompozíciója* asszociatív, de általában nem kommutatív. $(f \circ g)(x) = f\big(g(x)\big)$.

Nullelem, egységelem, ellentett, inverz

Definíció (K2.2.6)
Legyen + művelet az R halmazon. A $0 \in R$ elemet *nullelemnek* nevezzük, ha minden $a \in R$ esetén $a + 0 = 0 + a = a$.

Házi Feladat: legfeljebb egy nullelem lehet.

Definíció (K2.2.9)
Legyen + művelet az R halmazon és $0 \in R$ nullelem. Az $a \in R$ *ellentettje* b, ha $a + b = 0$. Jele: $b = -a$.

Házi Feladat: Minden elemnek legfeljebb egy ellentettje van.

Az előző definíciók szorzás művelet esetén:
Jelölje R-en a műveletet egymás mellé írás. Ekkor:
Az $1 \in R$ *egységelem*, ha $1a = a1 = a$ minden $a \in R$-re.
Az $a \in R$ *inverze* b, ha $ab = ba = 1$. Jele: $b = a^{-1}$.

A gyűrű és test definíciója

Az R *gyűrű* (K2.2.21), ha értelmezett az összeadás +-szal, és a szorzás egymás mellé írással jelölt művelete úgy, hogy

(1) Az összeadás asszociatív.

(2) Az összeadás kommutatív.

(3) Van az összeadásra nézve egy 0 nullelem.

(4) Minden elemnek van ellentettje.

(5) A szorzás asszociatív.

(6) Tetszőleges $x, y, z \in R$ esetén igaz a *disztributivitás*: $(x+y)z = xz+yz$ és $z(x+y) = zx+zy$.

Kommutatív gyűrű: a szorzás kommutatív.
Egységelemes gyűrű: a szorzásra nézve van egységelem (jele 1).
Test: egységelemes, kommutatív gyűrű, amelyben minden nem nulla elemnek van inverze (K2.2.23).

Elemi számolási szabályok

Állítás (K2.2.22, K2.2.10)
Legyen R gyűrű és $a, b \in R$ tetszőleges elemek.

(1) $0a = a0 = 0$.

(2) $(-a)b = a(-b) = -(ab)$.

(3) Ha a és b invertálható, akkor ab is, és inverze $b^{-1}a^{-1}$.

Mintabizonyítás

(1) A disztributivitás miatt $a0 = a(0+0) = a0 + a0$. Mindkét oldalhoz adjuk hozzá $a0$ ellentettjét.
$0 = (a0 + a0) + (-a0) = a0 + \big(a0 + (-a0)\big) = a0 + 0 = a0$.

(3) $b^{-1}a^{-1}(ab) = b^{-1}1b = 1$. Hasonlóan $(ab)b^{-1}a^{-1} = 1$.

Példa: szorzatmátrix inverze.

Nullosztómentesség

Definíció (K2.2.27)
Az R gyűrű *nullosztómentes*, ha egy szorzat csak akkor nulla, ha valamelyik tényezője nulla: $ab = 0 \implies a = 0$ vagy $b = 0$.
Szokásos gyűrű: kommutatív, egységelemes, nullosztómentes.

Példák
Mindegyik eddig tanult polinomgyűrű szokásos gyűrű (a többhatározatlanúak is).
A $\mathbb{Z}_6$ nem nullosztómentes: $2 *_6 3 = 0$, de $2 \neq 0$ és $3 \neq 0$.
A $\mathbb{Z}_5$ test, például a „2-*ben a* 3" osztás eredménye 4, mert $3 *_5 4 = 2$.
A 3 inverze 2, mert $3 *_5 2 = 1$.
Ha $n = ab$, ahol $0 < a, b < n$, akkor $a *_n b = 0$, de $a, b \neq 0$. Ezért ha n nem prím, akkor $\mathbb{Z}_n$ *nem* nullosztómentes.

Test nullosztómentes

Tétel (K2.2.31)
A $\mathbb{Z}_n$ a $+_n$ és $*_n$ műveletekre egységelemes, kommutatív gyűrű. A $\mathbb{Z}_n$ pontosan akkor nullosztómentes, ha n prímszám, és ebben az esetben test is.

Tétel (K2.2.29)
Minden test nullosztómentes.

Bizonyítás
Legyen T test, és $z, w \in T$. Tegyük föl, hogy $zw = 0$, de $z \neq 0$. Meg kell mutatnunk, hogy akkor $w = 0$. Mivel $z \neq 0$, van inverze: $uz = 1$. Ezzel szorozva

$$w = 1 \cdot w = (uz)w = u(zw) = u \cdot 0 = 0.$$

Példa: Az egész számok gyűrűje nullosztómentes, de nem test.

Az egyszerűsítési szabály

Tétel (K2.2.28)
Nullosztómentes gyűrűben érvényes az *egyszerűsítési szabály*: ha $ac = bc$ és $c \neq 0$, akkor $a = b$.

Bizonyítás
$ac = bc \implies 0 = ac - bc = (a - b)c$. Mivel $c \neq 0$, a nullosztómentesség miatt $a - b = 0$, azaz $a = b$.

Hasonlóképpen balról is lehet egyszerűsíteni: Ha $ca = cb$ és $c \neq 0$, akkor $a = b$.

Minden lineáris algebrából kimondott állítás tetszőleges test fölött is érvényes, ugyanazzal a bizonyítással. Legközelebb átismételjük a polinomokat „gyűrűs" szemszögből.

6. Összefoglaló

A 10. előadáshoz tartozó vizsgaanyag

Fogalmak
Komplex szám rendje, jó kitevője. Primitív n-edik egységgyök. Körosztási polinom. Művelet, asszociativitás, kommutativitás, nullelem, egységelem, ellentett, inverz. Gyűrű, nullosztómentesség. Egységelemes, kommutatív, szokásos gyűrű, test. A $\mathbb{Z}_m$ gyűrű.

Tételek
Komplex szám hatványainak egyenlősége. A rend és a jó kitevők kapcsolata. A rend leolvasása a trigonometrikus alakból. A hatvány rendjének képlete. A primitív egységgyökök jellemzései. A körosztási polinom rekurzív képlete. A körosztási polinom egész együtthatós és irreducibilis.
Elemi számolási szabályok gyűrűkben, az egyszerűsítési szabály, szorzat inverze. Minden test nullosztómentes. A $\mathbb{Z}_m$ mikor nullosztómentes, mikor test.