1. 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 $\underline{(2) \iff (3)}$.

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
$\underline{(1) \implies (2)}$ Ha ε hatványai pontosan az n-edik egységgyökök, akkor n darab hatványa van, így rendje n.
$\underline{(2) \implies (1)}$ 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. $\square$

A primitív n-edik egységgyökök száma

Állítás (K1.5.13)
A primitív n-edik egységgyökök száma $\varphi(n)$ (Euler-függvény).
Ezek $\varepsilon_k = \cos(2k\pi/n) + i\sin(2k\pi/n)$, ahol $(k, n) = 1$. $\square$

A *negyedik* primitív egységgyökök $i^1 = i$ és $i^3 = -i$,
mert 1 és 3 relatív prímek 4-hez, de 0 és 2 nem. $\varphi(4) = 2$.
Az i és a $-i$ hatványainak halmaza is $\{1, i, -1, -i\}$,
vagyis az összes negyedik egységgyökök.
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. $\varphi(6) = 2$.

2. A körosztási polinom

A körosztási polinom

Definíció (K3.9.1)
Ha $n \geq 1$ egész, akkor Φ_n az *n-edik körosztási polinom:*

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

ahol $\xi_1, \ldots, \xi_{\varphi(n)}$ az összes primitív n-edik egységgyök, vagyis az összes olyan komplex szám, melynek rendje n. Tehát Φ_n-nek egyszeres gyökei a primitív n-edik egységgyökök.

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

$$\Phi_3(x) = \left(x - \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)\right)\left(x - \left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\right) = x^2 + x + 1.$$
$$\Phi_6(x) = \left(x - \left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)\right)\left(x - \left(\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\right) = x^2 - x + 1.$$

A körosztási polinom kiszámítása

Tétel (K3.9.5, 3.9.7)
Ha $n \geq 1$, akkor $\prod_{d|n} \Phi_d(x) = x^n - 1$. Ezért mindegyik körosztási polinom egész együtthatós.

Valóban, tudjuk, hogy $x^n - 1$ az $x - \varepsilon$ gyöktényezők szorzata, ahol ε befutja az n-edik egységgyököket. Nyilván $\varepsilon^n = 1$ akkor és csak akkor, ha $o(\varepsilon) \mid n$. Ezért $x^n - 1$ gyöktényezői ugyanazok, mint a $\Phi_d(x)$ gyöktényezői együttvéve, ahol d befutja n osztóit. Azt, hogy Φ_n egész együtthatós, n szerint indukcióval bizonyítjuk. A képletből $\Phi_n(x)$-et ki lehet fejezni osztással, és mivel a nevezőben az indukciós feltevés szerint egész együtthatós, normált polinom áll, a hányados is egész együtthatós. $\square$

Példa: $\Phi_1(x)\Phi_3(x) = x^3 - 1$, ezért $\Phi_3(x) = \dfrac{x^3 - 1}{x - 1} = x^2 + x + 1$.

További módszerek

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

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

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

Állítás (K3.9.15, NB)

Ha $m \mid n$, és a prímosztóik ugyanazok, akkor $\Phi_n(x) = \Phi_m(x^{n/m})$.

Példa: $\Phi_4(x) = \Phi_2(x^2) = x^2 + 1$, $\Phi_{12}(x) = \Phi_6(x^2) = x^4 - x^2 + 1$.
Ha p prím, akkor $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}})$. Így $\Phi_{27}(x) = x^{18} + x^9 + 1$.
K3.9.12, HF: Ha $n > 1$ páratlan, akkor $\Phi_{2n}(x) = \Phi_n(-x)$.

Tétel (K3.9.9, nehéz)

Mindegyik *körosztási polinom irreducibilis* $\mathbb{Q}$ és $\mathbb{Z}$ fölött.

3. A harmad- és negyedfokú egyenlet

A másodfokú egyenlet

Az $y^2 + py + q = 0$ egyenletben vezessük be az $x = y + p/2$ új ismeretlent. Ekkor $y = x - p/2$, ahonnan $y^2 + py + q = (x - p/2)^2 + p(x - p/2) + q = x^2 + (q - p^2/4)$. Ha ez nulla, akkor $x = \pm\sqrt{p^2/4 - q}$, azaz $y = -p/2 \pm \sqrt{p^2/4 - q}$ a másodfokú egyenlet megoldóképlete.

Tanulságok

(1) Az $y \mapsto y - p/2$ helyettesítés eltünteti az elsőfokú tagot.

(2) Ezzel a problémát *négyzetgyökvonásra vezettük vissza.*

(3) Ha $p^2/4 - q \neq 0$, akkor két megoldás van, mert minden nem nulla komplex számnak két négyzetgyöke van.

(4) Ha $p^2/4 - q = 0$, akkor egy megoldás van, amely az $y^2 + py + q$ polinomnak kétszeres gyöke.

A harmadfokú egyenlet

Határozzuk meg az $a_3y^3 + a_2y^2 + a_1y + a_0 = 0$ egyenlet összes megoldását $\mathbb{C}$-ben ($a_3, a_2, a_1, a_0 \in \mathbb{C}$). Ha $a_3 \neq 0$, akkor ez az *általános harmadfokú egyenlet.*

A kézenfekvő redukciós lépések
Az egyenletet a_3-mal elosztva feltehető, hogy $a_3 = 1$.
Ezután végezzük el az $y = x - a_2/3$ helyettesítést. Kiesik az x^2-es tag, és az egyenlet a következő alakú lesz:

$$x^3 + px + q = 0.$$

Ha ezt sikerülne megoldani, akkor az eredetit is.

A másodfokú egyenlet megoldását (geometriai módszerekkel) már az ókori görögök is ismerték. A most következő ötletet *Scipione del Ferro* és *Niccolo Tartaglia* fedezte fel, 1530 körül.

A megoldás ötlete*

Ötlet (K, 1.2. Szakasz)
$(u+v)^3 = u^3 + 3u^2v + 3uv^2 + v^3 = u^3 + v^3 + 3uv(u+v)$. Átrendezve, és $x = u + v$-t helyettesítve:

$$\begin{aligned}(u+v)^3 &- 3uv(u+v) - (u^3+v^3) = 0\\ x^3 &- \quad 3uvx \quad - (u^3+v^3) = 0\\ x^3 &+ \quad\ px \quad + \qquad\quad q = 0\end{aligned}$$

Vagyis *HA* $-3uv = p$ és $-(u^3+v^3) = q$, *AKKOR* $x = u + v$ megoldása a harmadfokú egyenletnek. Innen $u^3v^3 = (-p/3)^3$, és $u^3 + v^3 = -q$. Ezért u^3 és v^3 gyökei a $z^2 + qz - (p/3)^3 = 0$ másodfokú egyenletnek. Így

$$x = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

Cardano képlete

Az $f(x) = x^3 + px + q$ gyökei *Cardano képletéből* kaphatók:

$$x = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

Tartaglia fedezte föl, Cardano publikálta (*Ars Magna*, 1545).

Tétel (K3.8.1, 3.8.2)

(1) Ha az itt szereplő u és v köbgyököket úgy választjuk, hogy szorzatuk $-p/3$ legyen, akkor f gyökét kapjuk.

(2) Az f mindegyik gyöke megkapható ezen a módon.

(3) Az f-nek pontosan akkor van többszörös gyöke, ha a négyzetgyök alatt álló $D = (q/2)^2 + (p/3)^3$ kifejezés nulla.

Bizonyítás: K, 3.8. Szakasz.

Példa a képlet használatára

Példa
Legyen $f(x) = x^3 - 21x + 20$. Ekkor a Cardano-képletből
$$x = \sqrt[3]{-10 + \sqrt{-243}} + \sqrt[3]{-10 - \sqrt{-243}}.$$
Könnyen ellenőrizhető: $(2 + i\sqrt{3})^3 = -10 + i\sqrt{243}$.
Ha $u = 2 + i\sqrt{3}$, akkor $v = (-p/3)/u = 7/(2 + i\sqrt{3}) = 2 - i\sqrt{3}$.
Ezért $x = u + v = (2 + i\sqrt{3}) + (2 - i\sqrt{3}) = 4$ az egyik gyök.
Az f másik két gyökét a $-10 + i\sqrt{243}$ másik két köbgyöke adja.
Ezek $u = 2 + i\sqrt{3}$ *harmadik egységgyökökszörösei*.
Ha $\varepsilon = \cos 120° + i \sin 120° = -1/2 + i\sqrt{3}/2$, akkor
$u_2 = u_1\varepsilon = -5/2 + i\sqrt{3}/2$ és $v_2 = (-p/3)/u_2 = -5/2 - i\sqrt{3}/2$
$u_3 = u_1\varepsilon^2 = 1/2 - i3\sqrt{3}/2$ és $v_3 = (-p/3)/u_3 = 1/2 + i3\sqrt{3}/2$.
Innen $x_2 = u_2 + v_2 = -5$ és $x_3 = u_3 + v_3 = 1$.
Ellenőrzés: $(x - 1)(x - 4)(x + 5) = x^3 - 21x + 20$.

Casus irreducibilis

Az $x^3 - 21x + 20$ mindhárom gyöke *valós*, mégis a Cardano-képletben negatív számból kellett négyzetgyököt vonni. Aki nem ismeri a komplex számokat, nem tudja megtenni. Ez a *Casus Irreducibilis*. Így fedezték fel a komplex számokat.

Tétel (K3.8.2)
$f(x) = x^3 + px + q$, ahol p, q *valósak*, és $D = (q/2)^2 + (p/3)^3$.

(1) Ha $D < 0$: három különböző gyök van, mind valós.

(2) Ha $D = 0$: minden gyök valós, az egyik legalább kétszeres.

(3) Ha $D > 0$: három különböző gyök van, az egyik valós, a másik kettő nem valós, és egymás konjugáltjai.

Az $\overline{(1)}$ esetben *semmilyen más, valósban maradó „gyökképlet” sem adhatja egyik gyökét sem!* (A Casus Irreducibilis Tétele, K6.10.2).

A negyedfokú egyenlet*

Határozzuk meg az $a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ egyenlet összes megoldását $\mathbb{C}$-ben ($a_4, a_3, a_2, a_1, a_0 \in \mathbb{C}$). Ha $a_4 \neq 0$, akkor ez az *általános negyedfokú egyenlet*.

A kézenfekvő redukciós lépések
Az egyenletet a_4-gyel elosztva feltehető, hogy $a_4 = 1$.
Az $x \mapsto x - a_3/4$ helyettesítéssel kiesik az x^3-ös tag.

Ötlet (K3.8.4, K3.8.5)
Egy harmadfokú egyenlet megoldásával a fenti polinom két másodfokú polinom szorzatára bontható. Ezért az összes gyök megkapható az együtthatókból a négy alapművelet és gyökvonás segítségével.

A legalább ötödfokú egyenletek

Abel–Ruffini-tétel (K6.9.7)
Ha $n \geq 5$, akkor az *általános* n-edfokú egyenletre *nem létezik* olyan képlet, amely a négy alapművelet és gyökvonások segítségével megadja a megoldásokat.

Tétel (lásd K, 6.9. Szakasz)
Konkrétan az $x^5 - 4x + 2$ polinom egyik gyöke sem írható föl ilyen gyökképlet segítségével.

A bizonyítások a *Galois-elmélet* eredményei.
Felfedezők: *Niels Henrik Abel*, *Evariste Galois* (1830 körül). Ezt az Algebra3-4 tárgyban tanuljuk majd (K, 6. Fejezet). Az elméletből következik, hogy bizonyos szerkesztések (szögharmadolás, körnégyszögesítés) nem végezhetők el körzővel és vonalzóval.

4. Összefoglaló

A 26. előadáshoz tartozó vizsgaanyag

Fogalmak
Primitív n-edik egységgyök (K1.5.12). Körosztási polinom (K3.9.1).

Tételek
A primitív egységgyökök jellemzései (K1.5.13).
A körosztási polinom rekurzív képlete (K3.9.5).
A körosztási polinom egész együtthatós (K3.9.7) és irreducibilis (K3.9.9).
Cardano képlete (a képletet nem kell tudni), a használat módja,
a többszörös gyökök létezésének leolvasása (K3.8.1-2).
A Casus Irreducibilis jelensége és tétele (K6.10.2).
A negyedfokú egyenlet* (K3.8.4, 3.8.5).
A magasabb fokú egyenletek nem megoldhatósága gyökjelekkel (K6.9.7).