1. A körosztási polinom

A körosztási polinom.

Definíció
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 (Kiss-jegyzet, 3.9.5. Lemma)
Ha $n \geq 1$, akkor $\prod_{d|n} \Phi_d(x) = x^n - 1$.

Bizonyítás
Házi feladat.

Példa
Legyen p prímszám. Előző tétel: $\Phi_1(x)\Phi_p(x) = x^p - 1$. Így

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

Következmény (Kiss-jegyzet, 3.9.7. Következmény)
Mindegyik körosztási polinom egész együtthatós.

2. 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 (Kiss-jegyzet, 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:

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

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 az $z^2 + qz - (p/3)^3 = 0$ 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

(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: Kiss-jegyzet, 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 $\varepsilon = \cos 120^\circ + i \sin 120^\circ = -1/2 + i\sqrt{3}/2$, 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 (Kiss-jegyzet, 3.8.2. Tétel)
Legyen $f(x) = x^3 + px + q$, ahol p, q *valósak*, és $D = p^2/4 - q$.

(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 (1) esetben *semmilyen más, valósban maradó „gyökképlet” sem adhatja egyik gyököt sem!* (A Casus Irreducibilis Tétele, Kiss-jegyzet, 6.10.2. Tétel.)

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 (lásd Kiss-jegyzet, 3.8.4. Tétel)
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.

Tétel (Kiss-jegyzet, 6.9.7. Tétel)
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 Kiss-jegyzet, 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 a harmadik félévben tárgyaljuk (Kiss-jegyzet, 6. Fejezet).