Magasabbfokú egyenletek 2.

Az eddig tárgyaltak összegzése.

1. Az iszlám matematikusok azt vallották, hogy a harmad- és a magasabb fokú egyenletek csak geometriai úton oldhatók meg.
2. Egészen a XX. század közepéig általánosan elfogadott nézet volt, hogy ezt csak a XVI. századi itáliai matematikusok cáfolták meg megadva a harmad- és a negyedfokú egyenletek általános (algebrai) megoldásának eljárását, a „gyökképletet".
3. XIV-XV. századi itáliai kéziratokból kiderült (a XX. század második felében), hogy számos részleges eredmény született az egyenletek algebrai megoldásával kapcsolatban.
4. A legföljebb negyedfokú egyenletek megoldásának a kulcsa minden esetben egy eggyel alacsonyabb fokú segédegyenlet, ún. *rezolvens egyenlet* megoldása volt.

Természetesen fölmerült kérdés:

Létezik-e bármely n-hez ($n \geq 2$) van olyan $k \leq n-1$, hogy tetszőleges n-edfokú egyenlet megoldása visszavezethető egy (vagy több) k-adfokú ún. rezolvens egyenlet megoldására.

A kutatások általános iránya egészen a XIX. század elejéig a rezolvens egyenletek keresésére volt (pl. Waring, Vandermonde, Lagrange, Malfati).

Újabb kérdés a XVIII. század utolsó harmadában.

Biztosan megoldhatók az egyenletek?

Az első ilyen irányú dolgozatot az olasz Paolo Ruffini publikálta 1798-ban. Ennek ismertetése előtt egy fontos kérdést kell tisztázni: ha negatív eredményt akarunk bizonyítani, előbb pontosan meg kell mondani, hogy

minek e nemlétét kívánjuk igazolni.

1. **Kérdés.** Legyen $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ tetszőleges polinom ($n \geq 2$). Létezik-e olyan csak n-től függő eljárás, amellyel az $f = 0$ egyenlet gyökei megkaphatók az $a_0, \ldots, a_{n-1}$ együtthatókból a négy alapművelet (összeadás, kivonás, szorzás és osztás), valamint gyökvonások (egész kitevős) véges sokszori alkalmazásával.
2. **Kérdés.** Ha az előbbire valamely n-re nemleges a válasz, akkor létezik-e olyan eljárás minden ilyen n-re, amely az n-en kívül az együtthatóktól is függ?

Mielőtt e kérdésekkel — korabeli módon — tovább foglalkoznánk, megfogalmazzuk a problémát XX. századi eszközökkel is a könnyebb érthetőség kedvéért.

1. Definíció. Legyen $A = \{a_1, \ldots, a_n\}$, $n \in \mathbb{N}$ tetszőleges halmaz. A $\varphi\colon A \to A$ bijektív leképezéseket *permutációknak* nevezzük. Ugyancsak permutációknak szokás nevezni az A halmaz elemeinek különböző sorrendű fölsorolásait is.

2. Definíció. Legyen G tetszőleges nemüres halmaz, és definiáljunk rajta egy (szorzásként jelölt) kétváltozós műveletet. Azt mondjuk, hogy a $(G, \cdot)$ rendezett pár *csoport*, ha

($\imath$) a művelet asszociatív, azaz minden $a, b, c \in G$-re $a(bc) = (ab)c$;
($\imath\imath$) van olyan $e \in G$, hogy minden $a \in G$-re $ae = ea = a$;
($\imath\imath\imath$) minden $a \in G$-hez van olyan $a' \in G$, hogy, $aa' = a'a = e$.

Példa. $(\mathbb{Z}, +)$, továbbá, ha S_A jelöli az A halmaz összes permutációit, akkor $(S_A, \cdot)$ szintén csoport, ahol „$\cdot$" az ismert leképezésszorzást jelöli.

3. Definíció. Legyen F nemüres halmaz, és definiáljunk rajta két — összeadásnak és szorzásnak jelölt — műveletet. Azt mondjuk, hogy az $(F;+,\cdot)$ rendezett hármas *test*, ha

($\imath$) $(F,+)$ és $(F\setminus\{0\},\cdot)$ kommutatív műveletű csoport,

($\imath\imath$) tetszőleges $a,b,c\in F$ elemekre $a(b+c)=ab+ac$, azaz a szorzás disztributív az összeadásra.

Példa. $(T;+,\cdot)$, ahol T lehet $\mathbb{Q},\mathbb{R},\mathbb{C}$ bármelyike.

4. Definíció. Valamely csoport (test) azon részhalmazait, amelyek az eredeti müvelettel (műveletekkel) szintén csoport (test) *részcsoportoknak* (*résztesteknek*) nevezzük

5. Definíció. A komplex számok testének résztesteit *számtesteknek* nevezzük.

Megjegyzés. A számtestek mindegyike tartalmazza a racionális számok testét.

Az olasz Paolo Ruffini volt az első matematikus, aki fölvetette, hogy az ötöd- és magasabbfokú egyenletek talán nem is oldhatók meg az kívánt módon. Első témába vágó dolgozata 1798-ban jelent meg és 324 oldalas volt. Ezt két lényegesen rövidebb mű követte.

Lényegében Lagrange módszerével dolgozott (a tanára volt), szintén a gyökök egy alkalmas racionális függvényével dolgozott, de az nem volt szükségképp lineáris.

Néhány eredménye.

Legyen $L=L(x_1,\dots,x_n)$ az

$$(*)\qquad x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0=0$$

egyenlet gyökei egy racionális függvénye (polinomja), ún. *rezolvense.*

Megjegyzés. Ez Lagrange esetén ez

$$L=x_1+\alpha x_2+\alpha^2x_3+\alpha^3x_4+\alpha^4x_5$$

volt, ahol α primitív ötödik egységgyök.

1. Már Euler sejtette, és Gauss be is bizonyította, hogy a $(*)$ egyenletnek n számú komplex gyöke van (közöttük természetesen lehetnek egyenlők is).

2. A $(*)$ egyenlet gyökjelekkel való megoldása azt jelenti, hogy
- megkonstruáljuk $\mathbb{C}$-nek az együtthatókkat tartalmazó legszűkebb résztestét,
- ezt e test elemeiből nyerhető gyökmennyiségek hozzávételével addig bővítjük (mindig testté téve), amíg tartalmazza a gyököket.

3. A $(*)$ egyenlet gyökeinek összesen $n!$ számú permutációja van. Tegyük föl, hogy közülük s számú olyan van, amellyel szemben L invariáns. Így L $n!/s$ számú különböző értéket vesz föl.

4. Igazolta:
- Ha $n=5$, akkor $n!/s$ lehetséges értékei 2,5,6, azaz nem fordulhat elő az, hogy L 3 vagy 4 értéket vesz csak föl. Ez azt jelenti, hogy a rezolvens nem lehet harmad- vagy negyedfokú egyenlet gyöke.
- Ha $n!/s\neq 2$, akkor $5\mid n!/s$. Ha $n!/5=5$, akkor létezik ötödfokú ún. rezolvens egyenlet, olyan ötödfokú egyenlet, amelynek a rezolvens gyöke.
- Ezen rezolvens egyenlet azonban nem redukálható

$$x^5-m=0$$

alakúra.

Egy hosszú sor hasonló jellegű állítás után bizonyítani vélte:

Tétel. *Az általános ötödfokú egyenlet nem oldható meg gyökvonásokkal, azaz nincsenek olyan gyökmennyiségek, amelyek megoldásai az egyenletnek.*

Sajnos a bizonyításban fölhasználta a következő nem bizonyított állítást: *Az előbbi gyökmennyiségek a gyökök racionális függvényei.*

E hiányosságra később Abel mutatott rá.

Neves kortársai is elutasították eredményét, de konkrét kifogással nem éltek. A legtöbb kortársa azt hitte, az egyenletek megoldhatók gyökvonásokkal.

Ruffini érdeme.

1. Először vetette föl a gyökjelekkel nem megoldhatóságot.
2. Először használta mai értelemben is korrekten a permutáció és a helyettesítés fogalmát, ami az első lépés volt a permutációcsoport fogalmához.
3. Implicite megkülönböztette azt a két fogalmat, amit ma tranzitív ill. intranzitív permutációcsoportnak neveznek.

Egy érdekes további eredménye. Valamely nem szimmetrikus racionális függvény vagy legalább öt értéket vesz föl, vagy legföljebb kettőt.

Cauchy általánosítása. Legyen az $n \in \mathbb{N}$ természetes szám legnagyobb prímosztója p. Egy n-változós nem szimmetrikus racionális függvény vagy legalább p értéket vesz föl, vagy legföljebb kettőt.

Cauchy néhány további releváns eredménye.

1. Permutációk egymás utáni végrehajtása tekinthető a permutációk szorzásának.
2. A „helyettesítések struktúrájának" vizsgálatakor bevezette a helyettesítések hasonlósága fogalmát: két helyettesítés hasonló, ha ugyanaz a „ciklus-struktúrájuk".
3. $P \sim Q \;\Leftrightarrow\; P = R^{-1}QP$ valamely R helyettesítésre.

Niels Henrik ABEL (1802-1829.)

Tizenévesen megoldani vélte az általános ötödfokú egyenletet, de hamarosan megtalálta eljárása hibáját.

1824-ben korrekten igazolta, hogy az általános ötödfokú egyenlet nem oldható meg gyökvonásokkal. Erről egy rövid francia nyelvű memoárt adott ki. Elküldte Gaussnak, de választ nem kapott.

Eredménye alapján állami ösztöndíjat kapott külföldi tanulmányutakra. Járt Németországban, Olaszországban és Párizsban, de sehol sem tárgyaltak vele érdemben.

Cauchy például azonnal félretette memoárját, mert „igen rossz francia nyelvtudásról tanúskodott".

1826-ban a kibővített (20 oldalas) német nyelvű változat,

Beweis der Unmöglichkeit algebraische Gleichnungen
von höreren Graden als dem vierten allgemein aufzulösen

címmel megjelent Berlinben a Journal für reine und angewandte Mathematik (az ún. „Crelle Journal" 1. számában. (Ez a legrégebbi olyan matematikai folyóirat, amely a mai napig megjelenik.)

Lagrange és Cauchy azon eredményeire alapozott, amelyek az n-változós nem szimmetrikus racionális függvények permutációkkal szembeni viselkedésére vonatkoztak, de egészen más módon alkalmazta azokat, mint elődei.

Már a kiindulópontja is más mint volt. Vizsgálandó egyenlete együtthatóit általánosoknak, puszta szimbólumoknak tekintette, amelyek között semmiféle összefüggés nincs.
1826-os dolgozatának azt a részét tekintjük át, amelyben „befoltozta" a Ruffini-féle bizonyítás hiányosságát.

Legyen

$$y^5 - ay^4 + by^3 - cy^2 + dy - e = 0 \tag{1}$$

általános ötödfokú egyenlet: az együtthatók „általánosak", azaz pusztán betűk, független változók. Föltéve, hogy y kifejezhető az együtthatókból az alapműveletekkel és gyökvonásokkal Abel föltételezte, hogy hogy a megoldás

$$y = p + p_1 R^{1/m} + p_2 R^{2/m} + \cdots + p_{m-1} R^{(m-1)/m} \tag{2}$$

alakban írható, ahol m prím, továbbá az $R, p, p_1, \ldots, p_{m-1}$ olyan mennyiségek, amelyek ugyanolyan alakúak, mint az y, legföljebb további gyökmennyiségeket (korábbi gyökvonások eredményeit) tartalmazzák.
Ezt kezdetlegesen megfogalmazott rekurzióként képzelte el: folytatva a lebontást (az $R, p, p_1, \ldots, p_{m-1}$ mennyiségek előbbi alakú részletezését), az eredeti egyenlet együtthatói racionális függvényeiig jutunk vissza.

Megjegyzés. Galoisnál ez bizonyos értelemben fordítva lesz, ő az a, b, c, d, e együtthatók racionális fügvényeiből indult ki, és ezekhez adjungált prímkitevős gyökmennyiségeket egymás után.

(2)-ben a konstans együthatók közé Abel mindig odaértette az m-edik egységgyököket, ahol m egy olyan prím kitevő, amely szerepel a megoldásban.
Föltehető — mondta Abel —, hogy $R^{1/m}$ nem fejezhető ki, mint az $a, b, \ldots, p, p_1, \ldots$ racionális függvénye, mert akkor a gyökmennyiségek adjungálása (gyökvonások végzése) fölösleges volna. Az is föltehető, hogy (2)-ben nem az összes $p_1, p_2, \ldots$ együttható zéró: ha R-et R/p_1^m-mel helyettesítjük, akkor $p_1 = 1$ adódik.
Írjunk $R^{1/m}$ helyébe z-t:

$$y = p + z + p_2 z^2 + \cdots + p_{m-1} z^{m-1}. \tag{3}$$

Ezt az (1)-be helyettesítve

$$q + q_1 z + q_2 z^2 + \cdots + q_{m-1} z^{m-1} = 0, \tag{4}$$

ahol $q, q_1, \ldots$ az $a, b, \ldots, p_1, p_2, \ldots$ és R polinomja.
A döntő lépés: Abel azt állítja, hogy ahhoz, hogy (4) teljesüljön szükséges az, hogy

$$q = 0,\ q_1 = 0, \ldots, q_{m-1} = 0.$$

Ezt zseniálisa bizonyította be.
A z közös gyöke a (4) egyenletnek, valamint a

$$z^m - R = 0 \tag{5}$$

egyenletek.
Amennyiben a $q, q_1, \ldots$ együtthatók nem mindegyike zéró a közös gyökök száma legföljebb $m-1$, mondjuk k.
Kiszámítva a (4) és az (5) bal oldalán álló polinomok legnagyobb közös osztóját, az egy k-adfokú polinom, így az

$$r + r_1 z + r_2 z^2 + \ldots + r_k z^k = 0 \tag{6}$$

egyenlethez jutunk.
Ha a (6) bal oldalán álló polinomot irreducibilis tényezőkre bontjuk, akkor azok valamelyike zéró mondjuk

$$t_0 + t_1 z + \ldots + t_{\mu-1} z^{\mu-1} + z^\mu = 0, \tag{7}$$

ahol a bal oldalon irreducibilis polinom áll.
Abel azt állítja föltehetjük, hogy lehetetlen ilyen alakú alacsonyabb fokú egyenletet találni.
(7)-nek μ számú gyöke van, amelyek egyúttal (5)-nek is gyökei. Ez utóbi gyökei azonban αz alakúak, ahol α m-edik egységgyök. Világos, hogy $\mu \geq 2$, különben a z az $a, b, \ldots, p, p_1, \ldots$ racionális függvénye lenne.
Ez pedig azt jelenti, hogy (7)-nek legalább két gyöke van, a z és az αz, tehát

$$\begin{aligned} t_0 + t_1 z + t_2 z^2 \ldots + t_{\mu-1} z^{\mu-1} + z^\mu &= 0 \\ t_0 + \alpha t_1 z + \alpha^2 t_2 z^2 \ldots + \alpha^{\mu-1} t_{\mu-1} z^{\mu-1} + \alpha^\mu z^\mu &= 0. \end{aligned} \tag{8}$$

Szorozzuk meg az első egyenletet α^μ-vel és vonjuk ki azt a másodikból. Így egy μ-nél alacsonyabb fokú egyenletet kapunk z-re, ami lehetetlen. Ez pedig azt jelenti, hogy a $q, q_1, \ldots, q_{m-1}$ mindegyike zéró, ahogy állítottuk.
Tekintsük ismét korábbi egyenleteinket.

$$y^5 - ay^4 + by^3 - cy^2 + dy - e = 0 \tag{1}$$

$$y = p + z + p_2 z^2 + \cdots + p_{m-1} z^{m-1}. \tag{3}$$

$$z^m - R = 0 \tag{5}$$

$$q + q_1 z + q_2 z^2 + \cdots + q_{m-1} z^{m-1} = 0, \tag{4}$$

(2) $$y = p + p_1 R^{1/m} + p_2 R^{2/m} + \cdots + p_{m-1} R^{(m-1)/m}$$

A (4) (3)-nak (1)-be helyettesítésével, és (5) fölhasználásával adódott. (5)-nek nemcsak a z a gyöke, hanem az $\alpha z, \alpha^2 z, \ldots, \alpha^{m-1} z$ is gyök. Így, ha (2)-ben az $R^{1/m}$-et rendre $\alpha^k R^{1/m}, \ldots$-mel helyettesítjük, akkor mindig az (1) valamely gyökét kapjuk.
Ezek mindegyike különböző, tehát az m nem lehet ötnél nagyobb, és ha a gyököket $y_1, \ldots, y_m$ jelöli, akkor

$$\begin{aligned} y_1 &= p + z + p_2 z^2 + \ldots + p_{m-1} z^{m-1} \\ y_2 &= p + \alpha z + \alpha^2 p_2 z^2 + \ldots + \alpha^{m-1} p_{m-1} z^{m-1} \\ &\vdots \\ y_m &= p + \alpha^{m-1} z + \alpha^{m-2} p_2 z^2 + \ldots + \alpha p_{m-1} z^{m-1}. \end{aligned}$$

Ezen egyenletek egyszerűen oldhatók meg
$p, z, p_2 z^2, \ldots, p_{m-1} z^{m-1}$-re.
Ebből már következik, hogy $p, p_2, \ldots, p_{m-1}$, és $z = R^{1/m}$ az (1) egyenlet $y_1, \ldots, y_5$ gyökei racionális függvénye. Természetesen az is igaz, hogy az $R = z^m$ szintén racionális függvénye a gyököknek.
Az R mennyiség korábban meghatározott $v^{\frac{1}{n}}$ gyökmennyiség racionális függvénye:

(9) $$R = S + v^{\frac{1}{n}} + S_2 v^{\frac{2}{n}} + \ldots + S_{n-1} v^{\frac{n-1}{n}}.$$

ha e mennyiséget ugyanúgy kezelhetjük, mint a (2)-beli
y-t, akkor a $v^{\frac{1}{n}}$ gyökmennyiség adjunkciója vagy fölösleges, vagy pedig a $v^{\frac{1}{n}}, S, S_2, \ldots$ mennyiségek kifejezhetők az $y_1, \ldots, y_5$ gyökök racionális függvényeként.
Ezen meggondolás ismétlésével kapjuk, hohy mindazon irracionális (gyökös) mennyiségek, amelyek az y gyök kifejezésében szerepelnek, e gyökök racionális függvényei.

Ez pontosan az a föltételezés, amivel Ruffini bizonyítását indította. A hézag kitöltetett.
Ezek után Abel már nyugodtan használhatta elődei, Lagrange, Ruffini és Cauchy, eredményeit. Például Cauchy (Lagrange) már említett tételét

> *Legyen az $n \in \mathbb{N}$ természetes szám legnagyobb prímosztója p. Egy n-változós nem szimmetrikus racionális függvény vagy legalább p értéket vesz föl, vagy legföljebb kettőt.*

Ez azt jelenti, hogy a (2)-beli m prím csak 2 vagy 5 lehet. Abel mindkét esetben korrekten igazolta, hogy az általános ötödfokú egyenlet nem oldható meg gyökmennyiségekkel.
Abel utolsó dolgozatában (1829-ben, két hónappal halála előtt publikálta) egyenletek olyan speciális osztályával foglalkozott, amelyek gyökjelekkel megoldhatók. Ebbe az osztályba tartoznak pl. az

$$x^n - 1 = 0$$

alakúak, az ún. ciklotomikus egyenletek is. Az alábbi igen általános tételt igazolta.

Abel tétele. *Ha egy egyenlet olyan, hogy az összes gyöke kifejezhető valamely gyökének, mondjuk x-nek, racionális függvényeként, továbbá, ha két gyöke, mondjuk ϑx és $\vartheta_1 x$ (ahol ϑ, ϑ_1 racionális függvények) az alábbi módon függ egymástól*

$$\vartheta\vartheta_1 x = \vartheta_1\vartheta x, \tag{10}$$

akkor az egyenlet gyökjelekkel megoldható.

Ma a kommutatív csoportot Abel-csoportnak nevezik, és a (10)-beli formájú egyenletet Abel-egyenletnek Kronecker egy 1853-as cikke alapján.

Abel előbbi tétele a Galois-elmélet klasszikus főtételének egy speciális esete, amely úgy is fogalmazható, hogy egy egyenlet pontosan akkor oldható meg gyökjelekkel, ha Galois-csoportjának van olyan

$$G \supset H_1 \supset H_2 \supset \ldots \supset H_m = E$$

részcsoportlánca, amelyben mindegyik részcsoport prímindexű az őt megelőzőben. Egyszerűen belátható ugyanis, hogy minden véges Abel-csoport föloldható. E főtétel bizonyítását Galois 1829 májusában mutatta be a Francia Akadémián Párizsban, ugyanabban az évben, amikor Abel cikke megjelent.