

ÚT AZ ÁLTALÁNOS ELMÉLET FELÉ.

Klukovits Lajos

TTIK Bolyai Intézet

2011.április 12.

A továbbblépés előtt.

Egy érdekes egyenlet.

- 1593-ban a flamand Adrian van ROOMEN a következő feladatot tette közzé.
- Oldjuk meg a következő egyenletet (röviden írva).

$$x^{45} - 45x^{43} + 945x^{41} - 12300x^{39} + \dots - 3795x^3 + 45x = A$$

- Megjegyezte, hogy egyenlete szabályos sokszögek vizsgálatából adódott, és
- először speciális eseteket kellene elintézni. Például

- ha $A = \sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{2}}}}$,

- akkor

$$x = \sqrt{2 - \sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{3}}}}}$$

A továbbblépés előtt.

Egy érdekes egyenlet.

- Ez igen jó közelítés, hiszen elvégezve a gyökvonásokat $A \approx 1,990369453344395$,
- és ekkor $x \approx 1,990369453344394$
- A hiba nagyságrendje mindössze 10^{-15} .

F. Viète megoldása

- IV. Henrik francia király udvari ügyésze, csillagásza és matematikusa észrevette, hogy a bal oldal megkapható $\sin 45x$ -ből, és egy alkalmas transzformációval.
- E fölismerés alapján Viète 23 megoldást talált

$$\sin\left(\frac{\varphi}{45} - n8^\circ\right) \quad 0 \leq n < 23$$

- alakban.

Hogyan tovább?

Fontos észrevétel.

- Az már rég óta ismert, hogy a másodfokú egyenlet megoldása visszavezethető egy elsőfokúéra. Az imént láttuk, hogy a harmadfokú egyenlet megoldása másodfokú, míg a negyedfokú egyenlet megoldása harmadfokú egyenletre vezethető vissza.
- **Kérdés.**
- **Magasabb kitevőkre is ugyanez igaz?**

1. lépés: Edward WARING.

Már Viète is tudta:

- Ha az

$$x^n - a_1 x^{n-1} + a_2 x^{n-2} - \dots + (-1)^n a_n = 0$$

egyenlet gyökei $x_1, x_2, \dots, x_n$,

- akkor

$$a_1 = x_1 + x_2 + \dots + x_n$$

$$a_2 = x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n$$

$$\vdots$$

$$a_n = x_1 x_2 \dots x_n.$$

- Azaz, **az együtthatók a gyökök elemi szimmetrikus polinomjai.**

Edward WARING.

E. WARING: Miscellanea analytica (Cambridge 1762)

- Ha $x_1, x_2, \dots, x_n$ az előbbi egyenlet gyökei, akkor az $s_m = x_1^m + x_2^m + \dots + x_n^m$ alakú kifejezések az együtthatók szimmetrikus polinomjai.
- Általánosan: az előbbi gyökök minden racionális szimmetrikus függvénye az egyenlet együtthatóinak racionális függvényeként is előállítható.

E. WARING: Meditationes algebraicae (Oxford 1770)

Már lényegében a mai formában megadta a szimmetrikus polinomok alaptételét (minden test fölötti szimmetrikus polinom elemi szimmetrikus polinomok ugyanazon test fölötti polinomja), és annak egy konstruktív bizonyítását.

Edward WARING.

E. WARING: Meditationes algebraicae (Oxford 1770)

- Behatóan vizsgálta az ún. *ciklotomikus* egyenletet:

$$x^n - 1 = 0,$$

- és azt, hogy milyen alakúak azok az egyenletek, amelyek gyökei

$$x = \sqrt[n]{\alpha_1} + \sqrt[n]{\alpha_2} + \dots + \sqrt[n]{\alpha_n}$$

alakban állíthatók elő az együtthatókból.

- Az α_i -k az együtthatók szimmetrikus függvényei.
- Ez utóbbi miatt ő tekinthető a Galois-elmélet első közvetlen előfutárának.

2. lépés: Alexandre-Theophile VANDERMONDE

Sul la resolution des equations (1770-es akadémiai előadássorozat).

- Az egyenletek megoldásának általános alapjait kereste,
- a másod- és a harmadfokú egyenletek ismert megoldásaiból indult ki.
- Például, ha egy másodfokú egyenlet gyökei x_1, x_2 , akkor a megoldás, akkor azok

$$\frac{1}{2}(x_1 + x_2 + \sqrt{(x_1 - x_2)^2}).$$

alakban is írhatók,

- ahol a négyzetgyök mindkét értékét figyelembe kell venni.

2. lépés: Alexandre-Theophile VANDERMONDE

Sul la resolution des equations (1770-es akadémiai előadássorozat).

- E formula

$$\frac{1}{2}((x_1 + x_2) + \sqrt{(x_1 + x_2)^2 - 4x_1x_2})$$

alakban is írható, amelyben már a gyökök elemi szimmetrikus polinomjai szerepelnek.

- Ezek után azt kérdezte: írhatók-e az általános n -edfokú egyenlet gyökei is hasonló alakban,

Alexandre-Theophile VANDERMONDE

Sul la resolution des equations

- azaz

$$\begin{aligned} \frac{1}{n}((x_1 + \dots + x_n) + \sqrt[n]{(\varrho_1 x_1 + \dots + \varrho_n x_n)^n} \\ + \sqrt[n]{(\varrho_1^2 x_1 + \dots + \varrho_n^2 x_n)^n} \\ + \dots + \sqrt[n]{(\varrho_1^{n-1} x_1 + \dots + \varrho_n^{n-1} x_n)^n}), \end{aligned}$$

- alakban, ahol $\varrho_1, \dots, \varrho_n$ az n -edik egységgyökök.
- Ma az $\varrho_1 x_1 + \dots + \varrho_n x_n$ alakú kifejezéseket **Lagrange-rezolvensnek** nevezzük.
- A harmadfokú egyenleteknél a Vandermonde-Lagrange módszer elvezet a gyökökhöz, negyedfokúnál is kisebb módosítással.
- Magasabb fokszámra már csak speciális esetekben**

Alexandre-Theophile VANDERMONDE

Az $x^{11} - 1 = 0$ egyenlet

- Először egy olyan ötödfokú egyenlet megoldására vezette vissza a problémát,
- amelynek gyökei

$$\varrho + \varrho^{-1}, \varrho^2 + \varrho^{-2}, \varrho^3 + \varrho^{-3}, \varrho^4 + \varrho^{-4},$$

ahol ϱ egy primitív 11-edik egységgyök.

- A kapott ötödfokú egyenletet annak „Lagrange-rezolvensével” oldotta meg, amely

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

alakú, és α egy primitív ötödik egységgyök, x_1, x_2, x_3, x_4, x_5 pedig az ötödfokú egyenlet gyökei.

Alexandre-Theophile VANDERMONDE

Az $x^{11} - 1 = 0$ egyenlet

- Ahhoz, hogy L^5 racionális módon megadható legyen az x_i gyököket speciális sorrendben kell szerepeltetni.
- Ez most próbálgatással elérhető.

Az $x^n - 1 = 0$ egyenlet.

- Ezen általános esetben a megfelelő sorrend létezését igazolni kellene.
- Vandermonde úgy vélte, hogy az $x^n - 1 = 0$ egyenlet megoldása tárgyalható módszerével, azaz minden esetben létezik a kívánalmaknak megfelelő sorrend.
- Azt is kijelentette, hogy ennek igazolása nem lehet nehéz.
- Bizonyosnak látszik, hogy nem volt tisztában a nehézségekkel

Alexandre-Theophile VANDERMONDE

Az $x^n - 1 = 0$ egyenlet.

- Később kiderült, hogy a kívánalmaknak megfelelő sorrend létezése ekvivalens azzal, hogy a kitevőhöz, mint modulushoz létezik primitív gyök.
- A primitív gyök fogalmát Euler vezette be, de csak Gaussnak sikerült igazolnia először, hogy minden prímhez létezik primitív gyök.
- Ma már tudjuk, hogy egy $n \in \mathbb{N}$ -hez pontosan akkor létezik primitív gyök *modulo* n , ha $n = 2, 4, p^k, 2p^k$, ahol p páratlan prím, $k \in \mathbb{N}$.

3. lépés az általános probléma megoldása felé: Joseph Louis LAGRANGE.

Réflexions sur la résolution algébrique des equations (Berlin, 1771.)

- Kiindulásul az $x^3 + nx + p = 0$ alakú harmadfokú egyenletet vizsgálta.
- Ennek megoldása jól ismert az Ars Magna alapján, $x = r + s$, ahol r^3, s^3 egy másodfokú egyenlet két gyöke.
- Lagrange megmutatta, hogy az r, s a következőképp áll elő az egyenlet a, b, c gyökeiből:

$$r = \frac{1}{3}(a + \alpha b + \alpha^2 c)$$

$$s = \frac{1}{3}(a + \alpha^2 b + \alpha c),$$

ahol az α egy harmadik primitív egységgyök.

Joseph Louis LAGRANGE.

Réflexions sur la résolution algébrique des equations (Berlin, 1771.)

- Lagrange kijelentette, ez közvetlenül is megkapható.
- Az a, b, c gyökök egy tetszőleges

$$y = Aa + Bb + Cc \quad (1)$$

lineáris függvényét tekintette,

- amiből a gyökök permutálásával összesen 6 ilyen lineáris kifejezést kaphatunk, amelyek természetesen egy hatodfokú egyenlet gyökei.
- Megmutatta, hogy ha ez az egyenlet y^3 -ben másodfokú,
- akkor a (1)-beli A, B, C együttható sorozat szükségképp arányos az $1, \alpha, \alpha^2$, vagy $1, \alpha^2, \alpha$ sorozattal,
- tehát visszakapjuk a korábban már megismert eredményt.

Előretekintés Galois felé.

Ezekben a gondolatmenetekben már a Galois-elmélet számos alapvető ötlete fölsejlik.

1. Határozatlanok, mint például az r, s kifejezhetők a gyökök szimmetrikus függvényeiként.
2. Vizsgálta a (1) alakú racionális függvények viselkedését permutációkkal szemben.
3. Az egységgyökök segítségével fölépített kifejezést használt rezolvensként (a Lagrange-rezolvenst).

Joseph Louis LAGRANGE.

A negyedfokú egyenlet.

- Lagrange módszerét eredményesen alkalmazta a negyedfokú esetre is.
- Az

$$x^4 + nx^2 + px + q = 0$$

egyenletről még Ferrari mutatta meg (természetesen még nem ebben az alakban), hogy

- a megoldás első lépése az

$$y^3 + \frac{1}{2}ny^2 - qy + \frac{1}{8}(4nq - p^2) = 0$$

egyenlet megoldása.

Joseph Louis LAGRANGE.

A negyedfokú egyenlet.

- Lagrange megmutatta, hogy ennek gyökei megadhatók az eredeti egyenlet a, b, c, d gyökei racionális függvényeként:

$$u = \frac{1}{2}(ab + cd), \quad v = \frac{1}{2}(ac + bd), \quad w = \frac{1}{2}(ad + bc).$$

- Ha permutáljuk az eredeti egyenlet gyökeit,
- akkor az u csak az u, v, w valamelyikébe mehet át,
- ami szintén mutatja, hogy egy harmadfokú egyenlet gyökei.

Joseph Louis LAGRANGE.

Az általános eset.

- Ezzel is megpróbálkozott, de csak részleges eredményeket ért el.
- A legtávolabbra mutatók egyike a következő.
- Tekintsük egy n -edfokú egyenlet gyökei valamely $f(x', x'', \dots, x^{(n)})$ racionális függvényét,
- ahol a gyököket független változónak tekintette és először használta rájuk a „határozatlan” elnevezést.

Joseph Louis LAGRANGE.

Az általános eset.

- Legyen t és y a gyökök két racionális függvénye. Azt mondjuk, hogy *hasonlók*, valahányszor az összes olyan permutáció, amellyel szemben az egyik invariáns, a másik is az.
- Bebizonyította a következő tételt (amely a könyv 100. tétele)
- Ha az összes olyan permutáció, amellyel szemben t invariáns az y is invariáns, akkor az y kifejezhető a t és az egyenlet együtthatói racionális függvényeként.*
- E tétel már ténylegesen tekinthető a Galois-elmélet előfutárának.

4. lépés az általános probléma megoldása felé:

Gianfrancesco MALFATI.

De aequationibus quadratocubicis dissertatio analytica (Siena 1771)

A harmadfokú egyenleteknél bevált módszert megkísérelte alkalmazni az ötödfokú egyenletekre.

- Az

$$x^5 + 5ax^3 + 5bx^2 + 5cx + d = 0 \quad (1)$$

egyenlet

- x gyökét most az

$$x + m\sqrt[5]{f^4} + p\sqrt[5]{f^3} + q\sqrt[5]{f^2} + n\sqrt[5]{f} = 0 \quad (2)$$

egyenletből akarta származtatni.

- Az előbbihez hasonlóan helyettesített: $\sqrt[5]{f}$ helyett rendre $\alpha\sqrt[5]{f}, \alpha^2\sqrt[5]{f}, \alpha^3\sqrt[5]{f}, \alpha^4\sqrt[5]{f}$ került, α primitív ötödik egységgyök.

Gianfrancesco MALFATI.

De aequationibus quadratocubicis dissertatio analytica (Siena 1771)

- Ezután megszorozta (2)-t a kapott lineáris kifejezésekkel, és egy ötödfokú ún. *kanonikus egyenletet* kapott.
- Ennek együtthatóit összehasonlítva (1)-gyel, és $f = 1$ helyettesítéssel
- m, p, q, n -re a következő föltételekhez jutott.

$$\begin{aligned} mn &= y, & pq &= u \\ 25uy - 5a^2 + 5\frac{c}{3} &= z \end{aligned}$$

- Rengeteg számolás után z-re egy hatodfokú egyenletet kapott.
- Ezen egyenletnek általában nincs első-, másod-, vagy harmadfokú racionális faktora, de ha speciális esetben van, akkor (1) megoldható gyökvonásokkal.

4. lépés az általános probléma megoldása felé:

Gianfrancesco MALFATI.

De aequationibus quadratocubicis dissertatio analytica (Siena 1771)

- először z, majd m, p, q, n határozható meg,
- majd megkapjuk a gyököket

$$\begin{aligned} x_0 &= -(m + p + q + n) \\ x_1 &= -(\alpha m + \alpha^2 p + \alpha^3 q + \alpha^4 n) \\ x_2 &= -(\alpha^2 m + \alpha^4 p + \alpha q + \alpha^3 n) \\ x_3 &= -(\alpha^3 m + \alpha p + \alpha^4 q + \alpha^2 n) \\ x_4 &= -(\alpha^4 m + \alpha^3 p + \alpha^2 q + \alpha n) \end{aligned} \quad (2)$$

alakban.

5. lépés az általános probléma megoldása felé: Lagrange.

Egy újabb megközelítés.

- Malfatitól függetlenül Lagrange is konstruált egy hasonló z rezolvenst.
- Ez a gyökök egy olyan függvénye, amely a gyökök permutációikor 6 különböző értéket vett föl.
- A hasonlóság abban állt, hogy ez is a gyökök 20 permutációjával szemben volt invariáns.
- Mai fogalmakkal e permutációcsoport a következőképp definiálható:

$$k' \equiv gk + h \pmod{5} \quad (3)$$

- ahol $1 \leq g \leq 4$ és $0 \leq h \leq 4$.
- Ugyanezen csoport fontos szerepet játszik a Galois-elméletben is.

6. lépés: Paolo RUFFINI.

- 1765-ben született, Lagrange tanítványa volt.
- 3 dolgozatot írt az ötöd- és magasabb fokú egyenletek gyökjelekkel való megoldhatatlanságáról. Az első dolgozat csak összegyűjtött munkáiból ismert, a másik kettőt 1802-ben ill. 1813-ban publikálta.
- Mesteréhez hasonlóan ő is az n -edfokú egyenlet gyökei egy racionális függvényéből indult ki.

Eredményei

- Ha a gyökök azon permutációinak száma p , amelyek függvényét fixen hagyják, akkor $p|n!$.
- Ez esetben a függvény $n!/p$ különböző értéket vesz föl a gyökök permutációikor.
- Lagrange: az ilyen függvények $n!/p$ -edfokú egyenletek gyökei.

Paolo RUFFINI.

Eredményei.

- Vizsgálta azon p permutáció alkotta halmazt (ma azt mondanánk **permutációcsoporthot**), amelyek e függvényt fixen hagyják.
- Speciálisan, ha $n = 5$, akkor $5!/p$ lehetséges értékei 2, 5, 6 de nem lehet 3, 4.
- Ebből következik, hogy a Lagrange rezolvens nem elégíthet ki harmad-, vagy negyedfokú egyenletet.
- Továbbá, ha $n!/p \neq 2$, akkor $5|(n!/p)$,
- valamint, ha $n!/p = 5$, akkor ugyan ötödfokú rezolvens egyenlet létezik, de az nem redukálható

$$z^5 - m = 0 \quad (4)$$

alakúra.

Paolo RUFFINI.

Összegzés.

- Bizonyítani vélte, hogy: az általános ötödfokú egyenlet nem oldható meg radikálokkal (gyökvonásokkal).
- Bizonyítása azért volt hiányos, mert azon a föltételezésen alapult, hogy ezen radikálok a gyökök racionális függvényei.
- Ezt azonban bizonyítania kellett volna. E „hézagot” később Abel szüntette meg.
- Abel: A kérdéses radikálok mindig előállíthatók a gyökök és bizonyos egységgyökök racionális függvényeként.
- A kortársak nem értékelték eredményét, nem fogadták el bizonyítását. DE nem tudtak igazi, konkrét kifogást emelni.

Augustin CAUCHY.

Sur le Nombre des Valeurs ... 1815.

- Általánosította Ruffini azon eredményét, miszerint
- *Egy nem szimmetrikus racionális függvény által fölvehető különböző értékek száma nem lehet ötnél kevesebb, kivéve ha csak két értéket vesz föl.*
- n változós függvényekre.
- Cauchy tétele. *Tekintsünk egy n változós nem-szimmetrikus függvényt, és legyen p az n legnagyobb prímosztója. Az e függvény által fölvehető különböző értékek száma nem lehet kevesebb p -nél, kivéve ha az 2.*
- Elsőként különböztette meg a **permutációt** és a **helyettesítést**.
- Változók valamely sorrendben írása: **permutáció**, áttérés egy permutációról egy másikra: **helyettesítés**.

Augustin CAUCHY.

A permutációcsoportok előfutára.

- Jelölésrendszere: Ha 1.2.4.3 és 2.4.3.1 két permutáció, akkor az elsőről a másodikra való áttérést (helyettesítést) a következőképp jelölte

$$\begin{pmatrix} 1. & 2. & 4. & 3. \\ 2. & 4. & 3. & 1. \end{pmatrix}$$

- Bevezette a helyettesítések szorzatának fogalmát: Ha S, T helyettesítések, akkor ST az a helyettesítés, amelyet S, T egymás utáni végrehajtásával kapunk.
- Galois ugyanígy használta e fogalmat.

Augustin CAUCHY.

Tovább a permutációcsoportok felé, 1844-46.

- Két helyettesítés **hasonló**, ha ugyanaz a ciklus struktúrájuk.
- Igazolta: a P, Q helyettesítések pontosan akkor hasonló, ha valamely R helyettesítésre $Q = R^{-1}PR$.
- Helyettesítések csoportja, helyettesítés ill. e csoport rendje.

- Helyettesítések bármely csoportjának rendje osztható bármely benne levő helyettesítés rendjével.
- n változó helyettesítései bármely csoportjának rendje osztója $n!$ -nak.
- Ez utóbbi tételt lényegében már Lagrange igazolta, Cauchy támaszkodott is Lagrange eljárására: ő is mellékosztályokra bontott.
- Később, amikor C. Jordan általánosította ezt tetszőleges véges csoportokra, elismerően hivatkozott mindkettőjükre.

7. lépés: Niels Henrik ABEL.

- Az 1802-ben született norvég matematikus — elődeihez hasonlóan — azt vélte: megtalálta az ötödfokú egyenlet gyökképletét, DE ő is megtalálta a hibát eljárásában.
- Első tényleges eredményeit 1824 tavaszán egy francia nyelvű kéziratban (saját kiadás) közölte, de gyors elutasításban részesült vele Párizsban.
- Az 1826-os német nyelvű dolgozatában már világos és korrekt bizonyítást adott a negyednél magasabb fokú egyenletek gyökjelekkel való megoldhatatlanságára.
- Beweis der Unmöglichkeit algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen**
- A 20 oldalas cikk a berlini **Journal für reine und angewandte Mathematik**, az ún. „Crelle Journal” 1. számában jelent meg. (A legrégebbi, a mai napig megjelenő matematikai folyóirat.)

Niels Henrik ABEL.

Abel bizonyítása 1.

- Az alap Lagrange és Cauchy azon eredményei, amelyek az n -változós nem szimmetrikus racionális függvények viselkedésére vonatkoztak akkor, ha a változókat permutálták.
- De egészen más módon alkalmazta azokat, mint elődei.
- Újszerű kiindulópontja: **az egyenlet együtthatóit általánosoknak, pusztán szimbólumoknak tekintette, amelyek között semmiféle összefüggés nincs.**
- A kezdeti lépés az

$$y^5 - ay^4 + by^3 - cy^2 + dy - e = 0 \quad (5)$$

egyenlet vizsgálata, ahol

- az együtthatók „általánosak”, azaz pusztán betűk, **független változók.**

Niels Henrik ABEL.

Abel bizonyítása 2.

- Föltéve, hogy (5)-beli y kifejezhető az együtthatókból az alpműveletekkel és gyökvonásokkal Abel föltételezte, hogy a megoldás

$$y = p + p_1 R^{1/m} + p_2 R^{2/m} + \dots + p_{m-1} R^{(m-1)/m} \quad (6)$$

alakban írható, ahol m prímszám.

- Föltételezte, hogy $R, p, p_1, \dots, p_{m-1}$ ugyanolyan formájú kifejezések, mint y , amelyek további gyökmennyiségeket is tartalmazhatnak.
- A „lebontási” eljárást addig kell folytatni, míg az együtthatók racionális függvényeihez jutunk (ilyenek állnak a „legbelső” gyökjelek alatt).

Niels Henrik ABEL.

Abel bizonyítása 3.

- A (5)-ben a konstans együtthatók közé Abel mindig odaértette az m -edik egységgyököket, ahol m egy olyan prím kitevő, amely szerepel a megoldásban.
- Megjegyzés.** Galoisnál ez bizonyos értelemben fordítva lesz, ő az a, b, c, d, e együtthatók racionális függvényeiből indult ki, és ezekhez adjungált prímkitevős gyökmennyiségeket egymás után.
- Föltehető — mondta Abel —, hogy $R^{1/m}$ nem fejezhető ki, mint az $a, b, \dots, p, p_1, \dots$ racionális függvénye, mert akkor a gyökmennyiségek adjungálása (gyökvonások végzése) fölösleges volna.
- Föltehető, hogy (5)-ben nem az összes $p_1, \dots$ együttható zéró.
- Első dolgozatában Abel föltételezte, hogy $p_1 \neq 0$, de később (második dolgozat) észrevette, hogy ez fölösleges.

Niels Henrik ABEL.

Abel bizonyítása 4.

- Ha R -et R/p_1^m -mel helyettesítjük, akkor $p_1 = 1$ adódik, majd $R^{1/m}$ helyébe z -t írva

- adódik

$$y = p + z + p_2 z^2 + \dots + p_{m-1} z^{m-1}. \quad (7)$$

- Ezt az (5) egyenletbe helyettesítve

$$q + q_1 z + q_2 z^2 + \dots + q_{m-1} z^{m-1} = 0, \quad (8)$$

- ahol $q, q_1, \dots$ az $a, b, \dots, p_1, p_2, \dots$ és R polinomja.

Niels Henrik ABEL.

Abel bizonyítása: döntő lépés.

- Abel azt állítja, hogy ahhoz, hogy (8) teljesüljön szükséges az, hogy

$$q = 0, \quad q_1 = 0, \dots, q_{m-1} = 0,$$

amit zseniálisan bizonyított be.

- A z közös gyöke a (8) egyenletnek, valamint a

$$z^m - R = 0 \quad (9)$$

egyenleteknek.

- Amennyiben a $q, q_1, \dots$ együtthatók nem mindegyike zéró a közös gyökök száma legföljebb $m - 1$, mondjuk k .

Niels Henrik ABEL.

Abel bizonyítása: a döntő lépés.

- A (8) és az (9) bal oldalán álló polinomok legnagyobb közös osztója egy k -adfokú polinom, így az

$$r + r_1 z + r_2 z^2 + \dots + r_k z^k = 0 \quad (10)$$

egyenlethez jutunk.

- Ha a (10) bal oldalán álló polinomot irreducibilis tényezőkre bontjuk, akkor azok valamelyike zéró, mondjuk

$$t_0 + t_1 z + \dots + t_{\mu-1} z^{\mu-1} + z^\mu = 0. \quad (11)$$

- Abel állítása: **Föltehetjük, hogy lehetetlen ilyen alakú alacsonyabb fokú egyenletet találni.**

Niels Henrik ABEL.

Abel bizonyítása: a döntő lépés.

- (11)-nek μ számú gyöke van, amelyek egyúttal (9)-nek is gyökei.
- Ez utóbi gyökei azonban αz alakúak, ahol α m -edik egységgyök.
- Világos, hogy $\mu \geq 2$, különben a z az $a, b, \dots, p, p_1, \dots$ racionális függvénye lenne (nem szerepelhetnének benne gyökjelek).
- Kaptuk: (11)-nek legalább két gyöke van, z és αz ,
- tehát

$$\begin{aligned} t_0 + t_1 z + t_2 z^2 + \dots + t_{\mu-1} z^{\mu-1} + z^\mu &= 0, \\ t_0 + \alpha t_1 z + \alpha^2 t_2 z^2 + \dots + \alpha^{\mu-1} t_{\mu-1} z^{\mu-1} + \alpha^\mu z^\mu &= 0. \end{aligned} \quad (12)$$

- Az első egyenletet α^μ -szosát kivonva a másodikból

Niels Henrik ABEL.

Abel bizonyítása: a döntő lépés.

- egy μ -nél alacsonyabb fokú egyenletet kapunk z -re, ami lehetetlen.
- Ez pedig azt jelenti, hogy a $q, q_1, \dots, q_{m-1}$ mindegyike zéró, ahogy állítottuk.
- Emlékezzünk: (8)-at úgy kaptuk, hogy (7)-et az (5) egyenletbe helyettesítettük, s fölhasználtuk (9)-et.
- (9)-et azonban nemcsak z elégíti ki, hanem

$$\alpha z, \alpha^2 z, \dots, \alpha^{m-1} z$$

is.

- Helyettesítsük (6)-ban $R^{1/m}$ -et $\alpha^k R^{1/m}$ -mel, $R^{2/m}$ -et $\alpha^k R^{2/m}$ -mel, $\dots$, mindig (5) gyökeit kapjuk.
- A kapott gyökök mind különbözők, így m nem lehet nagyobb 5-nél.

Niels Henrik ABEL.

Abel bizonyítása: a döntő lépés.

- Ha ezen különböző gyököket $y_1, \dots, y_m$ jelöli, akkor
- kapjuk, hogy

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

- Ezen egyenletekből megkapható $p, z, p_2 z^2, \dots, p_{m-1} z^{m-1}$.
- Továbbá $p, p_2, \dots, p_{n-1}$ valamint $z = R^{1/m}$ az (5) $y_1, \dots, y_5$ gyökei racionális függvénye.
- Természetesen $R = z^m$ is racionális függvénye a gyököknek.

Niels Henrik ABEL.

Abel bizonyítása: a döntő lépés.

- Az R mennyiség korábban meghatározott $v^{\frac{1}{n}}$ gyökmennyiség racionális függvénye.
- Ezen gyökmennyiség

$$R = S + v^{\frac{1}{n}} + S_2 v^{\frac{2}{n}} + \dots + S_{n-1} v^{\frac{n-1}{n}} \quad (13)$$

alakban írható.

- E mennyiség ugyanúgy kezelhető, mint a (6) -beli y , belátható ugyanis, hogy vagy $v^{1/n}$ -adjungálása fölösleges, vagy $v^{1/n}, S, S_2, \dots$ kifejezhető az $y_1, \dots, y_5$ gyökök racionális függvényeként.
- Az előbbiekhöz hasonlóan folytatva az eljárást kapjuk, hogy az y -ban előforduló irracionális kifejezés a gyökök racionális függvénye.

Niels Henrik ABEL.

Abel bizonyítása: a döntő lépés.

Ez az hipotézis, amelyből Ruffini bizonyítását indította az ötödfokú egyenlet megoldhatatlansága bizonyításakor. E hipotézis most igazolást nyert.

Összegzés

- Így 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 (6) -beli m prím csak 2 vagy 5 lehet. Abel mindkét esetben korrekten igazolta, hogy az általános ötödfokú egyenlet nem oldható meg gyökmennyiségekkel.

Mémoire sur une classe particulière d'equations résoluble algébraiquement

Utolsó dolgozata.

- 1829-ben, két héttel halála előtt publikálta a Crelle Journal 4. számában.
- Egy olyan egyenlettípussal foglalkozott, amely megoldható radikálokkal a fokszámtól függetlenül.
- Ebbe tartoznak az $x^n - 1 = 0$ ún. ciklotomikus egyenletek.
- Abel tétele. Ha egy egyenlet összes gyöke megkapható az egyik gyök — legyen ez x — racionális függvényeként, akkor bármely két gyök, $\vartheta x, \vartheta_1 x$ a következőképp függ össze:

$$\vartheta \vartheta_1 x = \vartheta_1 \vartheta x, \quad (14)$$

akkor az egyenlet gyökjelekkel megoldható.

- Abel e tétele a Galois-elmélet főtételének speciális esete.

Mémoire sur une classe particulière d'equations résoluble algébraiquement

Megjegyzés.

A Galois-elmélet főtétele. Egy egyenlet pontosan akkor oldható meg radikálokkal (gyökvonásokkal), ha az egyenlet Galois-csoportjának van olyan normállánca, amelyben előforduló normálosztók mindegyike prím indexű a megelőzőben.

Záró megjegyzés.

E főtétel bizonyítását Galois 1829 májusában mutatta be a Francia Akadémián Párizsban, ugyanabban az évben, amikor Abel cikke megjelent.