A megoldhatóság kérdésének megválaszolása: E. Galois elmélete.

Klukovits Lajos

TTIK Bolyai Intézet

2013. április 17.

Evariste Galois (1811 - 1832)

- 1811. október 25-én született egy Párizs közeli kisvárosban Bourg-la-Reine-ben, ahol apja polgármester volt.
- A család a forradalom 1789-es kitörésétől fogva annak őszinte híve lett, ami meghatározta neveltetését.
- 1823-tól a nagy múltú Louis-le Grand Líceumban tanult,
- amelyet eredetileg 1563-ban alapítottak jezsuita iskolaként.
- A XVII. századra egy olyan jóhírű intézmény lett, hogy XIV. Lajos a nevét adta neki.
- Az egyetlen olyan iskola Párizsben, amelyik zavartalanul működött a forradalom alatt is.
- Jó otthoni (elsősorban anyai) előképzettsége révén az iskola egyik legjobb tanulója lett, díjakat nyert görög és latin fordításaival.

Evariste Galois (1811 - 1832)

- 1826-ban új igazgató: a „vallásos nevelés” nagymérvű erősítése.
- Ez már nem találkozott Galois érdeklődésével és sok problémája adódott miatta.
- Szerencséjére, de egyben szerencsétlenségére is az új matematika tanára Vernier a korábbi Lacroix könyv helyett Lagrange geometriáját alkalmazta tankönyvként.
- Ez nagyon megtetszett Galoisnak, szinte napok alatt átolvasta az egészet, ami két tanév anyaga lett volna.
- Ez volt a döntő momentum, ami véglegesen a matematika felé fordította.
- Csak az elmélet szárnyalása érdekelte, a gyakorló feladatok nem.
- legtöbb tanárának ez nem tetszett.

Evariste Galois (1811 - 1832)

- Egy 1827-es jellemzéséből: *Semmi más nincs munkájában, csak furcsa fantáziálás és elutasítás; mindig azt csinálja amit nem kellene. Minden nap valami rosszat cselekszik. Szórakozott „dumaláda”.*
- Egyetlen támogatója, a matematika tanára javaslatára fölvételizett az ECOLE POLYTECHNIQUE-be. A vizsgán azonban megbukott 1828 júniusában. Visszatért régi iskolájába.
- Új matematika tanára: Louis-Paul-Emile-RICHAR, aki rögtön észrevette, tanítványa nem mindennapi tehetségét.
- Galois élete talán legboldogabb időszaka következett.
- Tanára jellemzése: *...e tanuló messze kimagaslik az osztály többi tagja közül.*
- Galois megismerkedett a korabeli matematikai kutatások fő irányaival, Legendre, Gauss, Lagrange és Cauchy fontosabb eredményeivel.

Evariste Galois (1811 - 1832)

- Az 1818-ban alapított Annales de Mathématique 1829. április 1-i számában jelent meg első dolgozata, a befutott tudósok dolgozatai között.
- A dolgozat főtétele: *Ha egy tetszőleges fokú racionális együtthatós egyenlet valamely gyöke egy tisztán periódikus lánctört, akkor az egyenletnek van még egy ilyen alakú gyöke, amelyet úgy kapunk, hogy a -1-et elosztjuk azzal a tisztán periódikus lánctörttel, amelynek periódusa éppen az előbbi lánctört periódusa, csak a abban a tagokat fordított sorrendben kell írni.*
- Részletesebben, ha $f(x) \in \mathbb{Q}[x]$, és $f(\alpha) = 0$, ahol $\alpha = \langle a_0; \overline{a_1, \ldots, a_k} \rangle$, akkor $f(\beta) = 0$ is teljesül, ahol $\beta = -1/\langle a_0; \overline{a_k, \ldots, a_1} \rangle$.
- A dolgozaton még erősen érződik Lagrange hatása, szinte semmit sem mutat Galois későbbi eredeti gondolataiból.

Evariste Galois (1811 - 1832)

Részletesebben:

$$\alpha = a_0 \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ddots}}}} = \langle a_0; a_1, a_2, a_3, a_4, \ldots \rangle$$

α *periódikus*, ha van olyan $k \in \mathbb{N}_0$ és $m, t \in \mathbb{N}$, hogy bármely $i \in \mathbb{N}$-re

$$a_{k+i} = a_{k+mt+i}$$

Ez esetben az következő írásmodot használjuk

$$\alpha = \langle a_0; a_1, \ldots a_k, \overline{a_{k+1}, \ldots, a_{k+m}} \rangle$$

Evariste Galois (1811 - 1832)

Két további dolgozata.

- 1829 májusában küldte el Galois az Akadémiának az egyenletek megoldhatóságával foglalkozó első dolgozatát,
- majd majd nyolc nappal később még egyet, amelyben prímszámfokú egyenletekkel foglalkozott.
- Mindkettőt Cauchy kapta meg referálásra, aki egyszerűen elvesztette azokat. A mai napig sem kerültek elő.

Evariste Galois (1811 - 1832)

Újabb fölvételi kudarc.

- Nyáron ismét fölvételizett az Ecole Polytechnique-be, de most sem járt sikerrel.
- A bizottság által feladott kérdésre a tanárok szerint túl röviden, tömören válaszolt. Galois nem méltányolta a professzorok szerinte „érthetetlenül lassú fölfogását", és rövid vita után a táblatörlőt hozzájuk dobta.
- Ez végét jelentette egyetemi karrierjének.

Evariste Galois (1811 - 1832)

- 1830. februárjában egy újabb dolgozatot küldött az Akadémiának szintén az algebrai egyenletek megoldhatóságáról.
- Az aktuális bíráló Fourier volt, aki meghalt azelőtt, hogy érdemben foglalkozott volna vele. E mű is elveszett.
- 1830. áprilisában végre megjelent egy rövid dolgozata nyomtatásban. Ebben a korábbi — az Akadémiához küldött — munkái néhány eredményét közölte bizonyítás nélkül.
- Az egyik fő állítás a következő volt.
- *Annak, hogy egy prímfokú egyenlet gyökjelekkel megoldható legyen szükséges és elégséges föltétele az, hogy amennyiben két gyökét ismerjük, akkor a többi gyök velük racionálisan kifejezhető legyen.*
- Utalt rá, hogy ebből már következik az ötödfokú egyenletek gyökjelekkel való megoldhatatlansága.

Evariste Galois (1811 - 1832)

Harmadik benyújtott dolgozata.

- 1931. januárjában a korábbi két dolgozata javított, bővített változatát nyújtotta be.
- Az új bírálók: Poisson és Lacroix, akik nem vesztették el,
- Poisson el is olvasta.
- DE egyszerűen azt mondta, hogy
- NEM ÉRTI.

Evariste Galois (1811 - 1832)

Poisson konkluziója.

- *Minden tőlünk telhetőt megtettünk, hogy megértsük Galois bizonyítását. Érvelései azonban nem eléggé világosak, nem eléggé kidolgozottak, így nem tudjuk megítélni pontosságukat, sőt érvelései egyikét sem tudjuk megfogalmazni e jelentésben.*
- *A szerző azt közli, hogy azon állítása, amely speciális szerepet játszik a dolgozatban egy általános elmélet része, amelynek számos alkalmazása képzelhető el.*
- *Gyakran előfordul, hogy egy elmélet részeit, amelyek egymásra épülnek, egyszerűbb teljességükben megérteni mint az egyes részleteket.*
- *Ezért, hogy megfontolt véleményt tudjunk mondani meg kell várnunk azt, hogy a szerző a teljes dolgozatát elénk tárja. Az Akadémiához benyújtott, jelen formájú részletek alapján nem tudjuk javasolni a dolgozat jóváhagyását.*

Evariste Galois (1811 - 1832)

Az 1831-s dolgozat főbb eredményei 1.

- Galois kiindulópontja az $f(x) = 0$ egyenlet, ahol $f(x)$ egy olyan polinom, amelynek együtthatói ismert mennyiségek,
- pl. racionális, vagy irracionális számok, esetleg egyszerűen betűk.
- Ezen együtthatók racionális függvényeit egyszerűen *racionálisoknak* nevezte.
- Ezekhez további mennyiségeket, például egységgyököket, azok racionális kifejezéseit adjungálta, s mindezeket *tágabb értelemben racionálisoknak* tekintette. Tehát
- **mai terminológiával:** *az együtthatók által generált testet gyökmennyiségekkel bővítette.*
- Ha az $f(x)$ polinom az alaptest (az együtthatók által generált test) fölött faktorizálható volt, akkor *reducibilisnek* nevezte, ha pedig nem, akkor *irreducibilisnek*.

Evariste Galois (1811 - 1832)

Az 1831-s dolgozat főbb eredményei 2.

- Cauchy-t követve használta a *permutáció* és a *helyettesítés* fogalmát, azaz az előbbi véges sok elem valamely sorrendjét, rendezését, míg az utóbbi az egyik sorrendről (rendezésről) egy másikra való áttérést jelentette.
- Bevezette a *helyettesítések csoportjának* fogalmát, ezen egyszerűen a helyettesítések szorzásra (egymás utáni végrehajtására) zárt halmazát értette.
- **Megjegyzés.** Abban a korban természetes volt, hogy amennyiben egy helyettesítést tekintettek, akkor mindig rendelkezésre állónak vették az inverzét is.
- **1. Lemma.** (Abel 1829-es dolgozatának 1. Tétele.) *Ha egy f polinomnak van közös gyöke valamely g irreducibilis polinommal, akkor $g|f$.*

Evariste Galois (1811 - 1832)

Az 1831-s dolgozat főbb eredményei 2.

- **Következmény.** *Ha V az irreducibilis $g(x) = 0$ egyenlet egy ismert gyöke, akkor a K alaptest ismeretében a $K(V)$ testbővítés is ismert.*
- **Bizonyítás. A testbővítések elméletéből ismert, hogy $K(V) \cong K[x]/(g)$.**
- **2. Lemma.** *Ha a $g(x) = 0$ egyenletnek nincs többszörös gyöke, s gyökeit $a, b, c, \ldots$ jelöli, akkor mindig megadható a gyökök egy olyan V függvénye, amely a gyökök minden permutálásakor különböző értéket vesz föl.*
- Galois szerint V lehet például a következő kifejezés:

$$V = Aa + Bb + Cc + \ldots, \tag{1}$$

ahol $A, B, C, \ldots$ alkalmas egészek.

Evariste Galois (1811 - 1832)

Az 1831-s dolgozat főbb eredményei 3.

- E lemmából speciális esetként rögtön adódik az az állítás, amit ma primitív elem létezéseként fogalmazunk meg. Ez Galois-nál a következő formát ölti.
- **3. Lemma.** *Ha V az előbbi, akkor az $a, b, c, \ldots$ mindegyike kifejezhető V racionális függvényeként.*
- **Galois bizonyítása.** Legyen

$$V = \varphi(a, b, c, \ldots).$$

- Most pemutáljuk úgy a $b, c, \ldots$ gyököket, hogy az a fixen marad, és képezzük a

$$[V - \varphi(a, b, c, \ldots)] \cdot [V - \varphi(a, c, b, \ldots)] \cdot \ldots$$

szorzatot.

Evariste Galois (1811 - 1832)

Az 1831-s dolgozat főbb eredményei 4.

- Ez utóbbi szimmetrikus függvénye a $b, c, \ldots$ gyököknek, amelyek a $g(x)/(x - a)$ polinom gyökei,
- tehát kifejezhető az a racionális függvényeként.
- Így egy

$$F(V, a) = 0 \tag{2}$$

egyenlethez jutunk,

- amelynek a

$$g(x) = 0 \tag{3}$$

egyenlettel csak az a a közös gyöke, tehát

- nem fordulhat elő, hogy $F(V, b)$ zéró legyen.
- Mivel (2) és (3)-nak csupán egy közös gyöke van, az racionálisan kifejezhető, tehát az a racionális függvénye a V-nek.

Evariste Galois (1811 - 1832)

Az 1831-s dolgozat főbb eredményei 5.

- **Megjegyzés.** Galois azon állítása, mely szerint $F(V, b) \neq 0$ korrekt, ha a bal oldal

$$[V - \varphi(b, a, c, \ldots)] \cdot [V - \varphi(b, c, a, \ldots)] \cdot \ldots,$$

ahol a φ argumentumaként az összes olyan permutáció előfordul, ahol az első helyen a b áll.

- Később szigorúan igazolták, hogy így elvégezhető a bizonyítás.
- Poisson megjegyzése a 3. Lemmáról: „annak bizonyítása fölösleges, mert már szerepel Lagrange egy dolgozatában."
- E megjegyzése érthető, mert Galois csak vázlatos bizonyítását adja annak, hogy $F(V, b)$ nem lehet zéró, míg Lagrange bizonyítása teljesebb.

Evariste Galois (1811 - 1832)

Az 1831-s dolgozat főbb eredményei 6.

- **Következmény.** Mai terminológiával

$$K(a, b, c, \ldots) = K(V), \tag{4}$$

ahol K az alaptest és V *primitív elem*, így az gyöke egy irreducibilis egyenletnek.

- Jelölje a továbbiakban ezen egyenlet összes gyökét

$$V, V', V'', \ldots, V^{(n-1)}.$$

- **4. Lemma.** *Ha $a = \varphi(V)$ gyöke az eredeti egyenletnek, vagyis (3)-nak, akkor $\varphi(V'), \varphi(V''), \ldots$ is gyöke annak.*
- Ezután csak annyit jegyzett meg, hogy az állítás igen egyszerűen igazolható,
- majd következik a főtétel.

Evariste Galois (1811 - 1832)

Az 1831-s dolgozat főbb eredményei 7.

- **1. Tétel.** *Van az $a, b, c, \ldots$ gyökök permutációinak egy olyan csoportja, hogy*
  - *($\imath$) a gyökök minden olyan függvénye, amely e helyettesítésekkel szemben invariáns racionálisan megadható;*
  - *($\imath\imath$) és megfordítva: a gyökök minden racionális függvénye invariáns e csoporttal szemben.*
- **Megjegyzés.** Következetlen szóhasználat: előbb permutációt említ, majd helyettesítések csoportját, de mondanivalója ennek ellenére teljesen világos. A bizonyítás korrekt, de tömörsége miatt igen nehéz megérteni.

Evariste Galois (1811 - 1832)

Az 1. Tétel bizonyítása (Galois)

- Az egyik lépésben Galois azt vizsgálta, hogy hogyan változik az egyenlethez tartozó csoport (a helyettesítések csoportja) akkor, ha az alaptestet egy segédegyenlet valamely, vagy összes gyökének adjungálásával bővítjük.
- Világos, hogy a bővítés révén az eredeti G csoport valamely H részcsoportját kapjuk. Ha a H egy valódi részcsoport, akkor G a következőképp bontható föl:

$$G = H + HS + HS' + \ldots \tag{5}$$

- vagy

$$G = H + TH + T'H + \ldots \tag{6}$$

alakban. (S ill. T permutációt, vagyis csoportelemet jelöl.)

Evariste Galois (1811 - 1832)

Az 1. Tétel bizonyítása (Galois)

- E lépések nem igazán világosak az eredeti dolgozatba, csak egy Chevalier-hez írott levél alapján lett az.
- Galois: „A két fölbontás általában nem egyezik meg. Ha megegyeznek, akkor a fölbontás valódi."
- Modern terminológiával: ez esetben a H normálosztó G-ben.
- Speciálisan, ha a segédegyenlet mindegyik gyökét adjungáljuk, akkor a fölbontás valódi.
- Ez éppen Galois 3. Tétele a dolgozatban. Ennek bizonyítását elhagyta, mint olyat, amelyet „az olvasó egyszerűen elvégezhet".

Evariste Galois (1811 - 1832)

A fő kérdés és a válasz.

- Most következik a fő kérdés:
- *Mely esetekben oldható meg az egyenlet gyökjelekkel?*
- Világos, hogy elég csak prímkitevőjű gyökvonásokkal foglalkozni. Galois mindig föltette, hogy a p-edik (p prím) egységgyököket már előre adjungáltuk.
- Ez nem jelent korlátozást, hiszen Gauss igazolta, hogy a p-edik egységgyökök mindig megkaphatók p-nél alacsonyabb fokú gyökvonásokkal.
- Hiszen azok az 1 és az

$$x^{p-1} + x^{p-2} + \ldots + x + 1$$

ún. *körosztási polinom* gyökei.

Evariste Galois (1811 - 1832)

A válasz.

- Tegyük föl, hogy ha egy olyan r gyökmennyiséget adjungálunk, amely az

$$x^p - s = 0 \tag{7}$$

egyenlet gyöke,
- a tekintetett helyettesítések csoportja (ma Galois csoport) redukálódik.
- Mivel az alaptest tartalmazza az

$$\alpha, \alpha^2, \ldots, \alpha^p = 1$$

p-edik egységgyököket, ugyanezt a redukálást eredményezi (7) összes gyökének adjungálása is.
- Galois 1831-es dolgozata 3. Tételéből következik, hogy ez esetben az (5) fölbontás valódi, azaz H normálosztó.

Evariste Galois (1811 - 1832)

A válasz.

- Bizonyítás nélkül állította, hogy az (5) fölbontásban szereplő tagok száma (a H G-beli indexe) a p prímszám.
- Megfordítva, ha van G-nek egy p indexű H normálosztója, akkor a G Galois csoport a H részcsoportra redukálódik p-edik gyökök adjungálásával.
- Ezen állítást a modern tankönyvekben is úgy bizonyítják, hogy egy olyan ϑ függvényt tekintenek, amely invariáns a H részcsoportbeli permutációkkal szemben, és megalkotják a

$$z = \vartheta + \alpha\vartheta_1 + \alpha^2\vartheta_2 + \ldots + \alpha^{p-1}\vartheta_{p-1} \tag{8}$$

Lagrange rezolvenst, ahol α egy p-edik egységgyök,

Evariste Galois (1811 - 1832)

A válasz.

- míg $\vartheta_1, \vartheta_2, \ldots, \vartheta_{p-1}$-et úgy kapjuk, hogy ϑ-ra alkalmazzuk azon $S, S', \ldots$ helyettesítéseket, amelyek az (5) mellékosztályokra bontásban szerepelnek.
- Ebből már következik, hogy a $g(x) = 0$ egyenelet akkor és csak akkor oldható meg gyökvonásokkal, ha létezik olyan

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

részcsoportlánc, hogy $H_k \triangleleft H_{k-1}$, vagy $H_k \triangleleft G$, s az összes index prím.
- Ez pedig (mai terminológiával) pontosan azt jelenti, hogy a G föloldható csoport.

Evariste Galois (1811 - 1832)

A válasz.

- Ezután föltette, hogy az $f(x) = 0$ irreducibilis egyenlet prímszámfokú, fokszámát n jelöli.
- Bebizonyította, hogy ezen egyenlet pontosan akkor oldható meg gyökjelekkel, ha az egyenlet G csoportjában minden olyan helyettesítés (permutáció), amely valamely x_k gyököt egy $x_{k'}$ gyökbe visz a k-nak egy *modulo* n lineáris transzformációja, azaz

$$k' \equiv ak + b \pmod{n}.$$

Evariste Galois (1811 - 1832)

Konklúzió.

- Mivel az általános ötödfokú egyenlet Galois csoportja nem ilyen alakú, így ezen egyenlet nem oldható meg gyökjelekkel.
- Tehát Abel eredménye következik Galois elméletéből. A dolgozat végleges változatában Galois említi is Abelt, de az első változatok idején még Abel nevét sem ismerte.

Az eddig megismertek összegzése 1.

Természetes kérdés.

Létezik-e bármely n-hez ($n \geq 2$) *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), de volt néhány „eretnek".

Újabb kérdés a XVIII. század utolsó harmadában.

BIZTOSAN MEGOLDHATÓK AZ EGYENLETEK?

Gauss 1799 (1816, 1849): a „klasszikus" algebra alaptétele

Minden legalább elsőfokú komplex együtthatós polinomnak van gyöke a komplex számok testében.

Az eddig megismertek összegzése 2.

A Ruffini-Abel tétel.

Az általános ötöd- és magasabbfokú egyenlet nem oldható meg gyökjelekkel. Másképpen mondva: nincs gyökképlet az ötöd- és magasabbfokú egyenletekre.

Amit Galois hozzátett.

Egy teljesen más úton, mint elődei egyrészt eljutott ugyanezen eredményre, sőt elegendő föltételt adott — ha nem is explicitet — az egyes egyenletek gyökjelekkel való megoldhatóságára.

Hogyan tovább?

Egy fontos kérdést kell tisztázni: amennyiben negatív eredményt (valaminek a nemlétét) akarunk bizonyítani, előbb pontosan meg kell mondani, hogy **minek a nemlétét kívánjuk igazolni.**

A probléma megfogalmazása.

Az első kérdés.

Legyen $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ tetszőleges polinom valamely test fölött, ahol ($n \geq 2$). 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.

A második 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 $a_0, \ldots, a_{n-1}$ együtthatóktól is függ?

A szükséges absztrakt algebrai fogalmak, összefüggések 1.

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.

Megjegyzések.

1. Ma ugyancsak permutációknak szokás nevezni az A halmaz elemeinek különböző sorrendű fölsorolásait is.
2. Emlékeztetünk, Galois (Cauchy nyomán) helyettesítésnek nevezte azt, amit mi ma permutációnak hívunk.

A szükséges absztrakt algebrai fogalmak, összefüggések 2.

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

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

Példák.

1. $(\mathbb{Z}, +)$, $(U_n, \cdot)$, ahol minden $n \in \mathbb{N}$-re U_n jelöli az összes n-edik egységgyökök halmazát.
2. Jelölje S_A az A halmaz összes permutációi halmazát. $(S_A, \cdot)$ szintén csoport, ahol „$\cdot$" az ismert leképezésszorzást jelöli, az n-edfokú szimmetrikus csoport, részcsoportjaik a permutációcsoportok.

A szükséges absztrakt algebrai fogalmak, összefüggések 3.

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

1. $(F, +)$ és $(F \setminus \{0\}, \cdot)$ kommutatív műveletű csoport,
2. 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 művelettel (műveletekkel) szintén csoport (test) *részcsoportoknak* (*résztesteknek*) nevezzük. A komplex számok testének résztesteit *számtesteknek* nevezzük.

A szükséges absztrakt algebrai fogalmak, összefüggések 4.

Megjegyzés.

Mindegyik számtest tartalmazza a racionális számok testét.

5. Definíció.

A G csoport N részcsoportja *normálosztó*, ha bármely $g \in G$-re $gN = Ng$, ahol $gN = \{ga \in G \mid a \in N\}$. Jelölése: $N \triangleleft G$.

1. Tétel.

Legyen G csoport és $N \triangleleft G$. Az összes különböző gN részhalmazok halmaza — jelölése G/N — G-nek egy osztályozását alkotját. A $gH \cdot hG = ghN$ művelettel G/N csoport, a G N-szerinti *faktorcsoportja*.

A szükséges absztrakt algebrai fogalmak, összefüggések 5.

6. Definíció.

Azt mondjuk, hogy a G véges csoport *föloldható*, ha léteznek olyan $H_1, \ldots, H_m$ részcsoportjai, hogy $\{1\} = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \ldots \triangleleft H_{m-1} \triangleleft H_m = G$, és a H_k/H_{k-1} faktorcsoportok kommutatívok $(1 \leq k \leq m)$.

Megjegyzés.

E tulajdonság a kommutativitás egy általánosítása.

A szükséges absztrakt algebrai fogalmak, összefüggések 6.

7. Definíció. (Testbővítések.)

- Legyenek $K \subseteq M$ testek. Ekkor azt is mondjuk, hogy M *bővítése* K-nak. Használni fogjuk erre az $M|K$ jelölést és a *testbővítés* elnevezést.
- **Megjegyzés.** Ha $M|K$ testbővítés, akkor M vektortér a K test fölött.
- Az $M|K$ testbővítés *végesfokú*, ha M véges dimenziós vektortér;
- *algebrai*, ha ha minden $a \in M$-hez van olyan K fölötti nemzéró polinom, amelynek ezen a gyöke;
- *normális*, ha valahányszor egy $f \in K[x]$ polinomnak van gyöke M-ben, mindannyiszor f minden gyöke M-ben van, azaz M fölött f lineáris tényezők szorzatára bomlik.

A szükséges absztrakt algebrai fogalmak, összefüggések 7.

8. Definíció.

- Legyen $M|K$ testbővítés és $a \in M$ algebrai elem. A legkisebb fokszámú olyan nemkonstans $f \in K[x]$ polinomot, amelyre $f(a) = 0$, az *a elem minimálpolinomjának* nevezzük.
- **Megjegyzés.** A minimálpolinom irreducibilis, és konstans szorzó erejéig egyértelműen meghatározott.
- Az $a, b \in M$ elemek *konjugáltak*, ha minimálpolinomjuk megegyezik.
- Legyenek M, K testek, $\varphi\colon M \to K$ bijektív leképezés. φ *izomorfizmus*, ha minden $a, b \in M$-re

$$(a+b)\varphi = a\varphi + b\varphi, \qquad (ab)\varphi = (a\varphi)(b\varphi).$$

Ha $K \subseteq M$ és $\pi\colon M \to M$ olyan izomorfizmus, hogy minden $a \in K$-ra $a\pi = a$, akkor π *K fölötti izomorfizmus*.

Galois elmélete modern terminológiával 1.

1. Tétel.

Legyen $L|K$ normális testbővítés. A $\mathrm{G}(L|K) = \{\pi\colon L \to L \mid \pi$ K fölötti izomorfizmus$\}$ halmaz a leképezésszorzással, mint művelettel csoport, e testbővítés Galois-csoportja.

A probléma megfogalmazása 1.

- Tekintsük az

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0 \tag{9}$$

egyenletet, ahol az együtthatók valamely $F \supseteq \mathbb{Q}$ test elemei.

- **Definíció.** Az (9) egyenlethez tartozó *alaptestnek* a $K = \mathbb{Q}(a_0, \ldots, a_{n-1})$ testet, azaz a $\mathbb{Q} \cup \{a_0, \ldots, a_{n-1}\}$ halmazt tartalmazó legszükebb testet, nevezzük.

Galois elmélete modern terminológiával 2.

A probléma megfogalmazása 2.

- A K testet gyökmennyiségekkel addig kell bővítenünk — minden újabb gyökmennyiség adjungálása előtt testté téve az előzőleg kapott struktúrát — ameddig olyan testhez jutunk, amely tartalmazza a gyököket.
- Másképpen mondva olyan — gyökmennyiségekkel konstruált és K-t tartalmazó — testet kell alkotni, amely fölött az (9) bal oldalán álló polinom lineáris tényezők szorzatára bomlik.

2. Tétel.

Legyen $L|K$ végesfokú normális bővítés.

1. *Tetszőleges $a \in L$ és $\pi \in \mathrm{G}(L|K)$ esetén a és $a\pi$ konjugáltak K fölött.*
2. *Ha $a, b \in L$ konjugáltak K fölött, akkor van olyan $\pi \in \mathrm{G}(L|K)$, hogy $b = a\pi$.*

Galois elmélete modern terminológiával 3.

3. Tétel.

Ha $L|K$ végesfokú normális bővítés, akkor $|\mathrm{G}(L|K)|$ megegyezik az L K fölötti vektortér dimenziójával.

Definíció.

Legyen $f \in K[x]$. Az f polinom K fölötti fölbontási testének, azaz a legszükebb olyan testnek, amely fölött f lineáris tényezőkre bomlik (ez az alaptest egy normális bővítése), Galois-csoportját az *f polinom Galois-csoportjának* nevezzük.

Polinom Galois-csoportja másképpen 1.

Legyen az f K fölötti fölbontási teste L, és jelölje $c_1, \ldots, c_k (\in L)$ az f különböző zéróhelyeit. Tetszőleges $\pi \in \mathrm{G}(L|K)$-ra és c_i-re $c_i\pi$ is zéróhelye az f polinomnak, tehát $c_i\pi = c_j$ valamely j-re.

Galois elmélete modern terminológiával 4.

Polinom Galois-csoportja másképpen 2.

- Így π meghatározza a gyökök egy $\tilde{\pi}$ permutációját:
- $$\tilde{\pi} = \begin{pmatrix} c_1 & c_2 & \cdots & c_k \\ c_1\pi & c_2\pi & \dots & c_k\pi \end{pmatrix}.$$
- **Jelölés:** $\mathrm{G}(f|K) = \{\tilde{\pi} | \pi \in \mathrm{G}(L|K)\}$

4. Lemma.

A $\mathrm{G}(L|K) \to \mathrm{G}(f|K)$, $\pi \mapsto \tilde{\pi}$ *leképezés bijektív és szorzástartó (azaz izomorfizmus).*

Megjegyzés.

Tehát, $G(f|K)$ az f gyökei egy permutációcsoportjával izomorf. $\mathrm{G}(L|K)$ helyett általában ezen $\mathrm{G}(f|K)$ permutációcsoportot hívjuk az f Galois-csoportjának.

Galois elmélete modern terminológiával 4.

5. Tétel.

Irreducibilis polinom Galois-csoportja a gyökök tranzitív permutációcsoportja.

Megjegyzés.

1. A tétel következik a 2. Tételből.
2. Fontos, de nem kellemes tény, hogy nincs „általános eljárás” a $\mathrm{G}(f|K)$ Galois-csoport meghatározására.

Galois egy briliáns ötlete.

Az „alaptest” gyökmennyiségekkel való megfelelő bővítése létezése egyenértékű azzal, hogy a polinom Galois-csoportja rendelkezik egy bizonyos tulajdonsággal.

Galois elmélete modern terminológiával 5.

5. A Galois-elmélet főtétele 1.

- Legyen $N|K$ végesfokú normális bővítés, és definiáljunk két halmazt, az N K-t tartalmazó résztesteinek — az ún. közbülső testeknek — halmazát,
- amit $\mathcal{T} = \{T \,|\, K \subseteq T \subseteq N,\ T \text{ test}\}$ jelöl,
- és a $\mathrm{G}(N|K)$ Galois-csoport részcsoportjai halmazát, a $\mathcal{G} = \{H \,|\, H \leq \mathrm{G}(N|K)\text{-nak}\}$ halmazt.
- Tekintsük a következő két leképezést:

$$\mathcal{T} = \{T \,|\, K \subseteq T \subseteq N,\ T \text{ test}\} \underset{\Delta}{\overset{\Gamma}{\rightleftarrows}} \mathcal{G} = \{G \,|\, G \leq \mathrm{G}(N|K)\text{-ban}\},$$

Galois elmélete modern terminológiával 6.

5. A Galois-elmélet főtétele 2.

- ahol
$$\Gamma\colon T \longmapsto \mathrm{G}(N|T),$$
- Vegyük észre, hogy $N|T$ végesfokú és normális bővítés, mert N szintén fölbontási test,
- továbbá
$$\Delta\colon G \longmapsto \{t \in N \,|\, t\pi = t\ \forall \pi \in G\text{-re}\}$$
- ugyanis egyszerűen belátható, hogy a jobb oldalon valóban közbülső test áll.

Galois elmélete modern terminológiával 6.

5. A Galois-elmélet főtétele 3.

A Γ, Δ leképezésekre teljesülnek a következők:

- Mindkét leképezés bijektív, és egymás inverze. Így
  - tetszőleges T közbülső testre $T = \{t \in N \mid t\pi = t\ \forall \pi \in T\Gamma\text{-ra}\}$;
  - $G(N|K)$ tetszőleges H részcsoportjára $H = G(N|T)$ teljesül, ahol $T = \{t \in N \mid t\pi = t\ \forall \pi \in H\text{-ra}\}$ test.
- Mindkét leképezés $\subseteq$-fordító, tehát
  - $$\forall T_1, T_2 \in \mathcal{T}\text{-re } T_1 \subseteq T_2 \Longrightarrow \mathrm{G}(N|T_1) \supseteq \mathrm{G}(N|T_2)$$
  - és
    $$\forall H_1, H_2 \in \mathcal{G}\text{-re } H_1 \subseteq H_2 \Longrightarrow H_1\Delta \supseteq H_2\Delta,$$
  - azaz
    $$T_1 \subseteq T_2 \iff \mathrm{G}(N|T_1) \supseteq \mathrm{G}(N|T_2).$$

Galois elmélete modern terminológiával 7.

5. A Galois-elmélet főtétele 4.

- Tetszőleges T közbülső testre $[N : T] = |\,\mathrm{G}(N|T)|$ és $[T : K] = (G(N|K) : G(N|T))$.
- Tetszőleges T közbülső testre
  $$T|K \text{ normális} \iff G(N|T) \triangleleft G(N|K).$$
- Ha a T közbülső testre $T|K$ normális, akkor
  $$\mathrm{G}(T|K) \cong \mathrm{G}(N|K)/\,\mathrm{G}(N|T).$$

Galois elmélete modern terminológiával 8.

Megjegyzések.

1. Tetszőleges G csoport és $H \leq G$ részcsoportra $(G : H)$ a H részcsoport szerinti (baloldali) mellékosztályok számát, azaz az összes különböző gH alakú részhalmaz számát jelöli. Ez a H részcsoport G csoportbeli *indexe*.
2. Ha T, K testek és $T|K$, akkor $[T : K]$ ezen testbővítés foka, azaz a T K fölötti vektortér dimenziója.

Galois elmélete modern terminológiával 9.

Definíció.

Azt mondjuk, hogy az $L|K$ testbővítés *radikálbővítés*, ha léteznek olyan

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_t = L$$

testek, hogy minden $i = 1, \ldots t$-re $K_i = K_{i-1}(\sqrt[p_i]{c_i})$, ahol p_i prím és $c_i \in K_{i-1}$. (Az egyes lépésekben szereplő prímek különbözők lehetnek.)

Megjegyzés.

1. Minden gyökvonás megkapható prímkitevőjű gyökvonások véges sokszori alkalmazásával, ezért szorítkozhatunk prímekre.
2. Az előbbi definícióban minden egyes lépésben egy $x^{p_i} - c_i \in K_{i-1}[x]$ alakú polinom valamely gyökével bővítünk.

Galois elmélete modern terminológiával 10.

7. Tétel.

Tetszőleges 0-karakterisztikájú $K \subseteq L$ testre valamely $a \in L$ pontosan akkor eleme K egy alkalmas radikálbővítésének, ha az a kifejezhető K elemeiből az $+, -, \cdot, ^{-1}$ műveletek és gyökvonás véges sokszori alkalmazásával.

Megjegyzés.

Valamely T test „0-karakterisztikájúsága" azt jelenti, hogy bármely nemzéró $a \in T$ és $n \in \mathbb{N}$-re $na \neq 0$. Az ilyen testeknek végtelenek.

8. Tétel.

Legyen K 0-karakterisztikájú test és $f \in K[x]$ egy irreducibilis polinom. Ha f valamely gyöke benne van a K egy radikálbővítésében, akkor a $\mathrm{G}(f, K)$ Galois-csoport föloldható. Megfordítva, ha az f polinom $\mathrm{G}(f, K)$ Galois-csoport föloldható, akkor e polinom minden gyöke benne van a K valamely radikálbővítésében.

Galois elmélete modern terminológiával 11.

Definíció.

Az *általános n-edfokú polinomnak* az alábbi

$$x^n + u_{n-1}x^{n-1} + \ldots + u_1 x + u_0 \tag{10}$$

polinomot nevezzük, ahol az $u_0, \ldots, u_{n-1}$ szimbólumok $\mathbb{Q}$ fölötti *határozatlanokat* jelölnek, azaz tetszőleges $h \in \mathbb{Q}[y_0, \ldots, y_{n-1}]$ polinomra $h(u_0, \ldots, u_{n-1}) = 0 \Leftrightarrow h = 0$.

Megjegyzés.

Ez utóbbi tény úgy is fogalmazható, hogy $u_0, \ldots, u_{n-1}$ algebrailag függetlenek $\mathbb{Q}$ fölött.

Galois elmélete modern terminológiával 12.

9. Tétel.

A (2) általános n-edfokú polinom együtthatói által generált test

$$K = \mathbb{Q}(u_0, \ldots, u_{n-1}) = \left\{ \frac{f(u_0, \ldots, u_{n-1})}{g(u_0, \ldots, u_{n-1})} : f, g \in \mathbb{Q}[y_0, \ldots, y_{n-1}], g \neq 0 \right\}.$$

10. Tétel.

A (2) általános n-edfokú polinom irreducibilis az együtthatói által generált K test fölött.

11. Tétel.

A (2) általános n-edfokú polinom K test fölötti Galois-csoportja izomorf S_n-nel.

Galois elmélete modern terminológiával 13.

12. Tétel.

Ha $n > 4$, akkor az S_n szimmetrikus csoport nem föloldható.

13. Következmény.

Ha $n > 4$, akkor a (2) általános n-edfokú polinom együtthatói által generált testnek nincs olyan radikálbővítése, amely tartalmazza e polinom gyökeit.

14. Következmény. A Ruffini-Abel Tétel.

Nem létezik gyökképlet egyetlen 4-nél magasabbfokú egyenlet megoldására sem.

Galois elmélete modern terminológiával 14.

További kérdés.

Ha nincs csak n-től függő eljárás, van-e minden $n > 4$-re olyan, amelyik az n-en kívül a polinom együtthatóitól is függ?

- E kérdésre a Ruffini-Abel tétel nem ad választ, sőt
- megközelíthetetlen a Galois-elméletet megelőzően ismert módszerekkel.
- Galois elmélete, Galois módszere segítségével erre is válasz kapunk.

15. Tétel.

Tetszőleges $n > 4$-re van olyan n-edfokú polinom, amelynek Galois-csoportja nem föloldható.

A 2. kérdés.

Példa.

Illusztrációként meghatározzuk az

$$f = x^5 - 4x + 2 \tag{11}$$

ötödfokú polinom Galois-csoportját, amely S_5-tel izomorf.

A Galois-csoport meghatározása 1.

Az alaptest.

Az együtthatók a racionális számok $\mathbb{Q}$ testét generálják. A klasszikus Schönemann-Eisenstein tétel szerint f irreducibilis $\mathbb{Q}$ fölött.

A gyökök kvalitatív vizsgálata 1.

- Fölhasználjuk, hogy f folytonos valós függvény, továbbá

$$\lim_{x\to-\infty} f = -\infty \qquad \lim_{x\to\infty} f = \infty,$$

azaz f-nek egy, három vagy öt valós gyöke van.

- Mivel

$$f(-2) < 0, \quad f(0) > 0, \quad f(1) < 0, \quad f(2) > 0,$$

f-nek legalább 3 valós gyöke van.

A Galois-csoport meghatározása 2.

A gyökök kvalitatív vizsgálata 2.

- Mivel azonban az $f' = 5x^4 - 4$ polinomnak csak 2 valós gyöke van, az f polinomnak 3 valós és 2 komplex (egy konjugált pár) gyöke van.
- Legyenek $x_1, x_2 \in \mathbb{C} \setminus \mathbb{R}$, $x_3, x_4, x_5 \in \mathbb{R}$ a gyökök ($x_1 = \overline{x_2}$)
- Legyen f fölbontási teste $N = \mathbb{Q}(x_1, \ldots, x_5)$.
- Világos, hogy N-re megszorítva a komplex konjugálás olyan $\mathbb{Q}$ fölötti automorfizmus, amelynek a gyökökre való megszorítása az x_1, x_2 fölcserélése.
- Kaptuk, hogy $\mathrm{G}(f, \mathbb{Q})$ tartalmaz transzpozíciót.

Egy csoportelméleti lemma.

Ha p prímszám, $G \subseteq S_p$ pedig egy olyan tranzitív permutációcsoport, amely tartalmaz transzpozíciót, akkor $G = S_p$.

A Galois-csoport meghatározása 3.

A végső konklúzió.

- E lemma alapján $G(f, \mathbb{Q}) \cong S_5$, így nem föloldható.
- Kaptuk: f gyökeit $\mathbb{Q}$ egyetlen radikálbővítése sem tartalmazza.