Povijest matematike

Franka Miriam Brückler

PMF-MO, Zagreb

Svibanj 2022.

Analiza i algebra u prvoj polovici 19. stoljeća

Determinante

- prvi objavljeni rezultati o determinantama: 1730-ih Colin Maclaurin dokazao Cramerovo pravilo za 2×2- i 3×3-sustave, koje je 1750. poopćio Gabriel Cramer (1704.–1752.)

Determinante

- prvi objavljeni rezultati o determinantama: 1730-ih Colin Maclaurin dokazao Cramerovo pravilo za 2×2- i 3×3-sustave, koje je 1750. poopćio Gabriel Cramer (1704.–1752.)
- Alexandre-Théophile Vandermonde (1735–1796) ih odvaja od jedine uloge vezane za rješavanje sustava
- Pierre-Simon Laplace je 1772. objavio poboljšanje starijih metoda računa *rezultanti*: Laplaceov razvoj

Determinante

- prvi objavljeni rezultati o determinantama: 1730-ih Colin Maclaurin dokazao Cramerovo pravilo za 2×2- i 3×3-sustave, koje je 1750. poopćio Gabriel Cramer (1704.–1752.)
- Alexandre-Théophile Vandermonde (1735–1796) ih odvaja od jedine uloge vezane za rješavanje sustava
- Pierre-Simon Laplace je 1772. objavio poboljšanje starijih metoda računa *rezultanti*: Laplaceov razvoj
- Joseph-Louis Lagrange (1736–1813) uočava njihovu primjenu u analitičkoj geometriji (volumeni)

Determinante

- prvi objavljeni rezultati o determinantama: 1730-ih Colin Maclaurin dokazao Cramerovo pravilo za 2×2- i 3×3-sustave, koje je 1750. poopćio Gabriel Cramer (1704.–1752.)
- Alexandre-Théophile Vandermonde (1735–1796) ih odvaja od jedine uloge vezane za rješavanje sustava
- Pierre-Simon Laplace je 1772. objavio poboljšanje starijih metoda računa *rezultanti*: Laplaceov razvoj
- Joseph-Louis Lagrange (1736–1813) uočava njihovu primjenu u analitičkoj geometriji (volumeni)
- naziv determinanta potječe od Augustin-Louis Cauchy (1789–1857): dokaz Binet-Cauchyjevog teorema (1812.)
- Carl Gustav Jacob Jacobi (1804.–1851.): 1841. prva algoritamska definiciju determinante, a iste godine je Arthur Cayley uveo ograničavanje determinanti vertikalnim crtama

Prethodnici teorije grupa

Pojam grupe

Grupa je skup opskrbljen asocijativnom binarnom operacijom $*$ u kom su jednoznačno rješive sve jednadžbe tipa $A * X = B$.

Prethodnici teorije grupa

Pojam grupe

Grupa je skup opskrbljen asocijativnom binarnom operacijom $*$ u kom su jednoznačno rješive sve jednadžbe tipa $A * X = B$.

Neka svojstva grupa korištena su davno prije nego su te strukture uvedene: svojstva operacija s brojevima; Eulerov dokaz malog Fermatovog teorema 1758 koristi svojstva koja se tiču grupe ostataka modulo prostog broja

Prethodnici teorije grupa

Pojam grupe

Grupa je skup opskrbljen asocijativnom binarnom operacijom $*$ u kom su jednoznačno rješive sve jednadžbe tipa $A * X = B$.

Neka svojstva grupa korištena su davno prije nego su te strukture uvedene: svojstva operacija s brojevima; Eulerov dokaz malog Fermatovog teorema 1758 koristi svojstva koja se tiču grupe ostataka modulo prostog broja
U drugoj polovici 18. st. su se Joseph-Louis Lagrange i Alexandre-Théophile Vandermonde: zašto postoje rješenja u radikalima za jednadžbe stupnjeva do 4?

Koeficijenti algebarske jednadžbe su simetrične racionalne funkcije njezinih rješenja, pa su i sve racionalne funkcije koeficijenata također simetrične s obzirom na rješenja.

Primjer

$$x^3 + ax^2 + bx + c = 0$$

Vièteove formule:

$$-a = x_1 + x_2 + x_3; \quad b = x_1x_2 + x_1x_3 + x_2x_3; \quad -c = x_1x_2x_3$$

Koeficijenti algebarske jednadžbe su simetrične racionalne funkcije njezinih rješenja, pa su i sve racionalne funkcije koeficijenata također simetrične s obzirom na rješenja.

Primjer

$$x^3 + ax^2 + bx + c = 0$$

Vièteove formule:

$$-a = x_1 + x_2 + x_3; \quad b = x_1x_2 + x_1x_3 + x_2x_3; \quad -c = x_1x_2x_3$$

$$r(a, b, c) = \frac{a}{b-c} = \frac{-x_1 - x_2 - x_3}{x_1x_2 + x_1x_3 + x_2x_3 + x_1x_2x_3}$$

Koeficijenti algebarske jednadžbe su simetrične racionalne funkcije njezinih rješenja, pa su i sve racionalne funkcije koeficijenata također simetrične s obzirom na rješenja.

Primjer

$$x^3 + ax^2 + bx + c = 0$$

Vièteove formule:

$$-a = x_1 + x_2 + x_3; \quad b = x_1x_2 + x_1x_3 + x_2x_3; \quad -c = x_1x_2x_3$$

$$r(a,b,c) = \frac{a}{b-c} = \frac{-x_1 - x_2 - x_3}{x_1x_2 + x_1x_3 + x_2x_3 + x_1x_2x_3}$$

Rješenje u radikalima: $+$, $-$, $\cdot$, $:$ te korijeni

Koeficijenti algebarske jednadžbe su simetrične racionalne funkcije njezinih rješenja, pa su i sve racionalne funkcije koeficijenata također simetrične s obzirom na rješenja.

Primjer

$$x^3 + ax^2 + bx + c = 0$$

Vièteove formule:

$$-a = x_1 + x_2 + x_3; \quad b = x_1x_2 + x_1x_3 + x_2x_3; \quad -c = x_1x_2x_3$$

$$r(a, b, c) = \frac{a}{b - c} = \frac{-x_1 - x_2 - x_3}{x_1x_2 + x_1x_3 + x_2x_3 + x_1x_2x_3}$$

Rješenje u radikalima: $+, -, \cdot, :$ te korijeni
Budući da općenito takvim formulama dobivamo različite vrijednosti za rješenja, slijedi da korijeni „ruše" simetriju.

Lagrange: $y = \sum_{i=1}^{n} \omega_{i-1} x_i$ — max. n! različitih vrijednosti (sustav linearnih jednadžbi za x-eve) — rješenja jednadžbe stupnja n!

Primjer

$$n = 3 \Rightarrow \omega_1 = 1, \omega_2 = \overline{\omega_3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

Lagrange: $y = \sum_{i=1}^{n} \omega_{i-1} x_i$ — max. n! različitih vrijednosti (sustav linearnih jednadžbi za x-eve) — rješenja jednadžbe stupnja n!

Primjer

$$n = 3 \Rightarrow \omega_1 = 1, \omega_2 = \overline{\omega_3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

$$y = x_1 + \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) x_2 + \left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) x_3$$

Lagrange: $y = \sum_{i=1}^{n} \omega_{i-1} x_i$ — max. $n!$ različitih vrijednosti (sustav linearnih jednadžbi za x-eve) — rješenja jednadžbe stupnja $n!$

Primjer

$$n = 3 \Rightarrow \omega_1 = 1, \omega_2 = \overline{\omega_3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

$$y = x_1 + \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) x_2 + \left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) x_3$$

$$(y - y_1)(y - y_2)(y - y_3)(y - y_4)(y - y_5)(y - y_6) = 0$$

Lagrange: $y = \sum_{i=1}^{n} \omega_{i-1} x_i$ — max. $n!$ različitih vrijednosti (sustav linearnih jednadžbi za x-eve) — rješenja jednadžbe stupnja $n!$

Primjer

$$n = 3 \Rightarrow \omega_1 = 1, \omega_2 = \overline{\omega_3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

$$y = x_1 + \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) x_2 + \left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) x_3$$

$$(y - y_1)(y - y_2)(y - y_3)(y - y_4)(y - y_5)(y - y_6) = 0$$

$$y^6 + P(x_1, x_2, x_3)y^3 + Q(x_1, x_2, x_3) = 0$$

Dakle, za jednadžbe stupnja 3 *postoji jednadžba stupnja* $3! = 6$ *za* y*-e, koja se dade svesti na jednadžbu stupnja* 2*.*

Lagrange je primijetio da se u svim slučajevima s poznatim rješenjima u radikalima ($n = 1, 2, 3, 4$) može jednadžba stupnja n! za y-e svesti na jednadžbu stupnja manjeg od n, rješivu u radikalima.

Lagrange je primijetio da se u svim slučajevima s poznatim rješenjima u radikalima ($n = 1, 2, 3, 4$) može jednadžba stupnja $n!$ za y-e svesti na jednadžbu stupnja manjeg od n, rješivu u radikalima.
Dakle, ako jednadžbu stupnja $n!$ možemo svesti na jednadžbu stupnja 4 ili manjeg, onda možemo izračunati y-e, a iz njih (preko sustava linearnih jednadžbi) dobiti x-eve, rješenje jednadžbe stupnja n u radikalima.

Lagrange je primijetio da se u svim slučajevima s poznatim rješenjima u radikalima ($n = 1, 2, 3, 4$) može jednadžba stupnja $n!$ za y-e svesti na jednadžbu stupnja manjeg od n, rješivu u radikalima.
Dakle, ako jednadžbu stupnja $n!$ možemo svesti na jednadžbu stupnja 4 ili manjeg, onda možemo izračunati y-e, a iz njih (preko sustava linearnih jednadžbi) dobiti x-eve, rješenje jednadžbe stupnja n u radikalima.
Među ostalim, Lagrange je iz ovih razmatranja (1771.) zaključio da ako imamo polinom s n varijabli, te ako te varijable permutiramo na svih $n!$ načina, dobit ćemo neki broj m različitih polinoma, pri čemu je m djeljitelj od $n!$. Bila je to prva verzija Lagrangeovog teorema teorije grupa: Red podgrupe konačne grupe G uvijek je djelitelj od reda od G.

Joseph-Louis Lagrange (1736.–1813.)

Definicija derivacije?

Joseph-Louis Lagrange (1736.–1813.)

Definicija derivacije?
Prema Lagrangeu, infinitezimalni račun treba svesti na algebru redova. Za njega je račun s redovima podjednako algebra kao račun s konačnim algebarski izrazima, isto kao što je račun se beskonačnim decimalnim razvojima i dalje aritmetika.

Joseph-Louis Lagrange (1736.–1813.)

Definicija derivacije?
Prema Lagrangeu, infinitezimalni račun treba svesti na algebru redova. Za njega je račun s redovima podjednako algebra kao račun s konačnim algebarski izrazima, isto kao što je račun se beskonačnim decimalnim razvojima i dalje aritmetika. *Théorie des fonctions analytiques* (1797.): svaka funkcija (analitički izraz) može se zapisati u obliku

$$f(x+h) = f(x) + p(x)h + q(x)h^2 + r(x)h^3 + \dots, \qquad (1)$$

za sve do na eventualno konačno mnogo x. Tako derivaciju od $f(x)$ definira kao $p(x)$, drugu derivaciju kao pola $q(x)$ itd.

Joseph-Louis Lagrange (1736.–1813.)

Definicija derivacije?
Prema Lagrangeu, infinitezimalni račun treba svesti na algebru redova. Za njega je račun s redovima podjednako algebra kao račun s konačnim algebarski izrazima, isto kao što je račun se beskonačnim decimalnim razvojima i dalje aritmetika. *Théorie des fonctions analytiques* (1797.): svaka funkcija (analitički izraz) može se zapisati u obliku

$$f(x+h) = f(x) + p(x)h + q(x)h^2 + r(x)h^3 + \dots, \qquad (1)$$

za sve do na eventualno konačno mnogo x. Tako derivaciju od $f(x)$ definira kao $p(x)$, drugu derivaciju kao pola $q(x)$ itd. Lagrange je pisao fx, $f'x$, $f''x$ za funkciju, njenu prvu i drugu derivaciju.

Prednost ovog pristupa: Izbjegava fizikalne argumente i kvocijente infinitezimalnih veličina. Derivacije su sad također funkcije.

Mana: Tvrdnja o razvoju nije točna!

Prednost ovog pristupa: Izbjegava fizikalne argumente i kvocijente infinitezimalnih veličina. Derivacije su sad također funkcije.
Mana: Tvrdnja o razvoju nije točna!
Prema Lagrangeu, temeljno svojstvo derivacije je

$$f(x+i) = f(x) + if'(x) + iV,$$

ako se i za svaki D može izabrati dovoljno malen da V bude između $-D$ i D. Iz toga izvodi

Teorem (Teorem srednje vrijednosti, izvorna formulacija)

Za svaki D može se naći i sa svojstvom

$$i(f'(x) - D) < f(x+i) - f(x) < i(f'(x) + D).$$

Koristeći ovaj teorem Lagrange je dokazao razne tvrdnje o derivacijama, primjerice vezu predznaka f' i rasta/pada f.

Cauchyjeva funkcija

Funkcija $f : \mathbb{R} \to \mathbb{R}$ zadana je s

$$f(x) = \begin{cases} \exp(-1/x^2), & x \neq 0 \\ 0, & x = 0 \end{cases}$$

Njen Taylorov razvoj je nulfunkcija, kao i Taylorov razvoj same nulfunkcije. Dakle, funkcije općenito nisu određene svojim Taylorovim razvojem!
Ovaj primjer i s time grešku u Lagrangeovoj argumentaciji, te 1820ih godina moderni oblik matematičke analiza dao je

Augustin-Louis Cauchy (1789–1857)

Definicija (Cauchyjeva definicija limesa (1821))

Ako se slijed vrijednosti koje se pripisuju nekoj varijabli neograničeno približava nekoj vrijednosti, tako da na kraju razlika do nje bude toliko mala, koliko želimo, posljednja se vrijednost zove graničnom vrijednošću ostalih vrijednosti.

Augustin-Louis Cauchy (1789–1857)

Definicija (Cauchyjeva definicija limesa (1821))

Ako se slijed vrijednosti koje se pripisuju nekoj varijabli neograničeno približava nekoj vrijednosti, tako da na kraju razlika do nje bude toliko mala, koliko želima, posljednja se vrijednost zove graničnom vrijednošću ostalih vrijednosti.

Cauchy dalje kaže da su infinitezimalne veličine one kojima je limes 0.

Augustin-Louis Cauchy (1789–1857)

Definicija (Cauchyjeva definicija limesa (1821))

Ako se slijed vrijednosti koje se pripisuju nekoj varijabli neograničeno približava nekoj vrijednosti, tako da na kraju razlika do nje bude toliko mala, koliko želima, posljednja se vrijednost zove graničnom vrijednošću ostalih vrijednosti.

Cauchy dalje kaže da su infinitezimalne veličine one kojima je limes 0.

Definicija (Cauchyjeva definicija derivacije (1823.))

Derivacija $f'(x)$ funkcije $f(x)$ je, ako postoji, limes kvocijenta $\dfrac{f(x+h)-f(x)}{h}$ kad h teži u 0.

Definicija (Cauchyjeva definicija funkcije (1821.))

Ako su varijabilne veličine tako povezane, da ako je zadan iznos jedne, iz njega možemo odrediti iznose ostalih, općenito te različite veličine izražavamo preko te jedne, koju nazivamo nezavisnom varijablom; ostale pak veličine, koje su izražene preko nezavisne varijable, zovu se funkcijama te varijable.

I dalje se funkcije poistovjećuju s formulama, iako je ovo pokušaj uključenja implicitno zadanih funkcija!

Definicija (Cauchyjeva definicija funkcije (1821.))

Ako su varijabilne veličine tako povezane, da ako je zadan iznos jedne, iz njega možemo odrediti iznose ostalih, općenito te različite veličine izražavamo preko te jedne, koju nazivamo nezavisnom varijablom; ostale pak veličine, koje su izražene preko nezavisne varijable, zovu se funkcijama te varijable.

I dalje se funkcije poistovjećuju s formulama, iako je ovo pokušaj uključenja implicitno zadanih funkcija!

Definicija (Cauchyjeva definicija neprekidne funkcije (1821))

Funkcija $f(x)$ *je neprekidna funkcija varijable* x *unutar dviju danih granica, ako se za svaki* x *između njih brojčani iznos razlike* $f(x+\alpha)-f(x)$ *skupa s* α *beskonačno smanjuje.*

Beskonačno mali prirast varijable izaziva beskonačno mali prirast funkcije!

Često se kaže da je Cauchy uveo $\varepsilon - \delta$-jezik u analizu. To nije sasvim točno, iako se njegove definicije i dokazi lako prevedu na taj jezik. Jedini dokaz u kojem stvarno koristi ε i δ je:

Teorem (Teorem srednje vrijednosti (Cauchy))

Ako je $f(x)$ neprekidna na $[x, x+a]$, onda je $\min_{[x,x+a]} f'(x) \leq \frac{f(x+a)-f(x)}{a} \leq \max_{[x,x+a]} f'(x)$.

Dokaz: Neka su δ, ϵ dva jako mala broja; prvi se bira tako da za sve iznose i manje od δ i sve iznose x omjer $(f(x+i) - f(x))/i$ uvijek bude veći od $f'(x) - \epsilon$ i manji od $f'(x) + \epsilon \ldots$

Često se kaže da je Cauchy uveo $\varepsilon - \delta$-jezik u analizu. To nije sasvim točno, iako se njegove definicije i dokazi lako prevedu na taj jezik. Jedini dokaz u kojem stvarno koristi ε i δ je:

Teorem (Teorem srednje vrijednosti (Cauchy))

Ako je $f(x)$ neprekidna na $[x, x+a]$, onda je $\min_{[x,x+a]} f'(x) \leq \frac{f(x+a)-f(x)}{a} \leq \max_{[x,x+a]} f'(x)$.

Dokaz: Neka su δ, ϵ dva jako mala broja; prvi se bira tako da za sve iznose i manje od δ i sve iznose x omjer $(f(x+i) - f(x))/i$ uvijek bude veći od $f'(x) - \epsilon$ i manji od $f'(x) + \epsilon$...

Bernard Bolzano (1781.–1848.): slična definicija neprekidnosti, koju je iskoristio za dokaz neprekidnost polinoma na $\varepsilon - \delta$-način (kod njega $D - \omega_1$-način). Bolzanovi su doprinosi postali poznati tek u drugoj polovici 19. st.

Jean Baptiste Joseph Fourier (1768.–1830.)

Poznat je po razvoju teorije trigonometrijskih redova i fizikalnim rezultatima. Uveo je oznaku $\int_a^b$. U sklopu naše teme zanimljiva je njegova definicija funkcije:

Definicija (Fourierova definicija funkcije (1822.))

Općenito funkcija $f(x)$ predstavlja niz vrijednosti ili ordinata, od kojih je svaka proizvoljna. Za beskonačno mnogo danih iznosa apscise x postoji jednako mnogo ordinata $f(x)$. Sve one imaju brojčane iznose, pozitivne, negativne ili nula. Ne pretpostavljamo da te ordinate poštuju neko opće pravilo; one slijede jedna za drugom na bilo koji način i svaka je dana kao da je jedina.

Johann Peter Gustav Lejeune Dirichlet (1805.–1859.)

Teorijom Fourierovih redova bavio se i . On je pak dao gotovo modernu definiciju funkcije (ne dajemo ju doslovno kao prethodne):

Definicija (Dirichletova definicija funkcije (1837))

Neka x poprima vrijednosti između a i b. Ako svakom x-u odgovara samo po jedan konačan y, tako da se postepeno mijenja kako se x postepeno mijenja, y je neprekidna funkcija od x.

Dirichlet dalje jasno kaže da ne treva pstojati jedinstveno pravilo, štoviše da ovisnost ne mora biti iskaziva matematičkim operacijama.

Johann Peter Gustav Lejeune Dirichlet (1805.–1859.)

Teorijom Fourierovih redova bavio se i . On je pak dao gotovo modernu definiciju funkcije (ne dajemo ju doslovno kao prethodne):

Definicija (Dirichletova definicija funkcije (1837))

Neka x poprima vrijednosti između a i b. Ako svakom x-u odgovara samo po jedan konačan y, tako da se postepeno mijenja kako se x postepeno mijenja, y je neprekidna funkcija od x.

Dirichlet dalje jasno kaže da ne treva pstojati jedinstveno pravilo, štoviše da ovisnost ne mora biti iskaziva matematičkim operacijama. Neprekidnoj funkciji odgovara neka neprekidna krivulja od a do b.
Sličnu je definiciju (također uz zahtjev neprekidnosti) dao Lobačevski 1838.

Dirichletovi rezultati u teoriji brojeva

- Prvi članak (1825.), kojim je odmah postao poznat, bio je dokaz jednog slučaja velikog Fermatovog teorema

Dirichletovi rezultati u teoriji brojeva

- Prvi članak (1825.), kojim je odmah postao poznat, bio je dokaz jednog slučaja velikog Fermatovog teorema
- Kasnije je Dirichlet dokazao VFT i za $n = 14$.
- u aritmetičkom nizu u kome su prvi član i diferencija međusobno relativno prosti ima beskonačno mnogo prostih brojeva (hipotezu je postavio Gauß)
- uveo Dirichletov red $\sum_n a_n n^{-s}$
- bavio se analitičkom i algebarskom teorijom brojeva

Veliki Fermatov teorem

- Dovoljno ga je dokazati za eksponent 4 (✓) i za proste eksponente;
- prvi značajniji generalni pristup: Sophie Germain (Monsieur Le Blanc, 1776.–1833.), dokazala je 1805. da teorem vrijedi za određenu klasu prostih p;

Veliki Fermatov teorem

- Dovoljno ga je dokazati za eksponent 4 (✓) i za proste eksponente;
- prvi značajniji generalni pristup: Sophie Germain (Monsieur Le Blanc, 1776.–1833.), dokazala je 1805. da teorem vrijedi za određenu klasu prostih p;
- do početka 20. st. dokazan je za sve eksponente manje od 100 te da vrijedi za beskonačno mnogo prostih eksponenata
- razvoj teorije brojeva sve je više odmicao od ovog problema
- do početka 1980-ih godina napredak se sastojao uglavnom u računalnim provjerama,

Veliki Fermatov teorem

- Dovoljno ga je dokazati za eksponent 4 (✓) i za proste eksponente;
- prvi značajniji generalni pristup: Sophie Germain (Monsieur Le Blanc, 1776.–1833.), dokazala je 1805. da teorem vrijedi za određenu klasu prostih p;
- do početka 20. st. dokazan je za sve eksponente manje od 100 te da vrijedi za beskonačno mnogo prostih eksponenata
- razvoj teorije brojeva sve je više odmicao od ovog problema
- do početka 1980-ih godina napredak se sastojao uglavnom u računalnim provjerama, a sredinom 1980-ih je G. Frey uočio da se ovaj teorem može dobiti iz jedne naizgled s njime potpuno nepovezane hipoteze (iz graničnog područja algebarske topologije i teorije brojeva): Shimura-Taniyama-Weil-ova hipoteza
- Veze između tih rezultata uspostavili su G. Frey, R. Taylor i A. Wiles. Andrew Wiles je 1995. konačno dokazao i zadnji potrebni korak.

Paolo Ruffini (1765.–1822.)

- 1799. prvi tvrdi da opća jednadžba stupnja 5 nema rješenje u radikalima;
- koristeći permutacije pokušao je to i dokazati i pritom *de facto* koristio svojstva grupa permutacija (zove ih *permutazione*) – koristi zatvorenost s obzirom na kompoziciju;
- tako je dobio prve rezultate o grupama prije nego su iste definirane;

Paolo Ruffini (1765.–1822.)

- 1799. prvi tvrdi da opća jednadžba stupnja 5 nema rješenje u radikalima;
- koristeći permutacije pokušao je to i dokazati i pritom *de facto* koristio svojstva grupa permutacija (zove ih *permutazione*) – koristi zatvorenost s obzirom na kompoziciju;
- tako je dobio prve rezultate o grupama prije nego su iste definirane;
- no, nije bilo reakcija!
- 1801. kopiju knjige šalje Lagrangeu, ne dobiva odgovor, ponovno šalje s molbom da ga upozori ako je što krivo ili beskorisno, ponovno bez odgovora;

- 1803. objavio novi, kako se nadao razumljiviji dokaz – samo poneki komentar talijanskih matematičara
- traži recenziju pariškog Nacionalnog instituta – recenzenti Lagrange, Legendre i Lacroix – zaključak: ništa bitnog;
- traži i *Royal Society* – zaključak: ne slažu se sa svime, ali smatraju uglavnom dokazanim;
- 1808. i 1813. nove verzije dokaza;
- jedini matematičar koji je priznao važnost rezultata i smatrao ga točnim (rupu u dokazu smatrao je minornom) – Cauchy 1821.
- Ipak, svi Ruffinijev pokušaji dokaza imaju rupu.

Niels Henrik Abel (1802.–1829.) i Évariste Galois (1811.–1832.)

Abel: Prvi potpun dokaz nerješivosti opće jednadžbe stupnja 5 u radikalima (1824.)

Niels Henrik Abel (1802.–1829.) i Évariste Galois (1811.–1832.)

Abel: Prvi potpun dokaz nerješivosti opće jednadžbe stupnja 5 u radikalima (1824.)

Galois se bavio pitanjem: Kako za zadanu algebarsku jednadžbu utvrditi ima li rješenja u radikalima? Shvatio je da je odgovor na to pitanje vezan za strukturu grupe koja se danas naziva Galoisovom grupom G jednadžbe (odnosno polinoma).

Niels Henrik Abel (1802.–1829.) i Évariste Galois (1811.–1832.)

Abel: Prvi potpun dokaz nerješivosti opće jednadžbe stupnja 5 u radikalima (1824.)

Galois se bavio pitanjem: Kako za zadanu algebarsku jednadžbu utvrditi ima li rješenja u radikalima? Shvatio je da je odgovor na to pitanje vezan za strukturu grupe koja se danas naziva Galoisovom grupom G jednadžbe (odnosno polinoma). G je podgrupa grupe S_n. U G se nalaze one permutacije korijena, koje ne mijenjaju nijednu racionalnu funkciju koeficijenata (uočimo utjecaj Lagrangea i Ruffinija!).

Niels Henrik Abel (1802.–1829.) i Évariste Galois (1811.–1832.)

Abel: Prvi potpun dokaz nerješivosti opće jednadžbe stupnja 5 u radikalima (1824.)

Galois se bavio pitanjem: Kako za zadanu algebarsku jednadžbu utvrditi ima li rješenja u radikalima? Shvatio je da je odgovor na to pitanje vezan za strukturu grupe koja se danas naziva Galoisovom grupom G jednadžbe (odnosno polinoma). G je podgrupa grupe S_n. U G se nalaze one permutacije korijena, koje ne mijenjaju nijednu racionalnu funkciju koeficijenata (uočimo utjecaj Lagrangea i Ruffinija!).

1844. Cauchy je objavio djelo o grupama permutacija i tim djelom teorija permutacija postaje samostalna teorija. Definirao je red permutacije, uveo cikličku notaciju, itd. Umjesto naziva grupa koristio je naziv *systeme des substitutions conjugués*.