Ка модерној алгебри

Зоран Петровић

7. мај 2024. године

Као што смо видели, проблем налажења решења алгебарских једначина трећег и четвртог степена, која се изражавају као рационалне функције корена израза добијених од коефицијената једначине, решен је у ренесансној Италији. Но, питање за једначине вишег степена остало је неразрешено. У овом делу ћемо се позабавити тим питањем, тј. како је разматрање овог проблема довело до резултата Еваристе Галоа са којим се може рећи да почиње развој модерне алгебре, дакле области која проучава алгебарске структуре попут група, прстена, поља.

Варинг

Слика 1: Едвард Варинг

Едвард Варинг (1736–1798) био је енглески математичар који је у два своја значајна дела *Miscellanea analytica* (Кембриџ 1762) и *Meditationes algebricae* (Оксфорд 1770) (при чему је заправо друго дело, упркос новом називу, било друго, проширено издање првог) дао прве резултате на том путу. Наиме, ако се посматра општа једначина степена

n:
$$x^n - a_1 x^{n-1} + a_2 x^{n-2} - \cdots + \cdots = 0,$$
и њени корени $x_1, \ldots, x_n$, онда нам је познато да су коефицијенти a_i заправо елементарне симетричне функције ових корена:

$$\begin{aligned} a_1 &= x_1 + \cdots + x_n, \\ a_2 &= x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n, \quad \text{итд.} \end{aligned}$$

Варинг је у свом првом делу показао да се свака рационална симетрична функција корена ове једначине може изразити као рационална функција коефицијената тако што је то најпре показао за суму степена

$$s_m = x_1^m + \cdots + x_n^m,$$

а потом за све остале симетричне функције. У другом делу је разматрао решења циклотомичне једначине (једначине „деобе круга” пошто се налажење правилног n-тоугла уписаног у дати круг своди на решавање ове једначине):
$$x^n - 1 = 0.$$

Разматрао је и проблем да се нађу једначине које се могу решити сумама облика
$$x = \sqrt[m]{\alpha_1} + \sqrt[m]{\alpha_2} + \cdots + \sqrt[m]{\alpha_n}.$$

Вандермонд

Слика 2: Вандермонд

Александар-Теофил Вандермонд (1735–1796) био је француски математичар, који је 1770. године представио париској Академији наука рад под насловом „О решавању једначина”. Он почиње од добро познатих решења квадратне и кубне једначине са жељом да нађе општи принцип за решавање алгебарских једначина. Најпре решења квадратне једначине x_1, x_2 напише у облику

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

Овај се израз може написати и у облику

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

и видимо да се овде појављују симетричне функције корена.

Вандермонд се потом пита да ли се општа једначина степена n може решити помоћу аналогног израза

$$\frac{1}{n}\left[(x_1 + \cdots + x_n) + \sqrt[n]{(\rho_1 x_1 + \cdots \rho_n x_n)^n} + \sqrt[n]{(\rho_1^2 x_1 + \cdots \rho_n^2 x_n)^n} + \cdots + \sqrt[n]{(\rho_1^{n-1} x_1 + \cdots \rho_n^{n-1} x_n)^n}\right],$$

где су $\rho_1, \ldots, \rho_n$ n-ти корени из јединице. Данас изразе облика

$$\rho_1 x_1 + \cdots + \rho_n x_n$$

називамо Лагранжовим решавачима, пошто их је Лагранж увео у раду приложеном берлинској Академији 1771. Наиме, Вандермондов рад јесте предат раније, али је објављен тек 1774.

Вандермондов метод у случају кубне једначине фино 'ради'. Наиме, ако је $\zeta^3 = 1$, а $\zeta \neq 1$, те су и ζ и ζ^2 примитивни корени из јединице, а x_1, x_2, x_3 решења кубне једначине, онда имамо једнакост

$$\left(x_1 + \zeta x_2 + \zeta^2 x_3\right)^3 = S + 3\zeta X + 3\zeta^2 Y, \tag{1}$$

где је

$$\begin{aligned} S &= x_1^3 + x_2^3 + x_3^3 + 6x_1x_2x_3 \\ X &= x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 \\ Y &= x_1 x_2^2 + x_2 x_3^2 + x_3 x_1^2. \end{aligned}$$

Видимо да S јесте симетрична функција корена, док X и Y нису, но $X + Y$ и XY јесу симетричне функције, па тиме изразиве преко коефицијената, а и корени су квадратне једначине. Стога се може добити колики је израз на десној страни једначине (1) те се могу добити и корени једначине. За једначину степена 4, Вандермонд је нешто модификовао свој метод, док за једначине вишег степена тај метод јесте успешан само у специјалним случајевима. На пример, он је решио једначину

$$x^{11} - 1 = 0.$$

Најпре ју је редуковао на једначину степена 5 чији су корени

$$\rho+\rho^{-1}, \quad \rho^2+\rho^{-2}, \quad \rho^3+\rho^{-3}, \quad \rho^4+\rho^{-4}, \quad \rho^5+\rho^{-5},$$

где је ρ примитивни једанаести корен из јединице. Затим је, за решавање те једначине петог степена користио раније наведене решаваче у облику

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

где је α примитивни пети корен из јединице. Но, овде се мора пажљиво изабрати редослед корена x_i да би се L^5 могао фино одредити и за овај случај се то може разрешити пробањем, али за општи случај је потребан доказ да се то може увек урадити. То је извео тек Гаус. Вандермонд је тврдио да се решења опште једначине $x^n-1=0$, његовим методом увек могу лако наћи, те се чини да није био свестан проблема избора редоследа корена.

Лагранж

Слика 3: Жозеф Луј Лагранж

Жозеф Луј Лагранж (1736-1813) рођен је у Торину и крштен је као Ђузепе Лодовико Лагранђа. Данас је познат као француски математичар, мада га Италијали 'воде' као италијанског математичара. У сваком случају, његова породица је имала веза са Француском. Он сам је дуго времена радио у Берлину и у Паризу, мада је започео каријеру у Италији. Био је свестран математичар, овде наводимо само његове резултате о решавању алгебарских једначина.

Веома занимљив (и обиман) рад од преко 200 страница, Лагранж је приложио берлинској Академији. Наслов тог рада је био „Размишљање о алгебарском решавању једначина”.

Ту најпре разматра кубну једначину у облику

$$x^3 + nx + p = 0.$$

Наравно, решење нам је познато из Кардановe књиге где се оно тражи у облику $x = u + v$, где су u^3 и v^3 корени квадратне једначине. Лагранж показује да се u и v могу изразити као функције корена a, b, c почетне кубне једначине:

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

где је наравно α примитивни трећи корен из јединице.

Лагранж каже да се овакав резултат може добити и директним методом. Наиме, он полази од произвољне линеарне функције по a, b, c:

$$y = Aa + Bb + Cc.$$

Пермутовањем корена a, b, c добија се 6 израза који су стога корени једначине шестог степена. Ако желимо да то буде једначина у којој ће се појављивати само степени од y^3 (можда можемо да је зовемо бикубна једначина), онда се може показати да су A, B, C пропорционални са $1, \alpha, \alpha^2$, или са $1, \alpha^2, \alpha$. Тако да се добијају ипак раније наведени изрази. Дакле, занимљиво је да он разматра понашање израза при пермутацији корена.

Потом разматра једначину четвртог степена у облику

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

Ферари је показао да се решења добијају помоћу решења кубне једначине („разрешавајућа кубика”):

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

Лагранж показује да се корени u, v, w ове једначине добијају као симетричне функције корена a, b, c, d почетне једначине четвртог степена:

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

У одељку под бројем 100, Лагранж разматра рационалне функције $f(x', x'', \dots, x^{(n)})$ корена опште једначине степена n. Ти корени се разматрају као неодређене. За две функције t и y ових корена каже да су сличне ако свака пермутација ових корена која оставља t инваријантним, оставља и y инваријантним и обратно. Лагранж доказује следећу теорему.

Ако све пермутације које остављају t инваријантним остављају и y инваријантним, онда се y може изразити као рационална функција од t и коефицијената дате једначине.

Он ову теорему примењује на једначине степена 2, 3 и 4, а каже да је примена на једначине вишег степена још увек превише компликована. Такође је разматрао и неке специјалне случајеве већ навођене циклотомичне једначине $x^n - 1 = 0$.

Малфати

Слика 4: Малфати

Ђанфранческо Малфати (1731–1807) био је италијански математичар који се бавио геометријом, механиком и вероватноћом, али нас занима његов допринос у решавању алгебарских једначина. Он је 1770. поднео Академији наука у Сијени интересантну расправу о једначинама петог степена и она је објављена од стране те Академије 1771.

Он најпре разматра кубну једначину

$$x^3 + ax + b = 0 \tag{2}$$

Следећи Ојлеров метод за решавање ове једначине (о коме истина нисмо причали, али ево сада је прилика да се спомене), он посматра корен x који задовољава линеарну једначину

$$x + m\sqrt[3]{f^2} + n\sqrt[3]{f} = 0. \tag{3}$$

Да би елиминисао треће корене, користи метод Габријела Манфредија (Манфреди, 1681–1761, био је италијански математичар који се највише бавио диференцијалним једначинама). Наиме, уместо $\sqrt[3]{f}$ посматра $\alpha\sqrt[3]{f}$ и $\alpha^2\sqrt[3]{f}$, где је α примитивни трећи корен из јединице, замени то у (3) и помножи та три израза те добије једначину трећег степена

$$x^3 - 3mnfx + m^3f^2 + n^3f = 0. \tag{4}$$

Потом постави $f = 1$ и добије

$$x^3 - 3mnx + m^3 + n^3 = 0. \tag{5}$$

Ова је једначина еквивалентна једначини (2) акко је

$$mn = -a, \quad m^3 + n^3 = b. \tag{6}$$

Одавде се наравно могу наћи m^3 и n^3, а онда наравно и m и n (видели смо већ овако нешто код решавања једначина трећег степена).

Но, Малфати сада ово жели да примени на једначину петог степена

$$x^5 + 5ax^3 + 5bx^2 + 5cx + d = 0. \tag{7}$$

Жели наравно да добије корен x из

$$x + m\sqrt[5]{f^4} + p\sqrt[5]{f^3} + q\sqrt[5]{f^2} + n\sqrt[5]{f} = 0. \tag{8}$$

Наравно, сада уместо $\sqrt[5]{f}$ посматра $\alpha^k\sqrt[5]{f}$ за $k = \overline{1,4}$, где је α пети примитивни корен из јединице, формира одговарајуће изразе, множи их и тако добија 'канонску' једначину петог степена. Поставља $f = 1$ и изједначава коефицијенте те канонске једначине с почетном једначином (7) те добија услове за m, p, q, n. Поставља затим $mn = y$, $pq = u$, $25uy - 5a^2 + 5c/3 = z$ и после доста рачунања добија једначину шестог степена по z. У општем случају, ова једначина нема рационалан фактор степена 1, 2, или 3, а ако би имала онда би једначина (7) била решива преко радикала.

Независно од Малфатија и Лагранж је конструисао 'решавач' z који је функција корена и који има шест вредности при пермутацији корена. И један и други решавач су инваријантни у односу на подгрупу групе пермутација од пет корена $x_1, \dots, x_5$, која је реда 20 за коју се $k \in \{1, \dots, 5\}$ слика у $k' = ak + b \pmod 5$ (при чему уместо 0 узимамо 5), где је $a \in \{1,2,3,4\}$, а $b \in \{0,1,2,3,4\}$. Занимљиво је, али не и неочекивано да ова подгрупа има значајну улогу и у Галоаовој теорији (наравно, она је решива).

Руфини

Слика 5: Руфини

Паоло Руфини (1765–1822) објавио је неколико радова у раздобљу од 1798. до 1813. (одговарајући на критике и поправљајући доказе) у којима је тврдио да је показао да једначине степена већег од четири не могу бити решене у радикалима.

Он ради слично Лагранжу. Посматра рационалне функције корена опште једначине степена n. Ако је p број пермутација које фиксирају такву функцију, онда је p делитељ од $n!$ и број различитих вредности које функција може узети при пермутовању корена је $n!/p$ (ако се сетимо дејства групе, орбита и стабилизатора, биће нам јасније зашто је ово тачно). Руфини је ово детаљно изучавао и показао је да у случају да је $n = 5$ тај број $5!/p$ може бити 2, 5 или 6, али не може бити ни 3 ни 4. То значи да Лагранжов решавач не може задовољавати једначину степена 3 или 4. Ако $5!/p$ није 2, он мора бити дељив са 5, а ако је $5!/p = 5$, онда заиста постоји решавач који задовољава једначину степена 5, али се не може свести на биномну једначину $z^5 - m = 0$.

Руфинијев доказ генерално није био добро прихваћен, њему је недостајало коришћење и корена из јединице у решавању и то је комплетирао Абел.

Коши

Слика 6: Коши

Огистен Луј Коши (1789–1857) је наравно био свестрани француски математичар који је дао велики допринос у више области математике, посебно у математичкој анализи, али овде ће нас занимати да укратко наведемо његове резултате за тему коју обрађујемо.

Коши је проширио резултате Руфинија на функције од n промењљивих. Наиме, доказао је да ако је p највећи прост број који дели n, онда број различитих вредности коју несиметрична рационална функција од n промењљивих може имати не може бити мањи од p сем ако је једнак 2. Он је увео и разлику између пермутација и супституција. Наиме, он је под пермутацијом подразумевао ређање n промењљивих (или слова) у неком поретку (дакле отприлике онако како се о пермутацијама прича у средњој школи), док су супституције функције којима се од једне пермутације прелази до друге. Галоа је такође користио ту терминологију, а и требало је извесно време да се пређе на назив „пермутације” за Кошијеве „супституције”. Коши је разматрао производе супституција. Ако су S и T супституције он је њихов производ означаао са ST и овде се прво примењивало S, а потом T (дакле, овде супституције „вуку” променљиве, не „гурају” их како се популарно каже).

У периоду од 1844. до 1846. године, Коши је написао низ радова о супституцијама. За две супституције каже да су „сличне” уколико имају исту поделу на циклусе. Показује да су P и Q сличне ако постоји R тако да је $Q = R^{-1}PR$ (видимо да је користио појам сличности, на који смо навикли изучавајући матрице; појам конјугације је касније уведен). Такође је доказао да је ред групе супституција дељив редом сваке супституције из те групе, као и да је ред ма које групе супституција n променљивих делилац броја $n!$. Овај резултат је већ доказао Лагранж. И код Кошија се у доказу појављује партиција групе на косете подгрупе. Општи резултат, који данас знамо као Лагранжова теорема дао је касније Жордан, али је приписао тај резултат Лагранжу. Иста прича важи и за Кошијеву теорему.

Абел

Слика 7: Абел

Нилс Хенрик Абел (1802–1829) био је норвешки математичар који је осим резултата везаних за решавање алгебарских једначина имао значајне резултате у области теорије елиптичких интеграла и данас многи математички објекти носе име по њему.

Он је 1824. о личном трошку објавио на француском дело о решавању алгебарских једначина, а 1826. је у Креловом Журналу објавио нешто проширену верзију. У тим радовима је дат јасан доказ да се једначине степена већег од 4 не могу решити у радикалима.

Он користи резултате осталих математичара који су се бавили овим проблемом, али ради и нешто есенцијално ново што комплетира овај доказ. Полази од једначине

$$y^5 - ay^4 + by^3 - cy^2 + dy - e = 0, \tag{9}$$

са „општим” коефицијентима – коефицијенти су независне променљиве. Претпостављајући да се y може изразити као функција коефицијената преко радикала, Абел каже да се y може написати у облику

$$y = p + p_1 R^{1/m} + p_2 R^{2/m} + \cdots + p_{m-1} R^{(m-1)/m} \tag{10}$$

где је m прост број. Величине $R, p, p_1, \ldots, p_{m-1}$ су све истог облика као и y, тј. укључују нове радикале, итд. све док се не дође до рационалних функција коефицијената почетне једначине. Он увек међу коефицијенте укључује и све m-те корене из јединице, за све просте m који се појављују као експоненти. $R^{1/m}$ је, да тако кажемо, последњи радикал који смо увели.

Наравно, он каже да се може претпоставити да се $R^{1/m}$ не може изразити као рационална функција од $a, b, \ldots, p, p_1, \ldots$ пошто би иначе додавање те величине било непотребно. Слично искључује могућност да $p_1, p_2, \ldots$ сви буду једнаки 0.

У првом раду претпоставља да $p_1 \neq 0$ (у другом показује да то ограничење није суштинско). Заменом R са R/p_1^m може да претпостави да је $p_1 = 1$. Означимо $R^{1/m}$ са z. Тада је

$$y = p + z + p_2 z^2 + \cdots + p_{m-1} z^{m-1}. \tag{11}$$

Заменом у (9) добија се да је

$$q + q_1 z + q_2 z^2 + \cdots + q_{m-1} z^{m-1} = 0, \tag{12}$$

где су $q, q_1, \ldots, q_{m-1}$ полиноми по $a, b, \ldots, p, p_2, \ldots$ и R (сетимо се да је $z^m = R$, те се тако уклањају виши степени од z). Абел сада тврди да је неопходно да сви ови q_i буду једнаки 0. Наиме, ако се претпостави да то није тако и посматра (12) и

$$z^m - R = 0, \tag{13}$$

видимо да је z заједнички корен две алгебарске једначине. Тада ће z бити корен и највећег заједничког делиоца одговарајућих полинома. Ако тај делилац није нерастављив, онда је z корен и неког његовог нерастављивог фактора за који можемо да претпоставимо да је степена бар 2 (јер би z иначе био већ рационална функција од постојећих величина). Дакле,

$$t_0 + t_1 z + \cdots + t_{k-1} z^{k-1} + z^k = 0, \tag{14}$$

при чему је одговарајући полином нерастављив. То је једначина најнижег степена коју z задовољава. Но, она има k корена заједничких са (13), а ова једначина има корене облика αz где је α нетривијалан m-ти корен из јединице. Дакле, имали бисмо

$$t_0 + t_1 z + \cdots + t_{k-1} z^{k-1} + z^k = 0 \quad \text{и} \quad t_0 + t_1 \alpha z + \cdots + t_{k-1} \alpha^{k-1} z^{k-1} + \alpha^k z^k = 0. \tag{15}$$

Множењем прве од ових са α^k и одузимањем од друге, добили бисмо једначину нижег степена који z задовољава, те то води до контрадикције. Стога сви коефицијенти $q, q_1, \ldots, q_{m-1}$ морају бити једнаки 0.

Користећи сада чињеницу да су решења једначине (13), сем z и αz, $\alpha^2 z, \ldots \alpha^{m-1} z$, заменом $R^{1/m}$ у (10) са $\alpha^i R^{1/m}$ такође се добијају корени почетне једначине (9). Ови корени су сви различити, m не може бити веће од 5. Ако су $y_1, \ldots, y_m$ тако добијени корени, онда имамо

$$\begin{array}{ccl} y_1 & = & p + z + p_2 z^2 + \cdots + p_{m-1} z^{m-1} \\ y_2 & = & p + \alpha z + \alpha^2 p_2 z^2 + \cdots + \alpha^{m-1} p_{m-1} z^{m-1} \\ \vdots & \vdots & \quad \vdots \qquad\qquad \ddots \qquad\qquad \vdots \\ y_m & = & p + \alpha^{m-1} z + \alpha^{m-2} p_2 z^2 + \cdots + \alpha p_{m-1} z^{m-1}. \end{array}$$

Ако се ово посматра као систем линеарних једначина по непознатим $p, z, p_2 z^2, \ldots, p_{m-1} z^{m-1}$, видимо да имамо систем од m једначина са m непознатих и то такав да има једнозначно решење (уочите која је матрица система). Стога се ове „непознате” све могу изразити као рационалне функције по $y_1, \ldots, y_m$ а тиме су и $p, p_2, \ldots, p_{m-1}$, $z = R^{1/m}$ (па онда наравно и $R = z^m$) рационалне функције корена.

Сама величина R је можда рационална функција неког раније уведеног радикала $v^{1/n}$. Понављањем претходног поступка добијамо да су све ирационалне величине које се појављују у изразу за корене y_i заправо неки радикали рационалних функција корена, укључујући свакако и одговарајуће корене из јединице. Руфини је пошао од те претпоставке, испуштајући корене из јединице и Абел је то оправдао. После овога он наставља користећи претходне резултате других математичара које смо навели и закључује да се општа једначина степена 5 не може решити преко радикала.

Два месеца пре смрти је објавио рад о једној класи решивих алгебарских једначина. У класу коју је разматрао спада и циклотомична једначина. Он ту доказује следећу општу теорему.

Ако су корени једначине такви да се сви корени могу изразити као рационалне функције једног од њих, на пример x, и ако су ма која два корена $\theta(x)$ и

$\theta_1(x)$ (где су θ и θ_1 рационалне функције), тако повезана да је $\theta(\theta_1(x)) = \theta_1(\theta(x))$ онда се једначина може решити у радикалима.

Данас наравно групе у којима је множење комутативно називамо Абелове групе. Овде је доказан специјални случај општег резултата који је дао Галоа. Наиме, знамо да је свака Абелова група решива и стога се одговарајућа једначина може решити преко радикала.

Гаус

Слика 8: Карл Фридрих Гаус

Карл Фридрих Гаус (1777–1855) свакако је био један од најзначајнијих математичара у историји, а имао је немале доприносе и у астрономији и физици. Овде ћемо се посветити његовим најважнијим доприносима нашој теми, а то је, најпре, комплетно решење циклотомичне једначине $x^n - 1 = 0$, а затим и резултатом да сваки реалан полином може да се факторише на линеарне и квадратне факторе, што пак повлачи „основну теорему алгебре”: сваки полином са комплексним коефицијентима може да се факторише на линеарне факторе.

Почнимо од „једначине деобе круга” $x^n - 1 = 0$. Још као студент математике, Гаус је дошао до изванредног открића, које је најавио, помало неочекивано, у литерарном часопису који је излазио у Јени. Ево његове најаве (када каже да се могу геометријски конструисати мисли на то да се могу конструисати искључиво користећи лењир и шестар) од априла 1796. године.

Познато је сваком почетнику у геометрији да су разни правилни многоуглови попут троугла, четвороугла, петоугла, петнаестоугла, као и они који се добијају непрекидним удвостручавањем страна претходних, могу геометријски конструисати.

То је већ урађено у време Еуклида и, чини се, генерално се каже да се поље елементарне геометрије не продужава даље: бар ја не знам ни за један успешан покушај да се њене границе продуже у том правцу.

Стога ми се чини да заслужује пажњу откриће да, сем наведених правилних многоуглова више њих, на пример 17-оугао допуштају геометријску конструкцију. Ово откриће је само специјалан додатак широј теорији, која још није комплетирана и која ће бити представљена јавности чим буде заокружена.

К. Ф. Гаус из Брауншвајга,
Студент математике у Гетингену

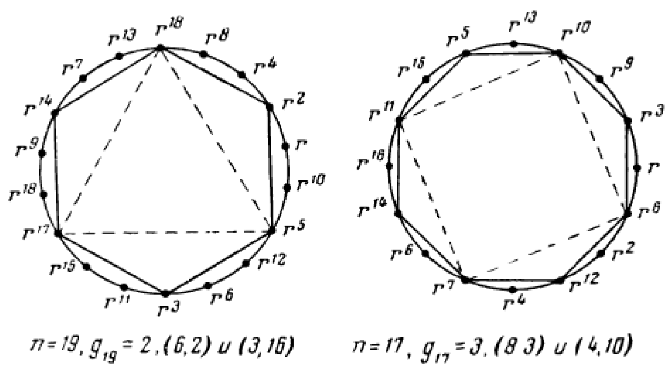
Овај резултат је представио у свом обимном делу „Аритметичка истраживања” објављеном у лето 1801. године. Заправо је томе била посвећена последња, седма глава овог дела. Претходне главе су биле посвећене теорији бројева.

Он ту показује да, ако је број страна правилног многоугла облика $p_1 p_2 \cdots p_l \cdot 2^k$, где су p_i различити прости бројеви облика $2^{2^n}+1$ (Фермаови прости бројеви), онда се тај многоугао може конструисати помоћу лењира и шестара (прича се да је он толико био поносан тим својим резултатом да је тражио да му цртеж правилног седамнаестоугла буде уклесан на надгробну плочу, али да је каменорезац то одбио тврдећи да се таква фигура не би разликовала од круга...). У једном одељку овог дела Гаус наводи да он има исправан метод да докаже да су то једини правилни многоуглови за које је могуће извршити конструкцију помоћу лењира и шестара и да, мада то превазилази границе овог дела, он то наводи због осећаја одговорности за то да други не би губили време покушавајући да овај резултат прошире.

Гаус најпре своди проблем на случај када је n прост број, и у даљем стално претпоставља да је то тако. Најпре, на доста компликован начин, доказује да је полином $x^{n-1}+x^{n-2}+\cdots+x+1$ (који он означава са X) нерастављив над рационалним бројевима. Скуп свих корена овог полинома Гаус означава са Ω. Он наводи потом да се идеја доказа састоји у томе да ако је $n-1$ производ фактора $\alpha\beta\gamma\cdots$), који се сви могу сматрати простим бројевима, онда се једначина $X=0$ може решити сукцесивним решавањем једначина степена $\alpha,\beta,\gamma,\ldots$. На пример, за $n=17$, $n-1=2\cdot2\cdot2\cdot2$, те за овај случај треба решити четири квадратне једначине.

За доказивање овог резултата, Гаус користи такозване „периоде”. Тачка 347 гласи: Сви корени из Ω разбијају се на неке класе (периоде). Наиме, нека је r неки од корена из Ω. Сматрамо да је n прост. Тада су сви корени заправо $r, r^2, r^3, \ldots, r^{n-1}$. Гаус је у трећој глави својих

„Истраживања” заправо доказао да ако је n прост број, онда је група $(\mathbb{Z}_n \backslash \{0\}, \cdot)$ циклична, те постоји „примитивни елемент” g који је генератор те групе. Тада су $1, g, g^2, \dots, g^{n-2}$ по модулу n заправо бројеви $1, 2, \dots, n-1$, али не нужно у истом поретку. Стога су $r, r^g, r^{g^2}, \dots, r^{g^{n-2}}$ такође сви корени из Ω при чему је сваки од њих g-ти степен претходног (приметимо да је и $\left(r^{g^{n-2}}\right)^g = r^{g^{n-1}} = r$ такође степен „претходног” ако их гледамо поређане на кругу. Поставимо те корене из Ω тако да деле круг на n једнаких делова.



Слика 9: Периоди

Они ће чинити темена правилног n-тоугла. Приметимо да на левој слици у врху уместо r^{18} треба да стоји r^{16}. Нека је $n-1 = ef$. Размотримо каква својства имају суме од по f тих корена тако да f тих темена која им одговарају чине темена правилног f-тоугла. Такве суме Гаус назива ПЕРИОДИМА дужине f (заправо скуп корена који се појављује у овој суми Гаус назива периодом, али каже да се и сама сума може тако назвати). Ако се у тој суми пође од корена r^λ она је једнака

$$r^\lambda + r^{\lambda h} + r^{\lambda h^2} + \cdots + r^{\lambda h^{f-1}},$$

где је $h = g^e$, а овде је сваки члан суме h-ти степен претходног (гледано циклички, тј. и први члан је h-ти степен последњег). Ову суму Гаус означава са (f, λ), при чему. Наравно, може се поћи од било ког темена, те је $(f, \lambda) = (f, \lambda h^k)$. Ако се стави $\lambda = 0$, добија се да је $(f, 0) = f$. И ту суму Гаус назива периодом, мада она нема исти статус као претходне. Ради прегледности писања, уместо r^μ пише $[\mu]$. Тада је $[\lambda] \cdot [\mu] = [\lambda + \mu]$, а такође важи: ако је $\lambda \equiv \mu \pmod p$, онда је $[\lambda] = [\mu]$; наравно, тада је и $(f, \lambda) = (f, \mu)$.

Гаус потом доказује низ лема за ове периоде, посебно како се налази формула за производе $(f,\lambda)\cdot(f,\mu)$. Наиме, ако је

$$(f,\lambda)=[\lambda]+[\lambda']+[\lambda'']+\cdots,$$

онда је

$$(f,\lambda)\cdot(f,\mu)=(f,\lambda+\mu)+(f,\lambda'+\mu)+(f,\lambda''+\mu)\cdots.$$

На пример, нека је $n=19$, тј. $n-1=18$ и $f=6$. Тада је $e=3$ и $g=2^3=8$ (2 је генератор за $(\mathbb{Z}_{19}\backslash\{0\},\cdot)$). У том случају је

$$(6,1)=[1]+[8]+[64]+[512]+[4096]+[32768],$$

односно после редукције по модулу 19 и приказа у растућем поретку.

$$(6,1)=[1]+[7]+[8]+[11]+[12]+[18].$$

Тада је

$$(6,1)^2=(6,1)\cdot(6,1)=(6,2)+(6,8)+(6,9)+(6,12)+(6,13)+(6,19).$$

Но, имамо једнакости:

$$(6,8)=(6,8\cdot 8)=(6,64)=(6,7)=(6,56)=(6,18)=(6,144)=(6,11)=(6,88)=(6,12)=(6,96)=(6,1),$$

$$(6,9)=(6,72)=(6,15)=(6,120)=(6,6)=(6,48)=(6,10)=(6,80)=(6,4),$$

$$(6,13)=(6,104)=(6,9)=(6,4),\qquad (6,19)=(6,0)=6.$$

Стога је $(6,1)^2=2(6,1)+(6,2)+2(6,4)+6.$

Ево приказа периода у овом случају:

$$\Omega=(18,1)\begin{cases}(6,1)\begin{cases}(2,1) & \ldots[1],[18]\\ (2,8) & \ldots[8],[11]\\ (2,7) & \ldots[7],[12]\end{cases}\\ (6,2)\begin{cases}(2,2) & \ldots[2],[17]\\ (2,16) & \ldots[3],[16]\\ (2,14) & \ldots[5],[14]\end{cases}\\ (6,4)\begin{cases}(2,4) & \ldots[4],[15]\\ (2,13) & \ldots[6],[13]\\ (2,9) & \ldots[9],[10]\end{cases}\end{cases}$$

Слика 10: Периоди за случај $n=19$

Без даљег разматрања, наведимо како се ти периоди појављују при формирању наведених помоћних једначина.

Ако је $n=19$, онда је $n-1=18=3\cdot 3\cdot 2$. Тада су периоди $(6,1),(6,2),(6,4)$ корени једначине $x^3+x^2-6x-7=0$. Периоди $(2,1),(2,8),(2,7)$ су корени једначине $x^3-(6,1)x^2+((6,1)+(6,4))x-2-(6,2)=0$, а r, r^{18} су корени једначине $x^2-(2,1)x+1$. Кад имамо r имамо и све остале.

За случај $n=17$, имамо $n-1=2\cdot 2\cdot 2\cdot 2$. Ево приказа периода за овај случај.

$$\Omega = (16,1)\begin{cases} (8,1)\begin{cases} (4,1)\begin{cases} (2,1)\ldots[1],[16] \\ (2,13)\ldots[4],[13] \end{cases} \\ (4,9)\begin{cases} (2,9)\ldots[8],[9] \\ (2,15)\ldots[2],[15] \end{cases} \end{cases} \\ (8,3)\begin{cases} (4,3)\begin{cases} (2,3)\ldots[3],[14] \\ (2,5)\ldots[5],[12] \end{cases} \\ (4,10)\begin{cases} (2,10)\ldots[7],[10] \\ (2,11)\ldots[6],[11] \end{cases} \end{cases} \end{cases}$$

Слика 11: Периоди за случај $n=17$

Периоди $(8,1),(8,3)$ су корени једначине $x^2+x-4=0$; $(4,1),(4,9)$ су корени једначине $x^2-(8,1)x-1=0$; $(2,1),(2,13)$ су корени једначине $x^2-(4,1)x+(4,3)=0$ и r, r^{16} су корени једначине $x^2-(2,1)x+1$. Тако смо добили те четири квадратне једначине. Како се решења квадратних једначина изражавају помоћу квадратних корена, а њих је могуће конструисати помоћу лењира и шестара (под условом да је поткорена величина већ конструисана), то се и правилни 17-угао може конструисати помоћу лењира и шестара. На пример, ако желимо да видимо колико је $\cos\frac{2\pi}{17}$ изражено алгебарски, онда можемо да приметимо да је $r=\cos\frac{2\pi}{17}+i\sin\frac{2\pi}{17}$, те је $r^{16}=r^{-1}=\bar{r}=\cos\frac{2\pi}{17}-i\sin\frac{2\pi}{17}$. Добијамо да је $\cos\frac{2\pi}{17}=\frac{1}{2}(r+r^{16})=\frac{1}{2}(2,1)$. Само треба наћи $(2,1)$...

Пређимо сада на разматрање основне теореме алгебре. Гаус се више пута враћао на ову теорему. Први доказ је објавио 1799, други и трећи 1816, а четврти 1849. Четврти доказ је базиран на истим идејама као и први, те је он заправо дао три различита доказа овог важног резултата.

Заправо је Гаусова теза, коју је одбранио код Фафа (Pfaff) 1799. у Хелмштету, садржала анализу ове теореме и први доказ. Наслов тезе:

„Нови доказ за теорему да се свака цела рационална алгебарска функција једне променљиве може разложити у реалне факторе првог или другог степена”. Теза није дуга, има неких 26 страница. Најпре Гаус анализира, уз критику, раније покушаје доказа овог резултата. Најпре се то односи на Даламберов доказ из 1746. године, а потом и на Ојлерову даљу разраду. Имајући у виду критику коју је дао, Гаус у другом делу представља свој доказ.

Гаус разматра полином са реалним коефицијентима

$$X = x^m + Ax^{m-1} + Bx^{m-2} + \cdots + Lx + M,$$

где је x неодређена. Он жели да докаже да или линеаран или квадратни фактор од X постоји. Треба приметити да ако одговарајућа једначина има двоструки корен, онда је он, као што знамо, нула и извода тог полинома, па се проблем може свести на полином мањег степена. Стога се може претпоставити да X нема вишеструких корена. Гаус избегава експлицитно коришћење комплексних бројева, што је рађено у претходним доказима и формулише следећу лему.

Лема. Ако је m произвољан позитиван цео број, онда је функција $\sin\varphi\cdot x^m - \sin m\varphi\cdot r^{m-1}x + \sin(m-1)\varphi\cdot r^m$ дељива са $x^2 - 2\cos\varphi\cdot rx + r^2$.

Констатује да се ово показује директном провером и формулише следећу лему.

Лема. Ако су величина r и угао φ одређени на такав начин да важе следеће једначине

$$r^m\cos m\varphi + Ar^{m-1}\cos(m-1)\varphi + Br^{m-2}\cos(m-2)\varphi + \ldots + Krr\cos 2\varphi + Lr\cos\varphi + M = 0, \tag{16}$$

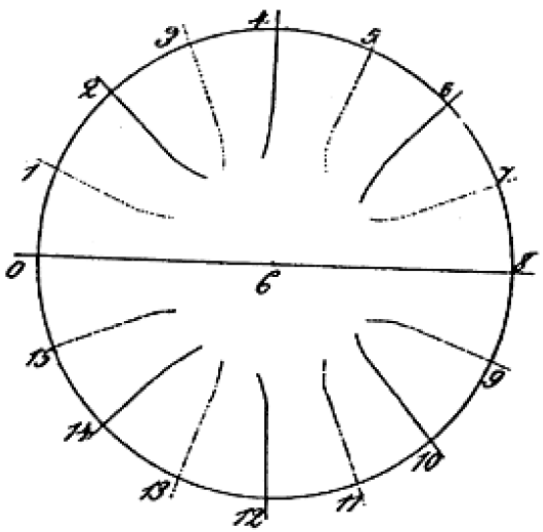
$$r^m\sin m\varphi + Ar^{m-1}\sin(m-1)\varphi + Br^{m-2}\sin(m-2)\varphi + \ldots + Krr\sin 2\varphi + Lr\sin\varphi = 0, \tag{17}$$

онда је функција $x^m + Ax^{m-1} + Bx^{m-2} + \ldots + KxxLx + M = X$ дељива фактором другог степена $xx - 2\cos\varphi\cdot rx + rr$, ако $r\cdot\sin\varphi$ није $= 0$. Али, ако јесте $r\cdot\sin\varphi = 0$, онда је та функција дељива простим фактором $x - r\cos\varphi$.

Ову лему доказује уз помоћ претходне. Гаус потом образлаже да се овако нешто доказује углавном коришћењем „имагинарних бројева” и наводи Ојлера, али да он, ето, сматра да је добро видети како се то може и директно доказати.

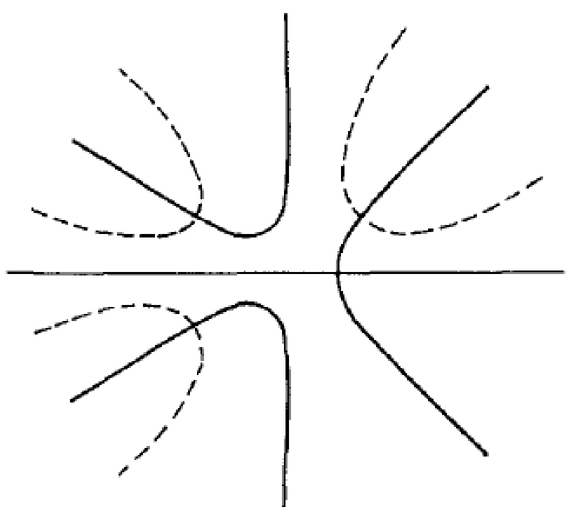
За једначине (16) и (17) он говори да су једначине алгебарских кривих степена m, само представљене у поларним координатама и леву страну у једначини (16) означава са U, а у једначини (17) са T.

Гаус сада жели да покаже да систем једначина $U = 0$, $T = 0$ има решење, тј. да се ове криве секу. Он тврди да за довољно велико R постоји тачно $2m$ тачака пресека криве $U = 0$ и круга полупречника R, као и тачно $2m$ тачака пресека криве $T = 0$ и тог круга, и то тако да се тачке пресека једне и друге криве појављују једна између друге. Ове алгебарске криве имају по m грана и он то илуструје цртежом:



Слика 12: Гаусов први доказ

Додаје и слику



Слика 13: Гаусов први доказ – додатна слика

ради појашњења. Каже да је она добијена помоћу функције $X = x^4 - 2xx + 3x + 10$. Парни бројеви на првој слици означавају пресеке круга и грана криве $T = 0$ (обратите пажњу да је x-оса једна од грана те криве), а непарни се односе на криву $U = 0$. Зашто се све дешава баш тако? Гаус каже да ако грана неке алгебарске криве улази у неки домен, она одатле и излази. Он ово сматра за јасно и не доказује, даје само следећи коментар у облику фусноте.

Чини се да је доказано са довољном сигурношћу да алгебарска крива нити може да се прекине било где (као што се дешава, на пример, са кривом чија је једначина $y = 1/\ln x$) нити се може изгубити, да тако кажемо, у некој тачки после бесконачно много намотаја (као код логаритамске спирале). Колико ја знам, нико није истакао било какву сумњу у вези овога. Ипак, ако би неко то тражио, онда бих се подухватио задатка да дам доказ, који не подлеже било каквој сумњи, неком другом приликом...

Но, ово тврђење о реалним алгебарским кривама није нимало једноставно и данас многи сматрају да је Даламберов доказ, који има мана, лакше поправити но Гаусов. Заправо је тек 1920. године Александар Островски дао непобитан доказ свих Гаусових тврдњи у овој тези и то је објављену у научном часопису у Гетингену. Но, тај доказ нимало није лак. Занимљиво је навести да је једноставнији доказ тога што Гаус тврди, дат у часопису *American Mathematical Monthly* 2017. године.

Наставак доказа да постоји пресек ове две криве Гаус изводи овако. Претпоставимо да пресек не постоји. Тачка 0 је повезана са тачком $2m$ x-осом (видети цртеж, ту је $m = 4$). Тачка 1 се онда не може повезати са неком тачком са друге стране x-осе а да је не пресече. Стога, ако је тачка 1 повезана са неком непарном тачком n, онда је $n < 2m$. На исти начин, ако је 2 повезано са парном тачком n' мора бити $n' < n$. Приметимо да је разлика $n' - 2$ парна и да је мања од разлике $2m - 0$. Настављањем поступка долазимо до ситуације да је тачка h повезана са тачком $h + 2$. Но, сада грана алгебарске криве која 'улази' у круг у тачки $h + 1$ мора обавезно сећи грану која повезује h и $h + 2$ што противречи претпоставци.

Гаусов други доказ је алгебарски, не укључује геометријска разматрања. Он је базиран на два резултата.

1. Сваки реални полином непарног степена има бар једну нулу.

2. Свака квадратна једначина са комплексним коефицијентима има два комплексна корена.

Гаус разматра реални полином степена m

$$Y = x^m - L' x^{m-1} + L'' x^{m-2} - \cdots + \cdots \tag{18}$$

Он овај полином мења полиномом y чије су нуле неодређене $a, b, c, \ldots$:

$$y = (x - a)(x - b)(x - c) \cdots \tag{19}$$

Посматра потом помоћни полином σ у новој променљивој u дефинисан као производ

$$\zeta = (u-(a+b)t+ab)(u-(a+c)t+ac)\cdots. \tag{20}$$

Видимо да је ово производ линеарних фактора који су добијени избором пара неодређених. Стога је $\deg\zeta = m' = \binom{m}{2} = \frac{1}{2}m(m-1)$. Дакле, овај полином је изражен помоћу u, t и симетричан је у неодређеним $a,b,c,\ldots$. Но, елементарне симетричне функције од ових неодређених дају коефицијенте $L',L'',\ldots$ полинома Y (присетимо се Вијетових формула; знаци коефицијената су тако бирани да су коефицијенти баш симетричне функције). Заменом добијамо помоћни полином Z степена m'. Гаус сада доказује да ако дискриминанта полинома Y није нула, онда ни дискриминанта од Z није 0 (дискриминанта неког полинома је једнака нули акко он има вишеструке корене). Потом бира за t реалну вредност тако да дискриминанта остаје различита од нуле и показује да, ако је корен од Z познат, пар корена оригиналног полинома се може добити (знамо колико су $a+b$ и ab, те онда решавањем квадратне једначине добијамо a и b). Главна ствар у овом доказу је да се итерирањем овог поступка добијају полиноми чији је степен све мање дељив са 2. Наиме, ако је $m=2^{\mu}(2k+1)$, онда је $m' = 2^{\mu-1}(2k+1)(2^{\mu}(2k+1)-1) = 2^{\mu-1}(2k'+1)$. Тако најзад добијамо полином непарног степена који има реалну нулу. И онда идемо уназад те добијамо и нуле почетног полинома.

Трећи Гаусов доказ користи математичку анализу. Можемо да га гледамо и као доказ, који у својој основи користи Гринову формулу из Анализе 2, или резултате из Комплексне анализе. Свакако је то директан доказ. О њему ћемо заиста кратко. Поново се полази од полинома са реалним коефицијентима

$$X = x^m + Ax^{m-1} + Bx^{m-2} + \cdots + Lx + M$$

и разматрају помоћне функције

$$t = r^m \cos m\varphi + Ar^{m-1}\cos(m-1)\varphi + Br^{m-2}\cos(m-2)\varphi + \cdots + Lr\cos\varphi + M;$$

$$u = r^m \sin m\varphi + Ar^{m-1}\sin(m-1)\varphi + Br^{m-2}\sin(m-2)\varphi + \cdots + Lr\sin\varphi.$$

Гаус наравно жели да докаже да систем једначина $t=0, u=0$ има решење. Претпоставимо да то решење не постоји, тј. да је $t^2+u^2 \neq 0$ за све вредности r и φ. Гаус посматра функцију

$$y = \frac{g}{r(t^2+u^2)^2},$$

при чему је g полином по t,u, као и њиховим првим и другим парцијалним изводима по φ (с обзиром на природу ових функција, ти парцијални изводи су функције истог облика). Затим тражи интеграл ове функције по довољно великом диску са центром у координатном почетку.

$$\Omega = \int\int_{0\leqslant\varphi\leqslant 2\pi, 0\leqslant r\leqslant R} y\,dr\,d\varphi.$$

Заправо код Гауса φ узима вредности од 0° до 360°. Ми смо то ипак мало модернизовали ☺. Но, испоставља се да ако се интеграли прво по φ добија се да је $\Omega = 0$, а ако се интеграли прво по r, па онда по φ, добија се да је $\Omega > 0$. Ова контрадикција показује да је $t^2 + u^2 = 0$ негде, а то је и тражено.

Галоа

Слика 14: Еварист Галоа

Еварист Галоа (1811–1832) био је син градоначелника једног малог града у околини Париза. Два пута (1828. и 1829) је покушао да се упише у École Polytechnique и после ових неуспелих покушаја уписао је École Normale. Треба рећи да је Политехничка школа била на знатно вишем нивоу од Нормалне, али је младог Галоа привлачила и због јаког студенцког политичког покрета у тој школи, а Галоа је републиканске идеје наследио од својих родитеља. Осим тога, Галоа је доживео породичну трагедију непосредно пре свог другог покушаја да упише Политехнику — отац му је извршио самоубиство због скандала изазваног његовим фалсификованим потписом на неким дописима.

Његов први објављени рад је чланак од 8 страна о верижним разломцима објављен у *Математичким аналима* Жергоња 1828. године

(Жозеф Жергоњ (1771–1859) био је француски математичар који је издавао овај утицајни часопис). Ту је он показао како се, ако се један корен алгебарске једначине ма ког степена изражава непосредно периодичним верижним разломком, онда се неки други корен изражава такође периодичним верижним разломком који се добија дељењем -1 истим верижним разломком, али написаним у обратном поретку.

У мају 1829, Галоа је приложио свој први рад о својим истраживањима о решавању алгебарских једначина, Академији наука Париза, а други, о једначинама простог степена осам дана касније, 1. јуна. Оба рада су послата Кошију који их је изгубио и они никада нису нађени.

У фебруару 1830. Галоа је Академији приложио још један рад на исту тематику да би био разматран за Велику награду Академије. Овај пут је рад добио стални секретар Академије Фурије, али је он умро пре него што је стигао да прегледа рад. Ни овај рукопис никада није нађен. Награду су поделили Јакоби и Абел (постхумно), док Галоаов рад није ни разматран.

Софи Жермен (1776–1831, француска математичарка која је имала значајне резултате посебно у теорији бројева) је писала о овоме:

> ...смрт господина Фуријеа је била превише за овог студента Галоу који, упркос својој дрскости, показује знаке паметне природе. Све ово је довело до тога да је он избачен са Нормалне школе. Сада је без новца... Кажу да ће потпуно полудети. Плашим се да је то тачно.

У априлу 1830. Галуа је објавио „ноту” (кратак рад) од две странице у *Билтену* (барона) Ферусака у којој су главни резултати рада који је приложио Академији били наведени без доказа. Прва и најзначајнија теорема која је наведена у овој ноти гласи:

> Да би једначина простог степена била решива у радикалима потребно је и довољно да се сви остали корени могу рационално изразити преко нека два од њих.

Јасно је да ово показује да општа једначина реда 5, која има 5 корена који су независни један од другог, не може решити у радикалима.

Изузетно значајан је рад крајње једноставног наслова „О теорији бројева” објављен у *Билтену* Ферусака у јуну 1830. године, а у коме је Галоа одредио структуру коначних поља (која се данас називају и Галоаовим пољима). Прикажимо до којих је резултата дошао.

И Абел и Галоа су имали јасан појам „поља”. Поља која су и Абел и Галоа разматрали у проблему решивости алгебарске једначине су увек поља која садрже у себи поље рационалних бројева. Садашњим језиком говорећи, ради се о пољима карактеристике 0. Но, у овом раду он се бави пољима карактеристике p за прост број p. Њега заправо занимају величине које постају 0 после множења са p. Ево шта он пише.

Ако се договоримо да сматрамо за нулу све величине које при алгебарском рачунању јесу умношци од p и ако се покуша да се, при овој конвенцији, нађе решење једначине $Fx = 0$, које господин Гаус означава нотацијом $Fx \equiv 0$, обичај је да се разматрају само целобројна решења. Како сам ја, вођен својим истраживањима, разматрао и несамерљива решења, добио сам неке резултате за које сматрам да су нови.

Дакле, Галуа јесте мотивисан разматрањем решавања конгруенција, али за разлику од Гауса који и за нелинеарне конгрупенције, попут $x^2 \equiv a \pmod p$, допушта само целобројна решења, Галуа би желео да размотри и 'ирационална решења', тј. желео би да посматра раширења од $\mathbb{Z}_p$ добијена додавањем нових елемената. Он претпоставља да је полином Fx нерастављив по модулу p. Пита се да ли може наћи нова решења увођењем нових 'симбола' који се могу показати исто тако корисним као и увођење имагинарне јединице i у анализу.

Галуа означава са i један од корена конгруенције $Fx \equiv 0$ степена ν (то i наравно није из $\mathbb{Z}$) и формира p^ν израза

$$a + a_1 i + a_2 i^2 + \cdots + a_{\nu-1} i^{\nu-1}. \tag{21}$$

где су $a, a_1, \ldots, a_{\nu-1}$ цели бројеви по модулу p. Ови елементи ће формирати поље, које данас називамо Галуаово поље и једна од ознака је и $GF(p^\nu)$.

Он даље показује да, ако се посматрају сви ненула елементи (и тако добије једна група у односу на множење) и овде, као у случају разматрања по модулу p постоје примитивни корени, тј. ова група је циклична (у данашњој терминологији). Дакле, сваки елемент Галоаовог поља је корен полинома $x^{p^\nu} - x$.

На крају свог рада, Галуа полази од ма ког раширења од $GF(p)$ у коме се горњи полином факторише на линеарне факторе. Посматрајући само потпоље генерисано коренима горњег полинома, он констатује да постоји „примитивни елемент” и у том потпољу. Каже да је то јасно на основу једне Абелове теореме. Тај елемент је нула неког нерастављивог полинома степена ν. Без обзира који полином да се узме, увек се долази до истог поља $GF(p^\nu)$. На пример, у случају $p = 7$ и $\nu = 3$ констатује да се за тај полином може узети $x^3 - 2$ који је нерастављив по модулу 7.

У јануару 1831. Академија је примила трећу, редиговану верзију, његовог централног рада под насловом „Мемоар о условима за решивост једначина радикалима”. Академија је замолила Поасона и Лакроа да напишу рецензију за овај рукопис. Поасон га је пажљиво прегледао и закључио да не може да га разуме. Ево и завршетка те рецензије.

Урадили смо све највише што смо могли да разумемо Галоаове доказе. Његово резоновање није довољно јасно, нити је довољно развијено да бисмо могли да дамо оцену његове тачности и чак нисмо у могућности да дамо идеју његовог резоновања у овој рецензији. Аутор тврди да је тврђење које је посебан циљ овог мемоара део опште теорије, која потенцијално има многе примене. Често се дешава да разни делови теорије, који појашњавају један други, буду лакше схватљиви као целина, него изоловани. Стога, да би се формирала сигурна оцена треба причекати док аутор не објави своје дело као целину. Но, у садашњем облику, за део који је поднесен Академији не можемо дати позитивно мишљење.

Галоа није стигао да представи своју комплетну теорију у облику научног рада. Он је погинуо у двобоју 30. маја 1832. Како је до двобоја дошло, јесте једна од мистерија које окружују овог младог човека. На основу најновијих истраживања, а која свакако нису рекла последњу реч о овом питању, укратко то можемо овако појаснити.

Већ је речено да је Галуа био истакнут у својим револуционарним активностима усмереним против уставне монархије установљене 1830. године у Француској. Дана 9. маја 1831. године 200 републиканаца се скупило да прослави ослобађање 19 артиљеријских официра Националне гарде који су крајем 1830. године ухапшени и оптужени за издају. Током ове вечере је Галоа, наводно, са бодежом у руци, претио краљу. Ухапшен је исте вечери, али је, изненађујуће, на суђењу 15. јуна ослобођен оптужбе. На Дан Бастиље 14. јула 1831. је поново ухапшен јер је носио забрањену униформу артиљеријског официра Националне гарде, а носио је и напуњену пушку, више пиштоља и нож. Ухапшен је и враћен у затвор у коме је претходно био. Током боравка у затвору, добио је обавештење да му је „Мемоар” одбијен. Покушао је самоубиство, али су га остали затвореници у томе спречили. У стању пијанства се жалио другима колико му недостаје отац. У марту 1832. дошло је до епидемије колере у овом затвору и затвореници су пребачени на друго место. Ту се, по свему судећи, заљубио у ћерку лекара из тог краја. Пошто је био отпуштен из затвора 28. априла, разменио је нека писма са њом, али је јасно да његова осећања нису била узвраћена.

Све те невоље које су га снашле, укључујући и ту неузвраћену љубав, довеле су до тога да је решио да се жртвује за револуционарну ствар. За покретање оружаног устанка, била је потребна и нека жртва и Галоа је решио да он буде та жртва. У наредним данима је написао неколико писама у којима је навео да је изазван на двобој од стране монархиста (а није пропустио да спомене да ће погинути и због „озоглашене кокете”). Заправо се договорио са својим пријатељем да одглуме двобој у коме ће Галуа страдати. Скоро је сигурно да је идентитет његовог пријатеља Перше Дербенвил (а то име је и Александар Дима навео у својим мемоарима). Галоа је навео да не замере онима који ће га убити, јер имају добру намеру. На његовој сахрани се скупило 3000 људи који су били спремни да нападну полицију и тиме започну побуну, но током сахране се сазнало да је генерал Ламарк, који је такође био велики критичар тренутног режима (генерал је био познат по значајним војним успесима под Наполеоном, касније је био критичар и рестаурације Бурбона и касније уставне монархије) и онда је закључено да би његова сахрана била боља прилика за побуну. До те побуне је и дошло у јуну 1832. године, али то није тема за нас.

У сваком случају, за нашу причу је значајно да је Галоа последњу ноћ пред двобој, дакле ноћ између 29. и 30. маја, провео састављајући подуже писмо свом пријатељу Огисту Шевалијеу у коме је објаснио основне идеје своје теорије. Ово писмо је објављено у Енциклопедијској ревији у септембру 1832. године. Галуа га завршава молбом пријатељу да јавно затражи мишљење од Јакобија и Гауса, не о тачности, него о значају теорема до којих је дошао.

После тога, наћи ће се, надам се, људи којима ће бити у интересу да распетљају сав овај галиматијас.

Нажалост, ни Јакоби ни Гаус се никада нису изјаснили овим поводом и шири круг математичара је тек 1846. године када је Лиувил у свом часопису објавио Галоаове математичке радове, сазнао за ове његове идеје.

Прикажимо сада, укратко, садржину Галоаовог „Мемоара”. Галоа почиње од једначине $f(x) = 0$. Коефицијенти овог полинома су познате величине, на пример рационални бројеви, или чак и само слова. Све рационалне функције ових коефицијената он назива рационалним. Могу се додавати и нове величине, на пример m-ти корени из постојећих. У савременој терминологији, Галоа почиње од неког основног поља и онда додаје нове елементе, те тако формира раширења поља. Он овде користи, али не сасвим конзистентно, термине пермутација и супституција. Посматра групе супституција које имају следеће својство: ако S и T припадају некој таквој групи, онда је у њој и ST. Обратите пажњу да он захтева само да је композиција две супституције у истој групи. Но, супституције су бијекције, а групе које разматра су коначне и ово му је довољно да може да закључи да је и идентична супституција ту, као и да је инверз сваке супституције у тој групи (размислите зашто).

Галоаова прва лема каже да ако неки полином f има заједнички корен са неким нерастављивим полиномом g, онда је f дељиво са g. Овај се резултат такође налази у Абеловом раду из 1829. Ова лема нам говори да је поље $K(V)$ које се добија додавањем неког корена нерастављивог полинома пољу коефицијената K потпуно одређено чим се зна базно поље K и нерастављив полином g – ми сада знамо да је то поље изоморфно количничком прстену $K[X]/\langle g\rangle$.

Он затим показује да ако једначина $g(x) = 0$ нема вишеструке корене и ако су корени $a, b, c, \ldots$ увек се може наћи функција ових корена V тако да су све вредности које се добијају свим пермутацијама $a, b, c, \ldots$ различите. Заправо Галуа каже да се за то може узети

$$V = Aa + Bb + Cc + \cdots$$

за неке целе бројеве $A, B, C, \ldots$. Одавде он добија да се тада сви корени $a, b, c, \ldots$ добијају као рационалне функције од V. Другим речима, $K(a, b, c, \ldots) = K(V)$. У овом доказу он неке међукораке и не доказује, те је Поасон исправно написао да је доказ овога некомплетан, али да је резултат тачан на основу једног Лагранжовог резултата. Тај елемент V је корен неког нерастављивог полинома. Ако су сви корени тог полинома $V, V', V'', \ldots, V^{(n-1)}$ онда следећа лема констатује да ако је $a = \varphi(V)$ корен почетне једначине, онда је $\varphi(V')$ такође корен те једначине.

Потом доказује главни резултат.

Став 1. Постоји група пермутација слова $a, b, c, \ldots$ тако да

1° Свака функција корена која је инваријантна на супституције у групи јесте рационално одредива.

2° Обратно, свака функција корена која је рационално одредива је инваријантна у односу на групу.

Видимо овде неконзистентност терминологије у вези пермутација и супституција, но јасно је о чему се ради. Он потом истражује како се мења група једначине ако се основно поље проширује додавањем једног, или чак свих корена неке помоћне једначине (задате нерастављивим полиномом). Јасно је да ће нова група бити нека подгрупа H почетне групе G. Он пажљивије говори о овоме у писму Шевалијеу.

Пише да се, уколико је H права подгрупа од G група G може раставити у облику

$$G = H + HS + HS' + \cdots \tag{22}$$

или у облику

$$G = H + TH + T'H + \cdots \tag{23}$$

Овде се наравно ради, у савременој терминологији, о разбијање групе на десне, односно леве косете по некој подгрупи. Галоа каже да се ове две декомпозиције не морају поклапати, а ако се поклапају, он каже да се ради о „правој” декомпозицији. У савременој терминологији наравно имамо тада у питању нормалну подгрупу. Он посебно наводи да је то случај када се додају сви корени помоћне једначине. Он доказ не наводи, само каже да се може наћи.

Сада он долази до основног питања: када се једначина може решити помоћу радикала. Наравно, довољно је посматрати радикале (корене) простог степена. Галоа овде претпоставља да се додају одговарајући корени из јединице на самом почетку, али на основу радова Гауса, то није неопходно претпоставити — p-ти корени из јединице могу се изразити преко радикала степена мањег од p.

Претпоставимо да додавање радикала r, који је корен једначине

$$x^p - s = 0 \tag{24}$$

доводи до редукције Галоаове групе. Како су сви p-ти корени из јединице по Галои већ у основном пољу, то смо заправо додали све корене једначине (24) (остали су облика αr, где је α p-ти корен из 1). Дакле, ради се о „правој” декомпозицији (подгрупа је нормална). Галоа тврди, али не доказује, да је број чланова у декомпозицији (22) (дакле, индекс подгрупе H у групи G) једнак p. Важи и обратно — ако је H подгрупа индекса p онда се Галоаова група G може редуковати на H додавањем радикала степена p.

Дакле, једначина $f(x) = 0$ је решива у радикалима ако и само ако постоји низ подгрупа

$$G \supset H_1 \supset H_2 \supset \cdots \supset H_m = \{e\}$$

тако је да H_k нормална подгрупа од H_{k-1} чији је индекс прост број. Наравно, те групе данас називамо решивим групама.

Галоа потом претпоставља да је једначина $f(x) = 0$ задата нерастављивим полином чији је степен прост број p. Доказује да се ова једначина може решити у радикалима ако и само ако свака супституција из G трансформише корен x_k у корен $x_{k'}$ линеарном трансформацијом k по модулу p:

$$k' \equiv ak + b \pmod p.$$

Галоаова група опште једначине петог степена нема овај облик, те стога ова једначина није решива у радикалима.

Почеци теорије скупова

Сада ћемо покушати да прикажемо како се развио савремени поглед на бесконачне скупове и како су скупови постали основа на којој градимо савремену математику. Но, у том приказу видећемо и како се развијао појам функције.

Наше излагање започињемо кратким освртом на рад Бернарда Болцана (1781–1848), који је био чешки филозоф и математичар италијанског порекла.

Слика 15: Бернард Болцано

Сигурно најпознатије дело овог математичара је његов рад из 1817. године у којем је доказао теорему да свака непрекидна функција узима све међувредности и која је свакако свим студентима позната из курса математичке анализе (сличан доказ је касније дао и Коши у свом *Курсу анализе*, те је зато та теорема и позната као Болцано-Кошијева теорема).

Но, ми се нећемо задржавати на овом раду, но на његовој постхумно објављеној расправи *Парадокси бесконачног* (1851). До овог рада, чак и велики математичари попут Даламбера и Гауса, су избегавали да прихвате стварно постојање бесконачног, но су о појму бесконачности писали као о *начину изражавања*, у контексту промењљивих величина које могу узимати произвољно велике вредности и слично. Болцано у овој својој расправи истиче да бесконачни објекти заиста постоје. На пример, он овде наводи да је реална права бесконачна, а није промењљива. Такође наводи и следећи пример (скоро идентичан пример је касније навео и Дедекинд (Јулијус Виљем Рихард Дедекинд, 1831–1916, немачки математичар) у својој дискусији о бесконачним скуповима, а о којој ће касније бити више речи): скуп свих истина је бесконачан. Наиме, узмимо било које истинито тврђење A. Онда можемо формирати ново тврђење B, које НИЈЕ идентично старом: „A је истинито". Дакле, на тај начин добијамо ново истинито тврђење B и потом C итд. Он указује да тако добијамо бесконачно много тврђења, а и истиче сличност формирања ових тврђења формирању скупа свих (природних) бројева.

Најзанимљивији део за ову нашу причу је вероватно следећи пример, који Болцано наводи. Он разматра два скупа: све реалне бројеве (за њега, све *величине*) између 0 и 5 и све реалне бројеве између 0 и 12 и истиче да постоји бијекција (овде користимо савремену терминологију, Болцано није то тако исказао) између ова два скупа задата једначином $5y = 12x$. Но, он нажалост пропушта могућност да препозна појам кардиналности бесконачних скупова, него истиче да ипак не можемо те скупове сматрати једнаким у односу на бројност својих чланова, пошто, тако каже Болцано, елементима 3 и 4 одговарају елементи $7\frac{1}{5}$ и $9\frac{3}{5}$ и док су елементи 3 и 4 на растојању 1, дотле су елементи који њима одговарају на растојању $2\frac{2}{5}$. И стога те скупове он не сматра истобројним. Очигледно је да код њега још увек превелики значај имају метричка својства. Из других примера које наводи види се да и Еуклидово „цело је веће од свог дела" има велики утицај на њега, чак и у разматрањима која се тичу бесконачних скупова (и сума). Занимљиво је да он чак понегде истиче да скупови могу имати исте елементе, а да су ипак различити! Наводи као пример крчаг и разбијени крчаг. Очигледно је да апстрактан појам скупа није још присутан код њега.

На крају треба још истаћи да Болцанови радови нису били довољно познати у своје време, па чак ни доста касније, те да стога нису имали значајан утицај на развој математике тога времена.

Први велики математичар (Болцано је као математичар имао одређени значај, али сигурно се не би могло рећи да је био велики математичар), који је имао значајан утицај на развој теорије скупова био је свакако Риман (Георг Фридрих Бернхард Риман (1826–1866), немачки математичар).

Слика 16: Георг Риман

Риманов живот је био нажалост кратак, али изузетно плодотворан са математичке тачке гледишта. Он је започео студије на универзитету у Гетингену 1846. године да би године од 1847. до 1849. провео у Берлину где је имао прилику да учи од Јакобија и Дирихлеа. По повратку у Гетинген започела је једна од сигурно најуспешнијих деценија у историји математике. Риман је одбранио докторат 1851. године из области комплексне анализе и у том докторату је увео појам Риманове површи. Године 1853, предао је своју тезу за хабилитацију на тему Фуријеових (Жан Баптист Жозеф Фурије (1768–1830), француски математичар) редова, у оквиру које је прецизирао појам интеграла. Наредне године је одржао своју лекцију за хабилитацију о нееуклидској геометрији у којој је увео појам многострукости и са којом се може рећи да започиње модерни развој диференцијалне геометрије. Значајан рад о Абеловим функцијама објавио је 1857. године, а рад о зета функцији 1859. године. Читаоцу је свакако јасно да би за приказ свих ових радова и њиховог значаја, била сигурно потребна не једна, но више књига, али ми ћемо се у нашем историјском осврту задржати само на најважнијим елементима који се тичу теорије скупова.

Први Риманов утицај на развој теорије скупова је садржан у његовој лекцији за хабилитацију, коју је имао обавезу да одржи да би добио одобрење да предаје у Гетингену. У ту сврху он је понудио три теме и Гаус је, што је било неуобичајено, одабрао да Риман одржи лекцију на трећу тему. И Римана је то изненадило (у писму свом брату је писао да је припремио прве две теме добро и да се надао да ће Гаус изабрати неку од њих, али да сада мора да припреми и предавање за ту трећу тему). Ово предавање је одржано 10. јуна 1854. године и наслов је био: *О хипотезама које леже у основи геометрије.* Сам Гаус, који је предложио тему, био је веома импресиониран Римановим излагањем.

Како је предавање било замишљено за ширу публику, у њему није било техничких резултата, као што би се популарно рекло „није било много формула”, но било је богато дубоким и новим идејама. У њему је Риман увео појам многострукости, на немачком *Mannigfaltigskeit*, као n-тоструко проширене величине. Ту је практично дата савремена дефиниција многострукости — (тополошки) простор, који је локално еуклидски простор од n димензија. Дискутовано је о појму растојања, дужине кривих и уопште о рачуну у таквим просторима. Треба истаћи да је Риман ту успутно навео и могућност разматрања, тј. постојања и бесконачно димензионалних многострукости (многострукости чије су тачке функције, за које је потребно задавање бесконачно много величина, другим речима вредности функција). Но, за нашу причу је значајно то што Риман разликује непрекидне многострукости и дискретне многострукости. Он каже да су индивидуалне специјализације непрекидних многострукости тачке, а дискретних, елементи многострукости.

Заправо, може се рећи да је он овим својим радом желео да учини и више од онога што је садржано у самом наслову. Док би се за непрекидне многострукости могло рећи да представљају истинску расправу о геометријском простору, дотле дискретне многострукости заправо представљају први почетак заснивања свих појмова математике на појму скупа. Наиме, дискретна многострукост није ништа друго него скуп. Заправо Кантор (Георг Фердинанд Лудвиг Филип Кантор, 1845–1918, немачки математичар), под очигледним утицајем Риманових идеја, у својим првим радовима посвећеним скуповима *није* користио за скупове термин ***Menge***, но Риманов термин ***Mannigfaltigskeit***. Ово Риманово предавање није било одмах доступно широј публици. Заправо, оно је објављено тек 1868. године, две године после Риманове смрти и имало је изванредан утицај на развој математичара те и будућих генерација.

Док се у овом Римановом предавању о геометрији налази клица каснијег заснивања математике на појму скупа и оно као такво представља методолошко-филозофску основу за почетак развоја теорије скупова, дотле његова хабилитациона теза, која је посвећена разматрању Фуријеових редова, представља конкретну основу на којој су започела истраживања која су довела до развоја апстрактне теорије скупова, основних тополошких појмова, као и теорије мере. Стога ћемо посветити пажњу и тој тези.

Да бисмо боље схватили проблеме који су се истраживали, морамо да се вратимо мало уназад у времену, до Ојлера.

У свом *Уводу у анализу бесконачности* из 1748. године, он је дефинисао функцију промењливе величине као „аналитички израз”, који је на произвољан начин направљен од те промењливе и разних константи. Дакле, за функцију је неопходно да има запис у облику формуле. Но, он је у свом ранијем раду из 1734. у области парцијалних диференцијалних једначина допуштао и могућност да функција буде „прекидна”, тј. да нема јединствен аналитички запис у целој области, него да *криве* које представљају график функције буду састављене од више делова са потенцијално различитим аналитичким записом. То је истакао и у расправи са Даламбером (Жан ле Рон Даламбер (1717–1783), француски математичар) који је 1747. показао да једначина струне која осцилује има решење $F(x,t) = \frac{1}{2}(f(x+t)+f(x-t))$. Даламбер је истицао да f мора бити „непрекидна”, тј. да има јединствен аналитички запис, док је Ојлер сматрао да може да буде и прекидна у горенаведеном смислу те речи. У ту дискусију се укључио и Данијел Бернули (1700–1782, швајцарски математичар), који је на основу физичког разматрања о струни која осцилује, навео да функција f мора бити представљива у облику реда

$$f(x) = a_1 \sin(\pi x/L) + a_2 \sin(2\pi x/L) + \cdots,$$

где је L дужина струне. Са математичке тачке гледишта, Бернулијево тврђење се своди на то да се свака функција може представити тригонометријским редом. То тврђење је већина водећих математичара одбацила.

Но, Фурије, најпре у свом раду о провођењу топлоте из 1807, који није објављен, а потом у свом значајном делу *Аналитичка теорија топлоте* из 1822, враћа се на ту идеју. Заправо, он тврди да се свака ограничена функција f на $(-\pi, \pi)$ може представити у облику

$$f(x) = \frac{1}{2}a_0 + \sum_{n=1}^{\infty} \left(a_n \cos(nx) + b_n \sin(nx)\right), \tag{$*$}$$

где су коефицијенти задати са

$$a_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos(nx)dx, \quad b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin(nx)dx.$$

Наравно, ово су сада свима добро познате формуле из теорије Фуријеових редова.

Фурије говори о произвољној функцији, али се из његовог излагања види да ипак размишља на начин својих претходника. На пример, њему је функција задата са e^{-x} за ненегативне x, а са e^{x} за негативне x (другим речима, функција $e^{-|x|}$) „прекидна" пошто је задата помоћу два аналитичка израза.

Он је заправо дао два доказа свог тврђења о развоју произвољне функције у тригонометријски ред. У првом доказу је претпоставио да се функција може развити у степени ред и затим решавајући систем од бесконачно много једначина са бесконачно много непознатих, дошао до траженог развоја. У другом доказу он разматра „произвољну" функцију (претпоставља се да је ограничена) и полази од једначине $(*)$. Множењем те једначине са $\cos(nx)$ и $\sin(nx)$ и интеграцијом (при чему интеграл пролази кроз суму) он добија коефицијенте у наведеном облику и тиме тврди да је функција f заиста представљена тим тригонометријским редом. Много се примедби може навести у вези таквог 'доказа'. Пре свега, није јасно зашто се ред може интегралити члан по члан, зашто чак и када се интеграли члан по члан, наведени интеграли постоје и напокон, зашто тако одређени коефицијенти заиста дају тригонометријски ред чија је сума једнака датој функцији. Дакле, много је примедби, а Фурије је покушао да оправда постојање интеграла о којима је реч. Наиме, он је објаснио да је функција $f(x)\sin x$ која се добија множењем произвољне функције функцијом синус сличног понашања као и синусна функција, она само представља синус који је 'увећан' за одговарајући фактор (као да имамо осцилацију тако да величина амплитуде варира у свакој тачки) и да онда интеграл јесте задат површином. Но, није дао објашњење зашто та површина постоји.

Дакле, модерни концепт непрекидне функције се сигурно не може наћи код Фуријеа и заправо се први пут појављује код Кошија. У свом *Курсу анализе*, он уводи појам непрекидности на следећи начин. функција f, која је дефинисана и ограничена на одсечку $[a,b]$ је непрекидна унутар тих граница уколико за x из тог одсечка „нумеричка вредност разлике $f(x+\alpha)-f(x)$ бесконачно опада како то чини α". Дакле, Коши дефинише не појам непрекидности у тачки, него непрекидности на одсечку. Заправо се појам непрекидности и појам равномерне непрекидности код њега не разликују. Године 1823, Коши дефинише одређени интеграл непрекидне функције помоћу интегралних сума. Он наиме разматра поделу одсечка $a=x_0<x_1<x_2<\cdots<x_{n-1}<x_n=b$ и суму $S=\sum_{i=1}^{n}(x_i-x_{i-1})f(x_i)$. Уз коришћење равномерне непрекидности функције f (као што је горе напоменуто), он показује да су за поделе чија је норма довољно мала (норма поделе је наравно максимална дужина интервала поделе) и одговарајуће суме произвољно близу и закључује да постоји јединствени лимес и тај лимес је заправо одређени интеграл. Он у даљем, за непрекидну функцију f, разматра и функцију $F(x)=\int_0^x f$ и количник $\frac{F(x+h)-F(x)}{h}$ и показује да је F једна примитивна функција за f, тј. $F'=f$, као и да се свака друга примитивна функција за f од F разликује за константу.

Као што видимо, резултати које је Коши добио су сасвим савремени и у модерном духу. Но, и поред тога, Коши ипак није разматрао опште функције, тј. за Кошија функција ипак није била произвољно придруживање, но се и код њега у основи крила концепција да функција мора бити задата аналитичким изразом. То се најбоље може видети у чињеници да је Коши у доказима који се тичу конвергенције Фуријеових редова, у функцији $f(x)$ реалну променљиву x замењивао комплексном променљивом $z=x+iy$, што заиста нема много смисла, сем уколико се подразумева да је f ипак задата неким аналитичким записом.

И поред дефиниције појма непрекидности, Коши није у пуној мери разматрао могућности постојања произвољних прекидних функција. „Најнеправилније" функције у том смислу које је он разматрао су заправо биле функције облика (наравно у модерној нотацији)

$$\chi_{I_1}g_1+\cdots+\chi_{I_n}g_n,$$

где су са χ_{I_j} означене карактеристичне функције одсечака I_j, а g_j су непрекидне функције у његовом смислу. Дакле, прекидне функције које је Коши разматрао су биле искључиво оне које су имале највише коначно много тачака прекида. Први математичар који је озбиљно разматрао функције са бесконачно много тачака прекида био је Дирихле (Јохан Петер Густав Лежен Дирихле, 1805–1859, немачки математичар).

Дирихле је лично познавао Фуријеа, пошто је од 1822. до 1825. године боравио у Паризу. Он је 1829. године дао први строг доказ о

Слика 17: Лежен Дирихле

конвергенцији Фуријевог реда дате функције f (наравно под одређеним условима). Наиме, он је разматрао парцијалну суму Фуријеовог реда $S_n(x) = \frac{1}{2}a_0 + \sum_{k=1}^{n}(a_k \cos(kx) + b_k \sin(kx))$ и приказао је ту суму у облику

$$S_n(x) = \frac{1}{\pi}\int_{-\pi}^{\pi} f(t)\frac{\sin\frac{(2n+1)(t-x)}{2}}{\sin\frac{t-x}{2}}dt,$$

коју су сигурно видели сви студенти на курсу анализе у којем се изучавају Фуријеови редови. Саму формулу наравно није тешко извести (присетимо се дефиниције коефицијената Фуријевог реда — одатле се добија интеграл). Дирихле је претпоставио да функција има или највећу или најмању вредност и да није непрекидна у највише коначно много тачака. Заправо тај услов му је требао да би се доказала егзистенција интеграла помоћу којих се одређују Фуријеови коефицијенти. Доказао је да парцијална сума конвергира ка $\frac{1}{2}(f(x-0)+f(x+0))$ за $x \in (-\pi,\pi)$, а ка $\frac{1}{2}(f(-\pi+0)+f(\pi-0))$ за $x = \pm\pi$. У доказу је ипак користио и претпоставку да је функција f монотона у довољно малом интервалу сваке тачке $x \in [-\pi,\pi]$.

Сматрао је да се случајеви када функција има бесконачно много екстремних вредности, или бесконачно много тачака прекида, могу свести на случај који је разматрао. Заправо је сматрао да је једини услов да функција има интеграл. Као довољан услов за постојање интеграла, он је навео (користимо модерну терминологију) да функција мора бити таква да је скуп D, тачака прекида те функције, нигде густ (подсетимо читаоца да је нигде густ скуп онај скуп чије затворење не садржи ниједан интервал). Дирихле то тврђење није доказао и навео је да ће доказ бити презентиран у неком наредном раду, али... Тај доказ никада није објавио.

Године 1864, у својој докторској дисертацији, Липшиц (Рудолф Ото Сигисмунд Липшиц,1832–1903, немачки математичар) је покушао да

Слика 18: Рудолф Липшиц

прошири Дирихлеове резултате о конвергенцији Фуријеових редова. Интересантно је да је упркос чињеници да је његова теза рађена чак 10 година после Риманових основних резултата о којима ћемо ускоро говорити, ти резултати нису утицали на Липшицов рад и по свему судећи, он их и није био свестан. Као што смо већ написали, многи Риманови главни резултати су постали опште познати тек после његове смрти. Липшиц је пажљиво анализирао Дирихлеов доказ и разматрао је могућности под којима Дирихлеов доказ 'не би прошао' за дату функцију. Установио је да проблем настаје у случају ограничене и деопо-део монотоне функције (као што смо већ навели, те претпоставке јесу стајале у основи Дирихлеовог доказа), која има бесконачно много тачака прекида између $-\pi$ и π. Заправо, закључио је да би Дирихлеов доказ и прошао под условом да та функција има интеграл (дакле уколико се појам интеграла може проширити и на ту класу функција). Закључио је да уколико функција задовољава услов који је Дирихле навео (да је скуп тачака прекида D нигде густ), то може бити изведено. Грешка коју је направио била је у томе што је сматрао да се тада може добити да је скуп D', тачака нагомилавања скупа D, коначан. Проблем је заправо био и у томе што у то време није било занимљивих, другим речима нетривијалних, примера скупова који су нигде густи и онда није било неочекивано да се дође то таквог закључка.

Но, Липшиц је ипак у својој тези дошао и до значајних резултата. Наиме, он се потрудио да замени Дирихлеов услов о монотоности неким другим условом и успео је да га замени другом претпоставком из које је успео да докаже Дирихлеов резултат. Услов који је дао данас је добро познат свим математичарима као Липшицов услов: $|f(x+h)-f(x)| \leqslant C|h|^\alpha$ за позитивне бројеве C и α.

Пре него што најзад пређемо на Риманов допринос у овој области, а који је био и основа за почетак Канторовог истраживања, а како ћемо видети и почетак озбиљног разматрања бесконачних скупова, наведимо ипак две значајне последице Дирихлеовог рада у овој области. Са његовим радом је први пут почела да се разматра разлика између појма непрекидних и појма интеграбилних функција. Такође је Дирихле био први значајни математичар који је заиста разматрао општи појам функције реалне променљиве, као придруживање $x \mapsto f(x)$ независно од цртежа и формула. Уосталом добро нам је позната Дирихлеова функција која је на један начин задата на рационалним, а на други начин на ирационалним бројевима и коју је свакако немогуће нацртати, а и задати формулом на начин како је то рађено до тада (поделом датог одсечка на мање одсечке и задавањем формулама на тим деловима). Дирихле је увео ту функцију као пример функције за коју појам интеграла нема смисла. Тек је са појавом Лебеговог (Анри Леон Лебег, 1875–1941, француски математичар) појма интеграла показано да то није тако, али то није већ није део наше приче.

Значајан помак у разумевању појма интеграла и у питањима конвергенције Фуријеових редова дао је Риман. Он је имао прилику да у Берлину прати Дирихлеова предавања из теорије бројева, интеграла, као и парцијалних диференцијалних једначина. Веома је ценио Дирихлеа и сматрао га је, уз Гауса, за највећег живог математичара.

Интересантно је да је Риман имао различит приступ комплексним и реалним функцијама. Наиме, у случају функција $f(z)$ комплексне променљиве, он је захтевао обавезно постојање извода $f'(z)$ док је у случају функција реалне променљиве допуштао, по угледу на Дирихлеа, произвољно придруживање. Но, треба имати у виду да је Риман као и Дирихле и Гаус сматрао да се свака реална функција на одсечку $[-\pi,\pi]$ може представити Фуријеовим редом. Заправо је Ди Буа-Рејмон (Паул Давид Густав ди Буа-Рејмон, 1831–1889, немачки математичар) био први математичар који је дао пример да то у општем случају није тачно.

У проблему представљања функција тригонометријским редовима, Риман је најпре истакао да је значајно установити под којим условима интеграл постоји. Као и Коши, он је разматрао интегралне суме и поставио је питање под којим условима те суме имају граничну вредност. Коши јесте показао да је то тачно за (равномерно) непрекидне функције, но Римана су занимали општи услови. Он је истакао да је то тачно ако и само ако сума $\sum_{i=1}^{n} D_i(x_i - x_{i-1})$ тежи нули када параметар поделе (максимална дужина интервала у подели) тежи нули, где је са D_i означена осцилација функције f на одсечку $[x_{i-1}, x_i]$. Осим овог услова разматрао је и следеће. Уколико је σ неки позитиван број, са

$s(P,\sigma)$ означимо збир дужина интервала на којима је осцилација већа од σ. Природно се поставља питање да ли можда $s(P,\sigma)$ тежи нули када параметар поделе и σ теже нули. Риман је показао да је тај услов еквивалентан претходно наведеном. То су дакле били услови које је он добио као потребне и довољне услове за постојање граничне вредности интегралних сума, тј. за постојање интеграла.

Риман је наравно истакао да такве услове испуњавају и поједине функције које имају бесконачно много тачака прекида на коначном одсечку и дао је следећи пример. Са (x) означимо функцију која реалном броју x придружује растојање до најближег целог броја, ако такав постоји и придружује 0 уколико је x полуцео број (тј. број облика $n/2$, где је n непаран број), пошто у том случају не постоји јединствени цео број који је најближи броју x. Јасно је да је функција (x) прекидна у свим полуцелим тачкама и непрекидна у осталим тачкама. Риман затим разматра ред $\sum_{n=1}^{\infty}\frac{(nx)}{n^2}$. Тај ред задаје функцију која је прекидна у свим тачкама облика $\frac{m}{2n}$, где су m и $2n$ узајамно прости. Дакле, функција је прекидна у свуда густом скупу тачака. И поред тога, како је у тачкама $x=\frac{m}{2n}$, $f(x+0)=f(x)+\frac{\pi^2}{16n^2}$ и $f(x-0)=f(x)-\frac{\pi^2}{16n^2}$ то је функција f интеграбилна пошто је „скок“ у свакој таквој тачки једнак $\frac{\pi^2}{8n^2}$, а очигледно да за свако $\sigma>0$ и сваки ограничени интервал реалне праве, постоји само коначно много тачака у којима је тај скок већи од σ. Стога је други наведени услов испуњен и функција је интеграбилна.

Да би установио потребне и довољне услове да би нека функција била представљена тригонометријским редом

$$\Omega(x)=\frac{a_0}{2}+\sum_{n=1}^{\infty}(a_n\cos nx+b_n\sin nx),$$

он је урадио следеће. Претпоставио је да низ функција $A_n(x)$ задат са: $A_0(x)=\frac{1}{2}a_0$, $A_n(x)=a_n\cos(nx)+b_n\sin(nx)$, равномерно конвергира ка нули када $n\to\infty$ и формално је интегрирао тај ред члан по члан те добио функцију F:

$$F(x)=C+C'x+A_0\frac{x^2}{2}-\sum_{n=1}^{\infty}\frac{A_n(x)}{n^2}.$$

Овај ред конвергира за све вредности x и представља непрекидну функцију. Риман је показао да та функција задовољава два важна услова:

$$D^2F(x)=\lim_{a,b\to 0}\frac{F(x+a+b)-F(x-a+b)-F(x+a-b)+F(x-a-b)}{4ab}=0,$$

$$\lim_{a\to 0}\frac{F(x+a)-2F(x)+F(x-a)}{a}=0.$$

Коришћењем ових резултата, Риман је добио потребне и довољне услове за представљање дате функције тригонометријским редом у датој тачки. Важно је истаћи да коефицијенти a_n и b_n нису добијени интеграцијом, но су то произвољни низови бројева, који морају да задовољавају горенаведени услов, који се тиче равномерне конвергенције низа функција $A_n(x)$.

Дакле, Риман је проширио појам интеграла на ширу класу функција, а дао је и метод за испитивање могућности представљања функција тригонометријским редом. Као што смо већ рекли, ови Риманови резултати су објављени тек 1867. године и тек тада је шири круг математичара имао прилику да настави та истраживања.