Univerzitet u Beogradu
Matematički fakultet

MASTER RAD

Rešivost algebarskih jednačina

mentor:
prof. dr Zoran Kadelburg

student:
Stevan Janković

Beograd 2011.

Sadržaj

1. Istorijat rešavanja algebarskih jednačina

Prema raspoloživim podacima, arapski matematičari srednjeg veka umeli su da rešavaju kvadratne jednačine.

Kubnu jednačinu prvi je rešio **Scipion del Fero** (Scipione del Ferro, 1465-1526, Bolonja). Del Fero je bio student i profesor Univerziteta u Bolonji koji je, kao i mnogi drugi stvaraoci te epohe, krio svoje rezultate. Treba znati da su u toj epohi bila veoma česta javna takmičenja matematičara koja su nalikovala dvobojima. Jedan drugome su zadavali zadatke, a pobednik je bio onaj koji bi rešio više protivnikovih problema. Iako nam nije poznato da je sam Del Fero učestvovao u tim takmičenjima, očigledno se držao običaja epohe. Nikakvi rukopisi Del Fera nisu sačuvani niti je za života išta objavio. Na samrtničkoj postelji, Del Fero je metod rešavanja kubne jednačine poverio svom učeniku Antoniju Mariji Fioru, a svesku sa beleškama predao svom zetu Hanibalu Naveu. Nave je po tastovoj smrti 1526. nasledio njegovu katedru na Univerzitetu u Bolonji, a i on i Fior su nastavili da čuvaju tajnu.

Ostaće tajna da li je Del Fero rešio oba slučaja kubne jednačine ili samo jedan, kao i kada ih je rešio. Što se vremena rešavanja tiče, o njemu ne možemo čak ni da nagađamo. Neki istoričari spekulišu da je početkom 16. veka Luka Pačoli sarađivao sa Del Ferom kada je bio u Bolonji na jednom od svojih mnogobrojnih putovanja. Međutim, ako se uzme u obzir da Pačolijeva *Summa* koja je je štampana nekoliko godina pre tvrdi da je kubnu jednačinu nemoguće rešiti, pitanje je koliko je Pačoli zaista mogao da koristi Del Feru.

Što se tiče pitanja koje sadrži konstataciju o dva slučaja kubne jednačine, treba pojasniti da mi danas kada izlažemo rešavanje kubne jednačine prezentiramo formule slične onima za rešavanje kvadratne jednačine. Kvadratna jednačina se prikazuje u takozvanom opštem obliku kao:

$$ax^2 + bx + c = 0,$$

a njena rešenja formulama

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}, \quad x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

To je u 16. veku bilo nezamislivo. Ne samo zbog nepostojanja savremene notacije, nego zbog odbijanja same pomisli da kvadratna

jednačina može imati negativna rešenja. Jednostavno, Evropa te epohe uopšte ne prihvata negativne brojeve, čak ni nulu, iako se nalazi u pozicionom decimalnom sistemu, ali samo kao simbol za prazno mesto, a ne kao broj.

Stoga se, po ugledu na Al Horezmija, svaka jednačina svodila na uravnoteženi oblik, gde su sa obe strane znaka jednakosti stajali pozitivni brojevi. Takođe, od davnina je bilo poznato da se odgovarajućom smenom kvadratni član može eliminisati iz kubne jednačine, te se svaka kubna jednačina pogodnim smenama mogla svesti na jedan od oblika $x^3 + mx = n$ ili $x^3 = mx + n$, gde su m i n pozitivni brojevi.

Nije poznato da li je Del Fero umeo da reši oba oblika ili, kako neki tvrde, samo prvi koji na italijanskom nosi skoro poetski naziv *cubo et cosa*. Ovakvi nazivi su nastajali jer nije bilo savremene algebarske notacije te su se u opisima postupaka uvodile razne skraćenice, pa je prvi slučaj tretiran kao situacija u kojoj se zbir *stvari* (nepoznate) i *kuba* (iste nepoznate) jednak broju.

Tvrdnja da je umeo da reši samo prvi slučaj proistekla je iz prve upotrebe njegovog, još uvek tajnog metoda. Naime, 1535. na scenu stupa drugi značajan matematičar te epohe koji je samostalno i nezavisno od Del Fera rešio kubnu jednačinu.

To je **Nikolo Fontana Tartalja** (Niccolo Fontana "Tartaglia", rođen 1500. u Bresi, umro 1577. u Veneciji). Tartalja je bio samouk u matematici, ali je učestvujući u brojnim raspravama i takmičenjima ubrzo stekao značajnu reputaciju. Na vrhuncu Tartaljine slave, desetak godina posle Del Ferove smrti, njegov učenik Antonio Marija Fior počeo je da se hvališe da ume da reši kubnu jednačinu. Kako je Tartalja tada bio najpoznatiji duelant, godine 1535. organizovano je takmičenje između njih dvojice u kojem je Tartalja odneo ubedljivu pobedu rešivši sve protivnikove probleme dok je Fior uspeo da reši samo jedan slučaj kubne jednačine. Ostajemo u nedoumici da li je Del Fero znao da reši samo jedan slučaj kubne jednačine ili je pak samo jedan saopštio svom učeniku Fioru. Tartalja je svoj metod takođe držao u tajnosti.

Takmičenje je privuklo pažnju matematičke javnosti Italije, i na scenu stupa **Đirolamo Kardano** (Girolamo Cardano, 1501-1576.). Kardano je bio pravnik, školovani lekar, matematičar, šahista i kockar. Jednom reči, pravi renesansni čovek. U tom trenutku, on je profesor matematike u Milanu i veruje Luki Pačoliju da je kubnu jednačinu nemoguće rešiti. Duel Tartalja - Fior mu privlači pažnju i on pokušava da uspostavi vezu sa Tartaljom ne bi li saznao tajnu tako uspešnog i efikasnog rešavanja svih problema koje mu je Fior zadao. Tartalja isprva odbija komunikaciju, ali se Kardano služi

teškim oružjem i nudi Tartalji da ga upozna sa milanskim vojvodom. Tartalja prihvata ponudu i 1539. dolazi u Milano, gde Kardanu odaje tajnu, ali sa obavezom da je nikada ne objavi. Za uzvrat Kardano mu daje pismo preporuke i otpravlja u Veneciju.

Međutim, godine 1545. Kardano publikuje *Ars magna* (*Velika Veština*), svoje glavno i kapitalno delo iz algebre, u kojem objavljuje - Tartalji se tako čini - Tartaljine formule za rešavanje kubne jednačine. Po Kardanovom mišljenju, zakletva ipak nije bila prekršena. Šta se zapravo dogodilo? Naime, godine 1543. on i njegov najbolji učenik **Lodoviko Ferari** (Lodovico Ferrari, 1522-1565.) putuju u Firencu. Usput svraćaju u Bolonju i upoznaju Hanibala dela Navea. On im je očigledno stavio do znanja da je u posedu tajne rešavanja kubne jednačine, ali nije bio spreman da je otkrije. Da bi ga uverili da i sami znaju tajnu, pokazuju mu da umeju da reše *cosa et cubo* problem, a on im za uzvrat pokazuje Del Ferovu beležnicu sa rešenjem. Zadovoljni što Tartalja nije prvi rešio kubnu jednačinu, Kardano i Ferari se vraćaju u Milano i tri godine kasnije izlazi *Ars Magna*. U knjizi koju su očigledno sačinili zajedno, mada je samo Kardano potpisan kao autor, Kardano i Ferari izlažu danas poznate formule za rešavanje kubne jednačine. Takođe se kao značajan doprinos izlaže i Ferarijev metod za rešavanje jednačine četvrtog stepena, koji je ovaj talentovani Kardanov učenik pronašao još 1540, ali kako metod počiva na svođenju jednačine četvrtog stepena na jednačinu trećeg stepena, on nije mogao biti objavljen a da se ne prekrši zakletva data Tartalji.

Tartalja je objavljivanje *Ars magna* doživeo kao stravičan udarac i počeo žestoke napade na Kardana, koji su bili osuđeni na neuspeh pošto je Kardanova slava tada bila na vrhuncu. Osim toga, veliki naučnik je bio i snalažljiva javna ličnost te je sistematski poturao Ferarija u rasprave sa Tartaljom, koga je to još više iritiralo pošto nije mogao ni da dosegne do rasprave sa svojim arhineprijateljem. Konačno, Tartalja i nije bio u pravu pošto je Del Fero zaista pre njega otkrio metod za rešavanje kubne jednačine, a povrh svega, Kardano je sasvim korektno preneo čitav istorijat u *Ars magna*, odakle i znamo sve ove činjenice.

Sa stanovišta interesa razvoja matematike Kardanovo publikovanje nije ni pod kakvom sumnjom za osudu, već naprotiv. Naučna znanja nisu i ne smeju biti tajna, iako se, razume se, mora voditi računa o autorstvu.

Značaj Kardana i njegove *Ars Magna* tu se ne završava, jer matematički svet je prvi put kroz *Ars Magna* dobio rezultat koji stari Grci nisu znali. Već samo ova okolnost bila bi dovoljna da se Kardanovo delo uvrsti u najvažnija matematička dela od helenizma

do novog doba. Međutim, zahvaljujući značaju i ugledu samog Kardana, delo je imalo veliki publicitet i veoma brzo postalo poznato i čitavoj matematičkoj javnosti. Treba imati na umu da je delo objavljeno u 16. veku kada već postoji štampa, što je dramatično povećalo cirkulaciju svih knjiga pa i onih matematičkih.

Ne treba međutim misliti da je Kardano samo kompilator ili eventualno hrabri promoter novih ideja i rezultata. U njegovom delu se nalaze i originalni rezultati, kako njegovi, tako i njegovog učenika Ferarija.

Osim toga, kao poslednje ali i najvažnije, *Ars Magna* sadrži nešto što bi najtačnije bilo nazvati *predosećanjem kompleksnog broja*. Opet, priča se ponavlja na skoro antički način. Kako Grci nisu mogli da pomire *veličine* i *brojeve*, renesansna Evropa je preuzela isti problem. Ne samo da je trebalo da proteknu vekovi da bi se uveo decimalni pozicioni sistem i prihvatila upotreba nule, nego ni negativni brojevi nisu prihvatani kao legitimni, što jasno pokazuje danas nepotrebni način podele rešavanja jednačine trećeg stepena na dva slučaja.

Nakon opisanog istorijskog toka rešavanja algebarskih jednačina trećeg i četvrtog stepena, logično je da se matematičarima nametnulo i pitanje da li svaka algebarska jednačina ima bar neko rešenje. Još u sedamnaestom veku matematičari su naslutili da svaki polinom u polju $\mathbb{C}$ ima korene, i to baš onoliko njih koliki je njegov stepen, ali u dokazivanju tog tvrđenja imali su malo uspeha. Posle nepuna dva veka, posle niza nepotpunih dokaza od strane raznih matematičara, na scenu stupa **Gaus** i 1815. godine izvodi prvi potpun dokaz ove teoreme.

Svakako, ovo je bio veliki korak u rešavanju algebarskih jedačina, ali je prirodno iskrslo još jedno teško pitanje. Naime, to što znamo da polinom n-tog stepena ima isto toliko rešenja ne govori nam ništa o nekom univerzalnom načinu kojim bismo ta rešenja i odredili. Kako su algoritmi za nalaženje rešenja jednačina trećeg u četvrtog stepena otkriveni, usledili su mnogobrojni pokušaji da se pronađu takvi univerzalni algoritmi i za jednačine petog i višeg stepena. Prvi koji je formulisao tvrđenje koje kaže da takav algoritam ne postoji kada su u pitanju jednačine petog stepena i višeg jeste italijanski fizičar **Paolo Ruffini** (1765-1822) godine 1798. u svojoj knjizi *Teoria generale delle equazioni*. Međutim, Rufinijev dokaz tog tvrđenja nije kompletan. Potpuni dokaz i tačku na ovo pitanje stavio je **Nils Abel** (Niels Henrik Abel, 1802-1829) godine 1826. i nezavisno od njega na slične rezultate naišao je i njegov vršnjak Galoa.

Evarist Galoa (Evariste Galois, 1811-1832.) poznat je po tome što je stvorio *teoriju grupa*. Njegova biografija je kratka i burna.

Kroz nju se prelamaju sva značajna istorijska zbivanja revolucionarne i postrevolucionarne Francuske koja su manje ili više uticala na istoriju čitave Evrope.

Kao doslovno dečak Galoa se zainteresovao za matematiku ali su izveštaji o njegovim školskim rezultatima konfuzni, možda i stoga što je bio politički aktivan te su neki od profesora, monarhisti uglavnom, bili skloni da ga ocene kao lenjog i čak slabo inteligentnog. Uporedo sa školovanjem on šalje rezultate veličinama poput Košija, koji brzo shvataju značaj njegovih pokušaja da dokaže koje se jednačine mogu a koje ne mogu rešiti u radikalima. Iz komunikacije sa Košijem Galoa saznaje da se deo njegovih rezultata poklapa sa radovima norveškog matematičara Nilsa Abela. Stoga odlučuje da nastavi dalje školovanje. Godine 1829, upisuje se na Veliku normalnu školu gde mu profesor postaje niko drugi do sam Furije, još jedna od ključnih osoba oko kojih će se okretati matematika prve polovine 19. veka. Neke od radova koje je u rukopisu poslao Furijeu potonji je razmatrao kao kandidate za veliku nagradu Akademije nauka, ali ga smrt 1830. sprečava da dalje posvećuje pažnju Galoau. U još jednoj u nizu revolucija Galoa biva hapšen, pa oslobođen, u međuvremenu opet ponešto piše i konačno strada u dvoboju, izgleda izazvanom sukobom oko neke žene, što je samo zvanična verzija priče.

Njegov vršnjak Abel je takođe bio iz porodice upletene u značajna zbivanja u periodu kada je Švedska okupirala Norvešku. Njegova interesovanja su šira od Galoaovih. Bavi se magnetizmom, eliptičkim integralima, rešavanjem polinomskih jednačina. Neki od njegovih radova stižu do nemačkog matematičara **Jakobija**. Jakobi uskoro počinje da sarađuje sa Abelom i objavljuju zajedničke radove iz eliptičkih jednačina. Odjek njegovih radova je bio veći nego Galoaovih pošto su imali neposrednu komunikaciju sa Gausom. Abel se ubrzo razboleo i posle nekoliko godina umro. Velika nagrada francuske Akademija nauke za rešavanje jednačina 1830. pripala je Jakobiju i Abelu. Nekoliko godina kasnije nepravda je ispravljena i Galoaov doprinos bio priznat.

Ukupno gledano, Galoau se danas priznaje da je razabrao da se uvođenjem nove strukture, grupe, određena svojstva nula jednačina mogu posmatrati kroz prizmu ove strukture. Abelu se priznaje da je dokazao određena svojstva nula iz kojih sledi da se nesvodljiva jednačina trećeg stepena ne može rešiti u kvadraturama, odnosno da se jednačine petog i višeg stepena ne mogu rešiti u radikalima.

2. Polinomi. Osnovna teorema algebre.

Definicija 2.1. Polinom po promenljivoj x nad prstenom $\mathbb{K}$ je izraz

$$a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{k=0}^{n} a_k x^k,$$

pri čemu je $n \in \mathbb{N}$ i $a_0, a_1, \ldots, a_n \in \mathbb{K}$. Ako je $a_n \neq 0$, broj n se naziva stepenom polinoma $a(x)$ (st $a(x) = n$), sabirak $a_n x^n$ se naziva najstarijim članom tog polinoma, sabirak a_0 slobodnim članom, a koeficijent a_n najstarijim koeficijentom polinoma $a(x)$.

Izuzetno značajan pojam u teoriji polinoma jeste pojam nule ili korena polinoma, tj. one vrednosti promenljive za koju polinom dobija vrednost nula.

Definicija 2.2. Nula (koren) polinoma $a(x)$ je bilo koje rešenje jednačine $a(x) = 0$.

Bezuova teorema Ostatak koji se dobija pri deljenju polinoma $a(x)$ polinomom $x - c$ iznosi $a(c)$.

Ako je α nula polinoma $a(x)$, neposredno po Bezuovoj teoremi sledi da je polinom $a(x)$ deljiv sa $x - \alpha$ jer je $a(\alpha) = 0$. Zapravo, polinom $a(x)$ može se napisati u obliku $a(x) = (x - \alpha)b(x)$, gde je polinom $b(x)$ stepena za jedan manjeg nego $a(x)$. Neposredno je jasno da važi i obratno.

Treba još i znati da je neki broj α nula k-tog reda polinoma $a(x)$, $k \in \mathbb{N}$, ako je

$$(x - \alpha)^k \mid a(x) \quad i \quad (x - \alpha)^{k+1} \nmid a(x).$$

Posebno značajno mesto u istoriji matematike zauzima pitanje da li svaki polinom sa koeficijentima iz prstena $\mathbb{K}$ ima bar jednu nulu u tom prstenu. Lako se zaključuje da ako je $\mathbb{K}$ jedan od prstena $\mathbb{Z}$, $\mathbb{Q}$ ili $\mathbb{R}$, ovakvo tvrđenje ne važi. Dovoljno je uočiti polinom $x^2 + 1$ sa celobrojnim koeficijentima, koji nema korene ni u jednoj od pomenutih struktura. Međutim, u polju kompleksnih brojeva, situacija je drugačija. Dokazuje se da svaki polinom stepena $n \geq 1$ sa koeficijentima iz polja $\mathbb{C}$ ima tačno n korena u polju $\mathbb{C}$ (računajući svaki

koren onoliko puta kolika je njegova višestrukost). Ovo tvrđenje sledi iz naredne teoreme koja je zbog svog značaja svojevremeno nazvana *osnovnom teoremom algebre*.

Teorema 2.1. (Osnovna teorema algebre) Svaki polinom stepena $n \geq 1$ sa koeficijentima iz polja kompleksnih brojeva ima bar jednu nulu u polju $\mathbb{C}$.

Matematičari su još u sedamnaestom veku naslutili da ovakvo tvrđenje važi, ali je prošlo gotovo dvesta godina dok ono nije i dokazano. Najpre se pojavilo više nepotpunih dokaza, a prvim potpunim dokazom smatra se Gausov dokaz iz 1815. godine.

Iz ovog tvrđenja posredno sledi da svaki polinom $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ stepena $n \geq 1$ sa koeficijentima iz polja kompleksnih brojeva ima tačno n korena u tom polju, pri čemu je svaki koren računat onoliko puta kolika je njegova višestrukost. Drugim rečima, taj polinom se može predstaviti u obliku

$$a(x) = a_n(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \cdots (x - \alpha_m)^{k_m},$$

gde su $\alpha_1, \alpha_2, \ldots, \alpha_m$ međusobno različite nule polinoma $a(x)$, dok su $k_1, k_2, \ldots, k_m$ prirodni brojevi takvi da je $k_1 + k_2 + \cdots + k_m = n = \text{st } a(x)$. Ovakvo predstavljanje se zove **kanonska faktorizacija** polinoma $a(x)$.

Međutim, to što svaki polinom n-tog stepena ($n \geq 1$) ima n korena, na znači da se oni mogu i efektivno odrediti. U narednim poglavljima upoznaćemo se sa dokazom osnovne teoreme algebre i algoritmima za rešavanje jednačina trećeg i četvrtog stepena. Zatim će biti prezentiran jedan od mnogih poznatih dokaza osnovne teoreme algebre. Poslednja dva poglavlja posvećena su dokazu Abelove teoreme o nemogućnosti izražavanja rešenja jednačina višeg stepena pomoću radikala.

3. Dokaz osnovne teoreme algebre

Ne postoje čisto algebarski dokazi *osnovne teoreme algebre* koju smo već formulisali. Navešćemo jedan dokaz te teoreme i to onaj koji je u najvećoj meri algebarski. Nealgebarski deo tog dokaza je topološkog karaktera. To su samo dve dobro poznate činjenice iz analize da je polje $\mathbb{R}$ realnih brojeva uređeno polje u kome je svaki pozitivni element kvadrat i u kome svaki polinom $f(x) \in \mathbb{R}[x]$ neparnog stepena ima bar jednu nulu.

Navešćemo najpre bez dokaza dobro poznatu činjenicu o uređenju polja realnih brojeva:

Lema 3.1. Polje $\mathbb{R}$ realnih brojeva je uređeno polje u kome je svaki pozitivni element kvadrat nekog elementa iz $\mathbb{R}$.

Primetimo odmah da je u svakom uređenom polju K svaki kvadrat a^2 $(a \in K)$ obavezno pozitivan. Naime, $a^2 = (-a)^2$, pa kako je $a \geq 0$ ili $-a \geq 0$ mora biti $a^2 = (-a)^2 \geq 0$. Specijalno je u svakom uređenom polju K jedinični element $e > 0$. Otuda je $e + e > 0$, itd. dakle $n \cdot e > 0$ $(n = 1, 2, \ldots)$, pa je *karakteristika uređenog polja K* obavezno jednaka 0.

Iz analize je dobro poznata i sledeća činjenica o polju realnih brojeva.

Lema 3.2. Svaki polinom $f(x) \in \mathbb{R}[x]$ neparnog stepena ima u polju $\mathbb{R}$ realnih brojeva bar jednu nulu.

Interesantno je da su navedene dve osobine polja $\mathbb{R}$ realnih brojeva bitne za ono što želimo da dokažemo. Važi naime sledeća teorema:

Teorema 3.1. Neka je K uređeno polje u kome je svaki pozitivni element kvadrat i u kome svaki polinom $f(x) \in K[x]$ neparnog stepena ima bar jednu nulu. Tada je polje $L = K(i)$ algebarski zatvoreno, pri čemu je i nula polinoma $x^2 + e \in K[x]$.

Pre svega treba prvo pojasniti određene matematičke pojmove. Ako je polje K izomorfno nekom potpolju polja L, onda se kaže da je L *proširenje polja* K. Svako proširenje L polja K može se

shvatiti kao vektorski prostor nad poljem K. Kad je dimenzija tog vektorskog prostora konačna onda se kaže da je L konačno proširenje polja K. Svako konačno proširenje je *algebarsko proširenje* tj. svaki element algebarskog proširenja L polja K je nula nekog polinoma $f(x) \in K[x]$ stepena većeg od nule. I još, za polje K kažemo da je *algebarski zatvoreno* ako nema pravih algebarskih proširenja.

Vratimo se navedenoj teoremi. Za dokaz ove teoreme potrebne su nam sledeće dve leme.

Lema 3.3. Polje L iz prethodne teoreme sadrži nule svakog kvadratnog polinoma $x^2 + \alpha x + \beta \in L[x]$.

Dokaz. Kako smo već konstatovali, polje K, a time i polje L ima karakteristiku $p = 0$. Dokažimo najpre da je svako $a + ib \in L$ kvadrat nekog elementa $x + iy \in L$. Ako je $b = 0$, onda je $a \geq 0$ ili $-a \geq 0$, pa postoji $x \in K$ za koje je $a = x^2$, odnosno $y \in K$ za koje je $-a = y^2$, tj. $a = (iy)^2$. Neka je sada $b \neq 0$. Tada

$$a + ib = (x + iy)^2 \Leftrightarrow x^2 - y^2 = a, 2xy = b.$$

Zbog $b \neq 0$ mora biti $2x \neq 0$. Za ovo je potrebno i dovoljno da bude $x \neq 0$, jer polje K ima karakteristiku 0. No, tada je $y = \frac{b}{2x}$, dakle

$$x^2 - \frac{b^2}{4x^2} = a, \quad tj. \quad (2x^2 - a)^2 = a^2 + b^2.$$

Kako je $a^2 + b^2 > 0$, zbog $b \neq 0$, postoji $c \in K$, $a^2 + b^2 = c^2$, $c > 0$. Uzmimo $x \in K$ tako da važi

$$2x^2 - a = c, \quad tj. \quad x^2 = \frac{a + c}{2e}.$$

Takvo $x \in K$ postoji, jer je zbog $c^2 = a^2 + b^2 > a^2$, $(c-a)(c+a) > 0$, dakle $a + c > 0$, pa kako je $2e > 0$, to je $\frac{a+c}{2e} > 0$.

Osim toga $x \neq 0$, pa postoji $y \in K$, $y = \frac{b}{2x}$. Za tako određene elemente $x, y \in K$ važi $a + ib = (x + iy)^2$.

Ako je $\gamma \in L(\gamma)$ nula kvadratnog polinoma $x^2 + \alpha x + \beta \in L[x]$, tada

$$(\gamma + \frac{\alpha}{2e})^2 + (\beta - \frac{\alpha^2}{4e}) = 0, \quad tj. \quad (\gamma + \frac{\alpha}{2e})^2 = \delta^2$$

za neko $\delta \in L$. Prema tome

$$\gamma = -\frac{\alpha}{2e} \pm \delta \in L.$$

Time je lema dokazana.

Lema 3.4. Polje K iz teoreme 3.1. nema konačnih proširenja M neparnog stepena $(M : K) > 1$.

Dokaz. Pretpostavimo da je M konačno proširenje polja K stepena $(M : K) > 1$. Kako je polje K karakteristike 0, M je separabilno, dakle jednostavno proširenje polja K, $M = K(\alpha)$. Ako je $f(x) \in K[x]$ minimalni polinom elementa α u odnosu na K, tada je

$$deg(f) = (M : K) > 1.$$

Kako je polinom $f(x) \in K[x]$ nerastavljiv, ne može biti $M : K$ neparan broj, jer bi inače polinom $f(x)$ imao u K bar jednu nulu β; kako mu je stepen $deg(f) > 1$ taj polinom ne bi bio nerastavljiv nad K.

Dokažimo još samo ovu lemu.

Lema 3.5. Ako je q prost broj, a polje K ima osobinu da je za svako proširenje M polja K konačnog stepena $(M : K) > 1$, stepen $(M : K)$ deljiv brojem q, tada je $(M : K) = q^m$ za neki prirodan broj m.

Dokaz. Ako je q karakteristika polja K, onda je M čisto inseparabilno proširenje međupolja M_s, dakle $(M : M_s) = q^{m'}$ za neki nenegativni ceo broj m'. Ako je $M_s = K$, onda možemo uzeti da je $m = m'$. Inače, treba dokazati da je $(M_s : K) = q^{m''}$ za neki prirodan broj m''.

Ako q nije karakteristika polja K, tad polje K iz ove leme mora biti savršeno. Inače bi za neko $a \in K$ polinom $x^p - a \in K[x]$ bio nerastavljiv nad K, pri čemu je $p \neq 0$ karakteristika polja K, pa bi za neku nulu α tog polinoma važilo $(K(\alpha) : K) = p > 1$, a ipak $(K(\alpha) : K)$ nije deljivo prostim brojem $q \neq p$.

Tako je ostao samo slučaj kada je M separabilno proširenje polja K. Možemo uzeti da je M normalno proširenje polja K, jer inače umesto M treba uzeti normalno zatvorenje polja M u odnosu na K. Ako to zatvorenje označimo sa M' i dokažemo da je $(M' : K) = q^{m'}$ za neki prirodan broj m', onda će zbog $(M' : K) = (M' : M) \cdot (M : K)$ važiti $(M : K) = q^m$ za neki prirodan broj m. Neka je, dakle, M konačno normalno i separabilno proširenje polja K stepena $(M : K) > 1$. Kada ne bi važilo $(M : K) = q^m$ za neki prirodan broj m, tada bi Silovska q-podgrupa H grupe $G = Gal(M/K)$ imala indeks $(G : H) > 1$ koji nije deljiv brojem q. Toj podgrupi odgovara u smislu osnovne teoreme teorije Galoa neko međupolje M_H stepena $(M_H : K) = (G : H) > 1$, za koje bi važilo $q \nmid (M_H : K)$, što je

nemoguće. Time je lema dokazana.

Sada možemo preći na dokaz teoreme 3.1.

Treba dokazati da za svako konačno proširenje M polja $L = K(i)$ važi $M = L$. Neka je M konačno proširenje polja L. Tada je L konačno proširenje i polja K. Kako polje K iz teoreme 3.1. ima karakteristiku $p = 0$, M je konačno i separabilno proširenje polja K. Možemo uzeti da je to proširenje još i normalno, jer inače umesto M treba uzeti normalno zatvorenje polja M u odnosu na K. Neka je, dakle, M konačno, normalno i separabilno proširenje polja K i osim toga $L \subseteq M$. Prema lemi 3.4. i lemi 3.5. mora važiti $(M : K) = 2^m$, za neki prirodan broj m. Kako je $(L : K) = 2$, jer zbog $i^2 = -e < 0$ uređeno polje K ne može sadržati element i, dovoljno je dokazati da je $m = 1$. U suprotnom, grupa $G = Gal(M/K)$ imala bi red $(G : id_M) = 2^m, m > 1$, pa bi kao takva bila rešiva i imala bi kompozicioni niz

$$G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_{m-1} \supset H_m = id_M$$

dužine $m > 1$. Faktori tog niza su cikličke grupe reda 2. Kako je $M \supseteq L$, možemo uzeti da je $L = M_{H_1}$, jer je L normalno proširenje polja K, pa mu pripada normalna podgrupa H grupe G indeksa $(G : H) = (L : K) = 2$. Ako normalni niz

$$G \supset H \supset id_M$$

produžimo do kompozicionog niza možemo uzeti da je to upravo gornji kompozicioni niz. Ako podgrupi H_2 odgovara međupolje M_2, tada je $(M_2 : L) = (H_1 : H_2) = 2$, pa bi i M_2 bilo kvadratno proširenje polja K. To je međutim, na osnovu leme 3.3. nemoguće, jer bi u suprotnom važilo $M_2 = L(\gamma)$ za neku nulu γ nekog nesvodljivog kvadratnog polinoma $x^2+\alpha x+\beta \in L[x]$. Prema tome, $m = 1$, tj. $M = L$.

Time je teorema 3.1. dokazana.

Polje $K = \mathbb{R}$ ispunjava na osnovu leme 3.1. i leme 3.2. uslove teoreme 3.1. Osim toga, za polje $\mathbb{C}$ kompleksnih brojeva važi $\mathbb{C} = \mathbb{R}(i)$, pri čemu je i imaginarna jedinica, tj. nula polinoma $x^2 + 1 \in \mathbb{R}[x]$. Zato iz teoreme 3.1. sledi

Teorema 3.2. Polje $\mathbb{C}$ kompleksnih brojeva je algebarski zatvoreno polje.

Tvrđenje poslednje teoreme predstavlja jedan od ekvivalentnih iskaza *osnovne teoreme algebre*.

4. Algebarske jednačine trećeg stepena

Ukratko ćemo prikazati postupak rešavanja jednačine trećeg stepena tj. *kubne jednačine*.

Proizvoljna algebarska jednačina trećeg stepena

$$a_3x^3+a_2x^2+a_1x+a_0=0, \qquad a_3,a_2,a_1,a_0\in\mathbb{R}, a_3\neq 0 \tag{4.1}$$

ekvivalentna je jednačini

$$x^3+ax^2+bx+c=0, \tag{4.2}$$

$a=\frac{a_2}{a_3}$, $b=\frac{a_1}{a_3}$, $c=\frac{a_0}{a_3}$, pa ćemo u daljem rešavati jednačinu (4.2).

Uvedimo novu nepoznatu y zamenom

$$y=x+\frac{a}{3}.$$

Jednačina postaje $y^3+(b-\frac{a^2}{3})y+\frac{2a^3}{27}-\frac{ab}{3}+c=0$, odnosno

$$y^3+py+q=0, \tag{4.3}$$

gde je $p=b-\frac{a^2}{3}$, $q=\frac{2a^3}{27}-\frac{ab}{3}+c$.

Pretpostavimo da je

$$y=u+v, \tag{4.4}$$

gde su u i v nove nepoznate. Ove dve nepoznate treba da zadovolje jednu jednačinu (4.3), pa možemo nametnuti još jedan uslov, koji ćemo podesno izabrati. Zamenom u jednačinu nalazimo

$$(u+v)^3+p(u+v)+q=0,$$

odnosno $u^3+v^3+3uv(u+v)+p(u+v)+q=0$, tj.

$$u^3+v^3+(3uv+p)(u+v)+q=0. \tag{4.5}$$

Sada zahtevamo da bude

$$3uv+p=0. \tag{4.6}$$

Time jednačina (4.5) postaje

$$u^3 + v^3 + q = 0. \tag{4.7}$$

Dakle, u i v zadovoljavaju

$$u^3 v^3 = -\frac{p^3}{27}, \quad u^3 + v^3 = -q,$$

pa kubovi u^3 i v^3 nepoznatih u i v, prema Vietovim formulama, predstavljaju rešenja kvadratne jednačine

$$z^2 - (u^3 + v^3)z + u^3 v^3 = 0,$$

odnosno

$$z^2 + qz - \tfrac{p^3}{27} = 0. \tag{4.8}$$

Rešenja jednačine (4.8) su

$$z_1 = u^3 = \frac{-q + \sqrt{q^2 + 4\frac{p^3}{27}}}{2} = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

$$z_2 = v^3 = \frac{-q - \sqrt{q^2 + 4\frac{p^3}{27}}}{2} = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Odatle, nalaženjem brojeva (realnih ili kompleksnih) čiji su kubovi jednaki nađenim brojevima, dobijamo

$$y = \sqrt[3]{-\tfrac{q}{2} + \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}}} + \sqrt[3]{-\tfrac{q}{2} - \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}}}, \tag{4.9}$$

gde smo radi jednostavnosti i preglednosti zapisa, upotrebili simbol $\sqrt[3]{}$ da označimo bilo koji od tri (kompleksna) broja, čiji je kub jednak vrednosti izraza pod korenom.

Na taj način nalazimo devet mogućnosti za y. Kako je jednačina (4.3) trećeg stepena, ona mora imati tri rešenja, što znači da od pomenutih devet vrednosti za y treba izabrati tri. Više od toga, znamo da jednačina trećeg stepena sa realnim koeficijentima ima bar jedno realno rešenje. Ako nisu sva rešenja realna, onda ima i jedan par konjugovano kompleksnih rešenja.

Ovde nećemo detaljno obrazlagati na koji način se od pomenutih devet mogučnosti biraju tri. Recimo samo da praktično postupamo na sledeći način. Nađemo po jednu od tri vrednosti $u = \alpha$, $v = \beta$,

takve da zadovolje uslov (4.6): $uv = -\frac{p}{3}$ i izaberemo $\omega = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$ (to je jedan od trećih korena jedinice; ostali su kao što znamo, ω^2 i $\omega^3 = 1$). Onda su rešenja jednačine (4.3)

$$y_1 = \alpha + \beta, \quad y_2 = \omega\alpha + \omega^2\beta, \quad y_3 = \omega^2\alpha + \omega\beta,$$

a rešenja polazne jednačine (4.2):

$$x_1 = \alpha + \beta - \frac{a}{3}, \quad x_2 = \omega\alpha + \omega^2\beta - \frac{a}{3}, \quad x_3 = \omega^2\alpha + \omega\beta - \frac{a}{3}.$$

Formula (4.9) poznata je kao **Kardanova formula**.

Primer. 4.1. Rešiti jednačinu

$$x^3 - 3x^2 + 9x - 5 = 0.$$

Rešenje. Zbog $a = -3$, zamenjujemo $x = y + 1$. Dobija se

$$(y+1)^3 - 3(y+1)^2 + 9(y+1) - 5 = 0,$$

$$y^3 + 3y^2 + 3y + 1 - 3y^2 - 6y - 3 + 9y + 9 - 5 = 0,$$

$$y^3 + 6y + 2 = 0, \quad p = 6, \quad q = 2.$$

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = -1 + \sqrt{1+8} = 2,$$

$$v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = -4.$$

Za realne brojeve $\sqrt[3]{2}$ i $-\sqrt[3]{4}$ važi $\sqrt[3]{2}\cdot(-\sqrt[3]{4}) = -\sqrt[3]{8} = -2 = -\frac{p}{3}$, pa možemo uzeti $\alpha = \sqrt[3]{2}$, $\beta = -\sqrt[3]{4}$. Stoga je

$$y_1 = \sqrt[3]{2} - \sqrt[3]{4};$$

$$y_2 = \sqrt[3]{2}(-\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}) - \sqrt[3]{4}(-\tfrac{1}{2} - i\tfrac{\sqrt{3}}{2});$$

$$y_3 = \sqrt[3]{2}(-\tfrac{1}{2} - i\tfrac{\sqrt{3}}{2}) - \sqrt[3]{4}(-\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}).$$

Ovde je y_1 realno rešenje, a y_2 i y_3 predstavljaju par konjugovano kompleksnih rešenja. Dalje nalazimo

$$x_1 = y_1 + 1, \quad x_2 = y_2 + 1, \quad x_3 = y_3 + 1.$$

Kardanova formula je relativno složena i, u praksi, koristimo se njome nakon što se uverimo da drugačije ne umemo. Prethodni

primer predstavlja ilustraciju takve situacije.

Primer. 4.2. Rešiti jednačinu

$$x^3 + 3x - 4 = 0.$$

Rešenje. Vidimo da jednačina ima realno rešenje $x_1 = 1$ (proveravanjem delilaca slobodnog člana). Stoga je ona ekvivalentna sa

$$(x-1)(x^2 + mx + n) = 0,$$

odnosno, nakon deljenja,

$$(x-1)(x^2 + x + 4) = 0,$$

i rešenja su

$$x_1 = 1, \quad x_2 = \frac{-1 + i\sqrt{15}}{2}, \quad x_3 = \frac{-1 - i\sqrt{15}}{2}.$$

Da smo prevideli ovu činjenicu, Kardanova formula dala bi nam

$$x = \sqrt[3]{2 + \sqrt{5}} + \sqrt[3]{2 - \sqrt{5}},$$

odakle se ne nazire rešenje $x_1 = 1$. Ipak, zbog

$$(\frac{1}{2}(1 + \sqrt{5}))^3 = \frac{1}{8}(1 + 3\sqrt{5} + 15 + 5\sqrt{5}) = 2 + \sqrt{5},$$

$$(\frac{1}{2}(1 - \sqrt{5}))^3 = \frac{1}{8}(1 - 3\sqrt{5} + 15 - 5\sqrt{5}) = 2 - \sqrt{5},$$

možemo uzeti da je $x_1 = \frac{1}{2}(1 + \sqrt{5}) + \frac{1}{2}(1 - \sqrt{5}) = 1$, a dalje treba slediti opisani postupak.

5. Algebarske jednačine četvrtog stepena

Proizvoljna algebarska jednačina četvrtog stepena

$$a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0, \quad a_4, a_3, a_2, a_1, a_0 \in \mathbb{R}, a_4 \neq 0 \tag{5.0}$$

ekvivalentna je jednačini

$$x^4 + ax^3 + bx^2 + cx + d = 0, \tag{5.1}$$

i njena rešenja x_1, x_2, x_3, x_4 mogu biti predstavljena u obliku

$$\begin{aligned} x_1 &= \alpha + \beta + \gamma + \delta, \\ x_2 &= \alpha + \beta - \gamma - \delta, \\ x_3 &= \alpha - \beta + \gamma - \delta, \\ x_4 &= \alpha - \beta - \gamma + \delta, \end{aligned}$$

gde su α, β, γ, δ kompleksni brojevi. Tada imamo da je:

$$\begin{gathered} 4\alpha = -a, \\ 6\alpha^2 - 2(\beta^2 + \gamma^2 + \delta^2) = b \\ 4\alpha^3 - 4\alpha(\beta^2 + \gamma^2 + \delta^2) + 8\beta\gamma\delta = -c \\ \alpha^4 + (\beta^2 + \gamma^2 + \delta^2)^2 - 2\alpha^2(\beta^2 + \gamma^2 + \delta^2) \\ -4(\beta^2\gamma^2 + \beta^2\delta^2 + \gamma^2\delta^2) + 8\alpha\beta\gamma\delta = d. \end{gathered} \tag{5.2}$$

Iz jednakosti (5.2) dobijamo

$$4^2(\beta^2 + \gamma^2 + \delta^2), \qquad 4^4(\beta^2\gamma^2 + \beta^2\delta^2 + \gamma^2\delta^2), \qquad 4^6\beta^2\gamma^2\delta^2$$

koji predstavljaju koeficijente kubne jednačine (5.3) ispod, čija su tri rešenja $(4\beta)^2$, $(4\gamma)^2$, $(4\delta)^2$.

$$\begin{gathered} (16v^2)^3 - (3a^2 - 8b)(16v^2)^2 \\ + (3a^4 - 16ba^2 + 16ca + 16b^2 - 64d)(16v^2) \\ -(a^3 - 4ba + 8c)^2 = 0. \end{gathered} \tag{5.3}$$

Zato, jednačine (5.2) određuju vrednost za α, $\alpha = -\frac{a}{4}$ i impliciraju kubnu jednačinu (5.3), po β^2, γ^2, δ^2.

Ako označimo

$$P = a^3 - 4ba + 8c$$

$$Q = 12d + b^2 - 3ca$$

$$R = 27da^2 - 9cba + 2b^3 - 72db + 27c^2$$

i

$$\alpha_0 = a^2 - \frac{8}{3}b$$

$$\beta_0 = \frac{4}{3}\sqrt[3]{\frac{R + \sqrt{R^2 - 4Q^3}}{2}},$$

$$\gamma_0 = \frac{4}{3}\sqrt[3]{\frac{R - \sqrt{R^2 - 4Q^3}}{2}},$$

onda je

$$\alpha = -\frac{a}{4}$$

$$\beta = \frac{1}{4}\sqrt{\alpha_0 + \beta_0 + \gamma_0},$$

$$\gamma = \frac{1}{4}\sqrt{\alpha_0 + q_1\beta_0 + q_2\gamma_0},$$

$$\delta = \frac{1}{4}\sqrt{\alpha_0 + q_2\beta_0 + q_1\gamma_0},$$

gde su q_1 i q_2 dva kompleksna kubna korena jedinice, čije su uloge međusobno zamenljive.

Bilo koji izbor grana za kubne korene za koje je

$$\beta_0\gamma_0 = \frac{16Q}{9}$$

dozvoljen je, i slično, svaki izbor znakova za kvadratne korene kod kojih je

$$\beta\gamma\delta = -\frac{P}{64}$$

takođe je dozvoljen. Ova restrikcija za izbor znakova β, γ, δ sledi iz prve tri jednakosti u (5.2).

Dokazano je da važi sledeća teorema:

Teorema 5.1. Neka je

$$x^4 + ax^3 + bx^2 + cx + d = 0 \tag{5.1}$$

realna jednačina četvrtog stepena i neka su

$$Q = 12d + b^2 - 3ca$$

$$R = 27da^2 - 9cba + 2b^3 - 72db + 27c^2$$

i

$$T = 3a^2 - 8b + 8Re(\sqrt[3]{\frac{R + \sqrt{R^2 - 4Q^3}}{2}}). \tag{5.4}$$

Tada važi:
1) ako je $R^2 - 4Q^3 > 0$ onda su tačno dva rešenja jednačine (5.1) realna;
2) ako je $R^2 - 4Q^3 = 0$ onda su dva rešenja jednačine (5.1) realna, dok su preostala dva realna *ako i samo ako* je $T \geq 0$ za sva tri moguća kubna korena u (5.4);
3) ako je $R^2 - 4Q^3 < 0$ onda

(a) sva četiri rešenja jednačine (5.1) su realna *ako i samo ako* je $T \geq 0$ za sva tri moguća kubna korena u (5.4);

(b) sva četiri rešenja jednačine (5.1) su kompleksna *ako i samo ako* je $T < 0$ za najmanje jedan od tri moguća kubna korena u (5.4).

Teorema 5.2. Jednačina četvrtog stepena (5.1) ima dva jednaka korena *ako i samo ako* je

$$R^2 - 4Q^3 = 0,$$

a ima tri jednaka korena *ako i samo ako* je

$$R = Q = 0,$$

gde su

$$R = 27da^2 - 9cba + 2b^3 - 72db + 27c^2$$

$$Q = 12d + b^2 - 3ca$$

Teorema 5.3.
1) Jednačina četvrtog stepena (5.1) ima dva para jednakih rešenja *ako i samo ako* je

$$R^2 - 4Q^3 = 0 \qquad i \qquad 32R = 27\alpha_0^3.$$

2) Jednačina četvrtog stepena (5.1) ima četiri jednaka rešenja *ako i samo ako* je

$$R = Q = \alpha_0 = 0.$$

6. Šturmov problem broja realnih korena

Naći broj realnih korena algebarske jednačine sa realnim koeeficijentima u datom intervalu.

Ovaj veoma važan algebarski problem, na iznenađujuće jednostavan način, rešio je 1829. francuski matematičar Charles Sturm (1803-1855). Rad koji sadrži poznatu Šturmovu teoremu pojavljuje se u jedanaestom tomu dela *Bulletin des sciences Férrusac* i nosi naslov *Mémoire sur la résolution des équations numériques.*

Ovim ogromnim otkrićem, kaže Liuvil, *Šturm je jednim potezom pojednostavio i usavršio elemente algebre, povezujući ih sa novim rezultatima.*

Rešenje. Razlikujemo dva slučaja:

I. Kada su svi realni koreni polazne jednačine na datom intervalu jednostruki.

II. Kada polazna jednačina na datom intervalu ima višestruke korene.

Prvo ćemo pokazati da se drugi slučaj može svesti na prvi.

Neka polazna jednačina $F(x) = 0$ ima međusobno različite korene α, β, γ,..., sa višestrukostima a, b, c,..., respektivno, tako da je

$$F(x) = (x-\alpha)^a(x-\beta)^b(x-\gamma)^c\cdots$$

Za izvodnu funkciju $F'(x)$ posmatramo količnik

$$\frac{F'(x)}{F(x)} = \frac{a}{x-\alpha} + \frac{b}{x-\beta} + \frac{c}{x-\gamma} + \cdots$$

$$= \frac{a(x-\beta)(x-\gamma)(x-\delta)\cdots + b(x-\alpha)(x-\gamma)(x-\delta)\cdots + \cdots}{(x-\alpha)(x-\beta)(x-\gamma)\cdots}$$

Ako označimo brojilac ovog razlomka sa $p(x)$ i imenilac sa $q(x)$, i celu racionalnu funkciju $F(x)/q(x)$ izjednačimo sa $G(x)$, biće

$$F(x) = G(x)\cdot q(x) \qquad \text{i} \qquad F'(x) = G(x)\cdot p(x).$$

Sada, funkcije $p(x)$ i $q(x)$ nemaju zajedničkih delilaca. Iz ovoga sledi

da je $G(x)$ najveći zajednički delilac za $F(x)$ i $F'(x)$. On se lako može odrediti Euklidovim algoritmom, te se stoga može smatrati poznatim, a na isti način i $q(x)$ se može smatrati poznatim.

Jednačina $F(x) = 0$ onda se grana u dve jednačine

$$q(x) = 0 \quad \text{i} \quad G(x) = 0$$

od kojih prva ima samo jednostruka rešenja, dok se druga može svesti na isti način kao i $F(x) = 0$.

Jednačina sa višestrukim rešenjima zato može uvek biti svedena na jednačinu (sa poznatim koeficijentima) koja ima samo jednostruka rešenja.

Iz toga sledi da je nepotrebno rešavati ovaj problem u drugom slučaju jer se on svodi na prvi.

Neka je $f(x) = 0$ algebarska jednačina čija su sva rešenja jednostruka. Tada se izvodna funkcija $f'(x)$ ne anulira ni za jedan od ovih korena, te je najveći zajednički delilac za funkcije $f(x)$ i $f'(x)$ neka konstanta K različita od nule. Koristimo Euklidov algoritam da odredimo najveći zajednički delilac za $f(x)$ i $f'(x)$, obeležavajući ih, radi jednostavnosti, sa $f_0(x)$ i $f_1(x)$ umesto $f(x)$ i $f'(x)$, i označavajući količnike nastale iz deljenja sa ostatkom sa $q_0(x)$, $q_1(x)$, $q_2(x)$, ... i ostatke sa $-f_2(x)$, $-f_3(x)$, ...

Ako takođe zanemarimo znak argumenta radi kratkoće zapisivanja, imaćemo naredni algoritam:

$$(0) \qquad f_0 = q_0 f_1 - f_2$$

$$(1) \qquad f_1 = q_1 f_2 - f_3$$

$$(2) \qquad f_2 = q_2 f_3 - f_4, \qquad \text{itd.}$$

U ovom algoritmu, pri poslednjem koraku, sa pojavom ostatka K, ostatak $-f_s(x)$ koji nije nula u bilo kojoj tački intervala poseduje isti znak na celom intervalu. Ovde prekidamo algoritam. Funkcije koje se u njemu pojavljuju

$$f_0, f_1, f_2, \ldots, f_s$$

obrazuju *Šturmov lanac* i u ovom kontekstu nazivaju se *Šturmovim funkcijama.*

Šturmove funkcije imaju sledeće tri osobine:

1. Dve susedne funkcije nisu istovremeno nula u nekoj tački intervala.

2. U nula-tački Šturmove funkcije dve susedne funkcije su različitog znaka.

3. U dovoljno maloj okolini nula-tačke za $f_0(x)$, $f_1(x)$ je svuda veća od nule, ili je svuda manja od nule.

Dokaz za 1. Ako su, na primer, f_2 i f_3 nula u bilo kojoj tački intervala, f_4 [prema (2)] takođe je nula u ovoj tački, i sledujući tome, f_5 takođe [prema (3)], i tako dalje, tako da konačno [prema poslednjem redu algoritma] i f_5 je takođe nula, što je inače suprotno našoj pretpostavci.

Dokaz za 2. Ako je na primer funkcija f_3 nula u tački intervala σ, onda iz (2) sledi da je

$$f_2(\sigma) = -f_4(\sigma).$$

Dokaz za 3. Ovaj dokaz sledi iz poznate teoreme: *Funkcija* $[f_0(x)]$ *raste ili opada u nekoj tački u zavisnosti od toga da li je njena izvodna funkcija* $[f_1(x)]$ *veća ili manja od nule u toj tački.*

Sada biramo proizvoljnu tačku x iz intervala, posmatrajući znakove vrednosti $f_0(x)$, $f_1(x)$, ..., $f_s(x)$, i dobijamo *Šturmov znakovni lanac* (da bi se dobio pouzdan znak, mora biti pretpostavljeno da nijedna od označenih $s+1$ funkcija nije nula). Znakovni lanac sadržaće znakovne sekvence ($++$ i $--$) ili znakovne promene ($+-$ i $-+$).

Posmatraćemo broj $Z(x)$ znakovnih promena u znakovnom lancu i promene kojima se $Z(x)$ podvrgava kada x prolazi kroz interval. Promena može da se javi jedino ako jedna ili više Šturmovih funkcija menja znak, npr. prelazi iz negativnih (pozitivnih) vrednosti kroz nulu do pozitivnih (negativnih) vrednosti. Mi ćemo prema tome posmatrati promene na $Z(x)$ koje nastaju pri prolasku funkcije $f_v(x)$ kroz nulu.

Neka je k tačka u kojoj je f_v nula, h tačka sa leve strane njoj, i l tačka sa desne strane, i to tako blizu k da na intervalu (h, l) važe sledeća tvrđenja:

(1) $f_v(x)$ nije nula izuzev u $x = k$;

(2) za f_v susedne funkcije (f_{v+1}, f_{v-1}) ne menjaju znak.

Moramo praviti razliku između slučajeva $v > 0$ i $v = 0$; u prvom slučaju posmatramo trojku f_{v-1}, f_v, f_{v+1}, dok u drugom posmatramo par f_0, f_1.

U slučaju trojke, f_{v-1} i f_{v+1} su redom znakova $+$ i $-$, ili znakova $-$ i $+$, u sve tri tačke h, k, l. Bez obzira na to koji znak f_v može imati u ovim tačkama, trojka će imati jednu promenu znaka za svaki

od argumenata h, k, l. Prolazak funkcije f_v kroz nulu ne utiče na broj znakovnih promena u lancu.

U slučaju para, f_1 ima ili znak + ili znak − u sve tri tačke h, k, l. U prvom slučaju, f_0 je rastuća i stoga negativna u h i pozitivna u l. U drugom slučaju, f_0 je opadajuća i stoga pozitivna u tački h i negativna u l. U oba slučaja izgubljena je znakovna promena.

Iz našeg istraživanja zaključujemo da: Šturmov znakovni lanac podvrgava se promeni broja znakovnih promena $Z(x)$ samo kada x prolazi kroz nula-tačku za $f(x)$; i posebno, lanac tada gubi (sa rastućim x) tačno jednu promenu znaka. Prema tome, ako x prolazi kroz interval (čiji krajevi ne predstavljaju rešenja za $f(x) = 0$) sleva nadesno, znakovni lanac gubi tačno onoliko znakovnih promena koliko je nula funkcije $f(x)$ u intervalu. Rezultat toga je:

Šturmova teorema: *Broj realnih rešenja algebarske jednačine sa realnim koeficijentima čija su realna rešenja jednostruka na nekom intervalu čije krajnje tačke ne predstavljaju rešenja te jednačine, jednak je razlici brojeva znakovnih promena u Šturmovom znakovnom lancu na krajevima intervala.*

Napomena: Isto tvrđenje može se odnositi isto tako na lanac koji se dobija kada pomnožimo f_0, f_1, f_2, $\ldots$, f_s bilo kojom pozitivnom konstantom; ovaj lanac je onda isto tako označen kao Šturmov lanac. U formiranju Šturmovog funkcionalnog lanca svi razlomci za koeficijente ovim postupkom su izbegnuti.

Primer 6.1. Odrediti broj realnih rešenja jednačine $x^5 - 3x - 1 = 0$, i intervale kojima pripadaju.

Za Šturmov lanac dobijamo funkcije:

$$f_0 = x^5 - 3x - 1, \qquad f_1 = 5x^4 - 3, \qquad f_2 = 12x + 5, \qquad f_3 = 1.$$

Znakovi funkcija u tačkama -2, -1, 0, $+1$, $+2$ su sledeći:

x	f_0	f_1	f_2	f_3
-2	$-$	$+$	$-$	$+$
-1	$+$	$+$	$-$	$+$
0	$-$	$-$	$+$	$+$

$$+1 \qquad - \qquad + \qquad + \qquad +$$

$$+2 \qquad + \qquad + \qquad + \qquad +$$

Jednačina prema tome ima tri realna rešenja: jedno između -2 i -1, jedno između -1 i 0, i jedno između $+1$ i $+2$. Preostala dva rešenja su kompleksna.

Primer 6.2. Odrediti broj realnih rešenja jednačine $x^5 - ax - b = 0$ kada su a i b pozitivni parametri i $4^4a^5 > 5^5b^4$.

Šturmov lanac glasi:

$$x^5 - ax - b, \qquad 5x^4 - a, \qquad 4ax + 5b, \qquad 4^4a^5 - 5^5b^4.$$

Ako za x uzmemo vrednosti $-\infty$ i $+\infty$, on će imati znakove

$$- + - + \qquad \text{i} \qquad + + + +$$

poštujući redosled.

Dakle, jednačina ima tri realna i dva kompleksna rešenja.

7. Abelova teorema

Algebarske jednačine stepena većeg od petog u opštem slučaju algebarski su nerešive.

Ovu slavnu teoremu prvi je formulisao italijanski fizičar Paolo Ruffini (1765-1822) u svojoj knjizi *Teoria generale delle equazioni*, objavljenoj u Bolonji 1798. Rufinijev dokaz je međutim nepotpun. Prvi strogi dokaz ove teoreme izveo je 1826. mladi norveški matematičar Niels Henrik Abel (1802-1829) u svom radu objavljenom u prvom tomu časopisa *Crelle's Journal für Mathematik*. Njegov proslavljeni rad nosio je naslov *Démonstration de l'impossibilité de la résolution algébraique des équatios générales qui dépassent le quatrième degré*.

Dokaz ove Abelove teoreme koji sledi baziran je na Kronekerovoj teoremi, publikovanoj 1856. godine u časopisu *Monatsberichte der Berliner Akademie*.

Počećemo tako što ćemo u kratkom uvodu predstaviti osnovne algebarske pojmove i teoreme neophodne za razumevanje Kronekerovog dokaza.

Sistem brojeva $\mathfrak{K}$ naziva se *poljem* kada sabiranje, oduzimanje, množenje i deljenje dva broja iz sistema daju takođe broj iz sistema, izuzev, naravno, što deljenje nulom nije definisano. Radi jednostavnosti, brojeve sistema nazivaćemo $\mathfrak{K}$-brojevima. Najjednostavnije polje je ono sastavljeno od svih racionalnih brojeva i to je *polje* $\mathfrak{R}$ *racionalnih brojeva* ili *prirodno racionalno polje*.

Proširenje $\mathfrak{R}' = \mathfrak{R}(\alpha, \beta, \gamma, \ldots)$ polja $\mathfrak{R}$ formirano dodavanjem elemenata α, β, γ, ... i korišćenjem jedne ili više operacija od četiri date, predstavlja, ustvari, skup svih racionalnih funkcija od α, β, γ, ... čiji su koeficijenti $\mathfrak{K}$-brojevi.

Funkcija $f(x)$ *ili jednačina* $f(x) = 0$ *u polju* jeste funkcija ili jednačina čiji su koeficijenti brojevi iz polja. U tom smislu, pod polinomom u $\mathfrak{R}$ podrazumeva se racionalna funkcija promenljive x čiji su koeficijenti $\mathfrak{R}$-brojevi.

Za polinom

$$F(x) = Ax^n + Bx^{n-1} + \cdots$$

ili jednačinu

$$F(x) = 0$$

u polju $\mathfrak{K}$ kažemo da je svodljiva ili nesvodljiva u ovom polju u zavisnosti od toga da li je $F(x)$ rastavljiv na proizvod polinoma manjeg stepena u $\mathfrak{K}$ ili ne.

Na primer, funkcija $x^2 - 10x + 7$ je nerastavljiva u polju $\mathfrak{R}$, dok je rastavljiva u polju $\mathfrak{R}(\sqrt{2})$:

$$x^2 - 10x + 7 = (x - 5 - 3\sqrt{2})(x - 5 + 3\sqrt{2}).$$

Abelova lema: *Stepena jednačina*

$$x^p = C$$

čiji je stepen p prost broj nesvodljiva je u polju $\mathfrak{K}$ kada je C broj iz polja, ali ne predstavlja p-ti stepen nekog broja iz polja.

Indirektan dokaz. Pretpostavimo da je $x^p - C = 0$ svodljiva, tako da je

$$x^p - C = \psi(x)\varphi(x),$$

gde su ψ i φ polinomi iz $\mathfrak{K}$, čiji su slobodni članovi A i B $\mathfrak{K}$-brojevi. Kako su rešenja jednačine

$$x^p = C$$

r, $r\varepsilon$, $r\varepsilon^2$, …, $r\varepsilon^{p-1}$, gde je r jedno od rešenja, a ε p-ti kompleksni koren jedinice, i slobodni član jednačine $\psi(x) = 0$ ili $\varphi(x) = 0$, u zavisnosti od znaka, predstavlja proizvod rešenja jednačine, na primer

$$A = r^\mu \varepsilon^M, \qquad B = r^\nu \varepsilon^N.$$

Kako μ i ν nemaju zajedničkih delilaca (jer je $\mu + \nu = p$), onda postoje brojevi h i k takvi da je

$$\mu h + \nu k = 1.$$

Prema tome, za proizvod K stepena A^h i B^k dobijamo vrednost $r\varepsilon^{hM+kN}$, i sledstveno tome, vrednost p-tog stepena $\mathfrak{K}$-broja K je $K^p = r^p = C$. Pretpostavljeno je međutim da C ne sme biti p-ti stepen nekog $\mathfrak{K}$-broja. Prema tome, $x^p = C$ ne može biti svodljiva.

Šonemanova teorema (Crelle's journal, tom XXXII, 1846.): *Ako su celobrojni koeficijenti C_0, C_1, C_2, …, C_{N-1} polinoma*

$$f(x) = C_0 + C_1 x + C_2 x^2 + \cdots + C_{N-1} x^{N-1} + x^N$$

deljivi prostim brojem p, pri čemu slobodni član C_0 nije deljiv sa p^2, onda polinom $f(x)$ nije rastavljiv u polju racionalnih brojeva.

INDIREKTAN DOKAZ. Pretpostavimo da je f rastavljiv polinom takav da je $f = \psi \cdot \varphi$, gde je

$$\psi = a_0 + a_1 x + a_2 x^2 + \cdots + a_{m-1} x^{m-1} + x^m,$$

$$\varphi = b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1} x^{n-1} + x^n.$$

Na ovom mestu neophodno nam je da iskoristimo Gausovu teoremu koja glasi:

GAUSOVA TEOREMA: *Ako je polinom* $f = x^N + C_1 x^{N-1} + C_2 x^{N-2} + \cdots + C_N$ *sa celobrojnim koeficijentima rastavljiv na proizvod dva polinoma* $\psi = x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m$ *i* $\varphi = x^n + \beta_1 x^{n-1} + \cdots + \beta_n$ *sa racionalnim koeficijentima* ($f = \psi\varphi$), *onda su koeficijenti ovih polinoma takođe celobrojni.*

Dokaz: Dovodimo α_ν i β_ν na njihove najveće zajedničke imenioce a_0 i b_0, respektivno, tako da je $\alpha_\nu = a_\nu/a_0$ i $\beta_\nu = b_\nu/b_0$, i brojevi a_0, a_1, a_2, …, a_m, kao i brojevi b_0, b_1, b_2, …, b_n, nemaju zajedničkih delilaca, pa dobijamo da je

$$F = \Psi\Phi \quad gde \quad je \quad F = a_0 b_0 f,$$

$$\Psi = a_0 x^m + a_1 x^{m-1} + \cdots + a_m \quad i \quad \Phi = b_0 x^n + b_1 x^{n-1} + \cdots + b_n.$$

Neka je p prost delilac broja $a_0 b_0$. Tada su svi koeficijenti od F deljivi sa p, ali ne i od Ψ i Φ. Kombinujemo članove iz Ψ i Φ, respektivno, čiji su koeficijenti deljivi sa p, da bismo formirali polinome U i V respektivno, i na isti način kombinovali ove članove čiji koeficijenti nisu deljivi sa p, da bismo formirali polinome u i v, tako da je $F = (U + u)(V + v)$, i kao posledica toga

$$uv = F - UV - Uv - Vu.$$

Desna strana ove jednakosti sadrži polinom u kojem, prema našoj pretpostavci za F, U i V, svaki koeficijent je deljiv sa p; na levoj strani međutim kako je koeficijent uz član najvećeg stepena proizvod dva broja a_r i b_s koji nisu deljivi sa p, onda ni on nije deljiv sa p.

Ove kontradikcije nema jedino kada $a_0 b_0$ nema prostih delilaca, odnosno kada je $a_0 = 1$ i $b_0 = 1$, i u tom slučaju su α_ν i β_ν celobrojni.
Kraj dokaza Gausove teoreme.

Sada nastavljamo gde smo stali u dokazu Šonemanove teoreme, i koristeći upravo formulisanu i dokazanu Gausovu teoremu, zaključujemo da su koeficijenti a i b celobrojni. Množimo članove

polinoma ψ i φ i za f dobijamo koeficijente

$$C_0 = a_0 b_0,$$

$$C_1 = a_0 b_1 + a_1 b_0$$

$$C_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 \quad itd.$$

Kako C_0 nije deljiv sa p^2, pretpostavimo da je a_0 deljiv sa p, a u tom slučaju b_0 nije. Sada, kako su C_1 i a_0 deljivi sa p, dok b_0 nije, iz drugog reda gornjeg izraza sledi da je a_1 deljivo sa p. Tada, prema trećem redu izraza kako su C_2, a_0, a_1 deljivi sa p sledi da je i a_2 takođe deljivo sa p, itd. Konačno, mogli bismo da zaključimo da je i $a_m = 1$ deljiv sa p, što je prirodno kontradikcija. Prema tome, f ne može biti rastavljiv polinom i time je teorema dokazana.

Rastavljivi i nerastavljivi polinomi igraju ključnu ulogu među polinomima kao složeni i prosti brojevi među celim brojevima. Prema tome, na primer, svaki rastavljiv polinom može biti predstavljen na samo jedan način kao proizvod nerastavljivih polinoma. Sve teoreme kojih smo se ovde dotakli zasnovane su na *osnovnoj teoremi nerastavljivih funkcija.*

ABELOVA TEOREMA NESVODLJIVOSTI: *Ako jedno rešenje algebarske jednačine $f(x) = 0$, koja je nesvodljiva u $\mathfrak{K}$, predstavlja takođe rešenje jednačine $F(x) = 0$ u $\mathfrak{K}$, onda su sva rešenja prve jednačine takođe rešenja i jednačine $F(x) = 0$. Istovremeno, $F(x)$ može biti podeljen sa $f(x)$ bez ostatka:*

$$F(x) = f(x) \cdot F_1(x),$$

gde je $F_1(x)$ takođe polinom u $\mathfrak{K}$.

Jednostavni dokaz ove teoreme zasniva se na dobro poznatom algoritmu za nalaženje najvećeg zajedničkog delioca $g(x)$ za dva proizvoljna polinoma $F(x)$ i $f(x)$ u $\mathfrak{K}$. Ovaj algoritam vodi nas kroz lanac deljenja, gde su koeficijenti $\mathfrak{K}$-brojevi, do para jednakosti

$$F(x) = F_1(x) \cdot g(x)$$

$$f(x) = f_1(x) \cdot g(x)$$

i do jednakosti

$$V(x)F(x) + f(x)v(x) = g(x),$$

pri čemu su sve navedene funkcije polinomi u $\mathfrak{K}$.

Ako određene funkcije F i f nemaju zajedničkih delilaca, onda je $g(x)$ konstanta za koju radi jednostavnosti možemo uzeti da je jednaka 1.

Ako je f nerastavljiv, a α rešenje jednačine $f = 0$ i istovremeno rešenje za $F = 0$, onda za njih postoji zajednički delilac najmanje prvog stepena $(x - \alpha)$. Kako je f nerastavljiv, f_1 mora biti 1 i $f(x) = g(x)$, i onda je

$$F(x)[= F_1(x) \cdot g(x)] = F_1(x) \cdot f(x).$$

Prema tome, $F(x)$ je deljivo sa $f(x)$ i nula je za svaku nula-tačku funkcije $f(x)$, što je i trebalo dokazati.

Ova osnovna teorema direktno povlači dve važne posledice:

I. *Ako je rešenje jednačine $f(x) = 0$, koja je nesvodljiva u $\mathfrak{K}$, takođe i rešenje jednačine $F(x) = 0$ u $\mathfrak{K}$ stepena manjeg od f, onda su svi koeficijenti od F jednaki nuli.*

II. *Ako je $f(x) = 0$ nesvodljiva jednačina u polju $\mathfrak{K}$, onda ne postoji druga nesvodljiva jednačina u $\mathfrak{K}$ koja ima zajedničkih rešenja sa $f(x) = 0$.*

Najčešći slučaj proširenja polja $\mathfrak{K}$ sastoji se u korišćenju korena α u nesvodljivoj jednačini n-tog stepena

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

u $\mathfrak{K}$. Broj ζ iz polja $\mathfrak{K}' = \mathfrak{K}(\alpha)$, jeste racionalna funkcija od α sa koeficijentima iz $\mathfrak{K}$ i može biti zapisan kao $\zeta = \Psi(\alpha)/\Phi(\alpha)$, gde su Ψ i Φ polinomi u $\mathfrak{K}$. Kako je $a^n = -a_1\alpha^{n-1} - -a_2\alpha^{n-2} - \cdots - a_n$, svaki stepen broja α eksponenta n ili većeg može biti izražen pomoću stepena α^{n-1}, α^{n-2}, $\ldots$, α, tako da možemo pisati $\zeta = \psi(\alpha)/\varphi(\alpha)$, gde su ψ i φ polinomi u $\mathfrak{K}$ stepena ne većeg od $n - 1$.

Kako $f(x)$ i $\varphi(x)$ nemaju zajedničkih delilaca, možemo naći dva polinoma $u(x)$ i $v(x)$ u $\mathfrak{K}$, takva da je $u(x)\varphi(x) + v(x)f(x) = 1$. Ako u ovoj jednakosti uzmemo da je $x = \alpha$, onda [kako je $f(\alpha) = 0$] važi $u(\alpha) \cdot \varphi(\alpha) = 0$ i $\zeta = \psi(\alpha) \cdot u(\alpha)$. Ovo množimo i još jednom eliminišemo svaki stepen broja α čiji je eksponent veći ili jednak od n. Konačno dobijamo da je

$$\zeta = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1},$$

pri čemu su c_ν $\mathfrak{K}$-brojevi; i takođe

III. *Svaki broj polja $\mathfrak{K}(\alpha)$, gde je α rešenje nesvodljive jednačine n-tog stepena u $\mathfrak{K}$, može biti predstavljen kao polinom $n-1$ stepena broja α sa koeficijentima koji su $\mathfrak{K}$-brojevi. Postoji samo jedan mogući način takve reprezentacije.*

[Iz jednakosti

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = C_0 + C_1\alpha + \cdots + C_{n-1}\alpha^{n-1}$$

sledi da je

$$d_0 + d_1\alpha + \cdots + d_{n-1}\alpha^{n-1} = 0, \quad d_\nu = C_\nu - c_\nu.$$

Tada, funkcija stepena $n-1$

$$d_0 + d_1 x + \cdots + d_{n-1}x^{n-1}$$

postaje nula za rešenje jednačine $f(x) = 0$ i, prema tvrđenju **I**, ne sme imati ništa od polaznih koeficijenata. Iz $d_\nu = 0$, sledi, međutim, da je $C_\nu = c_\nu$.]

Posmatrajmo opštiji slučaj u kome nerastavljiva funkcija $f(x)$ u $\mathfrak{K}$ čiji je stepen prost broj p, postaje rastavljiva zamenom rešenja α u nesvodljivoj jednačini q-tog stepena $g(x) = 0$ u $\mathfrak{K}$, u kojoj zato $f(x)$ može biti predstavljena kao proizvod dva polinoma $\psi(x, \alpha)$ i $\varphi(x, \alpha)$, koji mogu biti m-tog i n-tog stepena od x, respektivno.

Sada, funkcija u $\mathfrak{K}$

$$u(x) = f(r) - \psi(r, x)\varphi(r, x)$$

gde je r racionalni broj, ima vrednost nula za $x = \alpha$. Prema osnovnoj teoremi nerastavljivih funkcija, $u(x)$ je onda nula za sve korene α, α', α", ... nesvodljive jednačine $g(x) = 0$.

Kako je, na primer, jednačina

$$f(x) - \psi(x, \alpha')\varphi(x, \alpha') = 0$$

zato zadovoljena za svako racionalno x, zadovoljena je i za sve vrednosti x, tako da je

$$f(x) = \psi(x, \alpha')\varphi(x, \alpha')$$

i slično za sva ostala rešenja jednačine $g(x) = 0$.

Iz q tako dobijenih jednakosti

$$f(x) = \psi(x, \alpha)\varphi(x, \alpha)$$

$$f(x) = \psi(x, \alpha')\varphi(x, \alpha')$$

...

množenjem sledi da je

$$f(x)^q = \Psi(x)\Phi(x),$$

gde su $\Psi(x)$ i $\Phi(x)$ proizvodi q polinoma $\psi(x,\alpha)$, $\psi(x,\alpha')$, ... i $\varphi(x,\alpha)$, $\varphi(x,\alpha')$, ... , respektivno. Kako je svaki od ovih proizvoda simetrična funkcija rešenja jednačine $g(x) = 0$, svaki od proizvoda može biti izražen racionalno prema Varingovoj teoremi pomoću koeficijenata jednačine $g(x) = 0$ [i prirodno pomoću x], tako da su $\Psi(x)$ i $\Phi(x)$ polinomi u $\mathfrak{K}$.

Sada, $\Psi(x)$ je sigurno nula u nekoj od tačaka rešenja nesvodljive jednačine $f(x) = 0$, kao i $\Phi(x)$. Sledstveno tome, $\Psi(x)$ i $\Phi(x)$ mogu biti podeljeni sa $f(x)$ bez ostatka, i kako je f nerastavljiva, nijedan drugi delilac osim f nije moguć, i kao rezultat toga je

$$\Psi(x) = f(x)^\mu, \quad \Phi(x) = f(x)^\nu,$$

gde je $\mu + \nu = q$. Poredeći stepene leve i desne strane, dobijamo

$$mq = \mu p, \quad nq = \nu p$$

i iz toga, kako su m i n manji od p, sledi da p deli q. Prema tome, dobijamo teoremu:

IV. *Nesvodljiva jednačina čiji je stepen prost broj p u polju može postati svodljiva pomoću zamene rešenja neke druge nesvodljive jednačine iz ove grupe samo kada p deli stepen druge jednačine.*

Posle ovog uvoda možemo se vratiti dokazu Abelove teoreme. Prvo, međutim, razmatraćemo šta se podrazumeva pod *algebarski rešivom jednačinom.*

Jednačina n-tog stepena $f(x) = 0$ u polju $\Re$ je *algebarski rešiva* kada je rešiva *nizom radikala*, na primer, kada koren w može biti određen korišćenjem sledećih postupaka:

1. Određivanje a-tog korena $\alpha = \sqrt[a]{R}$ nekog $\Re$-broja R, koji nije a-ti stepen nekog $\Re$-broja, i ubacivanje α u $\Re$, tako da je formirano proširenje $\mathfrak{U} = \Re(\alpha)$;

2. Određivanje b-tog korena $\beta = \sqrt[b]{A}$ $\mathfrak{U}$-broja A, koji nije b-ti stepen nekog $\mathfrak{U}$-broja, i ubacivanje β u $\mathfrak{U}$, tako da je formirano proširenje $\mathfrak{B} = \mathfrak{U}(\beta) = \Re(\alpha, \beta)$;

3. Određivanje c-tog korena $\gamma = \sqrt[c]{B}$ $\mathfrak{B}$-broja B, koji nije c-ti stepen nekog $\mathfrak{B}$-broja, i zamena γ u $\mathfrak{B}$, tako da se formira proširenje

$\mathfrak{C} = \mathfrak{B}(\gamma) = \Re(\alpha, \beta, \gamma)$, itd., dok ove sukcesivne zamene radikala α, β, γ, ... ne formiraju polje u kojem se traženo rešenje w nalazi i u kojem $f(x)$ [kako ima delilac $x - w$] postaje rastavljiva. Ovde je pretpostavljeno da su svi radikalni eksponenti a, b, c, ... prosti brojevi. Ovo ne predstavlja ograničenje pošto svako izvlačenje korena sa složenim eksponentima može biti svedeno na sukcesivno izvlačenje korena za prostim eksponentom (npr. $\sqrt[15]{u} = \sqrt[5]{v}$ sa $v = \sqrt[3]{u}$).

U nameri da uprostimo naš zadatak, ograničićemo se na jednačinu $f(x) = 0$ sa racionalnim koeficijentima, tako da je $\Re$ prirodno racionalno polje, koja je nesvodljiva u $\Re$, i koja je stepena n koji je prost broj.

Neka prva zamena bude n-tog korena jedinice

$$\alpha = \eta = \sqrt[n]{1} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Prema **IV**, ova zamena i dalje ne čini f rastavljivom, pošto je η rešenje jednačine $x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$, stepena manjeg od n.

Takođe, sa svakim zamenjenim radikalom iz niza, koji još uvek ne dopušta deljenje $f(x)$, ujedno ćemo zameniti kompleksno konjugovani radikal. Iako ovo može delovati kao suvišno, sigurno ne može da škodi.

Neka je $\lambda = \sqrt[l]{K}$ radikal čijim dodavanjem prethodnim radikalima $f(x)$ postaje rastavljiva, ali tako da je $f(x)$ i dalje nerastavljiva u polju $\mathfrak{K}$ (kome pripada broj K), ali postaje u proširenju $\mathfrak{L} = \mathfrak{K}(\lambda)$:

$$f(x) = \psi(x, \lambda)\varphi(x, \lambda)\chi(x, \lambda)\ldots$$

Ovde su faktori ψ, φ, χ, ... nerastavljivi polinomi u $\mathfrak{L}$ (ali nisu polinomi u $\mathfrak{K}$) čiji su koeficijenti polinomi od λ u $\mathfrak{K}$.

Kako, prema **IV**, prost broj n mora biti delilac prostog broja l, l mora biti jednako sa n.

Jednačina $x^l = K$, koja je nesvodljiva u $\mathfrak{K}$, prema Abelovoj lemi ima l-te korene

$$\lambda_0 = \lambda, \lambda_1 = \lambda\eta, \lambda_2 = \lambda\eta^2, \ldots, \lambda_\nu = \lambda\eta^\nu, \ldots, \lambda_{n-1} = \lambda\eta^{n-1}$$

Kako je $\psi(x, \lambda)$ delilac od $f(x)$, onda se i $\psi(x, \lambda_\nu)$ sadrži u $f(x)$ bez ostatka (iz dokaza **IV**).

Svaka od n funkcija $\psi(x, \lambda_\nu)$ nerastavljiva je u $\mathfrak{L}$.

[Kao i u dokazu **IV**,iz $\psi(x, \lambda_\nu) = u(x, \lambda_\nu) \cdot v(x, \lambda_\nu)$ sledi da je $\psi(x, \lambda) = u(x, \lambda) \cdot v(x, \lambda)$, ali ova jednakost je nemoguća jer je $\psi(x, \lambda)$ nerastavljiva u $\mathfrak{L}$.]

Od n funkcija $\psi(x, \lambda_\nu)$ ne postoje dve jednake. [U jednakosti $\psi(x, \lambda\eta^\mu) = \psi(x, \lambda\eta^\nu)$, λ bi kao i pre moglo biti zamenjeno korenom $\lambda\eta^{\nu-\mu}$, iz čega bi sledilo da je

$$\psi(x, \lambda) = \psi(x, \lambda H),$$

gde H predstavlja koren jedinice $\eta^{\nu-\mu}$. Ovde bi λ moglo biti zamenjeno sa λH, što bi nam dalo

$$\psi(x, \lambda H) = \psi(x, \lambda H^2).$$

Na sličan način dobilo bi se i da je

$$\psi(x, \lambda H^2) = \psi(x, \lambda H^3),$$

itd. Prema tome, onda bismo imali jednakost

$$\psi(x, \lambda) = \psi(x, \lambda H) = \psi(x, \lambda H^2) = \cdots,$$

i takođe

$$\psi(x, \lambda) = \frac{\psi(x, \lambda) + \psi(x, \lambda H) + \cdots + \psi(x, \lambda H^{n-1})}{n}.$$

Međutim, desna strana ove jednakosti kao simetrična funkcija n rešenja λ, λH, λH^2, ... jednačine $x^n = K$, jeste polinom po x u $\mathfrak{K}$. To, međutim, protivreči pretpostavkama vezanim za $f(x)$.]

Iz ova dva razloga sledi da je $f(x)$ deljiv proizvodom $\Psi(x)$ n različitih faktora $\psi(x, \lambda)$, $\psi(x, \lambda\eta)$, ..., $\psi(x, \lambda\eta^{n-1})$ koji su nerastavljivi u $\mathfrak{L}$:

$$f(x) = \Psi(x) \cdot U(x),$$

gde Ψ (kao simetrična funkcija rešenja jednačine $x^n = K$), a takođe i U, jesu polinomi po x u $\mathfrak{K}$. Sada, kako je $f(x)$ nerastavljiv u $\mathfrak{K}$, $U(x)$ mora biti 1 i neophodno je da

$$f(x) = \Psi(x) = \psi(x, \lambda)\psi(x, \lambda\eta) \ldots \psi(x, \lambda\eta^{n-1}).$$

Pretpostavljena rastavljivost $f(x)$ u polju $\mathfrak{L}$ postaje rastavljivost u linearne faktore. Prema tome, ako su ω, ω_1, ω_2, ..., ω_{n-1} koreni i $x - \omega$, $x - \omega_1$, ..., $x - \omega_{n-1}$ linearni faktori od $f(x)$, onda važi

$$x - \omega = \psi(x, \lambda), x - \omega_1 = \psi(x, \lambda\eta), \ldots, x - \omega_{n-1} = \psi(x, \lambda\eta^{n-1}),$$

i sledstveno tome

$$\omega = K_0 + K_1\lambda + K_2\lambda^2 + \cdots + K_{n-1}\lambda^{n-1},$$

$$\omega_1 = K_0 + K_1\lambda_1 + K_2\lambda_1^2 + \cdots + K_{n-1}\lambda_1^{n-1},$$

$$\vdots$$

$$\omega_{n-1} = K_0 + K_1\lambda_{n-1} + K_2\lambda_{n-1}^2 + \cdots + K_{n-1}\lambda_{n-1}^{n-1},$$

pri čemu su K_ν $\mathfrak{K}$-brojevi.

Sada, jednačina $f(x) = 0$ ima najmanje jedno realno rešenje, zato što je neparnog stepena. Neka to realno rešenje bude oblika

$$\omega = K_0 + K_1\lambda + K_2\lambda^2 + \cdots + K_{n-1}\lambda^{n-1}.$$

Razlikujemo dva slučaja:

I. Baza K realnog radikala λ je realna;

II. Baza K je kompleksna.

Slučaj I. Ovde možemo pretpostaviti da je λ realno jer n-ti koreni jedinice pripadaju polju $\mathfrak{K}$. U tom slučaju, konjugovano kompleksni par za ω bio bi

$$\overline{\omega} = \overline{K}_0 + \overline{K}_1\lambda + \overline{K}_2\lambda^2 + \cdots + \overline{K}_{n-1}\lambda^{n-1},$$

gde su kompleksno konjugovani parovi $\overline{K}_\nu$ za K_ν takođe $\mathfrak{K}$-brojevi. Iz jednakosti $\overline{\omega} = \omega$ sledi da je

$$(\overline{K}_0 - K_0) + (\overline{K}_1 - K_1)\lambda + \cdots + (\overline{K}_{n-1} - K_{n-1})\lambda^{n-1} = 0,$$

a iz ovoga, uzimajući u obzir teoremu **I**, sledi da je $\overline{K}_\nu = K_\nu$ za svako ν. Brojevi K_0, K_1, ... , K_{n-1} su zato realni.

Osim toga,

$$\omega_\nu = K_0 + K_1\lambda_\nu + K_2\lambda_\nu^2 + \cdots + K_{n-1}\lambda_\nu^{n-1}$$

i slično

$$\omega_{n-\nu} = K_0 + K_1\lambda_{n-\nu} + K_2\lambda_{n-\nu}^2 + \cdots + K_{n-\nu}\lambda_{n-\nu}^{n-1}.$$

Međutim, kako su $\lambda_\nu = \lambda\eta^\nu$ i $\lambda_{n-\nu} = \lambda\eta^{n-\nu} = \lambda_{-\nu}$ kompleksno konjugovani, sledi da su i ω_ν i $\omega_{n-\nu}$ takođe kompleksno konjugovani, pa prema tome:

Jednačina $f(x) = 0$ ima jedno realno rešenje i ukupno $n-1$ uparenih kompleksno konjugovanih rešenja (ω_1 i ω_{n-1}, ω_2 i ω_{n-2}, itd.).

Slučaj II. U ovom slučaju zamenjujemo, osim rastavljivog radikala $\lambda = \sqrt[n]{K}$, njemu kompleksno konjugovani par $\overline{\lambda} = \sqrt[n]{\overline{K}}$. Na taj način je i realna veličina $\Lambda = \lambda\overline{\lambda}$ takođe zamenjena.

Ako je sama zamena $\Lambda = \sqrt[n]{K\overline{K}}$ bila dovoljna da $f(x)$ postane rastavljiva, dobili bismo situaciju iz **Slučaja I**. Stoga, možemo pretpostaviti da je $f(x)$ i dalje nerastavljiv u $\mathfrak{K}(\Lambda)$ i ne postaje rastavljiv sve do dodatne zamene λ.

Iz jednakosti

$$\omega = K_0 + K_1\lambda + \cdots + K_{n-1}\lambda^{n-1}$$

sledi da je

$$\begin{aligned}\overline{\omega} &= \overline{K}_0 + \overline{K}_1\overline{\lambda} + \cdots + \overline{K}_{n-1}\overline{\lambda}^{n-1} \\ &= \overline{K}_0 + \overline{K}_1(\frac{\Lambda}{\lambda}) + \cdots + \overline{K}_{n-1}(\frac{\Lambda}{\lambda})^{n-1},\end{aligned}$$

a dalje iz ovoga, kako je $\omega = \overline{\omega}$, da je

$$K_0 + K_1\lambda + \cdots + K_{n-1}\lambda^{n-1} = \overline{K}_0 + \overline{K}_1(\frac{\Lambda}{\lambda}) + \cdots + \overline{K}_{n-1}(\frac{\Lambda}{\lambda})^{n-1}.$$

U ovoj jednakosti sve veličine sa izuzetkom λ pripadaju polju $\mathfrak{K}(\lambda)$, i kako je jednačina $x^n = K$ (prema Abelovoj lemi) nesvodljiva u ovom polju, možemo da zamenimo λ u gornjoj jednakosti bilo kojim rešenjem λ_ν jednačine $x^n = K$.

Ako ovo uradimo, imajući u vidu da je

$$\frac{\Lambda}{\lambda_\nu} = \frac{\Lambda}{\lambda\eta^\nu} = \frac{\overline{\lambda}}{\eta^\nu} = \overline{\lambda}\overline{\eta}^\nu = \overline{\lambda\eta^\nu} = \overline{\lambda}_\nu,$$

dobijamo da je

$$K_0 + K_1\lambda_\nu + \cdots + K_{n-1}\lambda_\nu^{n-1} = \overline{K}_0 + \overline{K}_1\overline{\lambda}_\nu + \cdots + \overline{K}_{n-1}\overline{\lambda}_\nu^{n-1}$$

tj.

$$\omega_\nu = \overline{\omega}_\nu.$$

Prema tome, sva rešenja jednačine $f(x) = 0$ su realna.

Iz kombinacije rezultata **I** i **II** sledi:

Kronekerova teorema: *Algebarski rešiva jednačina neparnog stepena koji je prost broj, koja je nesvodljiva u prirodnom racionalnom polju ima ili samo jedno realno rešenje ili sva realna rešenja.*

Kronekerova teorema istovremeno nam pokazuje da jednačina stepena višeg od četvrtog ne može u opštem slučaju biti rešena algebarskim putem.

Na primer, prosta jednačina petog stepena

$$x^5 - ax - b = 0,$$

ne može biti rešena algebarski kada su a i b pozitivni celi brojevi deljivi prostim brojem p, b nije deljivo sa p^2, i važi $4^4a^5 > 5^5b^4$.

Prema Šonemanovoj teoremi jednačina je nesvodljiva. Šturmova teorema nam pokazuje na primeru 6.2. da ona ima tri realna i

dva kompleksna rešenja. Iz tih činjenica zaključujemo prema Kronekerovoj teoremi da je jednačina algebarski nerešiva.

Na potpuno identičan način može se pokazati da je jednačina

$$x^7 - ax - b = 0$$

algebarski nerešiva kada je $6^6 a^7 > 7^7 b^6$.

Literatura

[1] *Pregled istorije i filozofije matematike* - Milan Božić, Zavod za udžbenike, Beograd, 2000.

[2] *Analiza sa algebrom 3* - Zoran Kadelburg, Vladimir Mićić, Srđan Ognjanović, *Krug*, Beograd 2003.

[3] *Topics in polynomials: Extremal problems, inequalities, zeros* - G. V. Milovanović, D. S. Mitrinović, Th. M. Rassias, World Scientific, Singapore - New Jersey - London - Hong Kong, 1994.

[4] *100 great problems of elementary mathematics* - Heinrich Dörrie, Dover, New York, 1965.

[5] *Algebra II* - Veselin Perić, IGKRO *Svjetlost* OOUR Zavod za udžbenike, Sarajevo, 1980.

[6] *450 godina Velike veštine. Početak algebre* - Siniša Crvenković, *Prosvetni pregled*, Beograd 1996.