Polinomi

Peko-Lončar, Zrinka

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Zrinka Peko-Lončar

POLINOMI

Diplomski rad

Voditelj rada:
doc. dr. sc. Ana Prlić

Zagreb, rujan, 2023.

Ovaj diplomski rad obranjen je dana ____________________ pred ispitnim povjerenstvom u sastavu:

1. ____________________________, predsjednik
2. ____________________________, član
3. ____________________________, član

Povjerenstvo je rad ocijenilo ocjenom ________________.

Potpisi članova povjerenstva:

1. ____________________________
2. ____________________________
3. ____________________________

Zahvaljujem se svojoj mentorici, doc. dr. sc. Ani Prlić, na pomoći, strpljenju i svim korisnim savjetima tijekom pisanja diplomskog rada. Zahvaljujem svojoj obitelji i prijeteljima koji su mi olakšali i uljepšali cijelo razdoblje studiranja. Ovaj rad posvjećujem svojim roditeljima koji su mi uvijek bili podrška i vjerovali u mene.

Sadržaj

Uvod

Polinomi su jednostavne i korisne funkcije s kojima se, u najjednostavnijim oblicima, susrećemo već u osnovnoškolskom obrazovanju. Neizostavni su dio srednjoškolskih, ali i fakultetskih nastavnih sadržaja jer su vrlo značajni u teorijskoj i primijenjenoj matematici. Važnost polinoma je i u tome što pomoću njih možemo aproksimirati razne složene funkcije do željene preciznosti.

Zbog svoje važnosti, polinomi su stoljećima bili okupacija mnogih matematičara, stoga ćemo ovaj diplomski rad započeti povijesnim pregledom. Proučit ćemo kako su se polinomi razvijali kroz povijest, počevši od prvih kvadratnih jednadžbi u srednjem vijeku. Naglasit ćemo svako važno otkriće koje je vodilo k razvoju i konačnom dokazu osnovnog teorema algebre.

Tri klasična problema starogrčke matematike spadaju u najpoznatije probleme u povijesti matematike. Pokušaji rješavanja tih problema rezultirali su brojnim otkrićima u matematici. U drugom poglavlju definirat ćemo konstruktibilne brojeve te dokazati nerješivost tri klasična problema pomoću polinoma.

U trećem poglavlju ćemo detaljnije razraditi polinome i njihova svojstva. Definirat ćemo simetrične polinome te iskazati osnovni teorem o simetričnim polinomima. Na kraju poglavlja ćemo uvesti pojam polja razlaganja polinoma i dokazat ćemo dvije leme koje koristimo za dokaz osnovnog teorema algebre. Koristeći osnovni teorem o simetričnim polinomima, polje razlaganje polinoma i spomenute leme, prezentirat ćemo jedan algebarski dokaz osnovnog teorema algebre.

U posljednjem poglavlju obradit ćemo razne zadatke s polinomima koji su se pojavili na domaćim, stranim i međunarodnim natjecanjima iz matematike.

Poglavlje 1

Povijesni pregled

Za ovo poglavlje koristili smo literaturu [4], [8], [14], [15], [19] i [22].
Težnja matematičara za pronalaskom formule za određivanje nultočaka polinoma dovela je do otkrića osnovnog teorema algebre, a time i do razvoja moderne matematike. No, to otkriće razvijalo se stoljećima. Polinomi su funkcije, ali pojam funkcije, kao temeljnog matematičkog koncepta, prvi je postavio švicarski matematičar Leonhard Euler tek u 18. stoljeću, stoga povijesni razvoj polinoma pratimo kroz razvoj polinomijalnih (algebarskih) jednadžbi. Ovaj povijesni pregled ćemo započeti prvim kvadratnim jednadžbama.

1.1 Al-Khwarizmi i začetak algebre

Arapski matematičar, geograf i astronom Muhammad ibn Musa al-Khwarizmi (ca. 780.-850.) razvio je koncept algoritma u matematici zbog čega se smatra *„djedom računarstva"*, a zaslužan je i za prenošenje arapskih brojki u Europu koje je zatim popularizirao Fibonacci[1]. Svojim djelima donio je veliki doprinos astronomiji, geografiji i kartografiji, ali i trigonometriji u sklopu svojih astronomskih spisa. Njegova dva matematička djela, napisana oko 825. godine, zauvijek su promijenila matematiku. U djelu *Kitab al-Jam wa-l-tafriq bi-hisab al-Hind* („Aritmetika") opisuje računanje u indijskom dekadskom pozicijskom brojevnom sustavu. Original na arapskom jeziku je izgubljen, no sačuvani su neki dijelovi prevedni na latinski jezik. Najpoznatiji prijevod čine dva rukopisa pod nazivom *Dixit algorizmi* („Al-Khwarizmi je rekao") iz čega je očito da riječ *„algoritam"* potječe od latinske inačice njegova imena. Al-Khwarizmi je poznat kao *„otac algebre"* jer je svojim djelom *Kitab al-Jabr wa-l-Muqabala* („Algebra") započeo razvoj algebre. Algebra, kao matematička disciplina, dobiva ime po riječi *al-jabr* koju nalazimo već u nazivu knjige. Važnost ovog djela je u tome što daje prvi opis jednadžbi. Iako nije koristio ni-

[1] Leonardo Bonacci ili Leonardo iz Pise, poznatiji kao Fibonacci (ca. 1170.-1250.) - talijanski srednjovjekovni matematičar

kakvu algebarsku simboliku, opisao je jednadžbe i postupke rješavanja jednadžbi riječima. S obzirom da su arapski matematičari tog razdoblja bili pod utjecajem starogrčke matematike, Al-Khwarizmi je razmatrao samo pozitivna rješenja jednadžbi koja je interpretirao geometrijski kao duljine. Iz tog razloga, on dijeli jednadžbe na šest oblika koje bismo danas podijelili na linearne i kvadratne i zapisali bismo ih ovako:

1. $ax^2 = bx$ *(kvadrati jednaki korijenima)*
2. $ax^2 = c$ *(kvadrati jednaki broju jedinica)*
3. $bx = c$ *(korijeni jednaki broju jedinica)*
4. $ax^2 + bx = c$ *(kvadrati i korijeni jednaki broju jedinica)*
5. $ax^2 + c = bx$ *(kvadrati i broj jedinica jednaki korijenima)*
6. $bx + c = ax^2$ *(korijeni i broj jedinica jednaki kvadratima)*

pri čemu su a, b i c pozitivni brojevi (jer konstante predstavljanju duljine). U knjizi navodi razne primjere kojima objašnjava kako se svaka rješiva jednadžba (kvadratna ili linearna) može svesti na jedan od ovih šest oblika pomoću dvije tehnike - *al-jabr* i *al-muqabala*. Tehnika *al-jabr* („nadopunjavanje") jest eliminacija negativnih članova s obiju strana jednadžbe, npr. Al-Khwarizmi jednadžbu $x^2 = 40x-4x^2$ tehnikom *al-jabr* svodi na $5x^2 = 40x$. Tehnika *al-muqabala* („uravnoteživanje") jest oduzimanje pozitivnog člana jedne strane jednadžbe od člana s istom potencijom nepoznanice na drugoj strani, npr. Al-Khwarizmi jednadžbu $50 + 3x + x^2 = 29 + 10x$ tehnikom *al-muqabala* svodi na $21 + x^2 = 7x$. Za prva tri oblika jednadžbi, Al-Kwarizmi je dao samo kratke primjere bez detaljnih objašnjenja, no zanimljiva su objašnjenja koja daje za preostala tri oblika jer su postupci rješavanja potpuno računski, a interpretacija je geometrijska.

Primjer 1.1.1. *Kao primjer jednadžbe oblika $ax^2+bx = c$, Al-Khwarizmi navodi „dva kvadrata i deset korijena jednaka su četrdeset i osam jedinica", tj.* $2x^2 + 10x = 48$. *Postupak rješavanja je sljedeći:*

1. *Smanji dva kvadrata na jedan i znaš da je jedan korijen od dva kvadrata jednak polovini oba, a zatim broj jedinica prepolovi. Dobit ćeš jednadžbu jednaku polaznoj - „kvadrat i pet korijena jednaki su dvadeset i četiri jedinice" (dakle, dijeli obje strane jednadžbe s 2, odnosno koeficijentom a, i dobiva* $x^2 + 5x = 24$*).*

2. *Uzmi pola broja korijena i dobivaš dva i pol (dakle, računa* $\frac{b}{2}$ *i dobiva* $\frac{5}{2}$*, odnosno 2.5).*

3. *Pomnoži to samim sobom i dobivaš šest i četvrtinu (dakle, računa* $\frac{b^2}{4}$ *i dobiva* $\frac{25}{4}$*, odnosno 6.25).*

4. *Pridodaj to broju jedinica i dobivaš trideset i četvrtinu (dakle, računa* $c + \frac{b^2}{4}$ *i dobiva 30.25).*

5. *Korjenuj to i dobivaš pet i pol (dakle, računa* $\sqrt{c + \frac{b^2}{4}}$ *i dobiva 5.5).*

6. *Od toga oduzmi pola broja korijena i dobivaš tri. Korijen je jednak tri pa je kvadrat jednak devet (dakle, računa* $\sqrt{c + \frac{b^2}{4}} - \frac{b}{2}$ *i dobiva* $x = 3$*).*

Vidimo da je Al-Khwarizmi odredio jedno (pozitivno) rješenje kvadratne jednadžbe oblika $ax^2 + bx = c$ te u svom djelu navodi da ovaj postupak uvijek vodi do rješenja.

Primjer 1.1.2. *Kao primjer jednadžbe oblika* $ax^2+c = bx$*, Al-Khwarizmi navodi „kvadrat i dvadeset i jedna jedinica jednaki su deset korijena", tj.* $x^2+21 = 10x$*. Postupak rješavanja je sljedeći:*

1. *Uzmi pola broja korijena i dobivaš pet (dakle, računa* $\frac{b}{2}$ *i dobiva 5).*

2. *Pomnoži to samim sobom i dobivaš dvadeset i pet (dakle, računa* $\frac{b^2}{4}$ *i dobiva 25).*

3. *Od toga oduzmi broj jedinica i dobivaš četiri (dakle, računa* $\frac{b^2}{4} - c$ *i dobiva 4).*

4. *Korjenuj to i dobivaš dva (dakle, računa* $\sqrt{\frac{b^2}{4} - c}$ *i dobiva 2).*

5. *To oduzmi od polovine broja korijena i dobivaš tri. Korijen je jednak tri pa je kvadrat jednak devet (dakle, računa* $\frac{b}{2} - \sqrt{\frac{b^2}{4} - c}$ *i dobiva* $x = 3$*). Možeš i dodati polovinu broja korijena i dobiti sedam. Tada je korijen jednak sedam pa je kvadrat jedak četrvdeset i devet (dakle, računa* $\frac{b}{2} + \sqrt{\frac{b^2}{4} - c}$ *i dobiva* $x = 7$*).*

Na kraju primjera govori da će svaka jednadžba ovog oblika imati barem jedno rješenje, odnosno da se rješenje može dobiti kao zbroj $\frac{b}{2} + \sqrt{\frac{b^2}{4} - c}$ ili kao razlika $\frac{b}{2} - \sqrt{\frac{b^2}{4} - c}$. Upravo tu vidimo da je Al-Khwarizmi, prvi u povijesti, uočio da kvadratne jednadžbe mogu imati dva rješenja. Iako je to uočio samo za neke jednadžbe oblika $ax^2 + c = bx$, tj. one koje imaju dva pozitivna rješenja, to je otkriće kojim je započelo otkrivanje osnovnog teorema algebre.

Primjer 1.1.3. *Kao primjer jednadžbe oblika* $bx + c = ax^2$*, Al-Khwarizmi navodi „tri korijena i četiri jedinice jednaki su kvadratu", tj.* $3x + 4 = x^2$*. Postupak rješavanja je sljedeći:*

1. *Uzmi pola broja korijena i dobivaš jedan i pol (dakle, računa* $\frac{b}{2}$ *i dobiva 1.5).*

2. *Pomnoži to samim sobom i dobivaš dva i četvrtinu (dakle, računa* $\frac{b^2}{4}$ *i dobiva 2.25).*

3. *Pridodaj to broju jedinica i dobivaš šest i četvrtinu (dakle, računa* $c + \frac{b^2}{4}$ *i dobiva 6.25).*

4. *Korjenuj to i dobivaš dva i pol (dakle, računa* $\sqrt{c + \frac{b^2}{4}}$ *i dobiva 2.5).*

5. *To dodaj polovini broja korijena i dobivaš četiri. Korijen je jednak četitri pa je kvadrat jednak šesnaest (dakle, računa* $\frac{b}{2} + \sqrt{c + \frac{b^2}{4}}$ *i dobiva* $x = 4$*).*

Na kraju ovog primjera govori da svaku jednadžbu u kojoj se nalazi više ili manje od jednog kvadrata, najprije treba svesti na oblik u kojem imamo jedan kvadrat. Drugim riječima, kaže da rješavanje treba započeti normiranjem jednadžbe. Time završava svoja objašnjenja i naposlijetku zadnja tri oblika jednadžbi interpretira geometrijski pozivajući se na Euklidove Elemente[2].

Al-Khwarizmijeva *„Algebra"* bila je vrlo utjecajno djelo i mnogi matematičari su doprinijeli razvoju algebre vodeći se njime. Prvi veći doprinos razvoju osnovnog teorema algebre dao je arapski matematičar Omar Khayyam (1048.–1131.) jer je proširio Al-Khwarizmijevu klasifikaciju na kubne jednadžbe za koje je tvrdio da se njihova rješenja ne mogu konstruirati ravnalom i šestarom. Prvi je primijetio da postoje kubne jednadžbe s više od jednog rješenja, ali je pronašao samo jedan primjer s dva rješenja. Kao i Al-Khwarizmi, zanemario je kubne jednadžbe s negativnim rješenjima jer je rješenja interpretirao geometrijski, stoga je zahtijevao pozitivne koeficijente. Rješavanje je započinjao normiranjem i tako je dobio ukupno 19 oblika jednadžbi koje bismo danas zapisali ovako:

1. $x^3 = c$ *(kocka jednaka broju jedinica)*

2. $x^3 = bx$ *(kocka jednaka stranicama)*

3. $x^3 = ax^2$ *(kocka jednaka kvadratima)*

4. $x^3 + ax^2 = bx$ *(kocka i kvadrati jednaki stranicama)*

5. $x^3 = ax^2 + bx$ *(kocka jednaka kvadratima i stranicama)*

6. $x^3 + bx = ax^2$ *(kocka i stranice jednake kvadratima)*

7. $x^3 + bx = c$ *(kocka i stranice jednake broju jedinica)*

[2]Elementi su matematički spisi koje je stargogrčki matematičar Euklid objavio oko 300. pr. Kr. u 13 knjiga. U njima je sustavno, na aksiomatskoj osnovi, izložio i logički razvio cjelokupnu tada poznatu matematiku, tj. elementarnu geometriju.

8. $x^3 + c = bx$ *(kocka i broj jedinica jednaki stranicama)*
9. $x^3 = bx + c$ *(kocka jednaka stranicama i broju jedinica)*
10. $x^3 + ax^2 = c$ *(kocka i kvadrati jednaki broju jedinica)*
11. $x^3 + c = ax^2$ *(kocka i broj jedinica jednaki kvadratima)*
12. $x^3 = ax^2 + c$ *(kocka jednaka kvadratima i broju jedinica)*
13. $x^3 + ax^2 + bx = c$ *(kocka, kvadrati i stranice jednaki broju jedinica)*
14. $x^3 + ax^2 + c = bx$ *(kocka, kvadrati i broj jedinica jednaki stranicama)*
15. $x^3 + bx + c = ax^2$ *(kocka, stranice i broj jedinica jednaki kvadratima)*
16. $x^3 = ax^2 + bx + c$ *(kocka jednaka kvadratima, stranicama i broju jedinica)*
17. $x^3 + ax^2 = bx + c$ *(kocka i kvadrati jednaki stranicama i broju jedinica)*
18. $x^3 + bx = ax^2 + c$ *(kocka i stranice jednake kvadratima i broju jedinica)*
19. $x^3 + c = ax^2 + bx$ *(kocka i broj jedinica jednaki kvadratima i stranicama).*

Prvi oblik riješio je korjenovanjem, a sljedećih pet, bez konstantnog člana, supstitucijom je sveo na kvadratne jednadže zbog čega se često ne svrstavaju u njegovu klasifikaciju kubnih jednadžbi. Preostalih 13 oblika kubnih jednadžbi riješio je pomoću konika (kružnica, polukružnica, parabola i hiberbola). Omar Khayyam ponekad se, zbog svojih metoda rješavanja kubnih jednadžbi, smatra i prethodnikom analitičke geometrije. Prikazat ćemo jednu od tih metoda u sljedećem primjeru.

Primjer 1.1.4. *Kao primjer jednadžbe oblika $x^3 + bx = c$, Khayyam navodi „kocka i četiri stranice jednake su trideset i šest jedinica", tj. $x^3 + 4x = 36$. Postupak rješavanja je sljedeći:*

Koeficijenti b i c moraju zadovoljavati princip homogenosti (x^3 je volumen kocke brida x, pa se može zbrajati i izjednačavati samo s drugim volumenima), zato je $b = B^2$ iz čega slijedi da se c može zapisati u obliku $c = B^2C$, gdje su B i C neke duljine. Dakle, Khayyam je zapravo rješavao jednadžbe oblika $x^3 + B^2x = B^2C$. U ovom primjeru je $B = 2$ i $C = 9$.

1. *Nacrtaj kružnicu promjera 9 i odaberi točku (S) na toj kružnici (dakle, radijus kružnice je $\frac{C}{2}$).*
2. *Uzmi tu točku (S) za tjeme parabole čija je os tangenta na kružnicu, a udaljenost fokusa i ravnalice jednaka je 2 (dakle, udaljenost je jednaka B).*

3. *Uzmi točku presjeka kružnice i parabole (X) i nacrtaj njezinu ortogonalnu projekciju (Q) na promjer kružnice ($\overline{SS'}$) te zatim uzmi točku na osi parabole (P) čija je udaljenost od tjemena jednaka 2 (dakle, $|SP| = B$).*

   Napomena 1.1.5. *Nakon toga, Khayyam riječima dokazuje sličnost pravokutnih trokuta ($\triangle SQX \sim \triangle XQS'$) iz čega slijedi da je $x = |SQ|$ rješenje polazne jednadžbe.*

4. *Rješenje je udaljenost od tjemena parabole do ortogonalne projekcije točke presjeka parabole i kružnice na promjer kružnice (dakle, $x = |SQ|$).*

Napomena 1.1.6. *Ovaj primjer je zanimljiv jer je rješenje jednadžbe iracionalan broj koji Khayyam ondašnjim alatima nije mogao odrediti, stoga detaljno opisuje cijeli postupak. U primjerima jednadžbi oblika $x^3 + bx = c$ s cjelobrojnim rješenjima lako je odredio rješenje (npr. $x = 1$ je rješenje jednadžbe $x^3 + 4x = 5$). Ako bismo točku S stavili u ishodište koordinatnog sustava, vidimo da je duljina koju je Khayyam odredio kao rješenje zapravo jednaka apscisi točke presjeka krivulja, a znamo da to zaista jest rješenje. Koristeći današnju simboliku, rekli bismo da je Khayyam odredio jedno rješenje jednadžbe $x^3 + bx = c$ kao presjek kružnice i parabole:*

$$\begin{cases} x^2 + y^2 = qx \\ x^2 = py, \end{cases}$$

gdje su b, c, p i q pozitivni brojevi. Presjekom gornjih jednadžbi dobivamo

$$\frac{x^4}{p^2} = x(q - x),$$

odnosno

$$x^3 = p^2(q - x),$$

tj.

$$x^3 + p^2 x = p^2 q,$$

iz čega slijedi

$$\begin{cases} p^2 = b \\ q = \frac{c}{b}, \end{cases}$$

što je ekvivalentno

$$\begin{cases} p = \sqrt{b} \\ q = \frac{c}{b}, \end{cases}$$

jer su b, c, p i q pozitivni brojevi. Dakle, Khayyam je tražio presjek kružnice i parabole:

$$\begin{cases} x^2 + y^2 = \frac{c}{b}x \\ x^2 = \sqrt{b}y. \end{cases}$$

1.2 Jednadžbe trećeg i četvrtog stupnja u renesansi

U ostatku srednjeg vijeka nije bilo većih doprinosa razvoju osnovnog teorema algebre, no važno je spomenuti da se negativni brojevi počeli smatrati smislenima, što je važno za razvoj matematike općenito, a time i za osnovni teorem algebre. Naime, u djelima već spomenutog Fibonnacija vidimo da je razumio i koristio negativne brojeve. Talijanski matematičari 16. stoljeća otkrili su kako odrediti rješenja kubnih jednadžbi bez kvadratnog člana u radikalima[3], tj. jednadžbi koje u skladu s Khayyamovom klasifikacijom imaju jedan od oblika $x^3 + bx = c$, $x^3 = bx + c$ ili $x^3 + c = bx$ gdje su b i c pozitivni brojevi. Iako su se negativni brojevi ponegdje koristili u to vrijeme, rješenja jednadžbi su se još uvijek interpretirala geometrijski, stoga su matematičari tražili samo pozitivna rješenja. Štoviše, upravo zato su koeficijenti gornjih jednadžbi morali bili oblika $b = B^2$ i $c = C^3$. Supstitucijom $y = x \pm \frac{a}{3}$, gdje je a koeficijent uz kvadratni član, svaka se normirana kubna jednadžba svodi na jedan od tri navedena oblika.

Scipione del Ferro (ca. 1463.– 1526.), profesor matematike u Bologni, bio je prvi matematičar koji je oko 1515. godine znao odrediti rješenja kubne jednadžbe oblika $x^3 + bx = c$ u radikalima. Svoj postupak rješavanja otkrio je tek na samrti svom učeniku Antoniu del Fioreu. U međuvremenu je, samouki matematičar Niccolo Fontana Tartaglia (ca. 1500.–1557.), otkrio postupak za rješavanje kubne jednadžbe oblika $x^3 + ax^2 = c$. Del Fior je, uvjeren da samo on zna postupak za rješavanje kubnih jednadžbi oblika $x^3+bx = c$, izazvao Tartagliu na javno natjecanje. Tartaglia je očekivao takav oblik jednadžbi i uspio je otkriti postupak kojim se rješavaju, stoga je pobijedio na natjecanju jer je znao odrediti rješenja jednadžbi oba oblika, dok je del Fior znao odrediti rješenja jednadžbi samo jednog oblika. Za Tartagliainu pobjedu saznao je milanski liječnik i matematičar Girolamo Cardano (1501.–1576.). Cardano je tražio Tartagliau da mu otkrije svoju metodu rješavanja kubnih jednadžbi želeći ju objaviti u svojoj knjizi. Tartaglia mu je otkrio metodu, ali uz uvjet da ju ne objavi prije nego što ju sam objavi. Cardano je proširio Tartagliainu metodu rješevanja, a njegov učenik Lodovico Ferrari (1522.–1565.) je prvi pronašao rješenja jednadžbe četvrtog stupnja u radikalima. Njihove rezultate objavio je u svom djelu *Ars Magna* (1545.) u kojem navodi Tartagliau kao autora metode rješevanja kubnih jednadžbi,

[3]Polinomijalna jednadžba rješiva je u radikalima ako se njezina rješenja mogu odrediti u ovisnosti o koeficijentima jednadžbe koristeći konačno mnogo operacija zbrajanja, oduzimanja, množenja, dijeljenja i korjenovanja.

no time je prekršio obećanje koje je dao šest godine ranije. Tartaglia je tada optužio Cardana za izdaju i izazvao ga na natjecanje. Cardano je na to natjecanje poslao Ferrarija koji je pobijedio Tartagliu. Iako je i Cardano, zahtijevajući oblik jednadžbe s pozitivnim koeficijentima i pozitivnim rješenjima, razlikovao razne slučajeve kubnih jednadžbi, njegova (odnosno, del Ferro-Tartaglia-Cardanova metoda) za rješavanje kubnih jednadžbi u radikalima može se objediniti u jedinstvenu metodu koristeći modernu algebarsku simboliku. Pogledajmo postupak rješavanja jednadžbe oblika $x^3 + bx + c = 0$.

Prvo uvodimo supstituciju

$$x = u + v,$$

iz čega slijedi

$$u^3 + 3u^2v + 3uv^2 + v^3 + b(u + v) + c = 0,$$

tj.

$$u^3 + v^3 + (3uv + b)(u + v) + c = 0.$$

Za određivanje vrijednosti x, dovoljno je odrediti neke u i v koji zadovoljavaju dobivenu jednadžbu jer su matematičari tog doba tražili samo jedno rješenje kubne jednadžbe. Zato dodajemo uvjet

$$uv = -\tfrac{b}{3},$$

iz čega dobivamo sustav

$$\begin{cases} u^3 + v^3 = -c \\ u^3v^3 = -\frac{b^3}{27}, \end{cases}$$

koji svodimo na jednadžbu

$$-u^6 - cu^3 = -\frac{b^3}{27}.$$

Gornju jednadžbu supstitucijom $t = u^3$ svodimo na kvadratnu jednadžbu i dobivamo

$$t^2 + ct - \frac{b^3}{27} = 0.$$

Odatle je

$$t_{1,2} = -\frac{c}{2} \pm \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}.$$

Uvažavanjem supstitucije $t = u^3$, slijedi

$$u_{1,2}^3 = -\frac{c}{2} \pm \sqrt{\frac{c^2}{4} + \frac{b^3}{27}},$$

pa je

$$v_{1,2}^3 = -\frac{c}{2} \mp \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}.$$

Dakle, jedno od rješenja je

$$x = \sqrt[3]{-\frac{c}{2} + \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}} + \sqrt[3]{-\frac{c}{2} - \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}}.$$

Cardano je svoje postupke opravdao geometrijski. U njegovom djelu *Ars Magna* vidimo prvu pojavu kompleksnih brojeva.

Primjer 1.2.1. *Riješimo jednadžbu $x^3 = 15x + 4$ prethodno opisanim postupkom. Prvo uvodimo supstituciju*

$$x = u + v,$$

iz čega slijedi

$$u^3 + v^3 + (3uv - 15)(u + v) - 4 = 0.$$

Sada dodajemo uvjet

$$uv = -\tfrac{-15}{3} = 5,$$

iz čega dobivamo sustav

$$\begin{cases} u^3 + v^3 = 4 \\ u^3 v^3 = 125, \end{cases}$$

koji supstitucijom $v^3 = -u^3 + 4$ svodimo na jednadžbu

$$-u^6 + 4u^3 = 125.$$

Gornju jednadžbu supstitucijom $t = u^3$ svodimo na kvadratnu jednadžbu i dobivamo

$$t^2 - 4t + 125 = 0.$$

Odatle je

$$t_{1,2} = -\frac{-4}{2} \pm \sqrt{\frac{(-4)^2}{4} - 125} = 2 \pm \sqrt{-121}.$$

Uvažavanjem supstitucije $t = u^3$, slijedi

$$u_{1,2}^3 = 2 \pm \sqrt{-121},$$

pa je

$$v_{1,2}^3 = 2 \mp \sqrt{-121}.$$

Dakle, jedno od rješenja je

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}. \tag{1.1}$$

Napomena 1.2.2. *Primijetimo da određivanjem jedne nultočke α polinoma p trećeg stupnja lako možemo odrediti i ostale nultočke polinoma. Naime, kako je α nultočka polinoma p, to znači da je polinom p djeljiv polinomom $x - \alpha$, a dijeljenjem polinoma dobivamo polinom drugog stupnja čije nultočke lako odredimo koristeći dobro poznatu formulu.*

Iako drugi korijen negativnog broja nije smatrao smislenim, budući da je znao da jednadžba ima realno rješenje $x = 4$, Cardano je drugi korijen negativnog broja prihvatio kao međukorak u rješavanju. Pojava drugog korijena negativnih brojeva zaintrigirala je renesansne matematičare jer su im htjeli dati smisao. Sustavna teorija kompleksnih brojeva prvi se put pojavila 1572. godine u *Algebri* talijanskog matematičara i arhitekta Raffaela Bombellia (1526.–1572). U svome djelu je, među ostalim, pokazao i da je (1.1) zaista jednako 4. Bombelli je bio prva osoba u povijesti koja je kompleksne brojeve smatrala smislenim, a ujedno je i opisao pravila računanja s kompleksnim brojevima. To je otkriće važan korak u otkrivanju osnovnog teorema algebre. Pogledajmo još primjer kako je Cardanov učenik Ferrari rješavao jednadžbe četvrtog stupnja u radikalima.

Primjer 1.2.3. *Riješimo jednadžbu $x^4 - 4x^3 - x^2 + 16x - 12 = 0$ Ferrarijevom metodom:*

1. *Supstitucijom $x = y+1$ eliminiramo kubni član, tj. dobivamo jednadžbu $y^4-7y^2+6y = 0$ (u općem slučaju uzimamo supsituciju $x = y \pm \frac{a}{4}$, gdje je a koeficijent uz kubni član, čime eliminiramo kubni član jednadžbe).*

2. *Jednadžbu zapišemo u obliku $y^4-7y^2 = -6y$, a zatim lijevu stranu jednadžbe svodimo na potpuni kvadrat i dobivamo $(y^2 - \frac{7}{2})^2 = -6y + \frac{49}{4}$.*

3. *Pribrojimo $t^2-7t+2ty^2$ (odnosno $t^2+2t(y^2+A)$, gdje je A vrijednost u izrazu $(y^2+A)^2$ na lijevoj strani jednadžbe) objema stranama jednadžbe i dobivamo $((y^2 - \frac{7}{2}) + t)^2 = 2ty^2 - 6y + (\frac{49}{4} + t^2 - 7t)$, gdje je y nova nepoznanica.*

4. *Budući da nas zanima samo jedno rješenje, radi jednostavnosti računanja tražimo t za koji je diskriminanta desne strane jednadžbe s obzirom na y jednaka 0, stoga računamo $(-6)^2 - 4 \cdot 2t \cdot (\frac{49}{4} + t^2 - 7t) = 0$, tj. $-8t^3 + 56t^2 - 98t + 36 = 0$. Koristeći del Ferro-Tartaglia-Cardanovu metodu, dobivamo da je jedno rješenje te jednadžbe $t = 2$.*

5. *Za* $t = 2$ *imamo* $(y^2 - \frac{3}{2})^2 = 4y^2 - 6y + \frac{9}{4}$*, odnosno* $(y^2 - \frac{3}{2})^2 = (2y - \frac{3}{2})^2$*, što je ekvivalentno* $y^2 - \frac{3}{2} = \pm(2y - \frac{3}{2})$.

6. *Rješavanjem dobivenih kvadratnih jednadžbi dobivamo* $y_1 = 0, y_2 = 2, y_3 = -3$ *i* $y_4 = 1$ *iz čega konačno slijedi* $x_1 = 1, x_2 = 3, x_3 = -2$ *i* $x_4 = 2$.

Francuski matematičar François Viète (1540.–1603.) bio je prvi matematičar koji je značajno doprinijeo razvoju matematičke simbolike, a zbog njegovog utjecaja je algebra postala disciplina koja se bavi algebarskim jednadžbama oslonjena na simboličke oznake. Viète je prvi matematičar koji je dao primjere jednadžbi čiji je broj rješenja jednak njihovom stupnju, čime je nagovijestio osnovni teorem algebre. Otkrio je neke nove metode rješavanja jednadžbi stupnja manjeg ili jednakog četiri u radikalima, a najpoznatiji je po iskazu veze između koeficijenata i rješenja jednadžbe, tj. *Vièteovim formulama*. Za kvadratnu jednadžbu $x^2 + ax + b = 0$ pokazao je da vrijedi $x_1x_2 = b$ te $x_1 + x_2 = -a$ gdje su x_1 i x_2 rješenja kvadratne jednadžbe. Također, za kubnu jednadžbu $x^3 + ax^2 + bx + c = 0$ pokazao je da vrijedi $x_1x_2x_3 = -c$, $x_1x_2 + x_1x_3 + x_2x_3 = b$ i $x_1 + x_2 + x_3 = -a$ gdje su x_1, x_2 i x_3 rješenja kubne jednadžbe. Vidimo da je čak i Viète još uvijek razmatrao samo normirane jednadžbe i zahtijevao princip homogenosti. Također, u isto vrijeme je engleski matematičar Thomas Harriot (1560.–1621.) pokazao da se kubna jednadžba može zapisati u obliku $(x - a)(x - b)(x - c) = 0$, gdje su a, b i c rješenja jednadžbe.

1.3 Jednadžbe petog stupnja i Galoisova teorija

Kako su do 17. stoljeća matematičari otkrili razne metode za određivanje rješenja polinomijalnih jednadžbi stupnja manjeg ili jednakog četiri u radikalima, javilo se pitanje mogu li odrediti rješenja polinomijalne jednadžbe petog (ili većeg) stupnja u radikalima. Također, porastao je i interes za kompleksne brojeve.
Iako je Viète krajem 16. stoljeća dao prve primjere jednadžbi čiji je broj rješenja jednak njihovom stupnju, nije razmatrao kompleksna rješenja. Njemački matematičar Peter Roth (1580.-1617.) je 1608. godine prvi ustvrdio da algebarska jednadžba n-tog stupnja ima najviše n rješenja. Francuski matematičar Albert Girard (1595.–1632.) je 1629. godine ustvrdio da vrijedi osnovni teorem algebre. Preciznije, tvrdio je da svaka algebarska jednadžba stupnja n s realnim koeficijentima ima točno n rješenja u nekom skupu još većem nego što je skup kompleksnih brojeva. Tvrdnju o broju rješenja su matematičari tog vremena smatrali očiglednom, stoga su skoro dva stoljeća pokušavali dokazati da se rješenja nalaze u skupu kompleksnih brojeva, umjesto da je broj rješenja jednak stupnju jednadžbe. Nadalje, francuski filozof i matematičar Reniè Descartes (1596.–1650.) složio se s Girardovom tvrdnjom, no ističe kako imaginarna rješenja ne odgovaraju nikakvim realnim vrijednostima. Također, zahvaljujući Descartesu postalo je poznato i Harriotovo otkriće da

polinom p možemo zapisati u obliku $p(x) = (x - x_0)q(x)$, gdje je x_0 nultočka polinoma, a q polinom koji dobijemo dijeljenjem polinoma p binomom $x - x_0$.

Početkom 18. stoljeća, njemački filozof i matematičar Gottfried Wilhelm von Leibniz (1646.–1716.) pokušao je dokazati da se polinom četvrtog stupnja oblika $x^4 + c^4$ ne može faktorizirati kao umnožak dva kvadratna polinoma s realnim koeficijentima te da zato ne može biti umnožak četiriju linearnih polinoma s kompleksnim koeficijentima. Drugim riječima, pokušao je opovrgnuti osnovni teorem algebre misleći da u rastavu

$$x^4 + c^4 = (x + c\sqrt{i})(x - c\sqrt{i})(x + c\sqrt{-i})(x - c\sqrt{-i}), \tag{1.2}$$

$\sqrt{i}$ i $\sqrt{-i}$ nisu kompleksni brojevi. Švicarski matematičar Leonhard Euler (1707.–1783.) je 1742. godine pokazao da je Leibniz bio u krivu otkrivši da vrijedi

$$x^4 + c^4 = (x^2 + c^2)^2 - 2x^2c^2 = (x^2 + c^2 - \sqrt{2}xc)(x^2 + c^2 + \sqrt{2}xc). \tag{1.3}$$

Naime, uvrštavanjem $c = 1$ u (1.2) dobio je

$$x^4 + 1 = (x + \sqrt{i})(x - \sqrt{i})(x + \sqrt{-i})(x - \sqrt{-i}),$$

iz čega slijedi da su nultočke polinoma $x^4 + 1$ jednake $-\sqrt{i}, \sqrt{i}, -\sqrt{-i}, \sqrt{-i}$. Također, uvrštavanjem $c = 1$ u (1.3) dobio je

$$x^4 + 1 = (x^2 + 1 - \sqrt{2}x)(x^2 + 1 + \sqrt{2}x),$$

iz čega slijedi da su nultočke polinoma $x^4 + 1$ jednake $\frac{1+i}{\sqrt{2}}, \frac{1-i}{\sqrt{2}}, -\frac{1+i}{\sqrt{2}}, -\frac{1-i}{\sqrt{2}}$. Izjednačavanjem dobivenih nultočaka, Euler je otkrio da su $\sqrt{i}$ i $\sqrt{-i}$ kompleksni brojevi. Također, Euler je uveo simbol i za $\sqrt{-1}$, a uspio je i dokazati da svaki polinom s realnim koeficijentima stupnja $n, n \leq 6$ ima točno n nultočaka. Francuski matematičar Jean le Rond d'Alembert (1717.–1783.) je 1746. godine prvi pokušao dokazati osnovni teorem algebre, a zatim je 1749. godine Euler pokušao dokazati da svaki realni polinom stupnja n ima točno n kompleksnih rješenja. Francuski matematičar i kemičar Alexandre-Thèophile Vandermonde (1735.-1796.) je 1770. riješio jednadžbu $x^{11} = 1$ u radikalima i tvrdio je da njegova metoda djeluje za sve jednadžbe oblika $x^n = 1$, gdje je n prirodan broj, iako nije dokazao svoju tvrdnju. Joseph-Louis Lagrange (1736.–1813.) je proučavao nedostatke u Eulerovom dokazu osnovnog teorema algebre i dopunio je neke od njih 1772., a isto je učinio i 1795. Pierre-Simon Laplace (1749.–1827.). Vandermonde i Lagrange neposredni su prethodnici Galoisove teorije jer su prvi razmatrali zašto rješenja u radikalima postoje za jednadžbe stupnja manjeg ili jednakog 4. Lagrange je tvrdio da je polinomijalna jednadžba rješiva u radikalima ako postoje jednostavnije jednadžbe čije su nutočke jednake nultočkama polazne jednadžbe.

Kompleksni brojevi postali su šire prihvaćeni početkom 19. stoljeća, kad im je dana geometrijska interpretacija. Danski matematičar Caspar Wessel (1745.–1818.) je 1797. prvi opisao kompleksnu ravninu, no taj opis je postao poznat tek 1895. godine. U međuvremenu su, Carl Friedrich Gauss (1777.–1855.) i Jean-Robert Argand (1768.–1822.), nezavisno jedan od drugog, opisali geometrijsku interpretaciju kopleksnih brojeva i dali dokaze osnovnog teorema algebre. Gauss je bio prvi matematičar koji je primijetio da je potrebno dokazati da je broj nultočaka polinoma jednak stupnju polinoma, a dokazivanjem osnovnog teorema algebre bavio se pedeset godina. Svoj prvi dokaz dao je u sklopu svog doktorata 1799. U tom dokazu koristio se geometrijskom interpretacijom kompleksnih brojeva, no imao je neke nedostatke. Gauss je popravio dokaz i objavio tri nova dokaza - dva 1816. (jedan temeljen na Eulerovim idejama, a drugi topološki) i poslijednji 1849. godine (gdje je prvi put korišten naziv „*kompleksni broj*"). U međuvremenu je dokaz, temeljen na d'Alembertovoj ideji, 1813. dao i Argand, no taj je dokaz postao poznat tek krajem 19. stoljeća. Argand je ujedno prvi matematičar koji je osnovni teorem algebre iskazao i za polinome s kompleksnim koeficijentima, što je dokazao Gauss 1849. godine. Talijanski matematičar Paolo Ruffini (1765.–1822.) prvi je matematičar koji je ustvrdio da opća polinomijalna jednadžba petog stupnja nema rješenje u radikalima 1799. godine. To je pokušao dokazati koristeći permutacije pri čemu je koristio svojstva grupa permutacija. Najprije je 1801. poslao kopiju svog rada Lagrangeu, ali nije dobio odgovor. Nakon toga je poslao drugi primjerak, no ni na taj nije dobio odgovor, a 1802. poslao je i treći primjerak. Ruffini je objavio poboljšane verzije svog dokaza 1808. i 1813., ali jedino je Cauchy[4] prihvatio važnost njegovih rezultata. Usprkos tome, svi Ruffinijevi pokušaji dokaza imali su nedostatke. Cauchy je također objavio djelo o grupama permutacija u kojima je proširio Ruffinijeve rezultate. Prvi potpun dokaz nerješivosti opće polinomijalne jednadžbe petog stupnja u radikalima dao je 1824. norveški matematičar Niels Henrik Abel (1802.–1829.), koji je bio upoznat s Ruffinijevim i Cauchyjevim radovima. Najprije je 1821. naizgled dokazao nerješivost, no kada je predao rad na objavljivanje, trebao je dati konkretan primjer i tada je otkrio da ima grešku u dokazu. Nakon što je dokazao nerješivost opće polinomijalne jednadžbe petog stupnja u radikalima, Abel se posvetio proučavanju eliptičkih integrala. Tek na kraju svog kratkog života vratio se teoriji jednadžbi pokušavajući otkriti koje su polinomijalne jednadžbe rješive u radikalima. Nekoliko godina kasnije, taj je problem odgonetnuo francuski matematičar Èvariste Galois (1811.–1832.). On je, svojim radom na nerješivosti polinomijalnih jednadžbi u radikalima, utemeljio teoriju grupa. Galois je, 1832. godine, pokazao da se polinomijalna jednadžba može riješiti radikalima ako i samo ako je rješiva Galoisova grupa[5] odgovarajućeg polinoma. Galoisove rezultate je, tek nakon njegove smrti, sakupio i 1846. godine objavio francuski matematičar Joseph Liouville (1809.-1882.). Galoisova teorija grupa ušla je u prve udžbenike iz algebre 1860-ih. Tako

[4] Augustin-Louis Cauchy (1789.–1857.) - francuski matematičar

[5] Galoisova grupa G polinoma je podgrupa grupe permutacija svih njezinih nultočaka. Drugim riječima, u Galoisovoj grupi G se nalaze one permutacije nultočaka koje ne mijenjaju nijednu racionalnu funkciju koeficijenata.

je Galois svojim doprinosom algebri, odnosno osnivanjem teorije grupa, završio pitanje rješivosti polinomijalnih jednadžbi u radikalima.

Poglavlje 2

Konstruktibilni brojevi i tri klasična problema

Za ovo poglavlje koristili smo literaturu [8], [11], [13] i [17].
U ovom poglavlju definirat ćemo konstruktibilne brojeve, opisati tri klasična problema i dokazati njihovu nerješivost.

2.1 Konstruktibilni brojevi

Tijekom 5. st. pr. Kr. starogrčki matematičari počeli su zahtijevati da se geometrijske konstrukcije provode isključivo jednobridnim neoznačenim ravnalom i šestarom s promjenjivim rasponom. Iako se ne zna točan razlog tog ograničenja, mnogi autori smatraju da je razlog to što su pravci i kružnice jedine dvije krivulje, prisutne u stvarnom svijetu, koje su smatrane „savršenima" jer svaka dva njihova dijela izgledaju jednako. Za svaku veličinu koja se može konstruirati ravnalom i šestarom u konačno mnogo koraka kažemo da je konstruktibilna. Neka su u ravnini dane jedinična dužina te dvije dužine duljina a i b. Tada možemo konstruirati dužine duljina

$$a+b,\ a-b,\ n\cdot a,\ \tfrac{a}{n},\ a\cdot b,\ \tfrac{a}{b} \text{ ili } \sqrt{a} \text{ gdje je } n\in\mathbb{N}.$$

To nam govori sljedeći teorem:

Teorem 2.1.1. *Moguće je konstruirati svaku dužinu čiju duljinu možemo iz duljina konačno mnogo zadanih dužina izraziti konačnim brojem racionalnih operacija (zbrajanjem, oduzimanjem, množenjem, dijeljenjem) i vađenja kvadratnog korijena.*

Dokaz ovog teorema može se pronaći u [17]. Vrijedi i obrat ovog teorema:

Teorem 2.1.2. *Ako se iz zadanih dužina s duljinama $m_1, m_2, \ldots, m_n$ može pomoću ravnala i šestara konstruirati dužina duljine m', tada se taj broj m' može izračunati iz duljina $m_1, m_2, \ldots, m_n$ pomoću konačno mnogo racionalnih operacija i konačno mnogo vađenja kvadratnih korijena.*

Dokaz ovog teorema se također može naći u [17]. Na temelju prethodnih teorema možemo uočiti da rješivosti geometrijskih konstrukcija ravnalom i šestarom pristupamo algebarski. Za dokaz nerješivosti tri klasična problema, potrebna su nam još dva algebarska teorema koja ćemo dokazati. Definirajmo prvo kada je realan broj konstruktibilan.

Definicija 2.1.3. *Za realan broj x kažemo da je konstruktibilan iz brojeva $a_1, a_2, \ldots, a_n$, ako se taj broj x može izračunati iz $a_1, a_2, \ldots, a_n$, pomoću konačno mnogo racionalnih operacija i konačno mnogo vađenja kvadratnih korijena.*

Nadalje, za dokaz sljedećeg teorema potrebno nam je *proširenje polja* racionalnih brojeva takozvanom adjunkcijom jednog elementa. Neka je dano jedno polje K kojemu adjungiramo element $\sqrt{k}$ ($k \in K$, $\sqrt{k} \notin K$). Svi elementi oblika $a + b \cdot \sqrt{k}$ čine proširenje polja K, tj. polje $K[\sqrt{k}]$. Ako je $a + b \cdot \sqrt{k} = 0$, onda zbog $\sqrt{k} \notin K$ slijedi $a = 0$ i $b = 0$.

Uočimo da se realan broj x može izraziti pomoću konačno mnogo racionalnih operacija i kvadratnog korijenovanja racionalnih brojeva ako postoji konačan niz proširanja polja $\mathbb{Q}_0 \subseteq \mathbb{Q}_1 \subseteq \ldots \subseteq \mathbb{Q}_n$ gdje je $\mathbb{Q}_0 = \mathbb{Q}, \mathbb{Q}_1 = \mathbb{Q}_0[\sqrt{x_1}], \mathbb{Q}_2 = \mathbb{Q}_1[\sqrt{x_2}], \ldots, \mathbb{Q}_n = \mathbb{Q}_{n-1}[\sqrt{x_n}]$, $x_{i+1} \in \mathbb{Q}_i$ i $\sqrt{x_{i+1}} \notin \mathbb{Q}_i$ ($i = 0, 1, \ldots, n-1$), takav da je $x \in \mathbb{Q}_n$.

Teorem 2.1.4. *Ako kubna jednadžba*

$$x^3 + a_2 x^2 + a_1 x + a_0 = 0$$

s racionalnim koeficijentima nema ni jedno racionalno rješenje, onda ni jedno njeno rješenje nije konstruktibilno iz racionalnih brojeva.

Dokaz ovog teorema preuzet je iz [17].

Dokaz. Pretpostavimo suprotno, tj. da zadana jednadžba nema racionalnih rješenja, ali da postoji najmanje jedno rješenje koje je konstruktibilno iz racionalnih brojeva. Označimo s $n \in \mathbb{N}$ najmanji prirodan broj takav da postoji rješenje x_1 gornje jednadžbe za koje je $x_1 \in \mathbb{Q}_n$, gdje je $\mathbb{Q}_n$, kao i ranije, proširenje polja $\mathbb{Q}$ dobiveno dodavanjem n kvadratnih korijena. Tada rješenje x_1 možemo zapisati u obliku

$$x_1 = p + q \cdot \sqrt{w},$$

gdje su $p, q, w \in \mathbb{Q}_{n-1}$ i $\sqrt{w} \notin \mathbb{Q}_{n-1}$.
Dokažimo da je tada

$$x_2 = p - q \cdot \sqrt{w}$$

također rješenje jednadžbe.
Uvrstimo li $x_1 = p + q \cdot \sqrt{w}$ u polaznu jednadžbu, dobivamo

$$x_1^3 + a_2 x_1^2 + a_1 x_1 + a_0 = a + b \cdot \sqrt{w},$$

gdje je

$$\begin{aligned} a &= p^3 + 3pq^2 w + a_2(p^2 + q^2 w) + a_1 p + a_0 \in \mathbb{Q}_{n-1}, \\ b &= 3p^2 q + q^3 w + 2a_2 pq + a_1 q \in \mathbb{Q}_{n-1}. \end{aligned}$$

Kako je x_1 rješenje jednadžbe, slijedi $a + b \cdot \sqrt{w} = 0$ odnosno $a = 0$ i $b = 0$. Analogno, vrijedi sljedeća jednakost

$$x_2^3 + a_2 x_2^2 + a_1 x_2 + a_0 = a - b \cdot \sqrt{w} = 0.$$

Rješenja x_1 i x_2 su različita i $x_1 - x_2 = 2q\sqrt{w} \neq 0$ jer bi u suprotnom vrijedilo $q = 0$, iz čega bi slijedilo da je $x_1 = x_2 = p \in \mathbb{Q}_{n-1}$ što je kontradikcija s pretpostavkom o minimalnosti broja n. Koristeći Vièteove formule dobivamo

$$x_1 + x_2 + x_3 = -a_2,$$

odnosno

$$x_3 = -a_2 - (x_1 + x_2) = -a_2 - 2p,$$

iz čega slijedi $x_3 \in \mathbb{Q}_{n-1}$ što je kontradikcija s pretpostavkom o minimalnosti broja n pa je pretpostavka bila pogrešna. Dakle, nema rješenja konstruktibilnog iz racionalnih brojeva ako jednadžba nema racionalnog rješenja. □

Teorem 2.1.5. *Ako kubna jednadžba*

$$x^3 + a_2 x^2 + a_1 x + a_0 = 0$$

s cjelobrojnim koeficijentima ima racionalno rješenje x_1, onda je x_1 cijeli broj koji dijeli a_0.

Dokaz ovog teorema preuzet je iz [17].

Dokaz. Neka je x_1 jedno racionalno rješenje jednadžbe oblika $x_1 = \frac{l}{m}$ $(l, m \in \mathbb{Z}, m > 0,$ l i m relativno prosti). Tada je

$$\frac{l^3}{m^3} + a_2 \frac{l^2}{m^2} + a_1 \frac{l}{m} + a_0 = 0,$$

tj.

$$l^3 + a_2 l^2 m + a_1 l m^2 + a_0 m^3 = 0,$$

odnosno

$$l^3 = -m(a_2 l^2 + a_1 ml + a_0 m^2),$$

odakle slijedi da je $m = 1$ (jer su l i m relativno prosti). Sada je

$$l^3 = -(a_2 l^2 + a_1 l + a_0),$$

tj.

$$a_0 = -l(l^2 + a_2 l + a_1),$$

odakle slijedi da je l djelitelj od a_0. Kako je $x_1 = \frac{l}{m} = l$ slijedi da je x_1 djelitelj od a_0, što smo i željeli dokazati. □

Kombinacija teorema (2.1.4) (2.1.5) daje nam jednostavan kriterij kada kubna jednadžba oblika $x^3 + a_2 x^2 + a_1 x + a_0 = 0$ s racionalnim koeficijentima ima barem jedno konstruktibilno rješenje: onda kada je barem jedan od djelitelja njezinog slobodnog člana a_0 rješenje te jednadžbe.

2.2 Tri klasična problema

Tri klasična problema potječu iz atenskog razdoblja antičke grčke matematike. U to vrijeme, konstrukcije bisekcije kuta, podjele dužine na proizvoljan broj jednakih dijelova, duplikacije kvadrata, kvadrature mnogokuta i mnoge druge bile su poznate. Pokušaji njihove generalizacije i specijalizacije doveli su do tri klasična problema, koji su postali problemi upravo zbog uvjeta da se geometrijske konstrukcije provode isključivo ravnalom i šestarom. Tri klasična problema su:

1. **Problem duplikacije kocke**: Za danu kocku potrebno je, ravnalom i šestarom, konstruirati brid kocke dvostrukog volumena.

2. **Problem trisekcije kuta**: Dani kut potrebno je, ravnalom i šestarom, podijeliti na tri kuta jednake veličine.

3. **Problem kvadrature kruga**: Za dani krug potrebno je, ravnalom i šestarom, konstruirati stranicu kvadrata jednake površine.

Problem duplikacije kocke i problem trisekcije kuta svode se na kubne jednadžbe. Dokazat ćemo da ti problemi nisu rješivi ravnalom i šestarom jer rješenja odgovarajućih kubnih jednadžbi nisu konstruktibilni brojevi. S druge strane, problem kvadrature kruga svodi se na transcendentnost[1] broja π.

[1]Transcendentni broj je realan ili kompleksan broj koji nije algebarski (konstruktibilan), tj. onaj koji se ne može dobiti kao rješenje polinomijalne jednadžbe s racionalnim koeficijentima. Svi transcedentni brojevi su iracionalni (npr. π i e), no obrat ne vrijedi (npr. $\sqrt{2}$ je algebarski (konstruktibilan) iracionalan broj).

Primjer 2.2.1. *Nije moguće, ravnalom i šestarom, duplicirati kocku brida duljine a, tj. konstruirati brid kocke volumena* $2a^3$.

Dokaz. Neka je x dulijna brida kocke volumena $2a^3$. Rješavamo jednadžbu

$$x^3 = 2a^3$$

iz čega slijedi

$$x = a\sqrt[3]{2}.$$

Drugim riječima, trebamo konstruirati dužinu duljine $x = a\sqrt[3]{2}$ iz zadane dulljine a. Dakle, potrebno je, uz danu jediničnu dužinu, konstruirati dužinu duljine $\sqrt[3]{2}$. Kada bi to bilo moguće, prema teoremu (2.1.4) bi jednadžba

$$x^3 - 2 = 0$$

imala barem jedno rješenje, konstruktibilno iz racionalnih brojeva. Prema istom teoremu ova bi jednadžba morala imati najmanje jedno racionalno rješenje, koje bi prema teoremu (2.1.5) bilo djelitelj slobodnog koeficijenta jednadžbe, tj. djelitelj broja 2. Djelitelji broja 2 su $1, -1, 2$ i -2, a uvrštavanjem lako vidimo da ni jedan od tih brojeva nije rješenje jednadžbe $x^3-2 = 0$. Dakle, jednadžba nema racionalnih rješenja, stoga slijedi da konstrukcija nije rješiva ravnalom i šestarom. □

Primjer 2.2.2. *Nije moguće, ravnalom i šestarom, trisektirati kut veličine* φ*, tj. konstruirati kut veličine* $\frac{\varphi}{3}$.

Dokaz. Da bismo dokazali nerješivost ove konstrukcije ravnalom i šestarom za opći slučaj, dovoljno je dokazati nerješivost za jedan kut proizvoljne veličine. Kut se može konstruirat ako se može konstruirati njegov kosinus.
Koristeći adicijske formule za sinus i kosinus dobivamo:

$$\begin{aligned}\cos 3\varphi &= \cos(2\varphi + \varphi) = \cos 2\varphi \cos\varphi - \sin 2\varphi \sin\varphi \\ &= (\cos^2\varphi - \sin^2\varphi)\cos\varphi - 2\sin^2\varphi\cos\varphi \\ &= \cos^3\varphi - (1-\cos^2\varphi)\cos\varphi - 2(1-\cos^2\varphi)\cos\varphi \\ &= \cos^3\varphi - \cos\varphi + \cos^3\varphi - 2\cos\varphi + 2\cos^3\varphi \\ &= 4\cos^3\varphi - 3\cos\varphi.\end{aligned} \tag{2.1}$$

Budući da je

$$\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi,$$

vidimo da se problem trisekcije kuta supstitucijom svodi na kubne jednadžbe. S obzirom da je $\cos 3\varphi$ zadan jer je 3φ veličina kuta kojeg trisektiramo, supstitucijom $\cos 3\varphi = a$ i $\cos\varphi = x$ dobivamo kubnu jednadžbu

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

Odaberemo kut proizvoljne veličine, npr. $3\varphi = 60°$, odnosno $\varphi = 20°$. Tada je $a = \frac{1}{2}$ i slijedi

$$4x^3 - 3x - \frac{1}{2} = 0,$$

što je ekvivalentno

$$8x^3 - 6x - 1 = 0.$$

Supstitucijom $t = 2x$ dobivamo

$$t^3 - 3t - 1 = 0.$$

Da bi ova konstrukcija bila rješiva ravnalom i šestarom, jednadžba $t^3 - 3t - 1 = 0$ bi prema teoremu (2.1.4) trebala imati barem jedno racionalno rješenje, koje bi prema teoremu (2.1.5) moralo biti djelitelj slobodnog koeficijenta jednadžbe, tj. djelitelj broja -1. Djelitelji broja -1 su 1 i -1, a uvrštavanjem lako vidimo da ni jedan od tih brojeva nije rješenje jednadžbe $t^3 - 3t - 1 = 0$. Dakle, jednadžba nema racionalnih rješenja, stoga slijedi da konstrukcija nije rješiva ravnalom i šestarom. $\square$

Može se pokazati da postoji beskonačno mnogo vrijednosti $\cos 3\varphi$ za koje konstrukcija nije rješiva ravnalom i šestarom, stoga postoji beskonačno mnogo kutova čija trisekcija nije izvediva. No, za svaki kut oblika $\frac{\pi}{2^n}, n \in \mathbb{N}$ trisekcija je izvediva (lako se dokaže matematičkom indukcijom po $n \in \mathbb{N}$).

Primjer 2.2.3. *Nije moguće, ravnalom i šestarom, kvadrirati krug radijusa r, tj. konstruirati stranicu kvadrata površine $r^2\pi$.*

Konačni dokaz nerješivosti problema kvadrature kruga ravnalom i šestarom dao je 1882. godine njemački matematičar Ferdinand von Lindemann (1852.-1939.) dokazavši da je π transcendentan broj. Dokaz transcedentnosti može se pronaći u [6].

Dokaz. Uzmemo li da je radijus zadanog kruga jednak jedan, površina tog kruga će biti jednaka π. Neka je a duljina stranice kvadrata jednake površine. Rješavamo jednadžbu

$$\pi = a^2$$

iz čega slijedi

$$a = \sqrt{\pi}.$$

Dakle, da bismo konstruirali kvadrat jednake površine, trebamo konstruirati stranicu duljine $\sqrt{\pi}$. Pretpostavimo li da je moguće konstruirati $\sqrt{\pi}$, slijedi da je moguće konstruirati i π. No, budući je π transcendentan broj, slijedi da nije konstruktibilan po definiciji konstruktibilnog broja. Dakle, pretpostavka je bila kriva, stoga problem kvadrature kruga nije rješiv ravnalom i šestarom. $\square$

Poglavlje 3

Osnovno o polinomima

Za ovo poglavlje koristili smo literaturu [12], [16], [18] i [20].
U ovom poglavlju definirat ćemo polinom (jedne varijable), navesti osnovna svojstva polinoma, definirat ćemo kada je jedan polinom djeljiv drugim, nultočke polinoma i neka svojstva nultočaka. Iskazat ćemo osnovni teorem algebre, a zatim opisati faktorizaciju polinoma, Hornerov algoritam i Taylorov razvoj polinoma. Definirat ćemo simetrične polinome (dviju varijabli) te iskazati i dokazati osnovni teorem o simetričnim polinomima. Na kraju poglavlja prezentirat ćemo jedan algebarski dokaz osnovnog teorema algebre.

3.1 Pojam polinoma

Definicija 3.1.1. *Funkcija* $f : \mathbb{R} \to \mathbb{R}$ *zadana formulom*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \tag{3.1}$$

gdje su $a_0, a_1, \ldots, a_n \in \mathbb{R}$, $a_n \neq 0$, $n \in \mathbb{N}_0$ *naziva se* ***polinom n-tog stupnja*** *(nad* $\mathbb{R}$*). Brojeve* $a_0, a_1, \ldots, a_n$ *nazivamo koeficijentima polinoma.*

Definicija 3.1.2. *Polinom je suma pribrojnika* $a_n x^n, a_{n-1} x^{n-1}, \ldots, a_1 x, a_0$ *koje nazivamo* ***monomima****. Monome polinoma zovemo još i članovima polinoma.*

Koeficijent a_0 zovemo *slobodnim članom* ili *slobodnim koeficijentom* polinoma f, a koeficijent a_n zovemo *vodećim koeficijentom* polinoma f. Ako je vodeći koeficijent jednak jedan, tj. ako vrijedi $a_n = 1$, kažemo da je f *normirani polinom*. Broj n zovemo *stupanj polinoma* i pišemo $\deg f = n$. Polinom f je *nulpolinom* ako vrijedi

$$f(x) = 0, \forall x \in \mathbb{R}.$$

Nulpolinom je jedini polinom za koji se stupanj ne definira (ili se katkad stavlja $\deg 0 = -\infty$). Polinom f je *konstantni polinom*, ili kraće *konstanta*, ako za neki $a \in \mathbb{R}$ vrijedi

$$f(x) = a, \forall x \in \mathbb{R}.$$

Stupanj konstantnog polinoma je nula.
Zapis (3.1) nazivamo *kanonski oblik* polinoma. Drugi zapis je

$$f(x) = \sum_{k=0}^{n} a_k x^k.$$

Skup svih polinoma $f : \mathbb{R} \to \mathbb{R}$ označavamo s $\mathbb{R}[x]$ i zovemo **prsten polinoma** u jednoj varijabli x nad poljem $\mathbb{R}$. Skup $\mathbb{R}[x]$ je prsten, jer imamo prirodne definicije zbrajanja i množenja polinoma. Za $f, g \in \mathbb{R}[x]$ definiramo

$$(f + g)(x) = f(x) + g(x)$$

i

$$(f \cdot g)(x) = f(x) \cdot g(x), \forall x \in \mathbb{R}.$$

Neka su $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{j=0}^{m} b_j x^j$ i neka je $n \geq m$. Tada je

$$\begin{aligned} (f + g)(x) &= a_n x^n + a_{n-1} x^{n-1} + \ldots + (a_m + b_m) x^m + \ldots + \\ &\quad + (a_1 + b_1)x + a_0 + b_0 \end{aligned}$$

$$\begin{aligned} (f \cdot g)(x) &= a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \ldots + \\ &\quad (a_0 b_1 + a_1 b_0)x + a_0 b_0, \end{aligned}$$

odnosno

$$(f \cdot g)(x) = \sum_{k=0}^{m+n} c_k x^k, \text{gdje je } c_k = \sum_{i+j=k} a_i b_j.$$

Definicija 3.1.3. *Funkcija* $\deg : \mathbb{R}[x] \to \mathbb{N}_0$ *je funkcija koja polinomu pridružuje njegov stupanj.*

Neka su f i g dva polinoma različita od nulpolinoma. Funkcija deg tada ima sljedeća svojstva:

1. $\deg(f \cdot g) = \deg f + \deg g$
2. $\deg(f + g) \leq \max(\deg f, \deg g)$

3. deg($f \circ g$)=deg$f$·deg$g$

Ako je jedan od polinoma f i g nulpolinom, onda je njihov umnožak nulpolinom i njihova kompozicija nulpolinom. Prsten polinoma $\mathbb{R}[x]$ obzirom na zbrajanje i množenje je komutativan prsten s jedinicom. Ulogu jedinice ima konstantni polinom $e \in \mathbb{R}[x]$ definiran sa $e(x) = 1, \forall x \in \mathbb{R}$. Slično, skup svih polinoma s cjelobrojnim koeficijentima označavamo s $\mathbb{Z}[x]$ i zovemo prsten polinoma nad cijelim brojevima $\mathbb{Z}$, skup svih polinoma s racionalnim koeficijentima označavamo s $\mathbb{Q}[x]$ i zovemo prsten polinoma nad poljem racionalnih brojeva $\mathbb{Q}$ i skup svih polinoma s kompleksnim koeficijentima označavamo s $\mathbb{C}[x]$ i zovemo prsten polinoma nad poljem kompleksnih brojeva $\mathbb{C}$. No, mi ćemo se uglavnom baviti s $\mathbb{R}[x]$.

Definicija 3.1.4. *Polinomi $f, g : \mathbb{R} \to \mathbb{R}$ jednaki su ako vrijedi $f(x) = g(x)$ za svaki $x \in \mathbb{R}$.*

Da bismo karakterizirali jednakost polinoma pomoću njihovih koeficijenata, potreban nam je teorem o nulpolinomu.

Teorem 3.1.5 (Teorem o nulpolinomu)**.** *Polinom $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, za $a_0, a_1, \ldots, a_n \in \mathbb{R}$, jest nulpolinom ako i samo ako je $a_0 = a_1 = \ldots = a_n = 0$, tj. ako su mu svi koeficijenti jednaki nula.*

Dokaz ovog teorema je dio standardnog gradiva kolegija *Uvod u matematiku*. Zainteresirani čitatelj može ga pronaći u [12] i [18].

Iz prethodnog teorema se lako može dokazati i sljedeći teorem.

Teorem 3.1.6 (Teorem o jednakosti polinoma)**.** *Polinomi f i g zadani sa $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ i $g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$, $(f, g \neq 0)$ pri čemu je $a_n \neq 0$ i $b_m \neq 0$, jednaki su, tj. vrijedi*

$$f(x) = g(x), \forall x \in \mathbb{R},$$

ako i samo ako vrijedi $n = m$ i $a_n = b_m, \ldots, a_1 = b_1, a_0 = b_0$.

Dokaz ovog teorema je dio standardnog gradiva kolegija *Uvod u matematiku*. Zainteresirani čitatelj može ga pronaći u [12] i [18].

Primjer 3.1.7. *Koristeći teorem jednakosti polinoma odredimo polinom $f \in \mathbb{R}[x]$ ako je $f(x-2) = x^3 - 9x^2 + 28x - 29$.*

Rješenje: Uočimo najprije da polinom f mora biti kubni polinom, tj. polinom stupnja 3. Dakle, postoje $A, B, C, D \in \mathbb{R}$ takvi da je

$$f(x) = Ax^3 + Bx^2 + Cx + D.$$

Sada imamo

$$A(x-2)^3 + B(x-2)^2 + C(x-2) + D = x^3 - 9x^2 + 28x - 29,$$

odnosno

$$A(x^3 - 6x^2 + 12x - 8) + B(x^2 - 4x + 4) + C(x-2) + D = x^3 - 9x^2 + 28x - 29,$$

tj.

$$Ax^3 + (-6A + B)x^2 + (12A - 4B + C)x + (-8A + 4B - 2C + D) = x^3 - 9x^2 + 28x - 29.$$

Prema teoremu o jednakosti polinoma slijedi

$$\begin{aligned} A &= 1, \\ -6A + B &= -9, \\ 12A - 4B + C &= 28, \\ -8A + 4B - 2C + D &= -29. \end{aligned}$$

Rješavanjem gornjeg sustava jednadžbi dobivamo $A = 1, B = -3, C = 4$ i $D = -1$. Dakle, traženi polinom $f \in \mathbb{R}[x]$ je $f(x) = x^3 - 3x^2 + 4x - 1$.

3.2 Djeljivost polinoma

U ovom dijelu ćemo u prstenu polinoma $\mathbb{R}[x]$ uvesti pojam djeljivosti.

Definicija 3.2.1. *Kažemo da je polinom f djeljiv polinomom $g \neq 0$ ako postoji polinom h takav da za svaki $x \in \mathbb{R}$ vrijedi $f(x) = g(x) \cdot h(x)$. Tada je* $\deg f = \deg g + \deg h$.

Teorem 3.2.2 (Teorem o dijeljenju s ostatkom)**.** *Za svaka dva polinoma $f, g \in \mathbb{R}[x], g \neq 0$, postoje jedinstveni polinomi $q, r \in \mathbb{R}[x]$ takvi da je*

$$f(x) = g(x)q(x) + r(x), \forall x \in \mathbb{R},$$

pri čemu je $r = 0$ ili $\deg r < \deg g$.

Dokaz ovog teorema ćemo izostaviti jer je napravljen u sklopu kolegija *Uvod u matematiku*, a zainteresirani čitatelj može ga pronaći u [12] i [18].

Općenito, ako je $r \neq 0$, polinom q zove se *nepotpuni kvocijent polinoma* f i g, a polinom r *ostatak pri dijeljenju polinoma* f i g. Ako je $r = 0$, onda se q zove *kvocijent polinoma* f i g. Tada kažemo da je polinom f djeljiv polinomom g i pišemo $q = \frac{f}{g}$, a polinom g zovemo *mjera* polinoma f.

Teorem 3.2.3 (Teorem o najvećoj zajedničkoj mjeri)**.** *Za svaka dva polinoma $f, g \in \mathbb{R}[x]$, $f, g \neq 0$, postoji jedinstveno određena najveća zajednička mjera $M(f, g)$.*

Dokaz ovog teorema ćemo izostaviti jer je napravljen u sklopu kolegija *Uvod u matematiku*, a zainteresirani čitatelj može ga pronaći u [12] i [18].

Sljedeći teorem vrlo je koristan pri dijeljenju polinoma polinomom prvog stupnja.

Teorem 3.2.4 (Bèzoutov[1] teorem)**.** *Neka je $f(x) \in \mathbb{R}[x]$ i $\alpha \in \mathbb{R}$. Ostatak pri dijeljenju polinoma f s $x - \alpha$ iznosi $f(\alpha)$.*

Dokaz. Neka je $g(x) = x - \alpha$. Prema teoremu o dijeljenju s ostatkom postoje jedinstveni polinomi $q, r \in \mathbb{R}[x]$ pri čemu je r konstantni polinom, tj. $r(x) = c$, za svaki $x \in \mathbb{R}$, takvi da vrijedi:

$$f(x) = (x - \alpha)q(x) + r(x), \forall x \in \mathbb{R},$$

tj.

$$f(x) = (x - \alpha)q(x) + c, \forall x \in \mathbb{R}.$$

Kako ova jednakost vrijedi za svaki realan broj x, onda vrijedi i za $x = \alpha$. Tada je

$$f(\alpha) = c,$$

tj.

$$f(\alpha) = r(x).$$

Dakle, ostatak pri dijeljenju polinoma f s $x - \alpha$ jednak je $f(\alpha)$. □

Primjer 3.2.5. *Odredimo sve $a, b, c \in \mathbb{R}$ za koje je polinom $f(x) = 2x^4 + ax^2 + bx + c$ djeljiv polinomom $g(x) = x + 2$, a pri dijeljenju polinomom $q(x) = x^2 - 1$ daje ostatak $x + 2$.*

Rješenje: Prema Bèzoutovom teoremu slijedi

$$f(-2) = 32 + 4a - 2b + c = 0. \tag{3.2}$$

Kako polinom f pri dijeljenju polinomom q daje ostatak $x + 2$, onda prema teoremu o dijeljenju s ostatkom slijedi da postoji polinom p takav da je

$$f(x) = (x^2 - 1)p(x) + x + 2.$$

Uvrstimo nultočke 1 i -1 polinoma q u gornju jednakost i dobivamo

$$f(1) = 2 + a + b + c = 3 \tag{3.3}$$
$$f(-1) = 2 + a - b + c = 1. \tag{3.4}$$

[1] Ètienne Bèzout (1730.-1783.) - francuski matematičar

Uvažavanjem jednadžbi (3.2), (3.3) i (3.4) dobivamo sustav

$$\begin{cases} 32 + 4a - 2b + c = 0 \\ 2 + a + b + c = 3 \\ 2 + a - b + c = 1, \end{cases}$$

odakle slijedi $a = -10, b = 1$ i $c = 10$. Dakle, traženi polinom f je $f(x) = 2x^4 - 10x^2 + x + 10$.

3.3 Nultočke i faktorizacija polinoma

U ovom dijelu rada ćemo proučavati kompleksne polinome f, tj. $f \in \mathbb{C}[x]$. Sve što vrijedi za prsten polinoma s realnim koeficijentima, vrijedi i za prsten polinoma s kompleksnim koeficijentima.

Definicija 3.3.1. *Nultočka polinoma $f \in \mathbb{C}[x]$ je svaki kompleksni broj α za koji je $f(\alpha) = 0$. Ako je α realan broj, onda se α naziva realna nultočka, a ako je α kompleksan broj, onda se α naziva kompleksna nultočka. Ponekad se za nultočku polinoma kaže da je korijen polinoma.*

Teorem 3.3.2. *Broj $\alpha \in \mathbb{C}$ je nultočka polinoma $f(x) \in \mathbb{C}[x]$ ako i samo ako je polinom f djeljiv polinomom $g(x) = x - \alpha, g \in \mathbb{C}[x]$.*

Dokaz. Dokažimo prvi smjer naše tvrdnje, tj. ako je α nultočka polinoma f, onda je f djeljiv s $x - \alpha$. Prema Bèzoutovom teoremu, slijedi da je ostatak pri dijeljenju polinoma f s $x - \alpha$ jednak $f(\alpha)$. Budući da je α nultočka polinoma f, vrijedi $f(\alpha) = 0$. Dakle, postoji polinom q takav da je $f(x) = (x - \alpha)q(x)$.
Dokažimo sada obrnuti smjer naše tvrdnje, tj. ako je polinom f djeljiv s $x - \alpha$, onda je α nultočka polinoma f. Neka je f polinom djeljiv polinomom $g(x) = x - \alpha$. Tada, prema definiciji (3.2.1), postoji polinom q takav da je $f(x) = (x - \alpha)q(x)$. Kako ta jednakost vrijedi za svaki $x \in \mathbb{C}$, onda vrijedi i za $x = \alpha$. Slijedi da je $f(\alpha) = 0$, tj. α je nultočka polinoma f. □

Definicija 3.3.3. *Neka je $f \in \mathbb{C}[x]$, $f \neq 0$. Kažemo da je α nultočka kratnosti $k \in \mathbb{N}$ polinoma f ako je polinom f djeljiv polinomom $g(x) = (x - \alpha)^k$ i nije djeljiv polinomom $h(x) = (x - \alpha)^{k+1}$.*

Znamo da ne mora svaki realni polinom $f \in \mathbb{R}[x]$ imati realnu nultočku. Primjerice, polinom $f(x) = x^2 + 1$ nema realnu nultočku. No, svaki kompleksni polinom $f \in \mathbb{C}[x]$ ima kompleksnu nultočku. O tome govori *osnovni teorem algebre* koji je naziv, a time i pridjev *„osnovni”*, dobio u vrijeme kada je rješavanje algebarskih jednadžbi bilo glavni problem matematičara.

Teorem 3.3.4 (Osnovni teorem algebre)**.** *Svaki polinom $f(x) \in \mathbb{C}[x]$ stupnja $n \geq 1$ ima barem jednu nultočku u skupu kompleksnih brojeva.*

Neki matematičari osnovnim teoremom algebre smatraju sljedeći teorem.

Teorem 3.3.5 (Osnovni teorem algebre)**.** *Svaki polinom $f(x) \in \mathbb{C}[x]$ n-tog stupnja ima n nultočaka u skupu kompleksnih brojeva.*

Napomena 3.3.6. *Uočimo da egzistencija jedne nultočke prema Bèzoutovom teoremu povlači egzistenciju n nultočaka.*

Danas postoji mnogo različitih dokaza osnovnog teorema algebre. Dijelimo ih prema području matematike koje se koristi u dokazu na topološke, algebarske i analitičke dokaze. Topološki dokazi vežu se uz kompaktnost, analitički dokazi koriste kompleksnu analizu, a algebarski dokazi koriste Galoisovu teoriju ili zahtijevaju algebarska proširenja polja. Dva analitička dokaza napravili smo u sklopu kolegija *Kompleksna analiza*, a zainteresirani čitatelj može ih pronaći u [21]. Više različitih dokaza može se pronaći u [9]. Na kraju ovog poglavlja prezentirat ćemo jedan algebarski dokaz osnovnog teorema algebre, ali potreban nam je njegov iskaz za sljedeći važan teorem.

Teorem 3.3.7 (Teorem o faktorizaciji polinoma)**.** *Svaki polinom $f(x) \in \mathbb{C}[x]$ n-tog stupnja može se na jedinstven način prikazati u obliku produkta n linearnih faktora. Preciznije, ako je a_n vodeći koeficijent polinoma f, a $\alpha_1, \alpha_2, \ldots, \alpha_n$ nultočke od f, onda vrijedi*

$$f(x) = a_n(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n).$$

Dokaz ovog teorema preuzet je iz [18].

Dokaz. Prema osnovnom teoremu algebre, polinom f ima barem jednu nultočku. Neka je to α_1. Prema Bèzoutovom teoremu, polinom f djeljiv je polinomom $f_1(x) = x - \alpha_1$, tj. postoji polinom $q_1 \in \mathbb{C}[x]$ takav da vrijedi

$$f(x) = (x - \alpha_1)q_1(x).$$

Ako je q_1 konstantni polinom, onda je $q_1 = a_n$, a ako je q_1 barem prvog stupnja, onda zaključujemo, opet prema osnovnom teoremu algebre, da i polinom q_1 ima brem jednu nultočku. Prema Bèzoutovom teoremu postoji rastav:

$$q_1(x) = (x - \alpha_2)q_2(x).$$

Uvrstimo li q_1 u prethodnu jednakost, dobivamo

$$f(x) = (x - \alpha_1)(x - \alpha_2)q_2(x).$$

Ponavljanjem ovog postupka slijedi da se f može napisati kao produkt polinoma

$$f_1 = (x - \alpha_1), f_2 = (x - \alpha_2), \ldots, f_n = (x - \alpha_n) \cdot \beta, \text{ za neki } \beta \in \mathbb{C}.$$

Dakle, vrijedi

$$f(x) = \beta(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

odnosno, β je vodeći koeficijent polinoma f. Budući da je $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, prema teoremu o jednakosti polinoma slijedi da je $\beta = a_n$. Dakle, vrijedi

$$f(x) = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Time je dokazana egzistencija rastava. Dokažimo sada i jedinstvenost.
Pretpostavimo da postaje dva različita rastava polinoma f i neka su to

$$f(x) = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

i

$$f(x) = b_n(x - \beta_1)(x - \beta_2) \cdots (x - \beta_n).$$

Sada slijedi

$$a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = b_n(x - \beta_1)(x - \beta_2) \cdots (x - \beta_n).$$

Kada bi nultočka α_i bila različita od svih β_j, $i, j = 1, 2, \ldots, n$, onda bi uvrštavanjem $x = \alpha_i$ lijeva strana bila jednaka nuli, a desna različita od nule što je kontradikcija. Prema tome, svaka nultočka α_i jednaka je nekom β_j i obrnuto. Uočimo da je vodeći koeficijent polinoma f jednak a_n, odnosno b_n, zato vrijedi $a_n = b_n$. Potrebno je još provjeriti da ako je α_i k-struka nultočka polinoma $f(x) = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$, onda je i pripadni β_j k-struka nultočka polinoma $f(x) = b_n(x - \beta_1)(x - \beta_2) \cdots (x - \beta_n)$. Pretpostavimo suprotno, tj. da je α_i k-struka nultočka polinoma f, a pripadni β_j l-struka nultočka polinoma f. Tada je

$$a_n(x - \alpha_i)^k g(x) = b_n(x - \alpha_i)^l h(x),$$

gdje je g polinom stupnja $n - k$, a h polinom stupnja $n - l$, $g(\alpha_i) \neq 0, h(\alpha_i) \neq 0$. Kada bi vrijedilo $k > l$, onda bismo dijeljenjem gorne jednakosti sa $(x - \alpha_i)^l$ dobili jednakost

$$a_n(x - \alpha_i)^{k-l} g(x) = b_n h(x)$$

u kojoj je lijeva strana djeljiva s $x - \alpha_i$, a desna nije. Analogno, za $k < l$ dobivamo jednakost u kojoj je desna strana djeljiiva s $x - \alpha_i$, a lijeva nije. U svakom slučaju, dobivamo kontradikciju. Dakle, vrijedi $k = l$, čime je dokazana jedinstvenost rastava. □

Teorem 3.3.8. *Svaki polinom n-tog stupnja ima točno n nultočaka, računajući njihove kratnosti.*

Dokaz ovog teorema preuzet je iz [18].

Dokaz. Neka je f polinom stupnja n i neka su $\alpha_1, \alpha_2, \ldots, \alpha_p$ međusobno različite nultočke polinoma f, pri čemu je α_1 k_1-struka nultočka, α_2 k_2-struka nultočka, $\ldots, \alpha_p$ k_p-struka nultočka. Tada polinom f možemo zapisati u obliku

$$f(x) = a_n(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \cdots (x - \alpha_p)^{k_p},$$

pri čemu je $k_1 + k_2 + \ldots + k_p = n$. Dokazat ćemo da je svaki od brojeva $k_i, i = 1, 2, \ldots, p$, jednak kratnosti nultočke α_i.

Pretpostavimo da je kratnost nultočke α_i jednaka m_i. Tada je $k_i \leq m_i$. Kada bi vrijedilo $k_i < m_i$, imali bismo

$$f(x) = (x - \alpha_i)^{m_i}\varphi(x),$$

gdje $\varphi(\alpha_i) \neq 0$. Rastavimo li polinom φ na linearne faktore te zatim taj rastav uvrstimo u gornju jednakost, dobivamo rastav polinoma p različit od rastava

$$f(x) = a_n(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \cdots (x - \alpha_p)^{k_p},$$

što je u kontradikciji s jedinstvenošću faktorizacije. Prema tome, mora vrijediti $k_i = m_i$. □

Teorem 3.3.9. *Neka je $f \in \mathbb{C}[x]$ polinom zadan sa $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ i neka su $x_1, x_2, \ldots, x_n$ njegove nultočke. Tada vrijede* ***Vièteove formule****:*

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + \ldots + x_n = -\frac{a_{n-1}}{a_n} \\
\sigma_2 &= x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + x_2x_4 + \ldots + x_{n-1}x_n = \frac{a_{n-2}}{a_n} \\
\sigma_3 &= x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n = -\frac{a_{n-3}}{a_n} \\
&\vdots \\
\sigma_k &= x_1x_2 \cdots x_k + \ldots + x_{n-k+1}x_{n-k+2} \cdots x_n = (-1)^k\frac{a_{n-k}}{a_n} \\
&\vdots \\
\sigma_n &= x_1x_2 \cdots x_n = (-1)^n\frac{a_0}{a_n}.
\end{aligned}$$

Dokaz. Teorem ćemo dokazati matematičkom indukcijom po $n \in \mathbb{N}$. Dokažimo da tvrdnja vrijedi za polinom stupnja $n = 1$. Neka je $f_1 \in \mathbb{C}[x]$ polinom prvog stupnja oblika $f_1(x) = a_1x + a_0$ i neka je x_1 njegova nultočka. Tada je $\sigma_1 = x_1 = -\frac{a_0}{a_1}$. Dakle, tvrdnja teorema vrijedi za $n = 1$. Pretpostavimo da za neki $n \in \mathbb{N}$ vrijedi tvrdnja teorema, tj. da postoji polinom $f_n \in \mathbb{C}[x]$ n-tog stupnja oblika $f_n(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$ takav da su $x_1, x_2, \ldots, x_n$ njegove nultočke, tj. da vrijedi

$$\begin{aligned}
\sigma_1 &= -\frac{b_{n-1}}{b_n} \\
&\vdots \\
\sigma_k &= (-1)^k \frac{b_{n-k}}{b_n} \\
&\vdots \\
\sigma_n &= (-1)^n \frac{b_0}{b_n}.
\end{aligned}$$

Tvrdimo da za njegovog sljedbenika $n+1$ također vrijedi tvrdnja teorema. Neka je $f_{n+1} \in \mathbb{C}[x]$ polinom stupnja $n+1$ zadan s

$$f_{n+1}(x) = a_{n+1}x^{n+1} + a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

i neka su $x_1, x_2, \ldots, x_n, x_{n+1}$ njegove nultočke. Prema osnovnom teoremu algebre polinom f_{n+1} ima barem jednu nultočku x_{n+1}. Nadalje, prema (3.3.2) polinom f_{n+1} je djeljiv s $x - x_{n+1}$, tj. postoje $b_n, b_{n-1}, \ldots, b_1, b_0$ takvi da vrijedi

$$f_{n+1}(x) = (x - x_{n+1})(b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0),$$

tj.

$$a_{n+1}x^{n+1} + a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = (x - x_{n+1})(b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0).$$

Primjenom teorema o jednakosti polinoma na gornju jednakost slijedi:

$$\begin{aligned}
a_{n+1} &= b_n \\
a_n &= b_{n-1} - b_n x_{n+1} \\
&\vdots \\
a_{n-k+1} &= b_{n-k} - b_{n-k+1} x_{n+1} \\
&\vdots \\
a_1 &= b_0 - b_1 x_{n+1} \\
a_0 &= -b_0 x_{n+1},
\end{aligned}$$

odnosno

$$\begin{aligned}
b_n &= a_{n+1}\\
b_{n-1} &= a_n + b_n x_{n+1}\\
&\vdots\\
b_{n-k} &= a_{n-k+1} + b_{n-k+1}x_{n+1}\\
&\vdots\\
b_1 &= \frac{b_0 - a_1}{x_{n+1}}\\
b_0 &= -\frac{a_0}{x_{n+1}}.
\end{aligned}$$

Sada iz pretpostavke indukcije slijedi

$$x_1 + \ldots + x_{n+1} = \sigma_1 + x_{n+1} = -\frac{b_{n-1}}{b_n} + x_{n+1} = -\frac{a_n + a_{n+1}x_{n+1}}{a_{n+1}} + x_{n+1} = -\frac{a_n}{a_{n+1}}$$

$$\vdots$$

$$\begin{aligned}
x_1x_2\cdots x_k &+ x_{n-k+1}\cdots x_n + x_1\cdots x_{k-1}x_{n+1} + \ldots + x_{n-k+2}\cdots x_n x_{n+1}\\
&= \sigma_k + x_{n+1}\sigma_{k-1}\\
&= (-1)^{k+1}\frac{b_{n-k}}{b_n} + (-1)^k\frac{b_{n-k+1}}{b_n}x_{n+1}\\
&= \frac{(-1)^{k+1}(a_{n-k+1} + b_{n-k+1}x_{n+1}) + (-1)^k x_{n+1}b_{n-k+1}}{b_n}\\
&= (-1)^{k+1}\frac{a_{n-k+1}}{a_{n+1}}
\end{aligned}$$

$$\vdots$$

$$x_1\cdots x_{n+1} = \sigma_n x_{n+1} = (-1)^n\frac{b_0}{b_n}x_{n+1} = (-1)^n\frac{\frac{-a_0}{x_{n+1}}}{a_{n+1}}x_{n+1} = (-1)^{n+1}\frac{a_0}{a_{n+1}}.$$

Time smo dokazali da Vièteove fromule vrijede i za polinom stupnja $n+1$.

Budući da tvrdnja vrijedi za $n = 1$ te iz pretpostavke da tvrdnja vrijedi za neki $n \in \mathbb{N}$ slijedi da ona vrijedi i za njegovog sljedbenika $n+1$, primjenom aksioma matematičke indukcije slijedi da tvrdnja vrijedi za svaki $n \in \mathbb{N}$.

□

Primjer 3.3.10. *Odredimo koeficijent k polinoma $p(x) = x^3 - 9x + k$ tako da polinom p ima dvije nultočke koje su suprotni brojevi, a zatim odredimo sve tri nultočke.*

Rješenje: Vièteove formule za kubne polinome, tj. polinome oblika $p(x) = ax^3 + bx^2 + cx + d$ glase:

$$\begin{aligned} x_1 + x_2 + x_3 &= -\frac{b}{a} \\ x_1x_2 + x_2x_3 + x_3x_1 &= \frac{c}{a} \\ x_1x_2x_3 &= -\frac{d}{a}, \end{aligned}$$

gdje su x_1, x_2 i x_3 nultočke tog polinoma. S obzirom da polinom p ima dvije nultočke koje su suprotni brojevi, uzmimo da je $x_2 = -x_1$. Tada za zadani polinom p prema Vièteovim fromulama vrijedi:

$$\begin{aligned} x_1 - x_1 + x_3 &= -\frac{0}{1} \\ x_1(-x_1) - x_1x_3 + x_3x_1 &= -\frac{9}{1} \\ x_1(-x_1)x_3 &= -\frac{k}{1}, \end{aligned}$$

odnosno

$$\begin{aligned} x_3 &= 0 \\ x_1^2 &= 9 \\ x_1^2x_3 &= k. \end{aligned}$$

Dakle, nultočke zadanog polinoma su $x_1 = 3, x_2 = -3$ i $x_3 = 0$. Uvrštavanjem vrijednosti nultočaka u $x_1^2x_3 = k$ slijedi $k = 0$. Konačno, traženi polinom p je oblika $p(x) = x^3 - 9x$.

3.4 Svojstva nultočaka polinoma

Iako najčešće određujemo realne nultočke polinoma iz $\mathbb{R}[x]$, postoje teoremi koji nam olakšavaju određivanje cjelobrojnih, racionalnih i kompleksnih nultočaka nekih polinoma.

Teorem 3.4.1. *Neka je $f \in \mathbb{Z}[x]\backslash\{0\}$ polinom oblika $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$. Ako je $\alpha \neq 0$ cjelobrojna nultočka tog polinoma, onda je α djelitelj slobodnog člana polinoma f.*

Dokaz. Neka je $\alpha \in \mathbb{Z}$, $\alpha \neq 0$, nultočka polinoma f. Tada vrijedi:

$$f(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0,$$

tj.

$$a_0 = -\alpha(a_n\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a_1),$$

odnosno

$$\frac{a_0}{\alpha} = -(a_n\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a_1).$$

Kako su $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}$ i $\alpha \in \mathbb{Z}$, slijedi da je izraz na desnoj strani jednadžbe cijeli broj. Zato i izraz na lijevoj strani mora biti cijeli broj, tj. mora vrijediti $\frac{a_0}{\alpha} \in \mathbb{Z}$. Dakle, α je djeljitelj od a_0. □

Teorem 3.4.2. *Neka je $f \in \mathbb{Z}[x]\backslash\{0\}$ polinom dan s $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$. Ako je $\alpha = \frac{p}{q}, p, q \in \mathbb{Z}$ relativno prosti, $q \neq 0$, racionalna nultočka tog polinoma, onda je p djelitelj slobodnog člana i q djelitelj vodećeg koeficijenta polinoma f.*

Dokaz. Neka je $\alpha = \frac{p}{q}$ nultočka polinoma f. Tada vrijedi:

$$f\left(\frac{p}{q}\right) = a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + a_1\left(\frac{p}{q}\right) + a_0 = 0.$$

Množenjem gornje jednadžbe s q^n dobivamo

$$a_np^n + a_{n-1}p^{n-1}q + \ldots + a_1pq^{n-1} + a_0q^n = 0, \tag{3.5}$$

odnosno

$$a_0q^n = -p(a_np^{n-1} + a_{n-1}p^{n-2}q + \ldots + a_1q^{n-1}).$$

Ako je $p = 0$, onda je $\alpha = 0$ nultočka polinoma f. Tada je $a_0 = 0$ jer je $q \neq 0$. Ako je $p \neq 0$ onda gornju jednadžbu možemo podijeliti s p i time dobivamo

$$\frac{a_0q^n}{p} = -(a_np^{n-1} + a_{n-1}p^{n-2}q + \ldots + a_1q^{n-1}).$$

Kako su $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}$ i $p, q \in \mathbb{Z}$, slijedi da je izraz na desnoj strani jednadžbe cijeli broj. Zato i izraz na lijevoj strani mora biti cijeli broj, tj. mora vrijediti $\frac{a_0q^n}{p} \in \mathbb{Z}$, odnosno p mora biti djeljitelj od a_0q^n. Budući da su p i q relativno prosti, slijedi da je p djelitelj slobodnog člana a_0. Primijetimo da jednadžbu (3.5) možemo zapisati kao

$$a_np^n = -q(a_{n-1}p^{n-1} + \ldots + a_1pq^{n-2} + a_0q^{n-1}),$$

iz čega analogno slijedi da je q djelitelj vodećeg koeficijenta a_n. □

Teorem 3.4.3. *Neka je $f \in \mathbb{R}[x]\backslash\{0\}$ polinom dan s $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$. Ako je $z = a + bi, a, b \in \mathbb{R}, b \neq 0$ kompleksna nultočka tog polinoma, onda je $\overline{z} = a - bi$ također nultočka polinoma f.*

Dokaz. Neka je $g(x) = (x - z)(x - \overline{z})$. Tada vrijedi

$$\begin{aligned} g(x) = (x - z)(x - \overline{z}) &= x^2 - (z + \overline{z})x + z\overline{z} \\ &= x^2 - (a + bi + a - bi)x + (a + bi)(a - bi) \\ &= x^2 - 2ax + a^2 + b^2. \end{aligned}$$

Kako su $a, b \in \mathbb{R}$, slijedi da je $g \in \mathbb{R}[x]$. Podijelimo li polinom f polinomom g, prema teoremu o dijeljenju s ostatkom slijedi

$$f(x) = (x - z)(x - \overline{z})q(x) + r(x), \text{ pri čemu je } \deg r < \deg g.$$

Budući da su f i g iz $\mathbb{R}[x]$, slijedi da su i q i r iz $\mathbb{R}[x]$. Znamo da je $\deg g = 2$, zato slijedi da je $\deg r \leq 1$. Neka je $r(x) = Ax + B, A, B \in \mathbb{R}$. Za svaki $x \in \mathbb{C}$ vrijedi:

$$f(x) = (x - z)(x - \overline{z})q(x) + Ax + B.$$

Dakle, gornja jednakost vrijedi i za $x = z$. Imamo

$$f(z) = Az + B = 0.$$

Uvrstimo li $z = a + bi$ u gornju jednadžbu, dobivamo

$$Aa + B + Abi = 0.$$

Da bi gornja jednakost vrijedila, i realni i imaginarni dio moraju biti jednaki nuli. Dakle, rješavamo sustav

$$\begin{cases} Aa + B = 0 \\ Ab = 0. \end{cases}$$

Kako je $b \neq 0$, slijedi da je $A = 0$ iz čega slijedi da je i $B = 0$. Dakle, vrijedi $r(x) = 0$ i

$$f(x) = (x - z)(x - \overline{z})q(x),$$

odakle slijedi

$$f(\overline{z}) = 0.$$

Dakle, $\overline{z}$ je nultočka polinoma f. □

3.5 Hornerov algoritam i Taylorov razvoj polinoma

Hornerov[2] algoritam

Hornerov algoritam je efikasna metoda određivanja vrijednosti polinoma u nekoj točki i dijeljenja polinoma polinomom prvog stupnja. Metoda je korisna i za rastav polinoma po potencijama. Cijeli postupak temelji se na metodi neodređenih koeficijenata. Neka je $f \in \mathbb{R}[x]$ zadan s $f(x) = a_n x^n + \ldots + a_1 x + a_0$, $a_n \neq 0$ i neka je $\alpha \in \mathbb{R}$. Prema Bèzoutovom teoremu ostatak pri dijeljenju polinoma f s $x - \alpha$ jednak je $f(\alpha)$, stoga polinom f možemo zapisati kao

$$f(x) = (x - \alpha)q(x) + f(\alpha). \tag{3.6}$$

Želimo odrediti $q(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$, gdje su $b_m, \ldots, b_0$ nepoznati koeficijenti. Otuda dolazi naziv **metoda neodređenih koeficijenata**. Uvrštavanjem $f(x)$ i $q(x)$ u (3.6) dobivamo:

$$\begin{aligned} a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 &= (x - \alpha)(b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0) + f(\alpha) \\ &= b_m x^{m+1} + (b_{m-1} - \alpha b_m) x^m + \ldots + (b_0 - \alpha b_1) x + (f(\alpha) - \alpha b_0). \end{aligned}$$

Prema teoremu o jednakosti polinoma slijedi da je $n = m + 1$, tj. $m = n - 1$, i

$$\begin{aligned} a_n &= b_m & &\Longrightarrow & b_{n-1} &= a_n \\ a_{n-1} &= b_{m-1} - \alpha b_m & &\Longrightarrow & b_{n-2} &= \alpha b_{n-1} + a_{n-1} \\ &\vdots & & & &\vdots \\ a_1 &= b_0 - \alpha b_1 & &\Longrightarrow & b_0 &= \alpha b_1 + a_1 \\ a_0 &= f(\alpha) - \alpha b_0 & &\Longrightarrow & f(\alpha) &= \alpha b_0 + a_0 \end{aligned}$$

Sada možemo lako odrediti koeficijente polinoma q iz niza jednakosti na desnoj strani, računajući vrijednosti redom odozgo prema dolje. **Hornerov algoritam** jest upravo taj niz jednakosti smješten u tablicu:

	a_n	a_{n-1}	a_{n-2}	$\ldots$	a_1	a_0
α	a_n	$\alpha b_{n-1} + a_{n-1}$	$\alpha b_{n-2} + a_{n-2}$	$\ldots$	$\alpha b_1 + a_1$	$\alpha b_0 + a_0$

Uočimo da Hornerov algoritam možemo koristiti i za dijeljenje polinoma polinomom prvog stupnja. Dakle, dijeljenjem polinoma $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ polinomom

[2] William George Horner (1786.-1837.) - britanski matematičar po kojem je algoritam dobio ime. Iako je metoda nazvana po njemu, a sam Horner ju je pripisao Joseph-Louisu Lagrangeu, kineski i perzijski matematičari su je koristili još u srednjem vijeku, stoljećima prije njih.

prvog stupnja $x - \alpha$ dobit ćemo polinom $q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + b_{n-3}x^{n-3} + \ldots + b_0$ i ostatak $f(\alpha)$.

Primjer 3.5.1. *Koristeći Hornerov algoritam, odredimo (nepotpuni) kvocijent i ostatak pri dijeljenju polinoma f polinomom g ako je $f(x) = 2x^3 - 4x^2 + 5x - 7$ i $g(x) = x - 2$.*

Rješenje: Najprije odredimo α:

$$x - \alpha = x - 2 \Longrightarrow \alpha = 2.$$

Sada računamo tražene vrijednosti koristeći Hornerov algoritam:

	2	-4	5	7
2	2	$2 \cdot 2 + (-4) = 0$	$2 \cdot 0 + 5 = 5$	$2 \cdot 5 + 7 = 17$

Dakle, slijedi $q(x) = 2x^2 + 5$ i $f(2) = 17$, odnosno

$$f(x) = (x - 2)(2x^2 + 5) + 17.$$

Taylorov[3] razvoj polinoma

Neka je $f \in \mathbb{R}[x]$ polinom zadan s $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $a_n \neq 0$ i neka je $\alpha \in \mathbb{R}$. Rastaviti polinom f po potencijama od $x - \alpha$ znači prikazati ga u obliku

$$f(x) = A_n(x - \alpha)^n + A_{n-1}(x - \alpha)^{n-1} + \ldots + A_1(x - \alpha) + A_0,$$

gdje su $A_n, \ldots, A_1, A_0 \in \mathbb{R}$. O tome govori sljedeći teorem.

Teorem 3.5.2 (Taylorov razvoj polinoma oko točke $\alpha \in \mathbb{R}$)**.** *Neka je $\alpha \in \mathbb{R}$. Tada za svaki polinom $f \in \mathbb{R}[x]$ zadan s $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $a_n \neq 0$ postoje jedinstveni*

$$A_0, A_1, \ldots, A_n \in \mathbb{R}$$

takvi da vrijedi

$$f(x) = A_n(x - \alpha)^n + A_{n-1}(x - \alpha)^{n-1} + \ldots + A_1(x - \alpha) + A_0.$$

Tada je $A_n = a_n$ i $A_0 = f(\alpha)$.

[3] Brook Taylor (1685.-1731.) - engleski matematičar

Dokaz ovog teorema je napravljen u sklopu kolegija *Uvod u matematiku*, a zainteresirani čitatelj može ga pronaći u [12].

Rastav polinoma po potencijama možemo odrediti uzastopnom primjenom teorema o dijeljenju s ostatkom, ali i uzastopnom primjenom Hornerovog algoritma, što je brže i efikasnije. Pokazat ćemo oba načina u sljedećem primjeru.

Primjer 3.5.3. *Rastavimo polinom* $f(x) = x^4 - 2x^3 - 4x^2 + 10x$ *po potencijama od* $x - 1$.

Rješenje:
<u>1. način</u>: Uzastopnom primjenom teorema o djeljenju s ostatkom slijedi:

$$\begin{aligned} f(x) = x^4 - 2x^3 - 4x^2 + 10x &= (x-1)(x^3 - x^2 - 5x + 5) + 5 \\ &= (x-1)[(x-1)(x^2-5)] + 5 \\ &= (x-1)\{(x-1)[(x-1)(x+1) - 4]\} + 5 \\ &= (x-1)^4 + 2(x-1)^3 - 4(x-1)^2 + 5. \end{aligned}$$

<u>2. način</u>: Uzastopnom primjenom Hornerovog algoritma:

	1	-2	-4	10	0
1	1	-1	-5	5	$\boxed{A_0 = 5}$
1	1	0	-5	$\boxed{A_1 = 0}$	
1	1	1	$\boxed{A_2 = -4}$		
1	1	$\boxed{A_3 = 2}$			
1	$\boxed{A_4 = 1}$				

Poslijednji brojevi svakog retka su traženi koeficijenti uz potencije, redom od najmanje do najveće. Traženo rješenje je:

$$f(x) = 5 \cdot (x-1)^0 + 0 \cdot (x-1)^1 + (-4) \cdot (x-1)^2 + 2 \cdot (x-1)^3 + 1 \cdot (x-1)^4,$$

tj.

$$f(x) = (x-1)^4 + 2(x-1)^3 - 4(x-1)^2 + 5.$$

3.6 Simetrični polinomi

Simetrični polinomi posebna su vrsta polinoma dviju ili više varijabli. Definirat ćemo polinome dviju varijabli, a zatim simetrične polinome dviju varijabli i prezentirati nekoliko primjera. Na kraju ćemo definirati simetrične polinome n varijabli i za njih iskazati osnovni teorem o simetričnim polinomima.

Definicija 3.6.1. *Svako preslikavanje $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ zadano s*

$$f(x, y) = f_0(x) + f_1(x)y + f_2(x)y^2 + \ldots + f_n(x)y^n, (x, y) \in \mathbb{R} \times \mathbb{R}, \tag{3.7}$$

*gdje su $f_0, f_1, f_2, \ldots, f_n$ polinomi jedne varijable (x), zove se **polinom dviju varijabli** (nad $\mathbb{R}$).*

Svaki polinom oblika (3.7) može se zapisati u obliku:

$$f(x, y) = g_0(y) + g_1(y)x + g_2(y)x^2 + \ldots + g_m(y)x^m, (x, y) \in \mathbb{R} \times \mathbb{R}, \tag{3.8}$$

gdje su $g_0, g_1, g_2, \ldots, g_m$ polinomi jedne varijable (y).

Primjer 3.6.2. *Preslikavanje zadano formulom*

$$f(x, y) = x^5y^3 - x^3y^2 + 4x^2y^4 + x - 2y^5 + y^3 - 1$$

je polinom dvije varijabli. Zapišimo ga u oblicima (3.7) *i* (3.8)*.*

Rješenje: Zapišimo $f(x, y)$ po rastućim potencijama od y:

$$f(x, y) = x - 1 - x^3y^2 + (1 + x^5)y^3 + 4x^2y^4 - 2y^5,$$

slijedi

$$f_0(x) = x - 1,\ f_1(x) = 0,\ f_2(x) = -x^3,\ f_3(x) = 1 + x^5,\ f_4(x) = 4x^2,\ f_5(x) = -2.$$

Dakle, pokazali smo da se polinom f može zapisati u obliku (3.7). Zapišimo sada polinom f po rastućim potencijama od x:

$$f(x, y) = -2y^5 + y^3 - 1 + x + 4x^2y^4 - x^3y^2 + x^5y^3,$$

slijedi

$$g_0(y) = -2y^5 + y^3 - 1,\ g_1(y) = 1,\ g_2(y) = 4y^4,\ g_3(y) = -y^2,\ g_4(y) = 0,\ g_5(y) = y^3.$$

Dakle, pokazali smo da se polinom f može zapisati i u obliku (3.8). Time smo pokazali da je polinom f polinom dviju varijabli.

Preslikavanje $f(x, y) = ax^my^n$ je također polinom dviju varijabli koji se zove monom, a broj $a \in \mathbb{R}$ zovemo njegovim koeficijentom. Svaki je polinom dviju varijabli jednak zbroju svojih monoma. Monom ax^my^n ima stupanj m u varijabli x i stupanj n u varijabli y. Stupanj polinoma dviju varijabli je jednak maksimalnom stupnju njegovih monoma, a stupanj monoma $f(x, y) = ax^my^n$ jednak je $m + n$.

Primjer 3.6.3. *Odredimo stupanj polinoma*

$$f(x,y) = x^4y^3 - x^3y^2 + x^2y^5 - xy^4 + 2.$$

Rješenje: Polinom f je suma pet monoma od kojih je jedan konstanta, stoga vrijedi $\deg f = \max\{4+3, 3+2, 2+5, 1+4, 0\} = \max\{7,5,7,5,0\} = 7$. Dakle, stupanj polinom f jednak je 7.

Analogno kao kod polinoma u jednoj varijabli, konstantni polinom je polinom oblika $f(x,y) = a$, gdje je a neki realan broj, a polinom oblika $f(x,y) = 0$, za sve $x, y \in \mathbb{R}$ zovemo nulpolinomom. Skup svih polinoma dviju varijabli s realnim koeficijentima označavamo s $\mathbb{R}[x,y]$. U taj skup možemo uvesti operacije zbrajanja i množenja, a definiramo ih kao zbrajanje i množenje funkcija na sljedeći način:

$$(f+g)(x,y) = f(x,y) + g(x,y),\ (x,y) \in \mathbb{R} \times \mathbb{R}$$

i

$$(f \cdot g)(x,y) = f(x,y) \cdot g(x,y),\ (x,y) \in \mathbb{R} \times \mathbb{R}.$$

Odnosno, polinomi dviju varijabli se zbrajaju tako da se zbroje njihovi istoimeni monomi pa je zbroj dvaju polinoma opet polinom. Također, polinomi dviju varijabli se množe tako da se svaki član jednog polinoma pomnoži sa svakim članom drugoga, a zatim zbroje dobiveni umnošci. Tako dobiveni zbroj je ponovno polinom.

Lako se pokaže, kao i kod polinoma jedne varijable, da je $\mathbb{R}[x,y]$, s obzirom na operacije zbrajanja i množenja, komutativni prsten s jedinicom. Jedinica u prstenu je konstantni polinom $f(x,y) = 1$, za sve $x, y \in \mathbb{R}$. Također, možemo promatrati i prstene $\mathbb{Z}[x,y]$, $\mathbb{Q}[x,y]$, $\mathbb{C}[x,y]$ i $P[x,y]$, gdje je P bilo koji komutativni prsten s jedinicom.

Najvažniji polinomi dviju (ili više varijabli) su simetrični polinomi. Važni su za linearnu algebru, teoriju reprezentacija i Galoisovu teoriju, ali i u kombinatorici, gdje se uglavnom proučavaju kroz prsten simetričnih funkcija.

Definicija 3.6.4. *Polinom $f \in \mathbb{R}[x,y]$ zove se* ***simetrični polinom****, ako za sve $x, y \in \mathbb{R}$ vrijedi*

$$f(x,y) = f(y,x).$$

Drugim riječima, polinom je simetričan ako je invarijantan s obzirom na permutaciju unosa, tj. ako se on ne mijenja kada zamijenimo x i y.

Na primjer, polinom $f(x,y) = x^2y^3 + x^3y^2 + 1$ je simetričan polinom jer je

$$f(y,x) = y^2x^3 + y^3x^2 + 1 = f(x,y).$$

U skupu svih simetričnih polinoma ističu se ova dva jednostavna polinoma:

$$f(x, y) = x + y, \ g(x, y) = xy.$$

Ti polinomi imaju važnu ulogu u teoriji simetričnih polinoma, stoga imaju posebno ime i oznaku.

Definicija 3.6.5. *Polinomi $\sigma_1(x, y) = x + y$ i $\sigma_2(x, y) = xy$ zovu se **osnovni (elementarni) simetrični polinomi**.*

Osim elementarnih polinoma, u teoriji simetričnih polinoma susrećemo se i s polinomima $s_1(x, y) = x + y, s_2(x, y) = x^2 + y^2, s_3(x, y) = x^3 + y^3, \ldots$, općenito, $s_k(x, y) = x^k + y^k, k \in \mathbb{N}$. Te polinome zovemo **Newtonovim polinomima** i kraće ih označavamo sa $s_1, s_2, \ldots, s_k$. Ponekad se zovu još i **zbrojevi** ili **sume potencija**. Postoji jednostavan način kojim možemo dobiti simetrični polinom od bilo kojeg polinoma u varijablama σ_1 i σ_2. Na primjer:

$$f(\sigma_1, \sigma_2) = \sigma_1^2 - \sigma_1\sigma_2.$$

Izrazimo sada σ_1 i σ_2 pomoću x i y:

$$\begin{aligned} g(x, y) &= (x + y)^2 - (x + y)xy \\ &= x^2 + 2xy + y^2 - x^2y - xy^2. \end{aligned}$$

Primijetimo da je dobiveni polinom g zaista simetričan, vrijedi:

$$g(y, x) = y^2 + 2yx + x^2 - y^2x - yx^2 = g(x, y).$$

Postavlja se pitanje možemo li svaki simetrični polinom $g(x, y)$ zapisati u obliku polinoma $f(\sigma_1, \sigma_2)$. Pogledajmo prvo možemo li Newtonove polinome s_1, s_2 i s_3 zapisati kao polinome u varijablama σ_1 i σ_2. Imamo redom:

$$\begin{aligned} s_1(x, y) &= x + y \\ &= \sigma_1, \end{aligned}$$

$$\begin{aligned} s_2(x, y) &= x^2 + y^2 \\ &= (x + y)^2 - 2xy \\ &= \sigma_1^2 - 2\sigma_2, \end{aligned}$$

$$\begin{aligned} s_3(x, y) &= x^3 + y^3 \\ &= (x + y)^3 - 3x^2y - 3xy^2 \\ &= (x + y)^3 - 3xy(x + y) \\ &= \sigma_1^3 - 3\sigma_1\sigma_2. \end{aligned}$$

Dokažimo sada da svaki Newtonov polinom možemo zapisati kao polinom u varijablama σ_1 i σ_2. O tome nam govori sljedeća lema.

Lema 3.6.6. *Za sve prirodne brojeve $k > 2$ vrijedi Newtonova formula:*

$$s_k = \sigma_1 s_{k-1} - \sigma_2 s_{k-2}.$$

Dokaz. Prema definiciji Newtonovih polinoma, za svaki prirodan broj $k > 2$ vrijedi:

$$s_{k-1} = x^{k-1} + y^{k-1}.$$

Množenjem gornje jednakosti sa $\sigma_1 = x + y$ dobivamo:

$$\begin{aligned} s_{k-1}\sigma_1 &= (x^{k-1} + y^{k-1})\sigma_1 \\ &= x^k + xy^{k-1} + x^{k-1}y + y^k \\ &= x^k + y^k + xy(x^{k-2} + y^{k-2}) \\ &= s_k + \sigma_2 s_{k-2}, \end{aligned}$$

odnosno vrijedi $s_k = \sigma_1 s_{k-1} - \sigma_2 s_{k-2}$, što smo i htjeli pokazati. □

Da bismo dokazali da se svaki simetrični polinom može zapisati kao polinom u varijablama σ_1 i σ_2, potrebna nam je sljedeća lema.

Lema 3.6.7. *Za svaki Newtonov polinom s_k postoji polinom $f \in \mathbb{R}[x, y]$ takav da vrijedi*

$$s_k(x, y) = f(\sigma_1, \sigma_2), \text{ tj. } s_k(x, y) = f(x + y, xy)$$

Dokaz. Tvrdnju dokazujemo indukcijom. Tvrdnja je istinita za $k = 1$ i $k = 2$. Pokazali smo da vrijedi $s_1 = \sigma_1$ i $s_2 = \sigma_1^2 - 2\sigma_2$. Pretpostavimo da je tvrdnja istinita za polinome s_{k-1} i s_{k-2}, za neki $k > 2$, tj. da postoje polinomi $f_1, f_2 \in \mathbb{R}[x, y]$ takvi da vrijedi:

$$s_{k-1} = f_1(\sigma_1, \sigma_2), s_{k-2} = f_2(\sigma_1, \sigma_2).$$

Prema Newtonovoj formuli imamo

$$s_k = \sigma_1 s_{k-1} - \sigma_2 s_{k-2}$$

pa po pretpostavci indukcije dobivamo

$$s_k = \sigma_1 f_1(\sigma_1, \sigma_2) - \sigma_2 f_2(\sigma_1, \sigma_2).$$

Time smo dokazali da tvrdnja vrijedi za svaki $k \in \mathbb{N}$. Dakle, svaki polinom s_k može se napisati u obliku polinoma u varijablama σ_1 i σ_2. □

Teorem 3.6.8 (Osnovni teorem o simetričnim polinomima dviju varijabli)**.** *Za svaki simetrični polinom $f \in \mathbb{R}[x, y]$ postoji jedinstveni polinom $h \in \mathbb{R}[x, y]$ takav da vrijedi*

$$f(x, y) = h(\sigma_1, \sigma_2).$$

Dokaz. Svaki polinom dviju varijabli je zbroj monoma oblika $ax^m y^n$. Monomi mogu biti oblika $ax^m y^n$, gdje je $m \neq n$ ili oblika $bx^m y^m$. Ako u zadanom simetričnom polinomu f postoji monom oblika $bx^m y^m$, onda vrijedi:

$$bx^m y^m = b(xy)^m = b\sigma_2^m.$$

Ako u polinomu f postoji član oblika $ax^m y^n$, gdje je $m \neq n$, onda postoji i član oblika $ax^n y^m$ jer u suprotnom polinom f ne bi bio simetrični polinom. Prema tome, polinom f kao pribrojnik sadrži polinom

$$h(x, y) = a(x^m y^n + x^n y^m).$$

Bez smanjenja općenitosti možemo pretpostaviti da vrijedi $m < n$. Tada imamo:

$$h(x, y) = ax^m y^m (x^{n-m} + y^{n-m}) = a(xy)^m s_{n-m} = a\sigma_2^m s_{n-m}.$$

Prema (3.6.7) slijedi da se polinom s_{n-m} može napisati u obliku polinoma s varijablama σ_1 i σ_2 čime je teorem dokazan. □

Uočimo da nam dokaz ove leme daje i postupak kojim zadani simetrični polinom možemo napisati u obliku polinoma s varijablama σ_1 i σ_2. Slijedi primjer.

Primjer 3.6.9. *Napišimo polinom f zadan s*

$$f(x, y) = x^3 + 4x^2 y + 5xy^3 + 4xy^2 + 5x^3 y + y^3$$

u obliku polinoma s varijablama σ_1 i σ_2.

Rješenje: Najprije članove zadanog polinoma f grupiramo na sljedeći način:

$$f(x, y) = (x^3 + y^3) + 4(x^2 y + xy^2) + 5(xy^3 + x^3 y).$$

Sada slijedi:

$$\begin{aligned}
f(x, y) &= [(x + y)^3 - 3x^2 y - 3xy^2] + 4[xy(x + y)] + 5[xy(y^2 + x^2)] \\
&= [(x + y)^3 - 3xy(x + y)] + 4[xy(x + y)] + 5\{xy[(x + y)^2 - 2xy]\}) \\
&= \sigma_1^3 - 3\sigma_2\sigma_1 + 4\sigma_2\sigma_1 + 5\sigma_2(\sigma_1^2 - 2\sigma_2) \\
&= \sigma_1^3 + \sigma_1\sigma_2 + 5\sigma_2\sigma_1^2 - 10\sigma_2^2 \\
&= \sigma_1^3 - 10\sigma_2^2 + \sigma_1\sigma_2 + 5\sigma_1^2\sigma_2.
\end{aligned}$$

Dakle, vrijedi $f(x, y) = h(\sigma_1, \sigma_2) = \sigma_1^3 - 10\sigma_2^2 + \sigma_1\sigma_2 + 5\sigma_1^2\sigma_2$.

Za dokaz osnovnog teorema algebre potreban nam je osnovni teorem o simetričnim polinomima n varijabli.

Definicija 3.6.10. *Polinom f je polinom n varijabli nad $P \in \{\mathbb{R}, \mathbb{C}\}$ ako je element prstena $P[x_1, x_2, \ldots, x_n]$.*

Definicija 3.6.11. *Polinom $f \in P[x_1, x_2, \ldots, x_n]$ je simetričan ako vrijedi*

$$f(x_1, x_2, \ldots, x_n) = f(p(x_1), p(x_2), \ldots, p(x_n)),$$

za svaku permutaciju $p : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Kao i kod polinoma dviju varijabli, važnu ulogu imaju elementarni simetrični polinomi $\sigma_1, \sigma_2, \ldots, \sigma_n$, zadani s

$$\begin{aligned}
\sigma_1(x_1, x_2, \ldots, x_n) &= x_1 + x_2 + \ldots + x_n,\\
\sigma_2(x_1, x_2, \ldots, x_n) &= x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n,\\
&\vdots\\
\sigma_n(x_1, x_2, \ldots, x_n) &= x_1x_2 \cdots x_n.
\end{aligned}$$

Teorem 3.6.12 (Osnovni teorem o simetričnim polinomima n varijabli)**.** *Za svaki simetrični polinom $f \in \mathbb{R}[x_1, x_2, \ldots, x_n]$ postoji jedinstveni polinom $h \in \mathbb{R}[x_1, x_2, \ldots, x_n]$ takav da vrijedi*

$$f(x_1, x_2, \ldots, x_n) = h(\sigma_1, \sigma_2, \ldots, \sigma_n),$$

gdje su $\sigma_1, \sigma_2, \ldots, \sigma_n$ elementarni simetrični polinomi.

Dokaz ovog teorema može se pronaći u [18].

3.7 Algebarski dokaz osnovnog teorema algebre

U ovom poglavlju ćemo dokazati teorem (3.3.4), no za taj dokaz nam je potreban jedan teorem iz matematičke analize.

Teorem 3.7.1 (Teorem srednje vrijednosti)**.** *Neka je $f : [a, b] \to \mathbb{R}$ neprekidna funkcija. Ako postoji realan broj k takav da vrijedi $min\{f(a), f(b)\} < k < max\{f(a), f(b)\}$, onda postoji $c \in \langle a, b\rangle$ takav da je $f(c) = k$.*

Dokaz ovog teorema može se pronaći u [10]. Posljedica teorema srednje vrijednosti je sljedeći korolar.

Korolar 3.7.2. *Neka je $f : [a, b] \to \mathbb{R}$ neprekidna funkcija takva da vrijedi $f(a)f(b) < 0$. Tada postoji $c \in \langle a, b\rangle$ takav da je $f(c) = 0$.*

Posljedica ovog korolara su sljedeće dvije leme koje su nam potrebne za dokaz osnovnog teorema algebre.

Lema 3.7.3. *Svaki kvadratni polinom $f \in \mathbb{C}[x]$ ima kompleksnu nultočku.*

Dokaz. Kvadratni korijen kompleksnog broja je kompleksan broj, stoga dokaz ove leme slijedi iz formule za određivanje rješenja kvadratne jednadžbe. Rješenja jednadžbe $ax^2 + bx + c = 0$ su $x_{1,2} = \frac{-b\pm\sqrt{(b^2-4ac)}}{2a}$. Dakle, x_1 i x_2 su kompleksne nultočke polinoma $f(x) = ax^2 + bx + c$. □

Lema 3.7.4. *Svaki polinom $f \in \mathbb{R}[x]$ neparnog stupnja ima realnu nultočku.*

Dokaz. Neka je $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$. Definiramo $t = 1 + \sum_{i=0}^{n-1} |a_i|$. Slijedi $|a_i| \le t - 1$ za svaki $i = 0, 1, \ldots, n-1$. Neka je $h(x) = f(x) - x^n$. Tada vrijedi

$$
\begin{aligned}
|h(t)| &= |a_{n-1}t^{n-1} + \ldots + a_1t + a_0| \\
&\le (t-1)(t^{n-1} + \ldots + t + 1) \\
&= t^n - 1 \\
&< t^n.
\end{aligned}
$$

Dakle, slijedi da je $-t^n < h(t)$ i $0 = -t^n + t^n < h(t) + t^n = f(t)$. Analogno za $|h(-t)|$ pokažemo da vrijedi $|h(-t)| < t^n$. Tada je

$$f(-t) = h(-t) + (-t)^n < t^n + (-t)^n.$$

Za neparan broj n vrijedi $(-t)^n = -t^n$ i tada vrijedi $f(-t) < t^n - t^n = 0$. Prema prethodnom korolaru, slijedi da postoji realan broj c takav da je $f(c) = 0$. Dakle, polinom f ima realnu nultočku. □

Osim prethodne dvije leme, za dokaz osnovnog teorema algebre potrebno nam je *polje razlaganja*.

Definicija 3.7.5. *Neka je P polje i $f \in P[x]$ nekonstantni polinom. Kažemo da se polinom f **razlaže nad proširenjem polja** P' **polja P** ako se f može faktorizirati u linearne faktore u polju $P'[x]$, tj. ako postoji $a \in P$ i $\alpha_q, \ldots, \alpha_n \in P'$ takvi da je*

$$f(x) = a(x - \alpha_1)\cdots(x - \alpha_n).$$

*Polje P' zovemo **polje razlaganja polinoma** f.*

Teorem 3.7.6 (Egzistencija polja razlaganja)**.** *Neka je P polje i neka je $f \in P[x]$ nekonstantni poljinom. Tada postoji polje razlaganja za f.*

Dokaz ovog teorema može se pronaći u [20]. U nastavku slijedi dokaz osnovnog teorema algebre koji je također preuzet iz [20].

Dokaz osnovnog teorema algebre 3.3.4. Dokazat ćemo da $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{C}[x]$ ima kompleksnu nultočku. Definiramo $\overline{f}(x) = \sum_{i=0}^{n} \overline{a_i} x^i \in \mathbb{C}[x]$, gdje je $\overline{a_i}$ kompleksno konjugirani broj broja a_i. Sada je $f(x)\overline{f}(x) = \sum c_k x^k$, gdje je $c_k = \sum_{i+j=k} a_i \overline{a_j}$. Uočimo da je $\overline{c_k} = c_k$, iz čega slijedi da je $f\overline{f} \in \mathbb{R}[x]$. Ako je z kompleksna nultočka polinoma f, onda je z kompleksna nultočka polinoma $f\overline{f}$. Ako je z kompleksna nultočka polinoma $f\overline{f}$, onda je z kompleksna nultočka polinoma f ili polinoma $\overline{f}$. No, ako je z kompleksna nultočka polinoma $\overline{f}$, onda je $\overline{z}$ kompleksna nultočka polinoma f. Dakle, slijedi da polinom f ima kompleksnu nultočku ako i samo ako polinom $f\overline{f}$ ima kompleksnu nultočku. Kako je polinom $f\overline{f} \in \mathbb{R}[x]$, dovoljno je dokazati da svaki realni polinom ima kompleksnu nultočku.

Uočimo da je dovoljno dokazati da svaki nekonstantni normirani polinom $f \in \mathbb{R}[x]$ ima kompleksnu nultočku. Neka je $\deg f = 2^k m$, gdje je m neparan broj. Tvrdnju ćemo dokazati indukcijom po $k \geq 0$. Za $k = 0$ je $\deg f = m$, tj. f je polinom neparnog stupnja. Baza indukcije slijedi iz leme (3.7.4). Pretpostavimo da je $k \geq 1$. Neka su $\alpha_1, \ldots, \alpha_n$ nultočke polinoma f u nekom polju razlaganja polinoma f (koje postoji prema teoremu (3.7.6). Za proizvoljan $t \in \mathbb{R}$ definiramo

$$g_t(x) = \prod_{i,j \in \{1,\ldots,n\}, i \neq j} (x - \beta_{ij}),$$

gdje je $\beta_{ij} = \alpha_i + \alpha_j + t\alpha_i\alpha_j$ i $i, j \in \{1, \ldots, n\}, i \neq j$. Imamo

$$\deg(g_t) = \frac{1}{2}n(n-1) = 2^{k-1}m(n-1).$$

Sada je $n = 2^k m$ paran broj, zato što je $k \geq 1$. Zato je $n - 1$ neparan broj pa slijedi da je i $m(n-1)$ neparan broj. Pokažimo sada da su koeficijenti polinoma g_t realni brojevi. Iz Vièteovih formula slijedi da je svaki koeficijent polinoma g_t simetrični polinom u varijablama β_{ij}. Kako je $\beta_{ij} = \alpha_i + \alpha_j + t\alpha_i\alpha_j$, slijedi da su koeficijenti polinoma g_t simetrični polinomi s realnim koeficijentima u varijablama $\alpha_1, \ldots, \alpha_n$. Prema osnovnom teoremu o simetričnim polinomima, za svaki koeficijent c polinoma g_t postoji jedinstveni polinom h s realnim koeficijentima takav da vrijedi $c(\alpha_1, \ldots, \alpha_n) = h(\sigma_1, \ldots, \sigma_n)$, gdje su $\sigma_1, \ldots, \sigma_n$ elementarni simterični polinomi u varijablama $\alpha_1, \ldots, \alpha_n$. No, prema Vièteovim formulama $\sigma_1, \ldots, \sigma_n$ u varijablama $\alpha_1, \ldots, \alpha_n$ su koeficijenti polinoma f. Kako je f polinom s realnim koeficijentima, slijedi da je i g_t polinom s realnim koeficijentima. Iz pretpostavke indukcije slijedi da polinom g_t ima kompleksnu nultočku za svaki $t \in \mathbb{R}$. Jasno je iz definicije polinoma g_t da je za svaki $t \in \mathbb{R}$ ta kompleksna nultočka oblika $\alpha_i + \alpha_j + t\alpha_i\alpha_j$ za neki podskup $\{i, j\}$ skupa $\{1, 2, \ldots, n\}$. Postoji beskonačno mnogo $t \in \mathbb{R}$ i samo konačno mnogo dvočlanih podskupova $\{i, j\}$ skupa $\{1, 2, \ldots, n\}$. Prema *Dirichletovom principu*[4] postoji podskup $\{i, j\} \subset \{1, 2, \ldots, n\}$ i različiti realni brojevi t i s za koje su $\alpha_i + \alpha_j + t\alpha_i\alpha_j$ i $\alpha_i + \alpha_j + s\alpha_i\alpha_j$ kompleksne nultočke polinoma $g_t(x)$, odnosno $g_s(x)$. Oduzimanjem tih kompleksnih brojeva dobivamo kompleksni broj $(t - s)\alpha_i\alpha_j$. Kako je $t \neq s$, slijedi da je $\alpha_i\alpha_j \in \mathbb{C}$. Neka je $\alpha_i\alpha_j = u$. Kako je $\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$, slijedi da je $\alpha_i + \alpha_j \in \mathbb{C}$. Neka je $\alpha_i + \alpha_j = v$. Sada je α_i rješenje kvadratne jednadžbe $x^2 - vx + u = 0$. Iz leme (3.7.3) slijedi da je α_i kompleksan broj, a kako je to ujedno i nultočka polinoma f, slijedi da polinom f ima kompleksnu nultočku, što je i trebalo pokazati. $\square$

[4] Dirichletov princip, poznat i kao princip golubinjaka, jednostavan je kombinatorni princip kojeg je prvi formulirao i koristio njemački matematičar Johann P. G. Dirichlet (1805.-1859.).
Glasi: ako je m predmeta razmješteno u n kutija, onda barem jedna kutija sadrži $\lfloor \frac{m-1}{n} + 1 \rfloor$ predmet.

Poglavlje 4

Zadaci s matematičkih natjecanja

U ovom poglavlju ćemo obraditi razne zadatke s polinomima koji su se pojavili na domaćim, stranim i međunarodnim natjecanjima pri čemu koristimo literaturu [1], [2], [3], [5] i [7].

4.1 Zadaci s polinomima na domaćim natjecanjima

Primjer 4.1.1. (Školsko natjecanje, 2. razred, 2020., A-varijanta) *Odredi najveći prirodan broj n takav da $n + 10$ dijeli $n^3 + 100$.*

Rješenje: Ovaj zadatak možemo riješiti dijeljenjem polinoma. Neka su p i q polinomi zadani s $p(n) = n^3 + 100$ i $q(n) = n + 10$. Podijelimo polinom p polinomom q:

$$
\begin{array}{rrrrl}
n^3 & & & +\,100 & :(n+10) = n^2 - 10n + 100\\
-(n^3 & +\,10n^2) & & & \\
\cline{1-4}
& -10n^2 & & +\,100 & \\
& -(-10n^2 & -\,100n &) & \\
\cline{2-4}
& & 100n & +\,100 & \\
& & -\,(100n & +\,1000) & \\
\cline{3-4}
& & & -\,900 &
\end{array}
$$

Sada imamo

$$\frac{n^3 + 100}{n + 10} = n^2 - 10n + 100 - \frac{900}{n + 10}.$$

Ako je $n + 10$ djelitelj od $n^3 + 100$, onda $n + 10$ mora biti djelitelj broja 900, i obratno. Kako je najveći mogući djelitelj broja 900 broj 900, slijedi da za najveći mogući broj n koji zadovoljava tvrdnju zadatka mora vrijediti $n + 10 = 900$. Dakle, traženo rješenje je $n = 890$.

Primjer 4.1.2. (Županijsko natjecanje, 4. razred, 2022., A-varijanta) *Odredi sve polinome P trećeg stupnja koji imaju sljedeća tri svojstva:*

1. *$P(x)$ pri dijeljenju s $x^2 - 1$ daje ostatak $2x + 1$,*
2. *zbroj nultočaka polinoma p iznosi -2,*
3. *graf polinoma P prolazi točkom $(0, 3)$.*

Rješenje: Iz prvog svojstva slijedi da $P(x)$ možemo zapisati kao $P(x) = (x^2 - 1)Q(x) + (2x + 1)$. Budući da je P polinom trećeg stupnja, Q očito mora biti polinom prvog stupnja, tj. $Q(x) = ax + b$ pa slijedi

$$P(x) = (x^2 - 1)(ax + b) + (2x + 1) = ax^3 + bx^2 + (2 - a)x + (1 - b).$$

Iz Vièteovih formula slijedi da je zbroj nultočaka polinoma P jednak $-\frac{b}{a}$. Zato iz drugog svojstva slijedi $\frac{b}{a} = 2$. Iz trećeg svojstva slijedi da je $P(0) = 3$, što nam uvrštavanjem u izraz za $P(x)$ daje $(1 - b) = 3$, odakle je $b = -2$. Konačno, iz $\frac{b}{a} = 2$ i $b = -2$ slijedi $a = -1$ pa je traženi polinom P oblika

$$P(x) = -x^3 - 2x^2 + 3x + 3.$$

Primjer 4.1.3. (Državno natjecanje, 4. razred, 2021., B-varijanta) *Odredi sve polinome p s realnim koeficijentima za koje je jednakost*

$$x \cdot p(x - 1) = (x - 2021) \cdot p(x)$$

ispunjena za sve realne brojeve x.

Rješenje: Uvrštavanjem prirodnih brojeva $0, 1, \ldots, 2020$ u danu jednakost dobivamo:

$$\begin{array}{lcrcr}
x = 0 & \Rightarrow & 0 = -2021 \cdot p(0) & \Rightarrow & p(0) = 0 \\
x = 1 & \Rightarrow & p(0) = -2020 \cdot p(1) & \Rightarrow & p(1) = 0 \\
x = 2 & \Rightarrow & 2p(1) = -2019 \cdot p(2) & \Rightarrow & p(2) = 0 \\
 & & \vdots & & \\
x = 2020 & \Rightarrow & 2020p(2019) = -p(2020) & \Rightarrow & p(2020) = 0
\end{array}$$

Iz zadane jednakosti je očito da iz $p(x-1) = 0$ slijedi da je $p(x) = 0$ za sve prirodne brojeve $x < 2021$. Zaključujemo da su $0, 1, \ldots, 2020$ nultočke polinoma p pa je

$$p(x) = q(x) \cdot x(x - 1)(x - 2) \cdots (x - 2020)$$

za neki polinom $q(x)$. Sada iz dane jednakosti $x \cdot p(x-1) = (x-2021) \cdot p(x)$ imamo

$$x \cdot q(x-1) \cdot (x-1)(x-2) \cdots (x-2021) = (x-2021) \cdot q(x) \cdot x(x-1)(x-2) \cdots (x-2020)$$

iz čega slijedi da je $q(x-1) = q(x)$ za sve $x \in \mathbb{R}$, odnosno $q(x) = c, c \in \mathbb{R}$. Traženi polinomi p su oblika $p(x) = c \cdot x(x-1)(x-2) \cdots (x-2020)$, za neki $c \in \mathbb{R}$.

Primjer 4.1.4. (HMO[1], 2021.) *Odredite sve polinome P s realnim koeficijentima takve da izraz*

$$P(x+3y) + P(3x-y)$$

ima istu vrijednost za sve realne brojeve x, y za koje je $x^2 + y^2 = 1$.

Rješenje: Primijetimo da je preslikavanje $(x, y) \to (x+3y, 3x-y)$ bijekcija među skupovima

$$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\} \longleftrightarrow \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 10\}$$

Inverzna funkcija je $(a, b) \to \left(\frac{a+3b}{10}, \frac{3a-b}{10}\right)$. Zadatak se sada svodi na traženje svih polinoma takvih da izraz

$$P(x) + P(y)$$

ima istu vrijednost za sve realne brojeve x i y za koje je $x^2 + y^2 = 10$. Neka je P jedan takav polinom. Označimo sa A skup $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 10\}$. Primijetimo da je $(x, y) \in A$ ako i samo ako je $(x, -y) \in A$ te vrijedi

$$P(x) + P(y) = P(x) + P(-y), \forall (x, y) \in A,$$

odnosno

$$P(y) - P(-y) = 0, \forall y \in [-\sqrt{10}, \sqrt{10}].$$

Budući da je lijeva strana prethodne jednakosti polinom, i da ima beskonačno nultočaka, zaključujemo da je P parna funkcija. Sada znamo da postoji polinom R takav da je $P(x) = R(x^2)$. Neka je $C \in \mathbb{R}$ takav da je $P(x) + P(y) = C, \forall (x, y) \in A$. Tada vrijedi

$$C = P(x) + P(y) = R(x^2) + R(y^2) = R(x^2) + R(10 - x^2), \forall (x, y) \in A.$$

Ako je x nenegativan, onda možemo staviti $x = z^2$. Kako je $C = R(z^2) + R(10 - z^2)$, iz toga slijedi da je $C = R(x) + R(10 - x)$. Ukoliko je x negativan, možemo staviti $x = 10 - z^2$, za neki $z \in \mathbb{R}$ takav da je $|z| > \sqrt{10}$. Kako je $C = R(z^2) + R(10 - z^2)$, uvrštavanjem $z^2 = 10 - x$ ponovno dobijemo $C = R(10 - x) + R(x)$. Dakle, vrijedi

$$C = R(x) + R(10 - x), \forall x \in \mathbb{R}.$$

[1]HMO - Hrvatska matematička olimpijada

Nadalje, za sve realne brojeve x vrijedi

$$R(5+x)+R(5-x)=R(5+x)+R(10-(5+x))=C.$$

Definirajmo polinom $T(x)=R(5+x)-\frac{C}{2}$. Iz prethodnog identiteta direktno dobivamo da je T neparna funkcija pa postoji polinom Q takav da je $T(x)=xQ(x^2), \forall x\in\mathbb{R}$. Dobivamo sljedeći nužan uvjet na P:

$$P(x)=R(x^2)=T(x^2-5)+\frac{C}{2}=(x^2-5)Q(x^2-5)^2+\frac{C}{2}$$

Direktnom provjerom vidimo da svi polinomi ovog oblika zadovoljavaju uvjete zadatka.

4.2 Zadaci s polinomima na stranim i međunarodnim natjecanjima

Primjer 4.2.1. (IMO[2], 2004.) *Odredite sve polinome P koji zadovoljavaju jednakost $P(a-b)+P(b-c)+P(c-a)=2P(a+b+c)$, za sve realne brojeve a,b,c takve da je $ab+bc+ca=0$.*

Rješenje: Za svaki realan broj x uređena trojka $(a,b,c)=(6x,3x,-2x)$ zadovoljava $ab+bc+ca=0$. Za tu trojku iz dane jednadžbe slijedi

$$P(3x)+P(5x)+P(-8x)=2P(7x), \forall x\in\mathbb{R}.$$

Za $P(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$, prema teoremu o jednakosti polinoma, vrijedi

$$(3^k+5^k+(-8)^k-2\cdot 7^k)a_k=0, k=0,1,2,\ldots,n.$$

Budući da je izraz u zagradi negativan za neparne k, a pozitivan za $k=0$ i za sve parne $k\geq 6$, izraz je jednak 0 samo za $k=2$ i $k=4$. Zato je $P(x)=\alpha x^2+\beta x^4, \alpha,\beta\in\mathbb{R}$.

[2]IMO - Internacionalna matematička olimpijada (ili MMO - Međunarodna matematička olimpijada)

Dokažimo sada da svi polinomi tog oblika zaista zadovoljavaju uvjete zadatka.

$$\begin{aligned}
P(a-b)+P(b-c)+P(c-a) &= \alpha(a-b)^2+\beta(a-b)^4+\alpha(b-c)^2+\beta(b-c)^4 \\
&+\alpha(c-a)^2+\beta(c-a)^4 \\
&= \alpha(a^2-2ab+b^2)+\beta(a^4-4a^3b+6a^2b^2-4ab^3+b^4) \\
&+\alpha(b^2-2bc+c^2)+\beta(b^4-4b^3c+6b^2c^2-4bc^3+c^4) \\
&+\alpha(c^2-2ca+a^2)+\beta(a^4-4a^3c+6a^2c^2-4ac^3+c^4) \\
&= 2\alpha(a^2+b^2+c^2-2ab-2bc-2ca) \\
&+2\beta(a^4+b^4+c^4-2a^3b-2ab^3-2b^3c-2bc^3-2a^3c-2ac^3 \\
&+3a^2b^2+3b^2c^2+3a^2c^2) \\
&= 2\alpha(a^2+b^2+c^2+2ab+2bc+2ca-4ab-4bc-4ca) \\
&+2\beta(a^4+b^4+c^4+4a^3b+4ab^3+4b^3c+4bc^3+4c^3a+4ca^3 \\
&-6(a^3b+ab^3+b^3c+bc^3+a^3c+ac^3) \\
&+6a^2b^2+6b^2c^2+6a^2c^2-3a^2b^2-3b^2c^2-3a^2c^2 \\
&+12a^2bc+12ab^2c+12abc^2-12a^2bc-12ab^2c-12abc^2) \\
&= 2\alpha((a+b+c)^2-4(ab+bc+ca)) \\
&+2\beta((a+b+c)^4-6(a^3b+ab^3+b^3c+bc^3+a^3c+ac^3) \\
&-3a^2b^2-3b^2c^2-3a^2c^2-12a^2bc-12ab^2c-12abc^2) \\
&= 2\alpha(a+b+c)^2 \\
&+2\beta((a+b+c)^4-6((a^2+b^2+c^2)(ab+bc+ca) \\
&-a^2bc-ab^2c-abc^2)-3((ab+bc+ac)^2 \\
&-2(a^2bc+ab^2c+abc^2))-12(a^2bc+ab^2c+abc^2)) \\
&= 2(\alpha(a+b+c)^2+\beta(a+b+c)^4) \\
&= 2P(a+b+c)
\end{aligned}$$

Primjer 4.2.2. (Prijedlog za IMO, 2010.) *Odredite najmanji broj n za koji postoje polinomi $f_1, f_2, \ldots, f_n$ s racionalnim koeficijentima koji zadovoljavaju*

$$x^2+7 = f_1(x)^2+f_2(x)^2+\ldots+f_n(x)^2.$$

Rješenje: Jednakost $x^2+7 = x^2+2^2+1^2+1^2+1^2$ pokazuje da je $n \leq 5$. Preostaje pokazati da x^2+7 nije zbroj četiriju (ili manje) kvadrata polinoma s racionalnim koeficijentima.

Pretpostavimo suprotno, tj. da postoje polinomi f_1, f_2, f_3 i f_4 s racionalnim koeficijentima takvi da vrijedi $x^2+7 = f_1(x)^2+f_2(x)^2+f_3(x)^3+f_4(x)^2$. Očito su polinomi f_1, f_2, f_3 i

f_4 najviše stupnja 1, stoga vrijedi $f_i(x) = a_i x + b_i$ za neke $a_i, b_i \in \mathbb{Q}$ i $i = 1, 2, 3, 4$. Slijedi da je $x^2 + 7 = \sum_{i=1}^4 (a_i x + b_i)^2$ i zato vrijedi:

$$\sum_{i=1}^{4} a_i^2 = 1, \sum_{i=1}^{4} a_i b_i = 0, \sum_{i=1}^{4} b_i^2 = 7.$$

Neka su $p_i = a_i + b_i$ i $q_i = a_i - b_i$ za $i = 1, 2, 3, 4$. Tada vrijedi

$$\sum_{i=1}^{4} p_i^2 = \sum_{i=1}^{4} a_i^2 + 2\sum_{i=1}^{4} a_i b_i + \sum_{i=1}^{4} b_i^2 = 8,$$
$$\sum_{i=1}^{4} q_i^2 = \sum_{i=1}^{4} a_i^2 - 2\sum_{i=1}^{4} a_i b_i + \sum_{i=1}^{4} b_i^2 = 8,$$
$$\sum_{i=1}^{4} p_i q_i = \sum_{i=1}^{4} a_i^2 - \sum_{i=1}^{4} b_i^2 = -6,$$

što znači da postoji rješenje u cijelim brojevima $x_1, y_1, x_2, y_2, x_3, y_3, x_4, y_4$ i $m > 0$, gdje je m zajednički nazivnik koeficijenata $a_i = \frac{x_i}{m}$ i $b_i = \frac{y_i}{m}$ polinoma f_i, sustava jednadžbi:

$$\sum_{i=1}^{4} x_i^2 = 8m^2 \qquad (1)$$
$$\sum_{i=1}^{4} y_i^2 = 8m^2 \qquad (2)$$
$$\sum_{i=1}^{4} x_i y_i = -6m^2 \qquad (3)$$

Pokažimo da takvo rješenje ne postoji.

Prestpostavimo suprotno, tj. da postoji rješenje i neka je m minimalni prirodni broj za koji takvo rješenje postoji. Uočimo da ako je x neparan cijeli broj, onda je $x^2 \equiv 1 \pmod 8$. Suprotno, ako je x paran cijeli broj, onda je $x^2 \equiv 0 \pmod 8$ ili $x^2 \equiv 4 \pmod 8$. Iz (1) slijedi da su x_1, x_2, x_3 i x_4 parni brojevi. Naime, ako je samo jedan od brojeva x_1, x_2, x_3, x_4 neparan, onda je $\sum_{i=1}^4 x_i^2 \equiv 1 \pmod 8$ ili $\sum_{i=1}^4 x_i^2 \equiv 5 \pmod 8$. Ako su dva broja neparna, onda je $\sum_{i=1}^4 x_i^2 \equiv 2 \pmod 8$ ili $\sum_{i=1}^4 x_i^2 \equiv 6 \pmod 8$. Ako su tri broja neparna, onda je $\sum_{i=1}^4 x_i^2 \equiv 3 \pmod 8$ ili $\sum_{i=1}^4 x_i^2 \equiv 7 \pmod 8$. Ukoliko su svi brojevi x_1, x_2, x_3, x_4 neparni, onda je $\sum_{i=1}^4 x_i^2 \equiv 4 \pmod 8$. Dakle, ni u jednom slučaju suma $\sum_{i=1}^4 x_i^2$ nije djeljiva s 8 i slijedi da su x_1, x_2, x_3 i x_4 parni brojevi. Slično, iz (2) slijedi da su y_1, y_2, y_3 i y_4 parni brojevi. Nadalje, kako je lijeva strana jednadžbe (3) djeljiva brojem 4, slijedi da je m paran broj. Konačno, dobivamo da je

$$\left(\frac{x_1}{2}, \frac{y_1}{2}, \frac{x_2}{2}, \frac{y_2}{2}, \frac{x_3}{2}, \frac{y_3}{2}, \frac{x_4}{2}, \frac{y_4}{2}, \frac{m}{2}\right)$$

rješenje sustava jednadžbi (1), (2) i (3), što je kontradikcija s pretpostavkom da je m minimalan.

Primjer 4.2.3. (IMC[3], 1997.) *Neka je f polinom zadan s*

$$f(x) = x^{2012} + a_{2011}x^{2011} + \ldots + a_1x + a_0.$$

Albert Einstein i Homer Simpson igraju sljedeću igru. Na svom potezu, igrač odabire jedan od koeficijenata $a_0, a_1, \ldots, a_{2011}$ i daje mu proizvoljnu realnu vrijednost. Albert igra prvi. Nakon što je dao vrijednost odabranom koeficijentu, ta vrijednost se više ne može promijeniti. Igra završava kada se svim koeficijentima da vrijednost.

Homerov cilj je da polinom f bude djeljiv polinomom m, a Albertov je da to spriječi.
(a) *Koji od igrača ima pobjedničku strategiju ako je $m(x) = x - 2012$?*
(b) *Koji od igrača ima pobjedničku strategiju ako je $m(x) = x^2 + 1$?*

Rješenje: Pokazat ćemo da Homerova strategija vodi k pobjedi u oba slučaja - (a) i (b).
(a) Uočimo da će Homer igrati poslijednji te da je to jedini potez koji je bitan. Homer pobjeđuje ako i samo ako je $f(2012) = 0$, tj.

$$2012^{2012} + a_{2011}2012^{2011} + \ldots + a_k2012^k + \ldots + a_12012 + a_0 = 0.$$

Pretpostavimo da je dana vrijednost svim koeficijentima osim koeficijentu a_k. Tada je Homerov cilj osigurati gornju jednakost koja je zapravo linearna jednadžba s jednom nepoznanicom a_k. Očito je da Homer zna riješiti tu jednadžbu, tj. da Homer pobjeđuje.
(b) Definiramo polinome

$$g(y) = a_0 + a_2y + a_4y^2 + \ldots + a_{2010}y^{1005} + y^{1006} \text{ i } h(y) = a_1 + a_3y + a_5y^2 + \ldots + a_{2011}y^{1005}.$$

Vrijedi $f(x) = g(x^2) + h(x^2) \cdot x$. Homer pobjeđuje ako postigne da su $g(y)$ i $h(y)$ djeljivi sa $y + 1$, tj. ako vrijedi $g(-1) = h(-1) = 0$.

Primijetimo da i $g(y)$ i $h(y)$ imaju paran broj neodređenih koeficijenata na početku igre. Moguća strategija koja će Homeru osigurati pobijedu jest praćenje Alberta - kada Albert da vrijednost koeficijentu polinoma g ili polinoma h, u sljedećem potezu Homer da vrijednost koeficijentu istog polinoma. Na taj način Homer daje posljednju vrijednost koeficijenta oba polinoma. Analogno kao u (a), Homer tada može odrediti vrijednost posljednjeg koeficijenta oba polinoma tako da vrijedi $g(-1) = 0$ i $h(-1) = 0$ čime osigurava da je i $f(-1) = 0$.

[3]IMC - The International Mathematics Competition

Primjer 4.2.4. (USAMO[4], 2014.) *Neka su a, b, c, d realni brojevi takvi da vrijedi $b-d \geq 5$ i neka su x_1, x_2, x_3 i x_4 realne nultočke polinoma $P(x) = x^4 + ax^3 + bx^2 + cx + d$. Odredite najmanju vrijednost koju produkt $(x_1^2 + 1)(x_2^2 + 1)(x_3^2 + 1)(x_4^2 + 1)$ može postići.*

Rješenje: Koristeći Vièteove formule imamo:

$$x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 - x_1x_2x_3x_4 \geq 5,$$

odnosno

$$x_1(x_2 + x_3 + x_4 - x_2x_3x_4) + 1(x_2x_3 + x_2x_4 + x_3x_4 - 1) \geq 4.$$

Slijedi

$$4^2 \leq [x_1(x_2 + x_3 + x_4 - x_2x_3x_4) + 1(x_2x_3 + x_2x_4 + x_3x_4 - 1)]^2$$

pa prema Cauchy-Schwarzovoj nejednakosti imamo

$$\begin{aligned} 4^2 &\leq (x_1^2 + 1)[(x_2 + x_3 + x_4 - x_2x_3x_4)^2 + (x_2x_3 + x_2x_4 + x_3x_4 - 1)^2] \\ &= (x_1^2 + 1)(x_2^2 + 1)(x_3^2 + 1)(x_4^2 + 1). \end{aligned}$$

Jednakost vrijedi ako i samo ako je

$$x_1(x_2x_3 + x_2x_4 + x_3x_4 - 1) = 1(x_2 + x_3 + x_4 - x_2x_3x_4),$$

što je ekvivalentno

$$x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = x_1 + x_2 + x_3 + x_4,$$

tj. $a = c$. Stavimo li $P(x) = (x-1)^4$ dobivamo $b - d = 5$, stoga je najmanja moguća vrijednost zadanog produkta jednaka 16.
Navest ćemo i alternativno, brže rješenje: Za $i = \sqrt{-1}$ vrijedi $x^2 + 1 = (x - i)(x + i)$, zato imamo

$$\begin{aligned} (x_1^2 + 1)(x_2^2 + 1)(x_3^2 + 1)(x_4^2 + 1) &= (i - x_1)(i - x_2)(i - x_3)(i - x_4)(-i - x_1)(-i - x_2)(-i - x_3)(-i - x_4) \\ &= P(i)P(-i) \\ &= ((1 - b + d) + i(c - a))(1 - b + d - i(c - a)) \\ &= (b - d - 1)^2 + (c - a)^2 \\ &\geq (5 - 1)^2 + 0^2 \\ &= 16, \end{aligned}$$

gdje jednakost vrijedi ako i samo ako je $b - d = 5$ i $a = c$, što se postiže za $x_1 = x_2 = x_3 = x_4 = 1$. Dakle, 16 je najmanja moguća vrijednost zadanog produkta.

[4]USAMO - The United States of America Mathematical Olympiad

Bibliografija

[1] *International Mathematical Olympiad*, https://www.imo-official.org/, (kolovoz 2023.).

[2] *International Mathematics Competition for University Students*, https://www.imc-math.org.uk/, (kolovoz 2023.).

[3] *Matematička natjecanja*, https://natjecanja.math.hr/, (kolovoz 2023.).

[4] *Omar Khayyam's Cubic*, https://math-physics-problems.fandom.com/wiki/Omar_Khayyam%27s_Cubic, (kolovoz 2023.).

[5] *The United States of America Mathematical Olympiad*, https://artofproblemsolving.com/wiki/index.php/USAMO_Problems_and_Solutions, (kolovoz 2023.).

[6] A. Baker, *Transcendental Number Theory*, Cambridge University Press, 1990.

[7] M. Bašić, *Problemi s polinomima*, Hrčak, **vol. 3** (2005), br. 2, https://hrcak.srce.hr/file/996, (kolovoz 2023.).

[8] F. M. Brückler, *Povijest matematike*, https://www.pmf.unizg.hr/_download/repository/skripta.pdf, (srpanj 2023.).

[9] B. Fine i G. Rosenberger, *The fundamental theorem of algebra*, Springer-Verlag, New York, 1997.

[10] B. Guljaš, *Matematička analiza I & II*, https://www.pmf.unizg.hr/_download/repository/MATANALuR.pdf, (rujan 2023.).

[11] T. W. Hungerford, *Algebra*, Springer, New York, 1974.

[12] D. Ilišević i G. Muić, *Uvod u matematiku*, https://www.pmf.unizg.hr/_download/repository/uum-revizija-sijecanj2022.pdf, (srpanj 2023.).

[13] D. Jankov i I. Papić, *Tri klasična problema*, Osječki matematički list, **vol. 12** (2012), br. 1, https://hrcak.srce.hr/file/129926, (kolovoz 2023.).

[14] V. Krčadinac, *Osnove algoritama*, https://web.math.pmf.unizg.hr/~krcko/nastava/oa/oa-skripta.pdf, (srpanj 2023.).

[15] Franz Lemmermeyer, *Solving polynomial equations*, http://www.fen.bilkent.edu.tr/~franz/M300/solv.pdf, (kolovoz 2023.).

[16] Mladi nadareni matematičari "Marin Getaldić", *Vièteove formule i simetrični polinomi*, https://mnm.hr/wp-content/uploads/2015/10/Simetricni_polinomi_i_Vieteove_formule.pdf, (kolovoz 2023.).

[17] D. Palman, *Geometrijske konstrukcije*, Element, Zagreb, 1996.

[18] B. Pavković i D. Veljan, *Elementarna matematika 1*, Školska knjiga, Zagreb, 2004.

[19] F. Rosen, *Muhammad ibn Musa Al-Khwarizmi: Algebra (prijevod)*, (London, 1831.), https://legacy-www.math.harvard.edu/~knill/teaching/summer2019/exhibits/algebra/AlgebraMohammedBenMusa.pdf, (srpanj 2023.).

[20] J. J. Rotman, *Advanced modern algebra*, Prentice Hall, Upper Saddle River, NJ, 2002.

[21] Š. Ungar, *Kompleksna analiza*, https://web.math.pmf.unizg.hr/~ungar/kompleksna.pdf, (srpanj 2023.).

[22] M. Vali Siadat i A. Tholen, *Omar Khayyam: Geometric Algebra and Cubic Equations*, https://digitaleditions.sheridan.com/publication/?i=672591&article_id=3759503&view=articleBrowser, (kolovoz 2023.).

Sažetak

U ovom diplomskom radu opisujemo povijesni razvoj polinoma i osnovnog teorema algebre, od Al-Khwarizmijeve *Algebre* do Galoisove teorije. Zanimljivosti iz povijesti nastavljamo u sljedećem poglavlju s tri klasična problema starogrčke matematike. Uz uvođenje konstruktibilnih brojeva dokazujemo nerješivost tri klasična problema pomoću polinoma. U nastavku rada detaljno proučavamo polinome i njihova svojstva. Posebno se osvrćemo na nultočke i faktorizaciju polinoma, a zatim proučavamo kako pomoću Hornerovog algoritma efikasno dijelimo polinom polinomom prvog stupnja i pronalazimo Taylorov razvoj polinoma. Proučavamo simetrične polinome i iskazujemo osnovni teorem o simetričnim polinomima kao ključni za dokaz osnovnog teorema algebre. Uvodimo pojam polja razlaganja polinoma te prezentiramo jedan algebarski dokaz osnovnog teorema algebre. Na kraju rada obrađujemo razne zadatke vezane za polinome koji su se pojavili na domaćim, stranim i međunarodnim natjecanjima iz matematike.

Summary

In this master's thesis, we describe the historical development of polynomials and the Fundamental Theorem of Algebra, from Al-Khwarizmi's *Algebra* to Galois theory. We continue the next chapter with the three classical Greek problems of mathematics, another popular historical problem. By introducing constructible numbers, we prove the unsolvability of the three classical problems using polynomials. In the next chapter, we study polynomials and their properties in detail. In particular, we look at zeros and factorization of polynomials following with Horner's algorithm and examples how to efficiently divide a polynomial by the first degree polynomial. We study symmetric polynomials and state the Fundamental Theorem of Symmetric Polynomials as a key to proving the Fundamental Theorem of Algebra. Upon introducing a splitting field of a polynomial, we present an algebraic proof of the Fundamental Theorem of Algebra. At the end of the thesis, we show various problems related to polynomials that appeared at national, foreign and international competitions in mathematics.

Životopis

Rođena sam 31. svibnja 1997. godine u Karlovcu. Obrazovanje sam započela u Osnovnoj školi Grabrik i nastavila u Gimnaziji Karlovac, gdje sam odabrala opći smjer planirajući jednog dana studirati biologiju ili biokemiju. Tijekom srednjoškolskog obrazovanja razvila sam velik interes za matematiku, zato sam po završetku 2016. godine upisala preddiplomski sveučilišni studij Matematika; nastavnički smjer na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu. Godine 2021. godine upisala sam diplomski sveučilišni studij Matematika; nastavnički smjer na istom fakultetu.