# Osnovni teorem algebre

**Kišić, Nika**

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Nika Kišić

# OSNOVNI TEOREM ALGEBRE

Diplomski rad

Zagreb, lipanj, 2014.

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Nika Kišić

# OSNOVNI TEOREM ALGEBRE

Diplomski rad

Voditelj rada:
prof.dr.sc. Vedran Krčadinac

Zagreb, lipanj, 2014.

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. _____

# Sadržaj

**Sadržaj** **iv**

**Uvod** **2**

**1 Povijesni pregled** **3**

**2 Dokaz pomoću kompaktnosti** **6**
2.1 Uvod . . . . . 6
2.2 Dokaz osnovnog teorema algebre . . . . . 11

**3 Algebarski dokaz** **13**
3.1 Uvod . . . . . 13
3.2 Dokaz osnovnog teorema algebre . . . . . 21

**4 Dokazi pomoću kompleksne analize** **24**
4.1 Uvod . . . . . 24
4.2 Dokaz osnovnog teorema algebre . . . . . 31
4.3 Još dva dokaza osnovnog teorema algebre . . . . . 32

**Bibliografija** **37**

**Sažetak** **38**

**Summary** **39**

**Životopis** **40**

# Uvod

Cilj ovog diplomskog rada je dokazati osnovni teorem algebre. Koristit ćemo sljedeću formulaciju teorema:

*Svaki kompleksni polinom stupnja $n$ ima $n$ kompleksnih korijena.*

Navest ćemo četiri pristupa dokazu koristeći različita područja matematike. U svakom poglavlju ćemo prvo dati uvod u važna svojstva iz područja na kojem ćemo bazirati dokaz, a nakon toga prelazimo na sam dokaz.

Na početku rada navodimo detalje o razvoju dokaza kroz povijest. Krenut ćemo od Petera Rotha koji je prvi spomenuo teorem. Spomenut ćemo Descartesa koji je prvi objavio dokaz s nekoliko mana te Gaussa koji je napravio prvi dokaz koji je u potpunosti prihvaćen. Nakon povijesnog pregleda, u drugom poglavlju ćemo obraditi dokaz osnovnog teorema algebre koristeći kompaktnost i svojstva kompleksnih polinoma. Prvo ćemo definirati skup polinoma i pokazati da on čini komutativni prsten s jedinicom. Nakon toga podsjetit ćemo se teorema o dijeljenju s ostatkom te najvećeg zajedničkog djelitelja polinoma. U drugom dijelu poglavlja navest ćemo rezultate koji vrijede za kompleksne polinome te ih na kraju poglavlja iskoristiti za dokaz osnovnog teorema algebre.

U trećem poglavlju teorem ćemo dokazati koristeći činjenicu da kompleksni polinom možemo interpretirati kao algebarski objekt. Uvest ćemo pojmove proširenja polja $F$ te elemenata koji su algebarski nad poljem $F$. Dokazat ćemo Kroneckerov teorem koji govori o egzistenciji polja proširenja u kojem ireducibilni polinom ima korijen. Nakon toga definiramo pojam polja razlaganja te dokazujemo teorem o egzistenciji takvog polja. Definirat ćemo simetrične polinome te iskazati osnovni teorem o simetričnim polinomima. U drugoj točki trećeg poglavlja dokazujemo leme koje koristimo u dokazu osnovnog teorema algebre. Ključna je lema koja kaže da svaki nekonstantni realni polinom ima kompleksan korijen. Pomoću te leme dolazimo do dokaza teorema.

U posljednjem poglavlju koristimo rezultate iz kompleksne analize. Definirat ćemo pojam nulhomotopnog puta te jednostavno povezanog područja. Iskazat ćemo Cauchy-Riemannov teorem te Greenov teorem. Nakon toga dokazujemo nekoliko Cauchyjevih

rezultata, uključujući Cauchyjev teorem te Cauchyjevu integralnu formulu. Druga točka četvrtog poglavlja posvećena je dokazu osnovnog teorema algebre koji se temelji na primjeni Liouvilleova teorema. Rad završavamo posljednjom točkom četvrtog poglavlja u kojoj navodimo dokaz koji koristi nejednakost srednje vrijednosti te dokaz koji se bazira na principu maksimuma modula.

# Poglavlje 1

# Povijesni pregled

U ranoj fazi proučavanja jednadžbi, al-Khwarizmi u svojem radu nije imao potrebe za ovim teoremom jer su se tada koristili samo realni pozitivni korijeni. Tek je 1545. Cardano zaključio da postoje brojevi općenitiji od realnih brojeva. Do tog je zaključka došao kada je radio na formuli koja daje korijene kubične jednadžbe.

Prvi spomen osnovnog teorema algebre u ovom obliku dao je 1608. Peter Roth ali se zasluge za to najčešće pripisuju Girardu. Viète je definirao jednadžbe stupnja $n$ sa $n$ korijena, no Albert Girard je 1629. godine u svojem radu *L'invention en algèbre* tvrdio da jednadžbe $n$-tog stupnja uvijek imaju $n$ rješenja. Girard nije tvrdio da su ta rješenja kompleksni brojevi oblika $a + bi, a, b \in \mathbb{R}$, već je ostavio otvorenu mogućnost da rješenja dolaze iz većeg skupa od skupa $\mathbb{C}$. Descartes je 1637. godine u radu *La géométrie* napisao da se za svaku jednadžbu stupnja $n$ može „zamisliti" $n$ korijena, no imaginarni korijeni ne predstavljaju neku realnu količinu.

Leibniz je 1702. dao protuprimjer da osnovni teorem algebre ne vrijedi. Tvrdio je da se $x^4 + t^4$ ne može napisati kao produkt dva realna kvadratna faktora. Griješio je zato što nije znao da se $\sqrt{i}$ može napisati u obliku $a + bi, a, b \in \mathbb{R}$. Leibnizov protuprimjer opovrgnuo je Euler 1742.

Prvi objavljen dokaz ovog teorema dao je D'Alembert 1746. Međutim, njegov je dokaz imao nekoliko rupa. U dokazu je koristio lemu koja tada još nije bila dokazana - dokazao ju je tek 1851. godine Puiseux koristeći upravo osnovni teorem algebre. Također, D'Alembert nije koristio argument kompaktnosti kako bi kompletirao dokaz.

Euler je dokazao da svaki realni polinom stupnja $n$, $n \leq 6$ ima točno $n$ korijena. 1749. godine pokušao je dokazati osnovni teorem algebre za realne polinome u sljedećem obliku:

> *Svaki polinom stupnja $n$ s realnim koeficijentima ima točno $n$ korijena u $\mathbb{C}$.*

Eulerov se dokaz temeljio na dekompoziciji normiranog polinoma stupnja $2^m$ na produkt dva normirana polinoma stupnja $2^{m-1}$. Kompletan je dokaz napravio za $m = 4$, dok je opći slučaj ostao samo skica.

Koristeći svoje znanje o permutacijama korijena, Lagrange je 1772. godine popunio sve rupe Eulerova dokaza. No, i dalje je pretpostavljao da polinomi stupnja $n$ moraju imati $n$ korijena neke vrste kako bi kasnije pokazao da ti korijeni moraju biti oblika $a + bi, a, b \in \mathbb{R}$.

Laplace je 1795. pokušao dokazati osnovni teorem algebre koristeći diskriminantu polinoma. Jedini problem u tom dokazu bio je ponovno pretpostavka o postojanju korijena.

Prvi objavljen dokaz koji je u potpunosti prihvaćen napravio je Gauss u svojoj doktorskoj disertaciji 1799. godine koristeći topologiju. Gauss je koristio alternativnu formulaciju teorema koja glasi:

Svaki realni polinom može se faktorizirati u linearne i kvadratne faktore.

On je i prvi koji je pronašao ključni problem u prethodnim dokazima - pretpostavku o postojanju korijena. No, i njegov dokaz ima neke rupe te ne zadovoljava današnje standarde.

Na bazi D'Alembertove ideje, 1814. godine Jean Robert Argand objavljuje najjednostavniji dokaz teorema. U prijašnjim radovima interpretirao je množenje s $i$ kao rotaciju ravnine za $90^o$ i ustanovio Argandov dijagram kao geometrijsku reprezentaciju kompleksnih brojeva. U članku *Réflexions sur la nouvelle théorie d'analyse* Argand koristi opći teorem o postojanju minimuma neprekidne funkcije kako bi pojednostavio D'Alembertov dokaz. Argandov dokaz nije rigorozan samo zato što tada još nije razvijen koncept donje granice. Ovaj je dokaz stekao popularnost kroz Chrystalov udžbenik algebre iz 1886. godine koji je tada bio vrlo utjecajan.

Gauss je 1816. objavio drugi dokaz teorema koristeći Eulerov pristup i taj je dokaz potpun. Nije pretpostavio da postoje korijeni neke vrste već je radio s nepoznanicama. Treći dokaz Gauss je objavio također 1816. godine ponovno koristeći topologiju. Naziv *kompleksni broj* Gauss uvodi 1831. godine, a naziv *konjugat* Cauchy 1821. godine.

1849. godine Gauss je napravio prvi dokaz da kompleksni polinom stupnja $n$ ima $n$ kompleksnih korijena. Međutim, taj je dokaz bio vrlo sličan njegovom prvom dokazu i bilo je lako za izvesti taj rezultat iz rezultata za realne polinome. Iako je Gauss inzistirao na tome da se ne može pretpostaviti egzistencija korijena za koje će se kasnije dokazati da su oblika $a+bi, a, b \in \mathbb{R}$, vjerovao je da postoji cijela hijerarhija imaginarnih veličina od kojih su kompleksni brojevi najjednostavniji. On ih je zvao *sjenama sjena*.

Argandov dokaz dokazuje samo egzistenciju, no ne daje mogućnost da se korijeni kostruiraju. Weierstrass je još 1859. krenuo s konstruktivnim dokazom, no njega je napravio tek 1940. godine Hellmuth Kneser. Taj je dokaz 1981. godine pojednostavio njegov sin, Martin Kneser.

# Poglavlje 2

# Dokaz pomoću kompaktnosti

U ovom poglavlju dokazat ćemo osnovni teorem algebre koristeći svojstva kompleksnih polinoma. U prvom dijelu navodimo osnovne pojmove vezane uz kompleksne brojeve i kompleksne polinome, a zatim to primjenjujemo u drugom dijelu kada dokazujemo teorem.

## 2.1 Uvod

Na početku ovog odjeljka navest ćemo svojstva koja imaju operacije zbrajanja i množenja. Nakon toga definirat ćemo nekoliko algebarskih struktura na kojima su zadane te dvije operacije te ćemo ih upotrijebiti kako bismo precizno definirali skup kompleksnih polinoma.
Binarne operacije zbrajanja $+ : F \to F$ i množenja $\cdot : F \to F$ na skupu $F$ imaju sljedeća svojstva:

(1) Zbrajanje je komutativno: $a + b = b + a$, za svaki $a, b \in F$.

(2) Zbrajanje je asocijativno: $a + (b + c) = (a + b) + c$, za $a, b, c \in F$.

(3) Postoji neutralni element za zbrajanje koji označavamo s 0 takav da vrijedi $a + 0 = 0 + a = a$, za svaki $a \in F$.

(4) Za svaki $a \in F$ postoji inverz za zbrajanje $-a$ takav da vrijedi $a + (-a) = 0$.

(5) Množenje je komutativno: $ab = ba$, za svaki $a, b \in F$.

(6) Množenje je asocijativno: $a(bc) = (ab)c$, za $a, b, c \in F$.

(7) Postoji neutralni element za množenje koji označavamo s 1 takav da vrijedi $a1 = 1a = a$, za svaki $a \in F$.

(8) Za svaki $a \in F, a \neq 0$ postoji multiplikativni inverz $a^{-1}$ takav da vrijedi $aa^{-1} = 1$.

(9) Distributivnost množenja prema zbrajanju: $a(b+c) = ab + ac$, za $a, b, c \in F$.

Neprazan skup $R$ sa operacijama zbrajanja i množenja koji zadovoljava prvih četiri aksioma te aksiome (6) i (9) zove se **prsten**. Skup $G$ koji zadovoljava sve aksiome osim osmog naziva se **komutativni prsten s jedinicom**. Skup $F$ s operacijama zbrajanja i množenja je **polje** ako je komutativni prsten s jedinicom i svaki element skupa $F$ ima multiplikativni inverz, odnosno skup je polje ako zadovoljava svih devet gore navedenih aksioma.

Neka je $F$ polje i $n$ prirodan broj. Polinom stupnja $n$ nad poljem $F$ je formalna suma oblika $p(x) = a_n x^n + \cdots + a_1 x + a_0$, gdje su $a_i \in F$ za $i = 0, \ldots, n$ i $a_n \neq 0$. Polinom je normiran ukoliko je $a_n = 1$. Sa $F[x]$ označavamo skup svih polinoma nad $F$, a sa $F_n[x]$ skup svih polinoma stupnja manjeg ili jednakog $n$.

Definirajmo zbrajanje, oduzimanje i množenje na $F[x]$. Neka su $p, q \in F[x]$, $p(x) = a_n x^n + \cdots + a_1 x + a_0$ i $q(x) = b_m x^m + \cdots + b_1 x + b_0$. Tada je

$$p(x) \pm q(x) = (a_0 \pm b_0) + (a_1 \pm b_1)x + \cdots, \quad \text{i}$$

$$p(x)q(x) = (a_0 b_0) + (a_0 b_1 + a_1 b_0)x + \cdots + (a_n b_m)x^{n+m}.$$

Sada skup $F[x]$ čini komutativni prsten s jedinicom.
Polinom $p$ je **ireducibilan** ako se ne može napisati kao produkt $qr$, gdje su $q$ i $r$ polinomi stupnja barem 1.

U nastavku navodimo teorem o dijeljenju polinoma s ostatkom te teorem o najvećem zajedničkom djelitelju, koji će nam trebati kasnije.

**Teorem 2.1.1.** *(Teorem o dijeljenju s ostatkom) Za svaka dva polinoma $f, g \in F[x]$, $g \neq 0$ postoje jedinstveni polinomi $q, r \in F[x]$, $\deg r < \deg g$, takvi da vrijedi*

$$f = g \cdot q + r.$$

*Dokaz.* Prvo ćemo dokazati egzistenciju polinoma $q$ i $r$. Pretpostavimo da je $\deg f \geq \deg g$. Ukoliko nije, stavimo $q = 0$ i $r = f$ i teorem vrijedi. Neka je $f(x) = a_n x^n + \cdots + a_0$ i $g(x) = b_m x^m + \cdots + b_0$, $a_n, b_m \neq 0$.
Definirajmo polinom $f_1$ sa

$$f_1(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = a_{1,n_1} x^{n_1} + \cdots + a_{1,0}$$

i neka je $n_1 = \deg f_1$. Tada je $f_1$ polinom stupnja manjeg od $n$. Ukoliko je $n_1 \geq m$, ponavljamo postupak te definiramo $f_2$ sa

$$f_2(x) = f_1(x) - \frac{a_{1,n_1}}{b_m} x^{n_1 - m} g(x), \quad \deg f_2 = n_2.$$

Sada analogno nastavljamo postupak ako je $n_2 \geq m$. Na kraju imamo niz polinoma $f, f_1, f_2, \ldots$ te nakon $k$ koraka dobivamo polinom stupnja manjeg od $m$:

$$f_k(x) = f_{k-1}(x) - \frac{a_{k-1,n_{k-1}}}{b_m} x^{n_{k-1}-m} g(x).$$

Zbrajanjem jednakosti koje definiraju $f_1, \ldots, f_k$ dobivamo

$$f(x) = (\frac{a_n}{b_m} x^{n-m} + \frac{a_{1,n_1}}{b_m} x^{n_1-m} + \cdots + \frac{a_{k-1,n_k-1}}{b_m} x^{n_{k-1}-m}) g(x) + f_k(x).$$

Sada za $q(x) := \frac{a_n}{b_m} x^{n-m} + \frac{a_{1,n_1}}{b_m} x^{n_1-m} + \cdots + \frac{a_{k-1,n_k-1}}{b_m} x^{n_{k-1}-m}$ i $r(x) = f_k(x)$ slijedi egzistencija takvih polinoma.
Dokažimo još jedinstvenost. Neka je

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x), \tag{2.1}$$

te neka je $\deg r_1, \deg r_2 < \deg g$. Sada iz 2.1 imamo

$$r_2(x) - r_1(x) = (q_1(x) - q_2(x))g(x),$$

te slijedi da $g$ dijeli $r_2 - r_1$. S obzirom na to da je stupanj polinoma $r_2 - r_1$ manji od stupnja polinoma $g$, to je moguće samo ako je $r_2 - r_1 = 0$, tj. $r_1 = r_2$. Nadalje, $(q_1(x) - q_2(x))g(x) = 0$, iz čega slijedi $q_1 = q_2$. □

**Definicija 2.1.2.** Neka su $f, g \in F[x]$. Polinom $d \in F[x]$ je ***najveći zajednički djelitelj od*** $f$ ***i*** $g$ ako je normiran, dijeli i $f$ i $g$ te ako svaki polinom $d_1$ koji dijeli $f$ i $g$ ujedno dijeli i $d$. Koristimo oznaku $d = (f, g)$. Ukoliko je $(f, g) = 1$ kažemo da su $f$ i $g$ ***relativno prosti***.

**Teorem 2.1.3.** *Neka su $f, g \in F[x]$, $f, g \neq 0$. Tada postoji jedinstveni najveći zajednički djelitelj od $f$ i $g$.*

*Dokaz.* Egzistenciju možemo dokazati koristeći Euklidov algoritam. Pretpostavimo da je $\deg f \geq \deg g$. Koristeći teorem 2.1.1 dobivamo $f = g \cdot q_1 + r_1, \deg r_1 < \deg g$. Možemo ponovno primjeniti navedeni teorem na polinome $g$ i $r_1$ te dobivamo $g = r_1 \cdot q_2 + r_2, \deg r_2 < \deg r_1$. Sada nastavljamo isti postupak i nakon konačno mnogo koraka $k$ imamo ostatak $r_{k+1} = 0$. Dakle, posljednja jednakost je $r_{k-1} = r_k \cdot q_{k+1}$. Iz nje slijedi da $r_k$ dijeli $r_{k-1}$. Sada se vraćamo unatrag i zaključujemo da $r_k$ dijeli $r_{k-2}$ i tako dalje sve do druge jednakosti gdje vidimo da $r_k$ dijeli $g$ i prve jednakosti iz koje zaključujemo da $r_k$ dijeli i $f$. Dakle, $r_k$ je djelitelj od $f$ i $g$. Pokažimo da je $r_k$ i najveći zajednički djelitelj. Neka je $m$ neki drugi djelitelj od $f$ i $g$. Iz jedne od jednakosti gore slijedi da je $r_1 = f - g \cdot q_1$ pa imamo da $m$ dijeli $r_1$. Nastavljamo isti

postupak i na kraju zaključujemo da $m$ dijeli $r_k$ što znači da je $r_k$ najveći zajednički djelitelj $f$ i $g$.

Sada još moramo dokazati jedinstvenost. Pretpostavimo da postoje dva najveća zajednička djelitelja i neka su to $d$ i $d'$. Iz definicije najvećeg zajedničkog djelitelja slijedi da polinom $d$ dijeli $d'$ i $d'$ dijeli $d$. Zato polinome $d$ i $d'$ možemo zapisati kao

$$d = d'q', \qquad d' = dq.$$

Vrijedi $\deg d \leq \deg d'$ i $\deg d' \leq \deg d$, tj. $\deg d = \deg d'$. Zaključujemo da su $q$ i $q'$ konstante te, s obzirom na to da su $d$ i $d'$ normirani, $q = q' = 1$. Dakle, $d = d'$. □

Iz dokaza teorema 2.1.3 možemo zaključiti da se najveći zajednički djelitelj polinoma $f$ i $g$, $d$, može zapisati kao linearna kombinacija od $f$ i $g$, $d = uf + vg$, $u, v \in F[x]$. Posebno, ako su $f$ i $g$ relativno prosti tada je njihov najveći zajednički djelitelj jednak 1 pa to možemo zapisati kao

$$uf + vg = 1. \tag{2.2}$$

Sada ćemo navesti nekoliko osnovnih rezultata za kompleksne polinome.

**Definicija 2.1.4.** Neka je $p \in \mathbb{C}[x], p(x) = a_n x^n + \cdots + a_0$. Tada je njegov ***konjugat*** definiran sa $\overline{p}(x) = \overline{a_n}x^n + \cdots + \overline{a_0}$.

**Lema 2.1.5.** *Za svaki $p \in \mathbb{C}[x]$ vrijedi*

(1) *Ako je $z \in \mathbb{C}$ onda vrijedi $\overline{p(z)} = \overline{p}(\overline{z})$.*

(2) *$P$ je realni polinom ako i samo ako je $p(x) = \overline{p}(x)$.*

(3) *Ako je $p(x)q(x) = h(x)$, onda je $\overline{h}(x) = \overline{p}(x)\overline{q}(x)$.*

*Dokaz.* (1) Neka je $z \in \mathbb{C}$ i $p(z) = a_n z^n + \cdots + a_1 z + a_0$. Tada vrijedi:

$$\overline{p(z)} = \overline{a_n z^n + \cdots + a_1 z + a_0} = \overline{a_n}\overline{z^n} + \cdots + \overline{a_1 z} + \overline{a_0} = \overline{p}(\overline{z}).$$

(2) Neka je $p$ realni polinom. Tada je $a_i = \overline{a_i}$ za sve koeficijente pa je $p(z) = \overline{p}(z)$. Obratno, pretpostavimo da vrijedi $p(z) = \overline{p}(z)$. To znači da je $a_i = \overline{a_i}$ za sve koeficijente pa je $a_i \in \mathbb{R}, \forall i$ te je $p$ realni polinom.

(3) Neka su $p, q \in \mathbb{C}[x]$, $p(x) = a_n x^n + \cdots + a_1 x + a_0$ i $q(x) = b_m x^m + \cdots + b_1 x + b_0$. Tada je

$$\begin{aligned}\overline{p}(x)\overline{q}(x) &= (\overline{a_0}\overline{b_0}) + (\overline{a_0}\overline{b_1} + \overline{a_1}\overline{b_0})x + \cdots + (\overline{a_n}\overline{b_m})x^{n+m} \\ &= \overline{(a_0 b_0)} + \overline{(a_0 b_1 + a_1 b_0)}x + \cdots + \overline{(a_n b_m)}x^{n+m} \\ &= \overline{h}(x).\end{aligned}$$

□

**Lema 2.1.6.** *Neka je $g(x) \in \mathbb{C}[x]$. Tada je $h(x) = g(x)\overline{g}(x) \in \mathbb{R}[x]$.*

*Dokaz.* Vrijedi $\overline{h}(x) = \overline{g}(x)\overline{\overline{g}}(x) = \overline{g}(x)g(x) = g(x)\overline{g}(x) = h(x)$. Sada iz drugog dijela leme 2.1.5 slijedi da je $h$ realni polinom. □

**Lema 2.1.7.** *Ako je $c$ korijen polinoma $p \in F[x]$, onda $x - c$ dijeli $p$.*

*Dokaz.* Neka je $p(c) = 0$. Iz teorema 2.1.1 slijedi

$$p(x) = (x - c)q(x) + r(x),$$

gdje je $r(x) = 0$ ili $r(x) = k \in F$ zato što stupanj od $r$ mora biti strogo manji od stupnja polinoma $x - c$. Sada je $p$ oblika

$$p(x) = (x - c)q(x) + k.$$

Budući da je $p(c) = 0 + k = 0$, slijedi da je $k = 0$, tj. $x - c$ dijeli $p$.

□

**Teorem 2.1.8.** *Polinom stupnja $n$ nad poljem $F[x]$ može imati najviše $n$ korijena.*

*Dokaz.* Neka je $p$ polinom stupnja $n$ nad poljem $F[x]$. Dokazujemo teorem indukcijom po $n$. Za $n = 0$, $p$ je konstantni polinom pa nema korijena. Pretpostavimo da teorem vrijedi za sve polinome stupnja manjeg od $n$. Neka je $\alpha$ korijen od $p$. Iz leme 2.1.7 slijedi da $p$ možemo zapisati kao $p(x) = (x-\alpha)q(x)$, gdje je $q$ polinom stupnja $n-1$. Neka je sada $\beta$ neki drugi korijen od $p$, $\beta \neq \alpha$. Tada vrijedi $p(\beta) = (\beta - \alpha)q(\beta)$. S obzirom na to da je $\beta$ različit od $\alpha$, $q(\beta) = 0$. No, $q$ je polinom stupnja $n - 1$ pa po pretpostavci indukcije ima najviše $n-1$ korijena. Dakle, $p$ ima najviše $n$ korijena. □

U jednom od narednih dokaza koristimo DeMoivreov teorem za korijene. Za iskaz teorema potrebni su nam neki osnovni pojmovi vezani uz kompleksne brojeve. Kompleksni broj $z = (x, y) \in \mathbb{C}, x, y \in \mathbb{R}$ možemo zapisati u polarnom obliku,

$$z = r(\cos\theta + i\sin\theta),$$

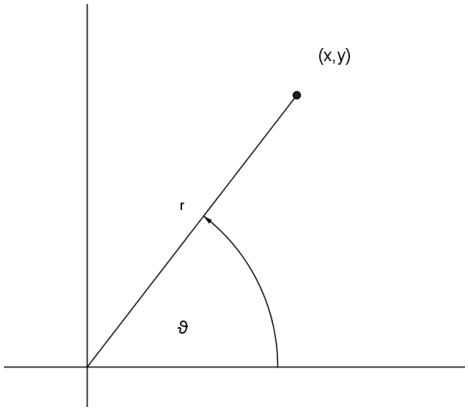
gdje je $\theta$ kut koji vektor od ishodišta do točke $(x, y)$ čini sa pozitivnom $x$-osi.
Eulerov identitet dan je sa

$$e^{i\theta} = \cos(\theta) + i\sin\theta.$$

Dakle, kompleksni broj $z$ može se zapisati kao $z = re^{i\theta}$.

**Teorem 2.1.9.** *(DeMoivreov teorem za korijene) Ako je $z \in \mathbb{C}$,$z \neq 0$, tada postoji točno $n$ različitih $n$-tih korijena od $z$, tj. rješenja jednadžbe $x^n = z$. Ako je $z = re^{i\theta}$, korijeni su dani sa*

$$x_k = r^{\frac{1}{n}} e^{i\frac{\theta+2nk}{n}}, \quad k = 0, 1, \ldots, n-1.$$




Slika 2.1: Kompleksni broj u polarnoj formi

## 2.2 Dokaz osnovnog teorema algebre

**Definicija 2.2.1.** *Skup $K \subset \mathbb{R}^n$ je **kompaktan** ako je ograničen i zatvoren.*

**Teorem 2.2.2.** *Neka je $f : K \to \mathbb{R}$ neprekidna i $K$ kompaktan podskup od $\mathbb{R}^n$. Tada $f$ postiže minimalnu i maksimalnu vrijednost.*

Dokaz ovog teorema može se naći u knjizi [6].

**Lema 2.2.3.** *Neka je $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ kompleksni polinom. Tada postoji točka $z_0 \in \mathbb{C}$ u kojoj $|f|$ postiže minimum.*

*Dokaz.* S obzirom na to da vrijedi $\lim_{|z|\to\infty} |f(z)| = +\infty$, minimum od $|f(z)|$ za $z \in \mathbb{C}$ bit će također i minimum na nekoj dovoljno velikoj kugli $K(0, r)$. Funkcija $|f|$ je neprekidna realna funkcija pa iz leme 2.2.2 slijedi da $|f|$ postiže minimum na kompaktnom skupu $K(0, r)$. □

**Lema 2.2.4.** *Neka je $f \in \mathbb{C}[x]$ nekonstantni kompleksni polinom. Ako je $f(x_0) \neq 0$, onda $|f(x_0)|$ nije minimum od $|f|$.*

*Dokaz.* Neka je $f(x) \in \mathbb{C}[x]$ nekonstantni polinom i neka je $x_0$ točka u kojoj vrijedi $f(x_0) \neq 0$. Translatirajmo varijablu $x$ za $-x_0$. Sada je točka $x_0$ translatirana u ishodište pa za ishodište vrijedi $f(0) \neq 0$. Nadalje, pomnožimo funkciju $f$ sa $f(0)^{-1}$ pa imamo $f(0) = 1$. Kako bi dokazali teorem, moramo pokazati da $|f|$ ne postiže minimum 1.

Neka je $k$ najmanja pozitivna potencija od $x$ koja se javlja u polinomu $f$. Tada je $f$ oblika

$$f(x) = 1 + ax^k + a_2x^{k+1} + a_3x^{k+2} + \cdots .$$

Iz teorema 2.1.9 slijedi da postoji $k-$ti korijen od $-a^{-1}$ koji označavamo s $\alpha$, $\alpha = (-a)^{-\frac{1}{k}}$. Napravimo ponovno zamjenu varijabli tako da $x$ zamijenimo sa $\alpha x$. Sada je $f$ oblika:

$f(x) = 1 - x^k + b_2x^{k+1} + b_3x^{k+2} + \cdots = 1 - x^k + x^{k+1}g(x)$, gdje je $g(x)$ neki polinom.

Iz nejednakosti trokuta imamo:

$$|f(x)| \leq |1 - x^k| + |x|^{k+1}|g(x)|.$$

Ako uzmemo male pozitivne $x$, $x^k < 1$ pa je i $1 - x^k > 0$ te vrijedi

$$|f(x)| \leq |1 - x^k| + x^{k+1}|g(x)| = 1 - x^k(1 - x|g(x)|).$$

Za male $x$, $x|g(x)|$ je isto mali pa možemo izabrati $x_0$ za koji će vrijediti $x_0|g(x_0)| < 1$. Tada je $x_0^k(1 - x_0|g(x_0)|) > 0$ i $|f(x_0)| < 1 = |f(0)|$, što znači da 1 nije minimum $|f|$. □

Sada imamo sve rezultate koji su nam potrebni za dokaz osnovnog teorema algebre.

**Teorem 2.2.5.** *(Osnovni teorem algebre) Ako je $f \in \mathbb{C}[x]$ nekonstantan polinom, tada $f$ ima bar jedan kompleksni korijen.*

*Dokaz.* Neka je $f$ nekonstantan kompleksni polinom. Tada iz leme 2.2.3 imamo da $|f|$ postiže minimum u nekoj točki $x_0 \in \mathbb{C}$ . Iz leme 2.2.4, s obzirom da je $x_0$ točka minimuma, slijedi $|f(x_0)| = 0$, tj. $f(x_0) = 0$. Dakle, $f$ ima kompleksni korijen.

□

# Poglavlje 3

# Algebarski dokaz

Kompleksni polinom možemo interpretirati kao algebarski objekt. Tada osnovni teorem algebre možemo formulirati na sljedeći način:

*Polje kompleksnih brojeva $\mathbb{C}$ je algebarski zatvoreno.*

U ovom ćemo poglavlju dokazati osnovni teorem algebre koristeći svojstva polja i proširenja polja. Dokaz će se bazirati na činjenicama da realni polinom neparnog stupnja ima realne korijene te da ako imamo ireducibilni polinom nad poljem $F$, tada možemo naći proširenje od $F$ u kojem će taj polinom imati korijen. U uvodu navodimo najvažnije rezultate koji će nam biti potrebni, a zatim krećemo s dokazom.

## 3.1 Uvod

Ako su $F$ i $F'$ polja i vrijedi da je $F \subseteq F'$ tada kažemo da je $F'$ **proširenje** polja $F$. Tada je $F'$ vektorski prostor nad poljem $F$. **Stupanj proširenja** definiramo kao $\dim_F F'$ i označavamo sa $|F' : F|$. Primjerice, $|\mathbb{C} : \mathbb{R}| = 2$ i baza vektorskog prostora $\mathbb{C}$ nad $\mathbb{R}$ je $(1, i)$.

Sljedeća lema pokazuje važno svojstvo proširenja polja vezano uz stupanj proširenja.

**Lema 3.1.1.** *Neka su $F \subset F' \subset F''$ polja i neka je $F''$ konačno proširenje polja $F$. Tada su $|F'' : F'|$ i $|F' : F|$ konačni te vrijedi*

$$|F'' : F| = |F'' : F'||F' : F|.$$

*Dokaz.* Znamo da je dimenzija potpolja manja od dimenzije polja pa konačnost $|F'' : F'|$ i $|F' : F|$ slijedi direktno. Neka je $|F' : F| = n$ i $|F'' : F'| = m$ te neka

$\alpha_1, \ldots, \alpha_m$ čine bazu za $F''$ nad $F'$ te $\beta_1, \ldots, \beta_n$ bazu za $F'$ nad $F$. Pokazat ćemo da $\alpha_i\beta_j, i = 1, \ldots, m, j = 1, \ldots, n$ čine bazu za $F''$ nad $F$.
Pokažimo prvo da su $\alpha_i\beta_j$ linearno nezavisni. Pretpostavimo da vrijedi

$$\sum_{i,j} f_{ij}\alpha_i\beta_j = 0.$$

Tada je

$$\sum_j (\sum_i f_{ij}\alpha_i)\beta_j = 0.$$

Elementi $\beta_1, \ldots, \beta_n$ čine bazu pa mora vrijediti $\sum_i f_{ij}\alpha_i = 0$. Nadalje, tada vrijedi $f_{ij} = 0$ za svaki $i = 1, \ldots, m$ te za svaki $j = 1, \ldots, n$. Dakle, $\alpha_i\beta_j$ su linearno nezavisni. Neka je sada $x \in F''$. Možemo ga zapisati kao $x = \sum_i g_i\alpha_i$. No, svaki $g_i$ je iz $F'$ pa njega možemo zapisati u obliku $g_i = \sum_j g_{ij}\beta_j$. Zaključujemo da svaki element iz polja $F''$ možemo prikazati u obliku

$$x = \sum_{i,j} g_{ij}\alpha_i\beta_j,$$

odnosno $\alpha_i\beta_j$ čine bazu za $F''$ nad $F$ te vrijedi

$$mn = |F'' : F| = |F'' : F'||F' : F|.$$

□

**Definicija 3.1.2.** Neka je $F'$ proširenje polja $F$. Za element $\alpha \in F'$ kažemo da je ***algebarski nad*** $F$ ako postoji nekonstantni polinom $p \in F[x]$ takav da je $p(\alpha) = 0$. Ako je svaki element $\alpha \in F'$ algebarski nad $F$ kažemo da je $F'$ ***algebarsko proširenje*** polja $F$.
Ako $\alpha$ nije algebarski nad $F$ kažemo da je ***transcendentan*** nad $F$.

**Teorem 3.1.3.** *Ako je $F'$ proširenje konačnog stupnja od $F$, onda je $F'$ algebarsko proširenje.*

*Dokaz.* Uzmimo proizvoljni element $\alpha \in F'$. Trebamo pokazati da postoji polinom $p \in F[x]$ kojem će $\alpha$ biti nultočka. S obzirom na to da je $F'$ proširenje konačnog stupnja od $F$, znamo da baza od $F'$ nad $F$ ima konačno mnogo elemenata, na primjer $n$ elemenata. Tada će svaki skup od $(n+1)$ elemenata biti linearno zavisan. Uzmimo elemente $1, \alpha, \alpha^2, \ldots, \alpha^n \in F'$. Oni su linearno zavisni pa postoje $\beta_0, \ldots, \beta_n \in F$ koji nisu svi nula takvi da vrijedi

$$\beta_0 + \beta_1\alpha + \cdots + \beta_n\alpha^n = 0.$$

Sada za $p(x) = \beta_0 + \beta_1 x + \cdots + \beta_n x^n$ slijedi tražena tvrdnja. □

**Definicija 3.1.4.** Polje $F$ je ***algebarski zatvoreno*** ako svaki nekonstantni polinom $p \in F[x]$ ima nultočku u polju $F$.

**Definicija 3.1.5.** Neka je $F'$ proširenje polja $F$. Kažemo da je $F'$ **algebarski zatvarač od** $F$ ako je $F'$ algebarsko nad $F$ i $F'$ je algebarski zatvoreno.

**Lema 3.1.6.** *Ako je $\alpha \in F'$ algebarski nad $F$, onda postoji jedinstveni normirani ireducibilni polinom $p \in F[x]$ za koji vrijedi $p(\alpha) = 0$. Taj polinom označavamo sa $irr(\alpha, F)$.*

*Dokaz.* Neka je $\alpha$ algebarski nad $F'$ i neka je $f \in F[x]$ nekonstantni polinom takav da je $f(\alpha) = 0$. Polinom $f$ će se faktorizirati u ireducibilne polinome $p_i, i = 1, 2, \ldots$. U polju ne postoje djelitelji nule pa $\alpha$ mora biti korijen jednog od faktora, na primjer od $p_1$. Polinom $p_1$ možemo normirati što znači da smo našli normirani ireducibilni polinom kojem je $\alpha$ korijen. Sada možemo uzeti takav polinom $p$ koji je najmanjeg stupnja.
Provjerimo sada jedinstvenost. Neka je $g \in F[x]$ neki drugi normirani ireducibilni polinom za koji vrijedi $g(\alpha) = 0$. Polinom $p$ je najmanjeg stupnja pa polinom $g$ ima veći ili jednak stupanj od $p$. Koristimo teorem o dijeljenju polinoma s ostatkom 2.1.1 i dobivamo:

$$g(x) = q(x)p(x) + r(x),$$

gdje je $r$ ili stupnja manjeg od $p$ ili $r \equiv 0$. Nadalje,

$$g(\alpha) = q(\alpha)p(\alpha) + r(\alpha),$$

iz čega slijedi da je $r(\alpha) = 0$. Sada znamo da $r$ mora biti identički jednak nuli jer bi u suprotnom imali polinom kojem je $\alpha$ korijen a manjeg je stupnja od $p$. Dakle, $g(x) = q(x)p(x)$. Polinom $g$ je ireducibilan i normiran pa $q(x) = 1$. Zaključujemo da je $g = p$ te je polinom $p$ jedinstven. □

Neka je $\alpha \in F'$ algebarski nad $F$. Tada definiramo polje $F(\alpha)$ sa

$$F(\alpha) = \{f_0 + f_1\alpha + \cdots + f_{n-1}\alpha^{n-1}; f_i \in F\}.$$

Ukoliko imamo $\alpha, \beta \in F'$ koji su algebarski nad $F$, sa $F(\alpha, \beta)$ označavamo $(F(\alpha))(\beta)$.

**Teorem 3.1.7.** *Ako je $F'$ proširenje konačnog stupnja od $F$, onda postoji konačni skup algebarskih elemenata $\alpha_1, \ldots, \alpha_n$ takvih da je $F' = F(\alpha_1, \ldots, \alpha_n)$.*

*Dokaz.* Neka je $F'$ proširenje konačnog stupnja od $F$, tj. $|F' : F| = k < \infty$. Tada je po teoremu 3.1.3 $F'$ algebarsko proširenje od $F$. S obzirom na to da su tada svi elementi iz $F'$ algebarski nad $F$, odaberimo neki $\alpha_1 \in F'$ koji nije u $F$. Vrijedi

$F \subset F(\alpha_1) \subset F'$ i $|F' : F(\alpha_1)| < k$. Ako je stupanj proširenja jednak jedan, stavimo $F' = F(\alpha_1)$. Ukoliko nije, odaberimo $\alpha_2 \in F'$ koji nije u $F(\alpha_1)$. Tada je $F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset F'$ i $|F' : F(\alpha_1, \alpha_2)| < |F' : F(\alpha_1)|$. Ako je stupanj proširenja jednak jedan, $F' = F(\alpha_1, \alpha_2)$. Ako je veći od jedan, nastavimo postupak. Znamo da je $k$ konačan pa će ovaj proces imati konačan broj koraka. □

**Teorem 3.1.8.** *(Kroneckerov teorem) Neka je $F$ polje i $f \in F[x]$ ireducibilni polinom. Tada postoji proširenje konačnog stupnja $F'$ od $F$ u kojem $f$ ima korijen.*

*Dokaz.* Neka je $f(x) = a_n x^n + \cdots + a_1 x + a_0$ i $a_n \neq 0$. Definirat ćemo $\alpha$ tako da vrijedi

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

Nadalje, definirajmo $F' = F(\alpha)$ kao

$$F(\alpha) = \{f_0 + f_1\alpha + \cdots + f_{n-1}\alpha^{n-1}; f_i \in F\}.$$

Sada ćemo na $F(\alpha)$ definirati zbrajanje i oduzimanje po komponentama i definirat ćemo množenje tako da sve potencije od $\alpha$ koje su veće od $\alpha^n$ zamijenimo koristeći

$$\alpha^n = \frac{-a_0 - a_1\alpha - \cdots - a_{n-1}\alpha^{n-1}}{a_n}. \tag{3.1}$$

Provjerimo sada zadovoljava li $F(\alpha)$ aksiome polja. S obzirom na to kako smo definirali zbrajanje i množenje, slijedi da $F(\alpha)$ zadovoljava sve aksiome $(1) - (9)$ osim osmog. Preostaje pokazati da za svaki nenul element iz $F(\alpha)$ postoji multiplikativni inverz. Neka je $g \in F[x], g \neq 0$. Ako je $\deg(g) < n = \deg(irr(\alpha, F))$ tada $g(\alpha) \neq 0$ jer je $irr(\alpha, F)$ ireducibilni polinom najmanjeg stupnja kojem je $\alpha$ korijen. Ako je $h \in F[x]$ polinom stupnja većeg od $n$, tada $h$ možemo poistovjetiti sa polinomom $h_1$ stupnja manjeg od $n-1$ kojeg ćemo dobiti kada zamijenimo potencije od $\alpha$ koje su veće od $\alpha^n$ koristeći izraz 3.1.
Neka je sada $g \in F(\alpha), g(\alpha) \neq 0$. Pogledajmo odgovarajući polinom $g \in F[x]$ stupnja manjeg od $n-1$. Polinom $irr(\alpha, F) =: p$ je ireducibilan pa su polinomi $g$ i $p$ relativno prosti. Iz diskusije u drugom poglavlju i jednadžbe 2.2 znamo da postoje $h$ i $k \in F[x]$ takvi da vrijedi

$$g(x)h(x) + p(x)k(x) = 1.$$

Za $x = \alpha$ slijedi

$$g(\alpha)h(\alpha) + p(\alpha)k(\alpha) = 1.$$

S obzirom na to da je $\alpha$ korijen od $p$ i $h(\alpha) = h_1(\alpha) \in F[\alpha]$, imamo

$$g(\alpha)h_1(\alpha) = 1,$$

tj. $h_1(\alpha)$ je multiplikativni inverz od $g(\alpha)$.

Ukoliko poistovjetimo skup $F$ sa skupom konstantnih polinoma, slijedi da je $F \subseteq F(\alpha)$. Dakle, $F' = F(\alpha)$ je proširenje od $F$. Nadalje, iz definicije $F(\alpha)$ znamo da $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ čine bazu pa je $F(\alpha)$ dimenzije $n$. Zaključujemo da je $F'$ proširenje konačnog stupnja od $F$ u kojem $f$ ima korijen.

□

Pokažimo na primjeru kako se definira polje proširenja te operacije na njemu.

**Primjer 3.1.9.** *Neka je $f(x) = x^3 - 3 \in \mathbb{Q}[x]$. Polinom $f$ je ireducibilan nad $\mathbb{Q}$, no u polju $\mathbb{R}$ ima korijen $\alpha = 3^{\frac{1}{3}}$. Tada je, prema postupku korištenom u dokazu teorema 3.1.8, proširenje polja $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, definirano sa*

$$\mathbb{Q}(\alpha) = \{f_0 + f_1\alpha + f_2\alpha^2; f_i \in \mathbb{Q} \text{ te } \alpha^3 = 3\}.$$

*Neka je $g(x) = -x^2 - 3x + 6$ i $h(x) = 6x^2 + x + 3$. Tada je*

$$g(\alpha) + h(\alpha) = 5\alpha^2 - 2\alpha + 9,$$

*te zbog $\alpha^3 = 3$,*

$$\begin{aligned} g(\alpha)h(\alpha) &= (-\alpha^2 - 3\alpha + 6)(6\alpha^2 + \alpha + 3) \\ &= -6\alpha^4 - 19\alpha^3 + 30\alpha^2 - 3\alpha + 18 \\ &= 30\alpha^2 - 21\alpha - 39. \end{aligned} \tag{3.2}$$

*Kako bismo pronašli multiplikativni inverz polinoma $g$, primjenjujemo Euklidov algoritam na polinome $g$ i $f$. Vrijedi*

$$x^3 - 3 = (-x^2 - 3x + 6)(-x + 3) + (15x - 21),$$

$$-x^2 - 3x + 6 = (15x - 21)(-\frac{1}{15}x - \frac{22}{75}) - \frac{4}{25}.$$

*Dakle,*

$$1 = -\frac{5}{12}(-\alpha^2 - 3\alpha + 6)(\alpha^2 + \frac{7}{5}\alpha + \frac{9}{5}),$$

*odnosno, inverz od $g$ u $\mathbb{Q}(\alpha)$ je polinom $g^{-1} = \alpha^2 + \frac{7}{5}\alpha + \frac{9}{5}$.*

Sada ćemo definirati polje razlaganja te dokazati teorem o egzistenciji takvog polja.

**Definicija 3.1.10.** Neka je $F$ polje i $f \in F[x]$ nekonstantni polinom. Kažemo da se polinom $f$ ***razlaže nad proširenjem*** $F'$ ***polja*** $F$ ako se $f$ faktorizira u linearne faktore u $F'[x]$, tj. postoji $a \in F$ i $\alpha_1, \ldots, \alpha_n \in F'$ takvi da je

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

Polje $F'$ je ***polje razlaganja za polinom*** $f$ ***nad poljem*** $F$ ako je $F'$ najmanje proširenje polja $F$ u kojem se $f$ razlaže.

**Teorem 3.1.11.** *(Egzistencija polja razlaganja) Neka je $F$ polje i $f \in F[x]$ nekonstantni polinom. Tada postoji polje razlaganja za $f$ nad $F$.*

*Dokaz.* Bez smanjenja općenitosti možemo pretpostaviti da je $f$ ireducibilni polinom stupnja $n$. Teorem dokazujemo indukcijom po stupnju polinoma $f$. Ako je $n = 1$, onda je $f$ oblika $f(x) = a(x - \alpha), \alpha \in F$ pa možemo staviti da je $F$ traženo polje razlaganja. Pretpostavimo sada da je $n \geq 2$ i da tvrdnja vrijedi za polinome stupnja manjeg od $n$. Teorem 3.1.8 povlači da postoji polje $F'$ koje sadrži korijen $\alpha_1$ i vrijedi $f(\alpha_1) = 0$. Tada je $f(x) = (x - \alpha_1)q(x)$, gdje je $q \in F'[x]$ polinom stupnja $n - 1$. Po pretpostavci indukcije slijedi da za $q$ postoji polje razlaganja, tj. postoje korijeni $\alpha_2, \ldots, \alpha_n \in F''$ takvi da je $q(x) = a(x-\alpha_2) \cdots (x-\alpha_n)$. Dakle, $p(x) = a(x-\alpha_1)(x-\alpha_2) \cdots (x - \alpha_n)$ i $\alpha_1, \ldots, \alpha_n \in F''$, odnosno postoji polje razlaganja za $p$ nad $F$. □

U nastavku uvodimo pojam $i$-tog elementarnog simetričnog polinoma te navodimo osnovni teorem o simetričnim polinomima.

**Definicija 3.1.12.** Polinom $f(y_1, \ldots, y_n) \in F[y_1, \ldots, y_n]$ je ***simetričan polinom*** u $y_1, \ldots, y_n$ ako je

$$f(y_1, \ldots, y_n) = f(\sigma(y_1), \ldots, \sigma(y_n))$$

za svaku permutaciju $\sigma$.

Ako su $F \subset F'$ polja i $\alpha_1, \ldots, \alpha_n$ su u $F'$, tada polinom $f(\alpha_1, \ldots, \alpha_n)$ sa koeficijentima u $F$ zovemo ***simetričnim u*** $\alpha_1, \ldots, \alpha_n$ ako je

$$f(\alpha_1, \ldots, \alpha_n) = f(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$$

za svaku permutaciju $\sigma$.

**Definicija 3.1.13.** Neka je $F'$ proširenje polja $F$ i neka su $x, y_1, \ldots, y_n \in F'$. Definirajmo polinom $p \in F[x, y_1, \ldots, y_n]$ sa

$$p(x, y_1, \ldots, y_n) = (x - y_1) \ldots (x - y_n).$$

***I-ti elementarni simetrični polinom*** $s_i$ u $y_1, \ldots, y_n$ za $i = 1, \ldots, n$ je $(-1)^i a_i$ , gdje je $a_i$ koeficijent uz $x^{n-i}$ u polinomu $p$.

**Primjer 3.1.14.** *Općenito, vrijede sljedeće formule za $s_i$:*

$$\begin{aligned}
s_1(y_1, y_2, \ldots, y_n) &= \sum_{i=0}^{n} y_i, \\
s_2(y_1, y_2, \ldots, y_n) &= \sum_{i<j} y_i y_j, \\
s_3(y_1, y_2, \ldots, y_n) &= \sum_{i<j<k} y_i y_j y_k, \\
&\vdots \\
s_n(y_1, y_2, \ldots, y_n) &= y_1 y_2 \cdots y_n.
\end{aligned}$$

*Za $n = 1$, elementarni simetrični polinom je $s_1(y_1) = y_1$.*
*Za $n = 2$, elementarni simetrični polinomi su:*

$$\begin{aligned}
s_1(y_1, y_2) &= y_1 + y_2, \\
s_2(y_1, y_2) &= y_1 y_2.
\end{aligned}$$

*Za $n = 3$, elementarni simetrični polinomi su:*

$$\begin{aligned}
s_1(y_1, y_2, y_3) &= y_1 + y_2 + y_3, \\
s_2(y_1, y_2, y_3) &= y_1 y_2 + y_1 y_3 + y_2 y_3, \\
s_3(y_1, y_2, y_3) &= y_1 y_2 y_3.
\end{aligned}$$

*Za $n = 4$, elementarni simetrični polinomi su:*

$$\begin{aligned}
s_1(y_1, y_2, y_3, y_4) &= y_1 + y_2 + y_3 + y_4, \\
s_2(y_1, y_2, y_3, y_4) &= y_1 y_2 + y_1 y_3 + y_1 y_4 + y_2 y_3 + y_2 y_4 + y_3 y_4, \\
s_3(y_1, y_2, y_3, y_4) &= y_1 y_2 y_3 + y_1 y_2 y_4 + y_1 y_3 y_4 + y_2 y_3 y_4, \\
s_4(y_1, y_2, y_3, y_4) &= y_1 y_2 y_3 y_4.
\end{aligned}$$

**Teorem 3.1.15.** *(Osnovni teorem o simetričnim polinomima) Za svaki simetrični polinom $f \in F[y_1, \ldots, y_n]$ postoji jedinstven polinom $g \in F[y_1, \ldots, y_n]$ takav da je $f(y_1, \ldots, y_n) = g(s_1(y_1, \ldots, y_n), \ldots, s_n(y_1, \ldots, y_n))$.*

Dokaz teorema ne navodimo, no može se naći u knjizi [3].

**Primjer 3.1.16.** *Neka je* $f(y_1, y_2, y_3) = y_1^3 + y_2^3 + y_3^3$. *Elementarne simetrične polinome znamo iz primjera 3.1.14. Tada* $f$ *možemo zapisati u obliku*

$$\begin{aligned} f(y_1, y_2, y_3) &= y_1^3 + y_2^3 + y_3^3 \\ &= (y_1 + y_2 + y_3)^3 - 3y_1^2y_2 - 3y_1y_2^2 - 3y_1^2y_3 - 3y_1y_3^2 - 3y_2^2y_3 - 3y_2y_3^2 \\ &\quad - 6y_1y_2y_3 \\ &= s_1^3 - 3(y_1^2y_2 + y_1y_2^2 + y_1^2y_3 + y_1y_3^2 + y_2^2y_3 + y_2y_3^2 + 3y_1y_2y_3) + 3s_3 \\ &= s_1^3 - 3(y_1 + y_2 + y_3)(y_1y_2 + y_1y_3 + y_2y_3) + 3y_1y_2y_3 \\ &= s_1^3 - 3s_1s_2 + 3s_3. \end{aligned}$$

**Lema 3.1.17.** *Neka je* $p \in F[x]$ *i neka* $p$ *ima korijene* $\alpha_1, \ldots, \alpha_n$ *u polju razlaganja* $F'$. *Tada za svaki elementarni simetrični polinom* $s_i$ *vrijedi* $s_i(\alpha_1, \ldots, \alpha_n) \in F$.

*Dokaz.* Neka je $p$ oblika $p(x) = f_nx^n + \ldots + f_1x + f_0 \in F[x]$. $p$ se razlaže nad $F'$ sa korijenima $\alpha_1, \ldots, \alpha_n$ pa je u $F'[x]$ $p$ oblika

$$p(x) = f_n(x - \alpha_1) \ldots (x - \alpha_n).$$

Koeficijenti su tada $f_n(-1)^i s_i(\alpha_1, \ldots, \alpha_n)$, gdje su $s_i(\alpha_1, \ldots, \alpha_n)$ elementarni simetrični polinomi u $\alpha_1, \ldots, \alpha_n$. S obzirom na to da je $p$ polinom nad poljem $F$, svi njegovi koeficijenti su iz $F$ pa je $f_n(-1)^i s_i(\alpha_1, \ldots, \alpha_n) \in F$, $\forall i$. Tada je i $s_i(\alpha_1, \ldots, \alpha_n) \in F$.

□

**Lema 3.1.18.** *Neka je* $p(x) \in F[x]$ *i pretpostavimo da* $p$ *ima korijene* $\alpha_1, \ldots, \alpha_n$ *u polju razlaganja* $F'$. *Nadalje, pretpostavimo da je* $g = g(x, \alpha_1, \ldots, \alpha_n) \in F'[x]$. *Ako je* $g$ *simetričan polinom u* $\alpha_1, \ldots, \alpha_n$, *onda je* $g \in F[x]$.

*Dokaz.* Ako je $g$ simetričan polinom u $\alpha_1, \ldots, \alpha_n$ tada iz teorema slijedi da je $g$ simetričan polinom u elementarnim simetričnim polinomima $s_i$ u $\alpha_1, \ldots, \alpha_n$. Iz leme 3.1.17 slijedi da su $s_i$ u polju $F$ pa su koeficijenti od $g$ u $F$. Dakle, $g \in F[x]$. □

Na kraju uvoda navedimo jedan važan teorem iz matematičke analize te njegov korolar. To ćemo primijeniti u dokazu leme koja se koristi za dokazivanje osnovnog teorema algebre.

**Teorem 3.1.19.** *(Teorem srednje vrijednosti) Neka je* $f : [a, b] \to \mathbb{R}$ *neprekidna funkcija. Ako je* $f(a) < k < f(b)$ *ili* $f(a) > k > f(b)$, *tada postoji* $c \in [a, b]$ *takav da je* $f(c) = k$.

**Korolar 3.1.20.** *Neka je* $f : [a, b] \to \mathbb{R}$ *neprekidna funkcija i* $f(a)f(b) < 0$. *Tada postoji* $c \in (a, b)$ *takav da je* $f(c) = 0$.

## 3.2 Dokaz osnovnog teorema algebre

U ovom odjeljku ćemo iskazati i dokazati četiri leme pomoću kojih će se osnovni teorem algebre moći jednostavno dokazati.

**Lema 3.2.1.** *Svaki polinom $p \in \mathbb{R}[x]$ neparnog stupnja mora imati realni korijen.*

*Dokaz.* Neka je $p(x) \in \mathbb{R}[x]$ i neka je $deg(p) = n = 2k+1, k \in \mathbb{N}$. Pretpostavimo da je koeficijent $a_n > 0$. Tada je polinom $p$ oblika $p(x) = a_n x^n + \cdots + a_0$. Nadalje, vrijedi

(1) $\lim_{x\to\infty} p(x) = \lim_{x\to\infty} a_n x^n = \infty$, jer je $a_n > 0$.

(2) $\lim_{x\to-\infty} p(x) = \lim_{x\to-\infty} a_n x^n = -\infty$, jer je $n$ neparan i $a_n > 0$.

Sada vidimo da $p$ može biti proizvoljno velik i pozitivan pa postoji točka $x_1$ u kojoj je $p(x_1) > 0$. Nadalje, $p$ može biti i jako negativan, tj. postoji $x_2$ takav da je $p(x_2) < 0$. Iz teorema srednje vrijednosti slijedi da postoji $x_3 \in [x_2, x_1]$ takav da je $p(x_3) = 0$. □

**Lema 3.2.2.** *Svaki polinom stupnja 2 mora imati kompleksan korijen.*

*Dokaz.* Dokaz ove leme je posljedica formule za rješavanje kvadratnih jednadžbi. Ako je $p(x) = ax^2 + bx + c, a \neq 0$, tada su korijeni dani sa

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

Iz DeMoivreova teorema 2.1.9 za korijene znamo da svaki kompleksan broj ima drugi korijen pa $x_1$ i $x_2$ postoje u $\mathbb{C}$. □

**Lema 3.2.3.** *Ako svaki nekonstantni realni polinom ima kompleksan korijen, onda svaki nekonstantni kompleksni polinom ima kompleksan korijen.*

*Dokaz.* Neka je $p \in \mathbb{C}[x]$ i neka svaki nekonstantni realni polinom ima bar jedan kompleksan korijen. Definirajmo $h(x) = p(x)\overline{p}(x)$. Iz leme 2.1.6 slijedi da je $h(x) \in \mathbb{R}[x]$. Po pretpostavci $h$ ima bar jedan kompleksan korijen, neka je to $z_0$. Sada imamo $h(z_0) = p(z_0)\overline{p}(z_0) = 0$. Polje $\mathbb{C}$ nema djelitelja nule pa jedan od članova u prethodnom umnošku mora biti jednak nuli. Ako je $p(z_0) = 0$, tada smo pronašli kompleksni korijen kompleksnog polinoma. Ukoliko je $\overline{p}(z_0) = 0$, iz leme 2.1.5 slijedi da je $\overline{p}(z_0) = \overline{\overline{p}}(\overline{z_0}) = p(\overline{z_0}) = 0$. Dakle, $\overline{z_0}$ je korijen od $p$. □

**Lema 3.2.4.** *Svaki nekonstantni realni polinom ima kompleksni korijen.*

*Dokaz.* Neka je $f(x) = a_n x^n + \cdots + a_0$ realni polinom, $n \geq 1$ i $a_n \neq 0$. Neka je $n$ oblika $n = 2^m q$, gdje je $q$ neparni broj. Dokazat ćemo lemu indukcijom po $m$. Za $m = 0$, $f$ je polinom neparnog stupnja pa iz leme 3.2.1 znamo da $f$ ima realan korijen i teorem vrijedi. Pretpostavimo da tvrdnja vrijedi za $2^{k-1}q, k = 2, \ldots, m$. Neka je stupanj polinoma jednak $n = 2^m q$ i $F'$ polje razlaganja za $f$ nad $\mathbb{R}$ u kojem su korijeni $\alpha_1, \ldots, \alpha_n$. Takvo polje postoji zbog teorema 3.1.11.

Pokazat ćemo da bar jedan od ovih korijena mora biti iz $\mathbb{C}$. Odaberimo $h \in \mathbb{Z}$ i definirajmo polinom $H$ sa

$$H(x) = \prod_{i<j} (x - (\alpha_i + \alpha_j + h\alpha_i\alpha_j)) \quad \in F'[x].$$

Kad smo formirali $H$ odabrali smo parove korijena $\alpha_i, \alpha_j$. Broj takvih parova jednak je broju načina na koji možemo odabrati dva elementa od njih $n = 2^m q$. To je dano sa

$$\binom{2^m q}{2} = \frac{(2^m q)!}{2!(2^m q - 2)!} = 2^{m-1} q(2^m q - 1) = 2^{m-1} q', \text{ gdje je } q' \text{neparan.}$$

Dakle, $H$ je stupnja $2^{m-1}q'$. $H$ je simetričan polinom u korijenima $\alpha_1, \ldots, \alpha_n$. S obzirom na to da su $\alpha_1, \ldots, \alpha_n$ korijeni realnog polinoma iz leme 3.1.18 slijedi da svaki polinom u polju razlaganja simetričan u tim korijenima mora biti realni polinom. Dakle, $H$ je realni polinom stupnja $2^{m-1}q$ pa po pretpostavci indukcije mora imati kompleksni korijen. To znači da postoji par $\alpha_i, \alpha_j$ takvi da vrijede $\alpha_i + \alpha_j + h\alpha_i\alpha_j \in \mathbb{C}$. Zbog proizvoljnosti od $h$ slijedi da za svaki cijeli broj $a$ mora postojati takav par $\alpha_i, \alpha_j$ da vrijedi $\alpha_i + \alpha_j + a\alpha_i\alpha_j \in \mathbb{C}$. Postoji konačan broj parova $\alpha_i, \alpha_j$ pa moraju postojati barem dva različita cijela broja $a_1, a_2$ za koje je

$$z_1 = \alpha_i + \alpha_j + a_1\alpha_i\alpha_j \in \mathbb{C} \quad \text{i} \quad z_2 = \alpha_i + \alpha_j + a_2\alpha_i\alpha_j \in \mathbb{C}.$$

Tada je $z_1 - z_2 = (a_1 - a_2)\alpha_i\alpha_j \in \mathbb{C}$ i $\alpha_i\alpha_j \in \mathbb{C}$ jer je $a_1, a_2 \in \mathbb{Z} \subset \mathbb{C}$. Nadalje, $a_1\alpha_i\alpha_j \in \mathbb{C}$ te iz toga slijedi da je $\alpha_i + \alpha_j \in \mathbb{C}$. Sada imamo

$$p(x) = (x - \alpha_i)(x - \alpha_j) = x^2 - (\alpha_i + \alpha_j)x + \alpha_i\alpha_j \in \mathbb{C}[x].$$

Polinom $p$ je kompleksni polinom stupnja 2 pa iz leme 3.2.2 znamo da mora imati kompleksan korijen. Dakle, $\alpha_i, \alpha_j \in \mathbb{C}$ pa $f$ ima kompleksan korijen.

□

Sada ćemo upotrijebiti sve rezultate koje smo naveli u ovoj točki te tako dokazati osnovni teorem algebre.

**Teorem 3.2.5.** *(Osnovni teorem algebre) Svaki nekonstantni kompleksni polinom ima kompleksni korijen. Drugim riječima, polje kompleksnih brojeva $\mathbb{C}$ je algebarski zatvoreno.*

*Dokaz.* Dokaz slijedi iz dvije leme. Iz leme 3.2.4 znamo da svaki nekonstantni realni polinom ima kompleksni korijen. Lema 3.2.3 kaže da ako svaki nekonstantni realni polinom ima kompleksni korijen, onda i svaki nekonstantan kompleksni polinom ima kompleksni korijen. □

# Poglavlje 4

# Dokazi pomoću kompleksne analize

Kako bismo napravili sljedeći dokaz osnovnog teorema algebre, potrebni su nam rezultati iz kompleksne analize. Krećemo od Cauchyjeva teorema te nakon njega navodimo rezultate koji se oslanjaju na taj teorem. U drugom odjeljku navodimo Liouvilleov teorem i koristimo ga u dokazu osnovnog teorema algebre. Poglavlje završavamo sa još dva dokaza osnovnog teorema algebre koji se temelje na teoremu srednje vrijednosti i na teoremu maksimuma modula.

## 4.1 Uvod

Za početak, navedimo definicije vezane uz svojstva skupova i funkcija koje ćemo koristiti u ovom poglavlju.

**Definicija 4.1.1.** Otvoren i povezan skup $\Omega \subseteq \mathbb{C}$ *je* ***područje****.*

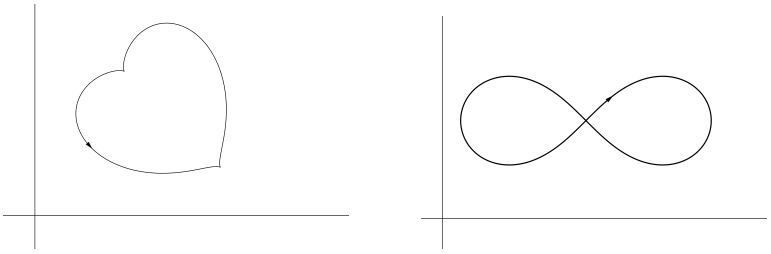
**Definicija 4.1.2.** Neka su $\gamma : [a,b] \to \Omega$, $\delta : [a,b] \to \Omega$ krivulje na području $\Omega$ takve da je $\gamma(a) = \delta(a) = z_1$ i $\gamma(b) = \delta(b) = z_2$. ***Homotopija*** u $\Omega$ od krivulje $\gamma$ do krivulje $\delta$ je neprekidno preslikavanje $H : [0,1] \times [a,b] \to \Omega$ za koje vrijedi:

$$H(0,s) = \gamma(s), \quad H(1,s) = \delta(s), \quad \forall s \in [a,b];$$
$$H(t,a) = z_1, \quad H(t,b) = z_2, \quad \forall t \in [0,1].$$

Kažemo da su krivulje ***homotopne*** ako postoji homotopija u $\Omega$ od krivulje $\gamma$ do krivulje $\delta$.

**Definicija 4.1.3.** Put $\gamma : [a,b] \to \Omega$ je ***nulhomotopan*** ako je homotopan s konstantnim preslikavanjem $\delta$, $\delta(t) = \gamma(a) = \gamma(b), \forall t \in [a,b]$.

**Definicija 4.1.4.** Kažemo da je put $\gamma : [a,b] \to \mathbb{C}$ ***jednostavno zatvoren*** ako vrijedi $\gamma(a) = \gamma(b)$ i $\gamma(t_1) \neq \gamma(t_2)$ za svaki $t_1, t_2 \in [a,b)$.



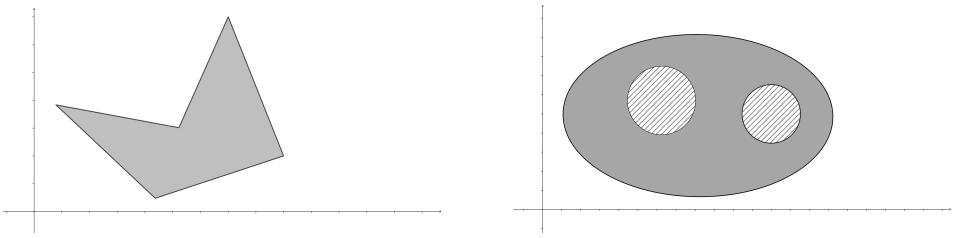
(a) Jednostavno zatvoren put

(b) Put koji nije jednostavno zatvoren

Slika 4.1

**Definicija 4.1.5.** Područje je ***jednostavno povezano*** ako je svaki zatvoren put nulhomotopan.

Na slici 4.2 su primjeri jednostavno povezanog područja te područja koje nije jednostavno povezano.



(a) Jednostavno povezano područje

(b) Područje koje nije jednostavno povezano

Slika 4.2

**Definicija 4.1.6.** Za funkciju $f : \Omega \to \mathbb{C}$ kažemo da je ***holomorfna*** na otvorenom skupu $\Omega \subset \mathbb{C}$ ako postoji derivacija $f'(z)$ za svaki $z \in \Omega$. Funkcija $f(z)$ je ***holomorfna u točki*** $z_0$ ako postoji okolina točke $z_0$ na kojoj je $f$ holomorfna. Ako je $f$ holomorfna na $\mathbb{C}$ kažemo da je $f$ ***cijela***.

**Teorem 4.1.7.** *(Cauchy-Riemannov teorem) Neka je $f = u + iv : \Omega \to \mathbb{C}$ i $z_0 = (x_0, y_0) \in \Omega$. Funkcija $f$ je derivabilna u $z_0$ ako i samo ako je funkcija $(x, y) \mapsto (u(x, y), v(x, y))$ diferencijabilna u $(x_0, y_0)$ i vrijede* ***Cauchy-Riemannovi uvjeti:***

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y} \quad i \quad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

Dokaz ovog teorema može se naći u knjizi [5].

**Definicija 4.1.8.** Neka je $f : \Omega \to \mathbb{C}$ holomorfna i $\gamma : [a, b] \to \Omega$ po dijelovima gladak put. Tada ***kompleksni integral*** definiramo s:

$$\int_\gamma f(z)dz = \int_a^b f(\gamma(t))\gamma'(t)dt.$$

**Teorem 4.1.9.** *(Greenov teorem) Neka je $D \subset \mathbb{R}^2$ povezan i kompaktan skup čiji je rub $\partial D$ sastavljen od konačno mnogo međusobno disjunktnih po dijelovima glatkih zatvorenih krivulja koje su pozitivno orijentirane u odnosu na $D$. Pretpostavimo da su $F, G : \Omega \to \mathbb{R}$ neprekidno diferencijabilne funkcije na otvorenom skupu $\Omega$ koji sadrži $D$ i $\partial D$. Tada vrijedi:*

$$\int_{\partial D} Fdx + Gdy = \int\int_D (\frac{\partial G}{\partial x} - \frac{\partial F}{\partial y})dxdy.$$

Ovaj teorem nećemo dokazivati, no dokaz se može naći u knjizi [7].

**Teorem 4.1.10.** *(Cauchyjev teorem) Neka je $f : \Omega \to \mathbb{C}$ holomorfna funkcija za koju vrijedi da je $f'$ neprekidna i neka je $\Omega \subset \mathbb{C}$ područje. Tada je*

$$\int_\gamma f(z)dz = 0$$

*za svaki po dijelovima gladak zatvoren nulhomotopan put $\gamma$.*

*Dokaz.* Neka je $z = x + iy$ i $f(z) = u + iv$. Raspišemo integral i imamo:

$$\int_\gamma f(z)dz = \int_\gamma (udx - vdy) + i\int_\gamma (vdx + udy).$$

Funkcije $\frac{\partial u}{\partial x}, \frac{\partial u}{\partial y}, \frac{\partial v}{\partial x}, \frac{\partial v}{\partial y}$ su neprekidne te možemo iskoristiti teorem 4.1.9 i slijedi

$$\int_\gamma f(z)dz = \int\int (-\frac{\partial v}{\partial x} - \frac{\partial u}{\partial y})dxdy + i\int\int (\frac{\partial u}{\partial x} - \frac{\partial v}{\partial y})dxdy.$$

Sada traženi rezultat slijedi iz Cauchy-Riemannovih uvjeta. □

**Napomena 4.1.11.** Gornji teorem vrijedi i bez pretpostavke da je $f'$ neprekidna. Tada se radi o Cauchy-Goursatovom teoremu za zvjezdaste skupove. Dokaz se temelji na sljedećem teoremu:

**Teorem 4.1.12.** *(Goursat-Pringsheim) Neka je $\Omega \subset \mathbb{C}$ otvoren skup, $\Delta \subset \Omega$ trokut i neka je $f : \Omega \to \mathbb{C}$ derivabilna funkcija. Tada vrijedi:*

$$\int_{\partial\Delta} f(z)dz = 0.$$

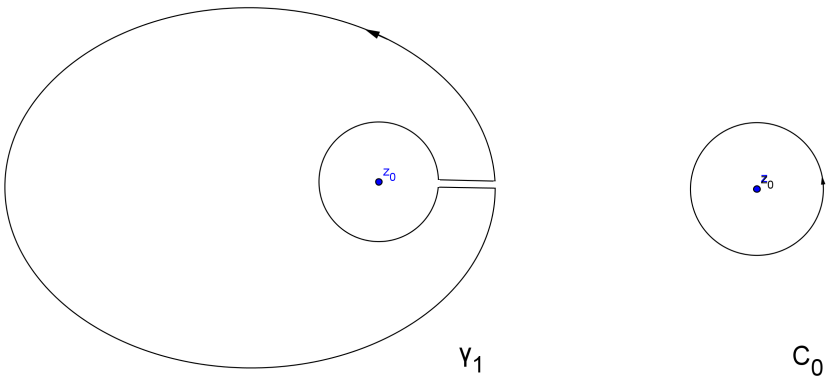
Dokaz Goursat-Pringsheimova teorema može se naći u knjizi [5].

**Teorem 4.1.13.** *(Cauchyjeva integralna formula) Neka je $f : \Omega \to \mathbb{C}$ holomorfna na području $\Omega$ , $\gamma$ po dijelovima gladak jednostavno zatvoren put čije je unutrašnje područje sadržano u $\Omega$ i neka točka $z_0$ pripada tom unutrašnjem području.*

*Tada vrijedi*

$$f(z_0) = \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{z - z_0}dz.$$

*Dokaz.* Neka je $C_0 = K(z_0, r_0)$. Put $\gamma$ možemo rastaviti na $\gamma = \gamma_1 + C_0$ gdje $\gamma_1$ zaobilazi $z_0$ a $C_0$ ga okružuje.




Slika 4.3: Rastav puta $\gamma$

Sada imamo:

$$\int_\gamma \frac{f(z)}{z - z_0}dz = \int_{\gamma_1} \frac{f(z)}{z - z_0}dz + \int_{C_0} \frac{f(z)}{z - z_0}dz.$$

Iz teorema 4.1.10 slijedi da je $\int_{\gamma_1} \frac{f(z)}{z-z_0}dz = 0$ jer $\gamma_1$ ne okružuje $z_0$. Slijedi:

$$\int_\gamma \frac{f(z)}{z - z_0}dz = \int_{C_0} \frac{f(z)}{z - z_0}dz = f(z_0)\int_{C_0} \frac{dz}{z - z_0} + \int_{C_0} \frac{f(z) - f(z_0)}{z - z_0}dz.$$

Na $C_0$ je $z = z_0 + r_0 e^{it} \Rightarrow dz = ir_0 e^{it} dt$, te vrijedi

$$\int_{C_0} \frac{dz}{z - z_0} = \int_0^{2\pi} \frac{ir_0 e^{it}}{z_0 + r_0 e^{it} - z_0} = i \int_0^{2\pi} dt = 2\pi i.$$

Zbog neprekidnosti od $f$ u $z_0$, za dovoljno mali $r_0$ i $z \in C_0$ vrijedi $|f(z) - f(z_0)| < \epsilon$. Tada slijedi

$$|I| := \left| \int_{C_0} \frac{f(z) - f(z_0)}{z - z_0} dz \right| \leq \int_{C_0} \frac{|f(z) - f(z_0)|}{|z - z_0|} |dz| < \frac{\epsilon}{r_0} 2\pi r_0 = 2\pi\epsilon.$$

U gornjoj nejednakosti $\epsilon$ može biti proizvoljno mali pa slijedi $I = 0$. Sada imamo

$$\int_\gamma \frac{f(z)}{z - z_0} dz = f(z_0) 2\pi i + 0 \quad \Rightarrow f(z_0) = \frac{1}{2\pi i} \int_\gamma \frac{f(z)}{z - z_0} dz.$$

□

**Teorem 4.1.14.** *(Deriviranje unutar integrala) Neka je $\Omega$ otvoren skup, a $f : \Omega \times [a, b] \to \mathbb{C}$ neprekidna funkcija čija derivacija po varijabli $z$ postoji i neprekidna je. Tada je $g : \Omega \to \mathbb{C}$, $g(z) = \int_a^b f(z, t) dt$ derivabilna na $\Omega$ i vrijedi*

$$g'(z) = \int_a^b \frac{\partial f}{\partial z}(z, t) dt.$$

*Dokaz.* Dokažimo prvo rezultat za funkcije $F : [a, b] \times [c, d] \to \mathbb{R}$ i $G(z) = \int_a^b F(z, t) dt$ uz pretpostavku da derivacija od $F$ po prvoj varijabli $z$ postoji i neprekidna je. Dakle, dokazujemo da je $G$ derivabilna te da vrijedi

$$G'(z) = \int_a^b \frac{\partial F}{\partial z}(z, t) dt. \tag{4.1}$$

Iz teorema srednje vrijednosti slijedi $\frac{F(z+h,t) - F(z,t)}{h} = \frac{\partial F}{\partial z}(z', t)$, gdje je $z \leq z' \leq z + h$. Nadalje, imamo

$$\begin{aligned}
\left| \frac{G(z + h) - G(z)}{h} - \int_a^b \frac{\partial F}{\partial z}(z, t) dt \right| &= \left| \int_a^b \left( \frac{F(z + h, t) - F(z, t)}{h} - \frac{\partial F}{\partial z}(z, t) \right) dt \right| \\
&= \left| \int_a^b \left( \frac{\partial F}{\partial z}(z', t) - \frac{\partial F}{\partial z}(z, t) \right) dt \right| \\
&\leq \int_a^b \left| \frac{\partial F}{\partial z}(z', t) - \frac{\partial F}{\partial z}(z, t) \right| dt.
\end{aligned}$$

Funkcija $\frac{\partial F}{\partial z}$ je neprekidna na kompaktu $[a,b]\times[c,d]$ pa je i uniformno neprekidna. To znači da za svaki $\epsilon > 0$ postoji $\delta > 0$ takvi da za $|h| < \delta$ vrijedi

$$\left|\frac{\partial F}{\partial z}(z',t) - \frac{\partial F}{\partial z}(z,t)\right| < \frac{\epsilon}{b-a}.$$

Odavde slijedi

$$\int_a^b \left|\frac{\partial F}{\partial z}(z',t) - \frac{\partial F}{\partial z}(z,t)\right| dt < \int_a^b \frac{\epsilon}{b-a}dt = \epsilon.$$

Dakle, izraz $\left|\frac{G(z+h)-G(z)}{h} - \int_a^b \frac{\partial F}{\partial z}(z,t)dt\right|$ konvergira u 0 kada $h \to 0$.

Sada možemo dokazati teorem. Neka je $z = x + iy$, $f(z,t) = f(x,y,t) = u(x,y,t) + iv(x,y,t)$ i $g(z) = \int_a^b f(z,t)dt$. Definirajmo još funkcije $p$ i $q$ sa $p(x,y) := \int_a^b u(x,y,t)dt$ i $q(x,y) := \int_a^b v(x,y,t)dt$. Tada za $g$ vrijedi

$$\begin{aligned} g(z) = g(x,y) = \int_a^b f(z,t)dt &= \int_a^b u(x,y,t)dt + i\int_a^b v(x,y,t)dt \\ &= p(x,y) + iq(x,y). \end{aligned}$$

Iz 4.1 slijedi:

$$\begin{aligned} \frac{\partial g}{\partial x}(x,y) &= \frac{\partial p}{\partial x}(x,y) + i\frac{\partial q}{\partial x}(x,y), \\ \frac{\partial g}{\partial y}(x,y) &= \frac{\partial p}{\partial y}(x,y) + i\frac{\partial q}{\partial y}(x,y). \end{aligned}$$

Parcijalne derivacije $p$ i $q$ po $x$ i $y$ su neprekidne a zbog neprekidnosti od $f$ i $\frac{\partial f}{\partial z}$ za $u, v, p$ i $q$ vrijede Cauchy-Riemannovi uvjeti. Dakle, vrijedi

$$\frac{\partial p}{\partial x} = \frac{\partial q}{\partial y} \quad \text{i} \quad \frac{\partial p}{\partial y} = -\frac{\partial q}{\partial x}.$$

Koristeći teorem 4.1.7, zaključujemo da je $g$ derivabilna.

□

**Korolar 4.1.15.** *Neka je $f : \Omega \to \mathbb{C}$ holomorfna na jednostavno povezanom području $\Omega$ koje sadrži po dijelovima gladak zatvoren put $\gamma$. Ako je $z_0$ unutrašnja točka od $\gamma$, tada za n-tu derivaciju od $f$ vrijedi*

$$f^{(n)}(z_0) = \frac{n!}{2\pi i}\int_\gamma \frac{f(z)}{(z-z_0)^{n+1}}dz.$$

*Dokaz.* Po teoremu 4.1.13 vrijedi

$$f(z_0) = \frac{1}{2\pi i} \int_\gamma \frac{f(z)}{z - z_0} dz.$$

Deriviranjem unutar integrala po varijabli $z_0$ imamo

$$f'(z_0) = \frac{1}{2\pi i} \int_\gamma \frac{f(z)}{(z - z_0)^2} dz$$

te indukcijom dobivamo traženu formulu.

□

**Teorem 4.1.16.** *(Cauchyjeva ocjena) Neka je $f(z) : \Omega \to \mathbb{C}$ holomorfna na jednostavno povezanom području $\Omega$ koje sadrži zatvoreni krug $C_0 = \overline{K(z_0, r_0)}$.*

*Tada vrijedi*

$$|f^{(n)}(z_0)| \leq \frac{n!M}{r_0^n}, \text{ gdje je } M = \max_{C_0} |f(z)|.$$

*Posebno, ako je $|f(z)| < M$ za $z \in C_0$, tada vrijedi*

$$|f'(z)| < \frac{M}{r_0} \quad \text{za sve } z \in K(z_0, r_0).$$

*Dokaz.* Iz korolara 4.1.15 slijedi:

$$|f^{(n)}(z_0)| \leq \left| \frac{n!}{2\pi i} \int_{C_0} \frac{f(z)}{(z - z_0)^{n+1}} dz \right| \leq \frac{Mn!}{2\pi} \left| \int_{C_0} \frac{dz}{(z - z_0)^{n+1}} \right|.$$

Na $C_0$, $z = z_0 + r_0 e^{it} \Rightarrow dz = i r_0 e^{it}$ pa je

$$\left| \int_{C_0} \frac{dz}{(z - z_0)^{n+1}} \right| = \left| \int_0^{2\pi} \frac{dt}{r_0^n e^{itn}} \right| = \frac{2\pi}{r_0^n}.$$

Tada je

$$|f^{(n)}(z_0)| \leq \frac{Mn!}{r_0^n}.$$

□

## 4.2 Dokaz osnovnog teorema algebre

U ovom odjeljku iskazujemo i dokazujemo Liouvilleov teorem te pomoću njega dokazujemo osnovni teorem algebre.

**Teorem 4.2.1.** *(Liouvilleov teorem) Neka je $f : \mathbb{C} \to \mathbb{C}$ cijela i neka je $f$ ograničena na $\mathbb{C}$. Tada je $f$ konstanta.*
*Općenitije, ako je $f^{(n)}$ ograničena na $\mathbb{C}$, tada je $f$ polinom stupnja najviše $n+1$.*

*Dokaz.* Neka je $f : \mathbb{C} \to \mathbb{C}$ cijela funkcija i neka je ograničena, tj. takva da postoji neki $M > 0$ za koji je $|f(z)| \leq M, \forall z \in \mathbb{C}$. Iz Cauchyeve ocjene za $z_0 = 0$ na $K(0,r)$ slijedi

$$|f'(z)| < \frac{M}{r} \quad \text{za sve } z \in K(0,r).$$

S obzirom na to da je $f$ cijela funkcija, možemo pustiti $r \to \infty$. Iz Cauchyjeve ocjene slijedi $|f'(z)| = 0$ te $f'(z) = 0$. Tada je $f$ konstantna.

Sada dokazujemo općenitiju tvrdnju. Ako je $f^{(n)}$ ograničena na $\mathbb{C}$ tada vrijedi $|f^{(n)}(z)| \leq M$ za svaki $z \in \mathbb{C}$. Iz Cauchyjeve ocjene primjenjene na $f^n$ slijedi

$$|f^{(n+1)}(z)| \leq \frac{M}{r} \text{ za sve } z \in K(0,r) \text{ i za svaki } r > 0.$$

Isto kao gore, puštajući da $r$ ide u beskonačnost, dobivamo $f^{(n+1)}(z) = 0$ te je $f^{(n)}$ konstanta. No, tada je $f$ polinom stupnja najviše $n+1$. □

**Teorem 4.2.2.** (Osnovni teorem algebre) *Neka je $P$ kompleksni polinom stupnja većeg ili jednakog jedan. Tada $P$ ima bar jedan kompleksni korijen, tj. postoji $z_0 \in \mathbb{C}$ takav da je $P(z_0) = 0$.*

*Dokaz.* Neka je $P(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0, n \geq 1$. Polinomi su derivabilni na $\mathbb{C}$ pa je $P$ cijela funkcija. Dokazujemo teorem kontrapozicijom tako da pretpostavimo $P(z) \neq 0, \forall z \in \mathbb{C}$. Definirajmo $f : \mathbb{C} \to \mathbb{C}$ sa $f(z) = \frac{1}{P(z)}$. S obzirom na to da je $P$ cijela funkcija i $f$ je cijela. Nadalje, vrijedi

$$\begin{aligned} |f(z)| &= \frac{1}{|P(z)|} = \frac{1}{|z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0|} \\ &= \frac{1}{|z|^n} \frac{1}{|1 + \frac{a_{n-1}}{z} + \cdots + \frac{a_0}{z^n}|}. \end{aligned}$$

Kada $|z| \to \infty$, vrijedi $\frac{1}{|z|^n} \to 0$ te tada i $\frac{a_{n-1}}{z}, \cdots, \frac{a_0}{z^n}$ teže u 0. Iz toga slijedi $\frac{1}{1+\frac{a_{n-1}}{z}+\cdots+\frac{a_0}{z^n}} \to 1$ te je $\lim_{|z|\to\infty} |f(z)| = 0$. Dakle, $f$ je ograničena funkcija. Iz Liouvilleova teorema slijedi da $f$ mora biti konstanta. Tada je i $P$ konstantan što je kontradikcija sa pretpostavkom da je $P$ polinom stupnja barem 1. □

## 4.3 Još dva dokaza osnovnog teorema algebre

U nastavku dajemo još dva dokaza pomoću kompleksne analize.

**Lema 4.3.1.** *(Teorem i nejednakost srednje vrijednosti za kompleksne integrale) Neka je funkcija f holomorfna na nekom $\Omega \subseteq \mathbb{C}$ koji sadrži $C = K(z_0, r)$ i neka je $\gamma(t) = z_0 + re^{it}, 0 \leq t \leq 2\pi$ parametrizacija od $\partial C$.*
*Tada vrijedi*

$$f(z_0) = \frac{1}{2\pi} \int_0^{2\pi} f(z_0 + re^{it})dt \qquad \textit{(Teorem srednje vrijednosti)}$$

*i*

$$|f(z_0)| \leq max_{\partial C}|f| \qquad \textit{(Nejednakost srednje vrijednosti).}$$

*Dokaz.* Neka je $\gamma$ navedena parametrizacija od $\partial C$. Iz teorema 4.1.13 slijedi

$$\begin{aligned} f(z_0) = \frac{1}{2\pi i} \int_\gamma \frac{f(z)}{z - z_0} dz &= \frac{1}{2\pi i} \int_0^{2\pi} \frac{f(\gamma(t))\gamma'(t)dt}{\gamma(t) - z_0} \\ &= \frac{1}{2\pi i} \int_0^{2\pi} \frac{f(z_0 + re^{it})}{z_0 + re^{it} - z_0} ire^{it} dt \\ &= \frac{1}{2\pi} \int_0^{2\pi} f(z_0 + re^{it})dt. \end{aligned}$$

Sada imamo

$$\begin{aligned} |f(z_0)| = \left| \frac{1}{2\pi} \int_0^{2\pi} f(\gamma(t))dt \right| &\leq \frac{1}{2\pi} \left| \int_0^{2\pi} f(\gamma(t))dt \right| \\ \leq \frac{1}{2\pi} \int_0^{2\pi} |f(\gamma(t))|\, dt &\leq \frac{1}{2\pi} \max_{\partial C} |f| \int_0^{2\pi} dt = \max_{\partial C} |f|. \end{aligned}$$

□

**Lema 4.3.2.** *Neka je $P(z) = a_n z^n + \cdots + a_1 z + a_0$ kompleksni polinom stupnja $n \geq 1$. Tada postoji $R \geq 1$ takav da za sve $z \in \mathbb{C}$ , $|z| \geq R$ vrijedi*

$$\frac{1}{2}|a_n||z^n| \leq |P(z)| \leq 2|a_n||z|^n.$$

*Posebno,* $\lim_{|z| \to \infty} |P(z)| = +\infty$.

*Dokaz.* Neka je $R(z) = |a_0| + |a_1||z| + \cdots + |a_{n-1}||z|^{n-1}$. Koristimo nejednakost trokuta:

$$|x| - |y| \leq |x + y| \leq |x| + |y|, \quad \forall x, y \in \mathbb{C}.$$

Tada za $x = a_n z^n$ i $y = a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$ slijedi:

$$\begin{aligned} |a_n z^n| - |a_{n-1}z^{n-1}| - \cdots - |a_0| &\leq |a_n z^n + \cdots + a_1 z + a_0| \\ &\leq |a_n z^n| + |a_{n-1}z^{n-1}| + \cdots + |a_0|. \end{aligned}$$

Dakle,

$$|a_n||z|^n - R(z) \leq |P(z)| \leq |a_n||z|^n + R(z).$$

Ako je $|z| \geq 1$, tada vrijedi $|z|^i \leq |z|^{n-1}$ za svaki $i < n$, i imamo da je $R(z) \leq \sum_{i=0}^{n-1} |a_i||z|^{n-1} =: k|z|^{n-1}$.

Iz toga za izbor $R := max\{1, 2k|a_n|^{-1}\}$ slijedi tražena nejednakost. □

Sada možemo napraviti dokaz osnovnog teorema algebre.

*Dokaz.* (Osnovni teorem algebre)

Neka je $P(z) = a_n z^n + \cdots + a_1 z + a_0$ kompleksni polinom, $n \geq 1$. Pretpostavimo da $P$ nema korijen u $\mathbb{C}$. Tada je $f(z) = \frac{1}{P(z)}$ holomorfna na $\mathbb{C}$ pa možemo primjeniti nejednakost srednje vrijednosti iz leme 4.3.1 te dobivamo izraz

$$|f(0)| \leq max_{\partial C_r}|f(z)|$$

za sve krugove $C_r = K(0, r), r > 0$. Iz leme 4.3.2 znamo da je $\lim_{|z|\to\infty} |P(z)| = +\infty$ te iz toga slijedi $lim_{z\to\infty}|f(z)| = 0$ i $f(0) = 0$ . To vodi do kontradikcije jer $f(0) = \frac{1}{P(0)} \neq 0$. □

Osnovni teorem algebre može se dokazati i koristeći princip maksimuma modula. U nastavku prvo navodimo iskaz i dokaz principa maksimuma modula za krug. Nakon toga dokazujemo teorem maksimuma modula te na kraju dajemo dokaz osnovnog teorema algebre.

**Teorem 4.3.3.** *(Princip maksimuma modula za krug) Neka je $f$ holomorfna na $K(z_0, R), R > 0$ i neka vrijedi*

$$|f(z)| \leq |f(z_0)|, \quad \forall z \in K(z_0, R).$$

*Tada je $f$ konstanta.*

*Dokaz.* Za fiksiran $0 < r < R$ iz leme 4.3.1 i pretpostavke teorema slijedi da je

$$|f(z_0)| \leq \frac{1}{2\pi}\int_0^{2\pi} |f(z_0 + re^{it})|dt \leq \frac{1}{2\pi}\int_0^{2\pi} |f(z_0)|dt = |f(z_0)|.$$

Dakle, vrijedi

$$\int_0^{2\pi} (|f(z_0)| - |f(z_0 + re^{it})|)dt = 0,$$

iz čega zbog neprekidnosti i nenegativnosti funkcije pod integralom zaključujemo da je ona identički jednaka nuli, tj. $|f|$ je konstanta.
Neka je $f = u + iv$. Tada je $|f| = |u + iv| = \sqrt{u^2 + v^2}$ te je

$$u^2 + v^2 = k, \tag{4.2}$$

gdje je $k$ konstanta. Sad ćemo prvo derivirati 4.2 po $x$ a zatim po $y$. Dobivamo

$$\begin{aligned} 2u\frac{\partial u}{\partial x} + 2v\frac{\partial v}{\partial x} &= 0, \\ 2u\frac{\partial u}{\partial y} + 2v\frac{\partial v}{\partial y} &= 0. \end{aligned} \tag{4.3}$$

Primjenimo Cauchy-Riemannove jednadžbe te imamo

$$\begin{aligned} u\frac{\partial u}{\partial x} - v\frac{\partial u}{\partial y} &= 0, \\ u\frac{\partial u}{\partial y} + v\frac{\partial u}{\partial x} &= 0. \end{aligned}$$

Pomnožimo prvu jednadžbu s $u$ i drugu s $v$, dobivene rezultate zbrojimo i dobivamo $(u^2 + v^2)\frac{\partial u}{\partial x} = 0$, odnosno $k\frac{\partial u}{\partial x} = 0$. Ako je $k = 0$, tvrdnja odmah slijedi. Neka je $k \neq 0$. Tada je $\frac{\partial u}{\partial x} = 0$ i iz Cauchy-Riemannovih jednadžbi slijedi da je $\frac{\partial v}{\partial y} = 0$. Sada iz jednadžbi 4.3 dobivamo

$$\begin{aligned} v\frac{\partial v}{\partial x} &= 0, \\ u\frac{\partial u}{\partial y} &= 0. \end{aligned}$$

Znamo da je $k \neq 0$ pa $u$ i $v$ ne mogu istovremeno biti jednaki nuli. Ako je $v \neq 0$, onda je $\frac{\partial v}{\partial x} = 0$ a time je i $\frac{\partial u}{\partial y} = 0$. Analogno slijedi ako je $u \neq 0$. Dakle, $u$ i $v$ su konstantne pa je $f$ konstantna. □

Sljedeći teorem bit će nam potreban u dokazu teorema maksimuma modula, dokaz se može naći u [5].

**Teorem 4.3.4.** *(Teorem o jedinstvenosti holomorfne funkcije) Neka je skup $\Omega \subseteq \mathbb{C}$ otvoren i povezan i neka su $f$ i $g$ holomorfne na $\Omega$. Ako se $f$ i $g$ podudaraju na nekom skupu koji ima gomilište u $\Omega$, onda je $f = g$ na $\Omega$.*

**Teorem 4.3.5.** *(Teorem maksimuma modula) Neka je $f$ nekonstantna i holomorfna na ograničenom području $D$ i neprekidna na $\partial D$. Tada $|f|$ ne postiže maksimum u unutrašnjoj točki od $D$, tj. maksimum se postiže na rubu od $D$.*

*Dokaz.* Znamo da je zatvoren i ograničen skup $\overline{D} = D \cup \partial D$ kompaktan. Funkcija $|f|$ je neprekidna na $\overline{D}$ pa prema teoremu 2.2.2 postiže maksimum na $\overline{D}$. Nazovimo točku u kojoj poprima maksimum $z_0$.

Pretpostavimo da $z_0 \notin \partial D$. Skup $D$ je otvoren te oko $z_0$ možemo opisati krug radijusa $R > 0$ koji će biti sadržan u $D$. Sada po principu maksimalnog modula za krug imamo da $|f|$ postiže maksimum na $K(z_0, R)$ u točki $z_0$ pa je $f$ konstanta na tom krugu. Nadalje, $f$ je tada po teoremu 4.3.4 konstantna na cijelom $D$ što nam daje kontradikciju. Dakle, maksimum je na rubu. □

**Korolar 4.3.6.** *(Princip minimuma) Neka je $f$ holomorfna na području $\Omega$ i neka postoji točka $z_0 \in \Omega$ koja je točka lokalnog minimuma za $|f|$, tj. postoji $C_\epsilon = K(z_0, \epsilon) \subseteq \Omega$ tako da vrijedi $|f(z_0)| \leq |f(z)|$ za sve $z \in C_\epsilon$. Tada je ili $f(z_0) = 0$ ili je $f$ konstanta na $\Omega$.*

*Dokaz.* Pretpostavimo da je $f \neq 0$. Pogledajmo funkciju $g := \frac{1}{f}$. Funkcija $f$ ima lokalni minimum u točki $z_0$ pa funkcija $g$ ima lokalni maksimum u $z_0$. Sada iz teorema maksimalnog modula za krug slijedi da je $f$ konstantna. □

Sada možemo primjeniti sve gore navedene teoreme i dati posljednji dokaz osnovnog teorema algebre.

*Dokaz.* (Osnovni teorem algebre)

Neka je $P(z) = a_n z^n + \cdots + a_1 z + a_0$ kompleksni polinom stupnja $n \geq 1$. Za svaki $r > 0$, neka je $C_r = \overline{K(0, r)}$. Svaki $C_r$ je kompaktan skup pa zbog neprekidnosti od $P$ slijedi da $|P|$ ima minimum u nekoj točki $z_m \in C_m$. S obzirom na to da vrijedi $\lim_{|z|\to\infty} |P(z)| = +\infty$, možemo odabrati dovoljno velik $R$ tako da točka minimuma $z_R$ bude u interioru od $C_R$. Kako bi to vidjeli, neka je $s > 0$ takav da je $|P(z)| > |P(0)| = |a_0|$ za $|z| > s$. Neka je $R > s$. Tada za svaku točku na rubu od $C_R$ vrijedi $|P(z)| > |P(0)|$ pa točka minimuma $z_R$ mora biti u interioru od $C_R$.

Oko $z_R$ možemo opisati otvorenu kuglu radijusa $\epsilon$, $C_\epsilon = K(z_R, \epsilon)$, $C_\epsilon \subset C_R$. No, $P(z)$ je holomorfna na $C_\epsilon$ i vrijedi $|P(z)| \geq |P(z_R)|$ za sve $z \in C_\epsilon$. Iz korolara 4.3.6 imamo da je ili $P(z_R) = 0$ ili je $P$ lokalno konstantan na $C_\epsilon$. Kada bi $P$ bio lokalno

konstantan na $C_\epsilon$, $P(z) = c, \forall z \in \mathbb{C}_\epsilon$, tada bi polinom $g(z) = P(z) - c$ imao beskonačno mnogo korijena. To nije moguće jer polinom nad nekim poljem može imati samo konačan broj korijena. Dakle, $P(z_R) = 0$. □

# Bibliografija


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

[2] J.J. O'Connor i E.F. Robertson, *The fundamental theorem of algebra*, 1996, `http://www-history.mcs.st-andrews.ac.uk/HistTopics/Fund_theorem_of_algebra.html`.

[3] B. Pavković i D. Veljan, *Elementarna matematika 1*, Tehnička knjiga, Zagreb, 1992.

[4] I. Stewart, *Galois Theory*, Chapman and Hall, London, 1973.

[5] Š. Ungar, *Matematička analiza 4*, skripta, 2001, `http://web.math.pmf.unizg.hr/~ungar/NASTAVA/MA/Analiza4.pdf`.

[6] Š. Ungar, *Matematička analiza 3*, PMF-Matematički odjel, Zagreb, 2002, `http://web.math.pmf.unizg.hr/~ungar/NASTAVA/MA/Analiza3.pdf`.

[7] Š. Ungar, *Matematička analiza u* $\mathbb{R}^n$, PMF-Matematički odjel, Zagreb, 2005.

# Sažetak

U ovom diplomskom radu obradili smo nekoliko dokaza osnovnog teorema algebre. Na samom početku rada naveli smo povijesni pregled ovog teorema. U drugom smo poglavlju iskoristili svojstva kompleksnih polinoma te dali prvi dokaz. U sljedećem poglavlju smo interpretirali kompleksne polinome kao algebarske objekte. Na taj smo način mogli dokazati teorem primijenivši svojstva polja i njihovih proširenja. Posljednje poglavlje posvećeno je kompleksnoj analizi. Pokazali smo da se osnovni teorem algebre može dokazati primjenom Liouvilleova teorema. Na kraju rada izložili smo još dva dokaza koji se temelje na teoriji kompleksne analize. U prvom smo koristili nejednakost srednje vrijednosti, a u drugom princip maksimuma modula.

# Summary

In this graduate thesis we prove the fundamental theorem of algebra in several ways. In the first chapter we give a the historical overview of this theorem. In the second chapter we outline the first proof using properties of complex polynomials. In the next chapter, we interpret complex polynomials as algebraic objects. In this way we are able to present the second proof by applying field and extension field properties. The final chapter is dedicated to complex analysis. We demostrate that the fundamental theorem of algebra can be proved by using Liouville's theorem. At the end of the work, we give two additional proofs rooted in complex analysis. The first one uses the mean value inequality and the second one is based on the maximum modulus principle.

# Životopis

Rođena sam 23. ožujka 1991. godine u Varaždinu. Pohađala sam VI. osnovnu školu u Varaždinu. Tijekom osnovnoškolskog i srednjoškolskog obrazovanja učila sam engleski, njemački i francuski jezik. Nakon završetka osnovne škole, 2005. godine upisujem opći smjer Prve gimnazije Varaždin. Maturirala sam 2009. godine te tada na Prirodoslovno-matematičkom fakultetu u Zagrebu upisujem preddiplomski studij matematike. Godine 2012. završila sam preddiplomski studij te upisujem Diplomski sveučilišni studij Financijske i poslovne matematike.