Polja, Galoisova teorija i primjene

Milanović, Lada

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Lada Milanović

POLJA, GALOISOVA TEORIJA I PRIMJENE

Diplomski rad

Voditelj rada:
doc. dr. sc. Ana Prlić

Zagreb, prosinac, 2022.

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. _____

Mojim roditeljima ♡

Sadržaj

Uvod

Godinama se postavljalo pitanje postoje li opća algebarska rješenja svih polinomijalnih jednadžbi. Tako je pod utjecajem brojnih matematičara, Simon Stevin došao do formule, kakvu danas znamo, za rješenje kvadratne jednadžbe:

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Ubrzo nakon otkrivene su i opće formule za računanje bikvadratne i kubne jednadžbe. Godine 1824. izašao je dokaz Abel-Ruffinijevog teorema koji tvrdi da je najviši stupanj polinoma za kojeg postoji opće rješenje u radikalima četiri. Potaknut tim teoremom i člancima drugih matematičara, Évariste Galois započinje proučavati polinomijalne jednadžbe i kada one imaju rješenje u radikalima, odnosno opće algebarsko rješenje.

Slika 0.1: Évariste Galois

Évariste Galois (1811.-1832.) francuski je matematičar koji se bavio pitanjem rješivosti algebarskih jednadžbi u radikalima. Iako je kratko živio, uvelike je doprinio razvitku algebre te ga smatramo osnivačem rane teorije grupa. Svoj prvi znanstveni rad objavio je početkom 1829. godine, a ubrzo nakon toga napisao je još dva rada na temu rješivosti algebarskih jednadžbi. Zanimljivo je da je osoba koja je trebala recenzirati te radove bio upravo

jedan od najutjecajnijih matematičara svih vremena - Augustin-Louis Cauchy. Nažalost, Cauchy je te radove izgubio te se nikada nije saznalo što je Galois u njima napisao. Galoisa se smatralo osebujnim i neshvaćenim matematičarom koji se nije uspio upisati u prestižnu matematičku školu upravo zbog svoje velike genijalnosti. Nakon tragične smrti u dvoboju za svoju ljubav, na želju samog Galoisa, svi njegovi spisi poslani su drugim matematičarima. Na sreću, dospjeli su kod Josepha Liouvillea koji ih je objavio 1846. godine.

Galoisova teorija dala je odgovor na pitanje kada se algebarske jednadžbe proizvoljnog stupnja mogu riješiti u radikalima. Odgovor na to pitanje vezan je uz proširenja polja te strukturu pod nazivom Galoisova grupa. Glavna je ideja te teorije povezati proširenja polja $K \subset F$ s grupom automorfizama polja F koji fiksiraju K.

Ovaj diplomski rad sastoji se od tri dijela. Prvi dio bit će podsjetnik na osnovne definicije i tvrdnje vezane za grupe, prstene i polja, koje će nam kasnije pomoći u definiranju i razumijevanju same Galoisove teorije. Upravo je to tema drugog dijela ovog rada, gdje ćemo osim opisa teorije, izreći i dokazati Fundamentalni teorem Galoisove teorije. U trećem dijelu ovog rada primijenit ćemo opisanu teoriju na najpoznatije konstrukcijske probleme u geometriji. Da bismo to mogli napraviti, prvo ćemo objasniti što znači da je broj konstruktibilan, zatim ćemo konstrukcijske probleme svesti na algebarske jednadžbe te ih pokušati riješiti.

Poglavlje 1

Osnovni pojmovi i teoremi

U ovom poglavlju, podijeljenom na četiri dijela, prisjetit ćemo se osnovnih pojmova i teorema iz teorije grupa, prstena i polja te dokazati neke od kriterija ireducibilnosti polinoma. Većinu dokaza ćemo izostaviti jer su navedeni u sklopu kolegija Algebarske strukture ([9]).

1.1 Grupe, prsteni i polja

Definicija 1.1.1. *Neprazan skup $G = (G, \cdot)$, gdje je $\cdot : G \times G \to G$ binarna operacija, zove se **grupa** ako vrijede sljedeća svojstva:*

1) $(x \cdot y) \cdot z = x \cdot (y \cdot z), \quad \forall x, y, z \in G$ *asocijativnost*

2) $(\exists e \in G) \quad e \cdot x = x \cdot e = x, \quad \forall x \in G$ *neutralni element*

3) $(\forall x \in G)(\exists! x^{-1} \in G) \quad x \cdot x^{-1} = x^{-1} \cdot x = e$ *inverzni element.*

Definicija 1.1.2. *Za grupu G kažemo da je **Abelova grupa** ako vrijedi svojstvo komutativnosti, odnosno $x \cdot y = y \cdot x$, za sve $x, y \in G$.*

Navedimo jedan klasični primjer grupe.

Primjer 1.1.3. *Skup cijelih brojeva s operacijom zbrajanja $(\mathbb{Z}, +)$ je grupa, štoviše Abelova grupa. Znamo da je zbrajanje asocijativno i komutativno. Nadalje, neutralni element je 0, a inverz od $a \in \mathbb{Z}$ je $-a$ koji se također nalazi u $\mathbb{Z}$.*

Definicija 1.1.4. *Podskup H grupe $(G, \cdot)$ zovemo **podgrupa** od G ako je H grupa s obzirom na istu operaciju. Oznaka: $H \leq G$.*

Vrlo efikasna metoda provjere je li nešto podgrupa dana je sljedećom propozicijom.

Propozicija 1.1.5. *Neprazan podskup H grupe G je podgrupa od G ako i samo ako vrijedi*

$$xy^{-1} \in H, \quad \forall x, y \in H.$$

Definicija 1.1.6. *Podgrupa N grupe G je* ***normalna podgrupa*** *ako vrijedi*

$$xNx^{-1} = N \quad \forall x \in G.$$

Oznaka: $N \trianglelefteq G$.

Pojam normalne podgrupe nam je potreban da bismo definirati kvocijentnu grupu.

Teorem 1.1.7. *Neka je G proizvoljna grupa i N neka njezina normalna podgrupa. Tada kvocijentni skup G/N s operacijom*

$$G/N \times G/N \to G/N, \quad (xN, yN) \mapsto xyN$$

ima strukturu grupe te G/N zovemo ***kvocijentna grupa*** *od G po N.*

Definicija 1.1.8. *Neka su G i H grupe. Preslikavanje $f : G \to H$ je* ***homomorfizam*** *grupa ako vrijedi*

$$f(xy) = f(x)f(y) \quad \forall x, y \in G.$$

Oznaka:

$$Hom(G, H) := \text{skup svih homomorfizama iz } G \text{ u } H$$

Homomorfizam f koji je i injekcija zovemo ***monomorfizam****, homomorfizam koji je i surjekcija zovemo* ***epimorfizam****, a homomorfizam koji je bijekcija zovemo* ***izomorfizam****.*

Za dvije grupe G i H kažemo da su izomorfne ako postoji neki izomorfizam među njima. Oznaka: $G \cong H$.

Nadalje, ako je $G = H$, odnosno ako imamo homomorfizam $f : G \to G$, kažemo da je f ***endomorfizam*** *od G. Oznaka:*

$$End(G) := \text{skup svih endomorfizama od } G$$

Endomorfizam koji je bijekcija zove se ***automorfizam*** *od G. Oznaka:*

$$Aut(G) := \text{skup svih automorfizama od } G$$

Definicija 1.1.9. *Za proizvoljni homomorfizam $f : G \to H$ definiramo njegovu* ***jezgru***

$$Ker\, f := \{x \in G \mid f(x) = e_H\}$$

i njegovu ***sliku***

$$Im\, f := \{f(x) \mid x \in G\}.$$

Propozicija 1.1.10. *Ako je $f : G \to H$ homomorfizam, tada je $f(e_G) = e_H$ i za sve $x \in G$ vrijedi*

$$f(x^{-1}) = f(x)^{-1.}$$

Dokaz. Budući da je f homomorfizam, za sve $x, y \in G$ vrijedi $f(xy) = f(x)f(y)$. Posebno imamo $f(y) = f(e_G y) = f(e_G)f(y)$, iz čega zaključujemo da je $f(e_G) = e_H$. Nadalje,

$$e_H = f(e_G) = f(xx^{-1}) = f(x)f(x^{-1}).$$

Dakle, mora vrijediti da je $f(x^{-1}) = f(x)^{-1}$. □

Sada ćemo navesti poznati teorem koji povezuje jezgru i sliku homomorfizma grupa.

Teorem 1.1.11 (Prvi teorem o izomorfizmu). *Neka je $f : G \to H$ proizvoljni homomorfizam grupa. Tada je $Ker\ f \trianglelefteq G$, $Im\ f \leq H$ i preslikavanje $\overline{f} : G/Ker\ f \to Im\ f$, dano s $\overline{f}(gKer\ f) := f(g)$ je izomorfizam grupa, odnosno vrijedi*

$$G/Ker\ f \cong Im\ f.$$

Sada ćemo definirati pojam skupa generatora grupe koji nam je jako bitan za razvijanje daljnje teorije. U tu svrhu potrebna nam je sljedeća lema čiji je dokaz elementaran pa ga izostavljamo.

Lema 1.1.12. *Neka je G grupa i neka su $\{H_i \mid i \in I\}$ neke njezine podgrupe. Tada je i njihov skupovni presjek*

$$\bigcap_{i \in I} H_i$$

također podgrupa od G.

Definicija 1.1.13. *Za proizvoljan podskup S neke grupe G, definiramo*

$$\langle S \rangle := \bigcap_{\substack{H \leq G \\ S \subseteq H}} H.$$

*To je podgrupa od G koju zovemo **grupa generirana** sa S. Skup S zovemo **skup generatora** grupe $\langle S \rangle$.*

Definicija 1.1.14. *Kažemo da je G **konačno generirana** grupa ako postoji konačan podskup $S = \{x_1, \ldots, x_n\}$ takav da je $G = \langle S \rangle$. Pišemo: $G = \langle x_1, \ldots, x_n \rangle$.*

Prisjetimo se sada osnovnih definicija i tvrdnji vezanih uz strukturu prstena.

Definicija 1.1.15. *Neprazan skup $R = (R, +, \cdot)$ zovemo **prsten** ukoliko za operacije zbrajanja $+ : R \times R \to R$ i množenja $\cdot : R \times R \to R$ vrijedi sljedeće:*

1) $(R, +)$ *je komutativna grupa*

2) $x \cdot (y \cdot z) = (x \cdot y) \cdot z, \quad \forall x, y, z \in R$

3) Distributivnost množenja prema zbrajanju:
$x \cdot (y + z) = x \cdot y + x \cdot z, \quad \forall x, y, z \in R$
$(x + y) \cdot z = x \cdot z + y \cdot z, \quad \forall x, y, z \in R.$

Definicija 1.1.16. *Za prsten R kažemo da je* ***prsten s jedinicom*** *ako postoji jedinični element,* $1 = 1_R \in R$ *takav da je* $1 \cdot x = x \cdot 1 = x$*, za sve* $x \in R$*.*

Definicija 1.1.17. *Prsten R je* ***komutativni prsten*** *ako vrijedi* $x \cdot y = y \cdot x$*, za sve* $x, y \in R$*.*

Pojam homomorfizma prstena možemo definirati analogno kao i za grupe.

Definicija 1.1.18. *Neka su R i S dva prstena. Preslikavanje* $f : R \longrightarrow S$ *je* ***homomorfizam*** *prstena ako vrijedi:*

1) $f(x + y) = f(x) + f(y), \forall x, y \in R$

2) $f(xy) = f(x)f(y), \forall x, y \in R$

Sljedeći pojam je analogan pojmu normalne podgrupe.

Definicija 1.1.19. *Neka je R prsten. Podskup* $I \subseteq R$ *je* ***lijevi*** *(odnosno* ***desni****)* ***ideal*** *u R ako vrijedi sljedeće:*

1) I je potprsten od R;

2) Za sve $r \in R$ *i* $x \in I$ *je* $rx \in I$ *(odnosno* $xr \in I$*).*

Podskup $I \subseteq R$ *je* ***ideal*** *ako je on istovremeno i lijevi i desni ideal. Oznaka:* $I \trianglelefteq R$*.*

Pojam ideala važan nam je pri definiranju pojma kvocijentnog prstena.

Teorem 1.1.20. *Neka je R prsten i I neki njegov ideal. Tada kvocijentna grupa* R/I *s operacijom*

$$R/I \times R/I \longrightarrow R/I \quad (x + I)(y + I) := xy + I$$

ima strukturu prstena te R/I *zovemo* ***kvocijentni prsten*** *od R po I.*

Definicija 1.1.21. *Prsten R je* ***tijelo****, ili* ***prsten s dijeljenjem****, ako je svaki ne-nul element u R invertibilan.*

Definicija 1.1.22. *Komutativno tijelo zovemo* ***polje****.*

Definicija automorfizma važna nam je za shvaćanje Galoisove teorije, stoga ćemo dokazati da je skup svih automorfizama s operacijom kompozicije grupa.

Teorem 1.1.23. *Neka je K polje. Skup svih automorfizama od K (u oznaci Aut K) čini grupu s operacijom kompozicije.*

Dokaz. Kompozicija je asocijativna. Za svaki $x \in K$ i sve $a, b, c \in \text{Aut } K$ vrijedi sljedeće:

$$[(a \circ b) \circ c](x) = (a \circ b)[c(x)] = a\Big(b(c(x))\Big),$$
$$[a \circ (b \circ c)](x) = a([b \circ c](x)) = a\Big(b(c(x))\Big).$$

U Aut K postoji identiteta i za koju vrijedi $i(x) = x$, za svaki $x \in K$ te $i \circ a = a \circ i = a$, za svaki $a \in \text{Aut } K$. Za svaki automorfizam $a \in \text{Aut } K$, postoji inverz a^{-1} definiran tako da je $a^{-1}(x)$ jedinstveni $y \in K$ za koji vrijedi $a(y) = x$. Ovo preslikavanje je također automorfizam. Neka su $x, y \in K$ i $a^{-1}(x) = z$, $a^{-1}(y) = t$. Tada vrijedi $a(z) = x$, $a(t) = y$ i $a(z + t) = x + y$. Slijedi

$$a^{-1}(x) + a^{-1}(y) = z + t = a^{-1}(a(z + t)) = a^{-1}(x + y).$$

Slično možemo pokazati:

$$(a^{-1}(x))(a^{-1}(y)) = zt = a^{-1}(a(zt)) = a^{-1}(xy).$$

Stoga je $a^{-1} \in \text{Aut } K$ te vrijedi $a \circ a^{-1} = a^{-1} \circ a = i$. Dakle, Aut K je grupa.

□

1.2 Proširenja polja

U drugom potpoglavlju definiramo što je proširenje polja te objašnjavamo razliku između algebarskog i transcedentnog proširenja polja. Također, dokazujemo teorem od stupnju proširenja polja.

Definicija 1.2.1. *Ako su K, L polja takva da je $K \subseteq L$, onda kažemo da je K **potpolje** od L, ili da je L **proširenje** od K. Oznaka: $L \mid K$.*

Napomena 1.2.2. *Ukoliko je $K \neq L$, onda kažemo da je K **pravo potpolje** polja L.*

Definicija 1.2.3. *Neka su K, L i M polja takva da je $K \subseteq L \subseteq M$ te vrijedi $M \mid L \mid K$. Tada kažemo da je L **međupolje** koje sadrži K i sadržano je u M.*

Napomena 1.2.4. *Ako imamo proširenje polja $L \mid K$, tada možemo gledati L kao vektorski prostor nad K.*

Pokažimo da je L zaista vektorski prostor nad poljem K.

Teorem 1.2.5. *Ako je $L \mid K$ proširenje polja, tada operacije*

$$(\lambda, u) \longmapsto \lambda u \qquad (\lambda \in K, u \in L)$$
$$(u, v) \longmapsto u + v \qquad (u, v \in L)$$

definiraju L kao vektorski prostor nad K.

Dokaz. Trebamo pokazati da vrijede sljedeća svojstva:

1) $u + v \in L, \forall u, v \in L$
2) $u + (v + w) = (u + v) + w, \forall u, v, w \in L$
3) $(\exists 0 \in L) \quad u + 0 = 0 + u = u, \forall u \in L$
4) $(\forall u \in L)(\exists - u \in L) \quad u + (-u) = -u + u = 0$
5) $u + v = v + u, \forall u, v \in L$
6) $\lambda u \in L, \forall \lambda \in K, \forall u \in L$
7) $\lambda(\mu u) = (\lambda\mu)u, \forall \lambda, \mu \in K, \forall u \in L$
8) $(\lambda + \mu)u = \lambda u + \mu u, \forall \lambda, \mu \in K, \forall u \in L$
9) $\lambda(u + v) = \lambda u + \lambda v, \forall \lambda \in K, \forall u, v \in L$
10) $1 \cdot u = u, 1 \in K, \forall u \in L$

Budući da znamo da je L polje, svojstva 1), 2), 3), 4) i 5) slijede iz svojstava polja. Provjerimo je li $\lambda u \in L$ ako su $\lambda \in K$ i $u \in L$. Znamo da je L proširenje od K, tj. da je $K \subseteq L$. Sada možemo zaključiti da je $\lambda u \in L$ jer su $\lambda, u \in L$. Svojstva 7) - 10) proizlaze iz činjenice da je L polje. Dakle, L je vektorski prostor nad K. □

Definicija 1.2.6. ***Stupanj proširenja*** *$L \mid K$ je dimenzija od L kao vektorskog prostora nad K. Oznaka:* $[L : K] := dim_K L$.

Definicija 1.2.7. *Kažemo da je $L \mid K$* ***konačno proširenje*** *ako je* $[L : K] < \infty$.

Teorem 1.2.8. *Neka je F konačno proširenje polja E i neka je E konačno proširenje polja K. Tada vrijedi*

$$[F : K] = [F : E][E : K].$$

Dokaz. Neka je $\alpha_1, \ldots, \alpha_m$ baza od E nad K i $\beta_1, \ldots, \beta_n$ baza od F nad E. Dokažimo da skup $\{\alpha_i\beta_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ tvori bazu od F nad K. Svaki element γ od F

možemo zapisati kao $\gamma = \sum_{j=1}^{n} \lambda_j \beta_j$ za neke $\lambda_j \in E$. Svaki λ_j se može zapisati u obliku $\lambda_j = \sum_{i=1}^{m} \mu_{ij} \alpha_i$ za neki $\mu_{ij} \in K$. Kada spojimo ove izraze, dobijemo

$$\gamma = \sum_{j=1}^{n} \sum_{i=1}^{m} \mu_{ij} \alpha_i \beta_j$$

što pokazuje da je $\{\alpha_i \beta_j\}$ skup izvodnica od F nad K. Provjerimo sada linearnu nezavisnost. Pretpostavimo da je

$$\sum_{j=1}^{n} \sum_{i=1}^{m} \mu_{ij} \alpha_i \beta_j = 0$$

za neke $\mu_{ij} \in K$. Budući da je skup $\{\beta_j \mid j \in \{1, \ldots, n\}\}$ baza od F nad E, zaključujemo da je

$$\sum_{i=1}^{m} \mu_{ij} \alpha_i = 0$$

za sve $j = 1, \ldots, n$. Budući da je skup $\{\alpha_i \mid i \in \{1, \ldots, m\}\}$ baza od E nad K, slijedi da je $\mu_{ij} = 0$ za sve i, j. Stoga možemo zaključiti da su vektori $\alpha_i \beta_j$ linearno nezavisni.

Skup $\{\alpha_i \beta_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ je linearno nezavisan sistem izvodnica od F nad K, stoga je baza od F nad K te vrijedi

$$[F : K] = nm = [F : E][E : K].$$

□

Lema 1.2.9. *Neka je F polje i neka su $\{H_i \mid i \in I\}$ neka njegova potpolja. Tada je i njihov skupovni presjek*

$$\bigcap_{i \in I} H_i$$

također potpolje od F.

Definicija 1.2.10. *Ako je F polje i $X \subseteq F$, tada je potpolje generirano s X presjek svih potpolja od F koja sadrže X. Ako je F proširenje polja K i $X \subseteq F$, tada se potpolje generirano s $K \cup X$ zove potpolje generirano s X nad K. Oznaka: $K(X)$.*

Definicija 1.2.11. *Ako je $X = \{u_1, \ldots, u_n\}$, tada potpolje $K(X)$ od F označavamo s $K(u_1, \ldots, u_n)$. Za polje $K(u_1, \ldots, u_n)$ kažemo da je **konačno generirano proširenje** od K.*

Definicija 1.2.12. *Neka je L proširenje polja K. Kažemo da je $\alpha \in L$ **algebarski nad** K ako postoji ne-nul polinom $f \in K[X]$ takav da je $f(\alpha) = 0$, to jest, α je nultočka od f. Inače, kažemo da je α **transcedentan nad** K. Kažemo da je L **algebarsko proširenje** polja K ako je svaki element od L algebarski nad K. Za F kažemo da je **transcedentno proširenje** ako je barem jedan element od L transcedentan nad K.*

Primjer 1.2.13. *Broj* $\sqrt{2}$ *je algebarski nad* $\mathbb{Q}$ *jer je on korijen polinoma* $f(x) = x^2 - 2 \in \mathbb{Q}[X]$*, dok je* π *transcedentan nad* $\mathbb{Q}$*.*

Definicija 1.2.14. *Ako* α *ima minimalan polinom nad* K*, kažemo da je* $K(\alpha)$ ***jednostavno algebarsko proširenje*** *od* K*.*

Teorem 1.2.15. *Ako je* F *konačno dimenzionalno proširenje polja* K*, onda je* F *konačno generirano i algebarsko proširenje polja* K*.*

Dokaz. Ako je $[F : K] = n$ i $u \in F$ proizvoljan, onda je skup $\{1, u, u^2, \ldots, u^n\}$ od $n + 1$ elemenata linearno zavisan. Stoga postoje koeficijenti $a_i \in K$, koji nisu svi nula, takvi da vrijedi $a_0 + a_1u + a_2u^2 + \cdots + a_nu^n = 0$. Dakle, u je algebarski nad K. Budući da je u bio proizvoljan, polje F je algebarsko nad K. Ako je $\{v_1, \ldots, v_n\}$ baza od F nad K, tada vrijedi $F = K(v_1, \ldots, v_n)$. □

1.3 Polinomi i kriteriji ireducibilnosti

U trećem potpoglavlju govorimo o ireducibilnim i minimalnim polinomima te dokazujemo neke od kriterija ireducibilnosti - Gaussovu lemu i Eisensteinov kriterij.

Definicija 1.3.1. *Normirani polinom s koeficijentima u polju* F *je ireducibilan ako se ne može zapisati kao produkt dva ili više polinoma stupnja većeg ili jednakog jedan, s koeficijentima u polju* F*.*

Teorem 1.3.2. *Neka je* L *polje,* K *potpolje od* L *te* $\alpha \in L$*. Tada vrijedi ili*

(i) $K(\alpha) \cong K(X)$

ili

(ii) postoji jedinstveni normirani ireducibilan polinom $m \in K[X]$ *sa svojstvima da za sve* $f \in K[X]$ *vrijedi:*

a) $f(\alpha) = 0$ *ako i samo ako* $m \mid f$*,*

b) polje $K(\alpha)$ *se podudara s prstenom* $K[\alpha]$*,*

c) $[K[\alpha] : K] = \deg m$*.*

Dokaz. Pretpostavimo najprije da ne postoji polinom f iz $K[X]$, različit od nul-polinoma, za koji vrijedi $f(\alpha) = 0$. Dokažimo da je tada $K(X) \simeq K(\alpha)$, odnosno da vrijedi (i). Primijetimo da $\alpha \notin K$ jer bismo inače mogli uzeti polinom $f(X) = X - \alpha$. Prisjetimo

se da je $K(X)$ polje racionalnih funkcija s koeficijentima u K. Definirajmo preslikavanje $\rho : K(X) \to K(\alpha)$ dano pravilom

$$\rho(f/g) = f(\alpha)/g(\alpha).$$

To je dobro definirano preslikavanje jer je $g(\alpha) = 0$ ako i samo ako je g nul-polinom. Lako se vidi da je ρ homomorfizam i da je surjekcija. Preostaje dokazati da je ρ injekcija. Pretpostavimo da su dani polinomi f, g, p, q takvi da su $g, q \neq 0$. Tada vrijedi

$$\begin{aligned}
\rho(f/g) = \rho(p/q) &\iff f(\alpha)q(\alpha) - p(\alpha)g(\alpha) = 0 \quad \text{u } L \\
&\iff (fq - pg)(\alpha) = 0 \quad \text{u } L \\
&\iff fq - pg = 0 \quad \text{u } K[X] \qquad \text{(jer smo pretpostavili da ne postoji ne-nul polinom koji poništava } \alpha) \\
&\iff f/g = p/q \quad \text{u } K(X).
\end{aligned}$$

Dakle, ρ je izomorfizam, odnosno vrijedi (i).

Pretpostavimo sada da postoji polinom g, različit od nul-polinoma, za koji vrijedi $g(\alpha) = 0$. Izaberimo g s najmanjim mogućim stupnjem za kojeg vrijedi $g(\alpha) = 0$. Dokažimo da u tom slučaju vrijedi tvrdnja (ii) ovog teorema. Ako je a vodeći koeficijent od g, tada je g/a normirani polinom. Označimo g/a s m. Vrijedi $m(\alpha) = 0$.

Očito je $f(\alpha) = 0$ ako $m \mid f$. Obratno, pretpostavimo da vrijedi $f(\alpha) = 0$. Polinom f možemo zapisati kao $f = qm + r$, gdje je $\deg r < \deg m$. Sada imamo

$$\begin{aligned}
0 &= f(\alpha) \\
&= q(\alpha)m(\alpha) + r(\alpha) \\
&= 0 + r(\alpha) \\
&= r(\alpha).
\end{aligned}$$

Budući da je $\deg r < \deg m$, dobivamo kontradikciju, osim u slučaju kada je r nul-polinom. Dakle, $f = qm$ i zato $m \mid f$. Trebamo pokazati da je m jedinstven polinom s navedenim svojstvom. Pretpostavimo da postoji polinom m' s istim svojstvima kao polinom m. Tada vrijedi $m(\alpha) = m'(\alpha) = 0$ te $m \mid m'$ i $m' \mid m$. Budući da su oba polinoma normirana, možemo zaključiti da je $m' = m$.

Dalje, trebamo pokazati da je m ireducibilan polinom. Pretpostavimo da postoje polinomi p i q za koje vrijedi $pq = m$, gdje je $\deg p, \deg q < \deg m$. Tada vrijedi $p(\alpha)q(\alpha) = m(\alpha) = 0$. Iz ovoga možemo zaključiti da je ili $p(\alpha) = 0$ ili $q(\alpha) = 0$. No, to je nemoguće jer su stupnjevi polinoma p i q manji od stupnja polinoma m.

Pogledajmo proizvoljni element $f(\alpha)/g(\alpha)$ u $K(\alpha)$, gdje je $g(\alpha) \neq 0$. Tada m ne dijeli g i, kako je m ireducibilan, slijedi da je najveći zajednički djelitelj polinoma g i m broj 1.

Dakle, postoje polinomi a, b za koje vrijedi $ag + bm = 1$. Supstitucijom α za X dobivamo $a(\alpha)g(\alpha) = 1$. Zato vrijedi

$$\frac{f(\alpha)}{g(\alpha)} = f(\alpha)a(\alpha) \in K[X].$$

Iz toga slijedi da je $K(\alpha) = K[\alpha]$. Preostaje još pokazati da je $[K(\alpha) : K] = \deg m$.

Pretpostavimo da je $\deg m = n$ i neka je $p(\alpha) \in K[\alpha] = K(\alpha)$, gdje je p polinom. Polinom p možemo zapisati kao $p = qm + r$, gdje je $\deg r < \deg m = n$. Nadalje, vrijedi $p(\alpha) = r(\alpha)$ pa postoje $c_0, c_1, \ldots, c_{n-1}$ (koeficijenti polinoma r u K) za koje vrijedi

$$p(\alpha) = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}.$$

Dakle, skup $\{1, \alpha, \ldots, \alpha^{n-1}\}$ je sustav izvodnica za $K[\alpha]$. Štoviše, skup $\{1, \alpha, \ldots, \alpha^{n-1}\}$ je linearno nezavisan skup nad K. Za elemente $a_0, a_1, \ldots, a_{n-1} \in K$ za koje je $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$ vrijedi $a_0 = a_1 = \cdots = a_{n-1} = 0$. Naime, kad ne bi svi koeficijenti a_i bili jednaki nula, imali bismo ne-nul polinom $p = a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$ stupnja najviše $n-1$ za koji bi vrijedilo $p(\alpha) = 0$, što je u kontradikciji s činjenicom $\deg m = n$. Zaključujemo da je skup $\{1, \alpha, \ldots, \alpha^{n-1}\}$ baza od $K(\alpha)$ nad K pa vrijedi $[K(\alpha) : K] = n$. □

Definicija 1.3.3. *Neka je F proširenje polja K i $\alpha \in F$ algebarski nad K. Normiran ireducibilan polinom m iz teorema 1.3.2 (ii) a) zovemo minimalan polinom od α nad K.*

Teorem 1.3.4. *Neka je K polje i $g(X)$ ireducibilan polinom u $K[X]$. Tada je $K[X]/\langle g(X)\rangle$ polje koje sadrži polje K do na izomorfizam.*

Dokaz. Dokaz da je $K[X]/\langle g(X)\rangle$ polje može se pronaći u [5]. Lako se vidi da je preslikavanje $\rho : K \to K[X]/\langle g(X)\rangle$ dano s

$$\rho(a) = a + \langle g(X)\rangle, \quad a \in K$$

homomorfizam. Također je i monomorfizam jer vrijedi

$$a + \langle g(X)\rangle = b + \langle g(X)\rangle \implies a - b \in \langle g(X)\rangle \implies a = b.$$

Kako je ρ monomorfizam, slijedi da je $\rho(K)$ potpolje od $K[X]/\langle g(X)\rangle$ izomorfno polju K. □

Sljedeći teorem nam omogućuje da, ukoliko imamo unaprijed zadani normirani ireducibilni polinom $m \in K[X]$, konstruiramo proširenje polja K koje sadrži element čiji je minimalni polinom jednak m.

Teorem 1.3.5. *Neka je K polje i m normirani ireducibilni polinom s koeficijentima iz K. Tada je $L = K[X]/\langle m\rangle$ jednostavno algebarsko proširenje $K[\alpha]$ od K, gdje je $\alpha = X + \langle m\rangle$. Nadalje, minimalni polinom od α nad K je m.*

Dokaz. Iz teorema 1.3.4 slijedi da je L proširenje polja K. Neka je $\alpha = X + \langle m \rangle$. Za svaki polinom $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$ vrijedi sljedeće:

$$\begin{aligned} f(\alpha) &= a_0 + a_1\alpha + \cdots + a_n\alpha^n \\ &= a_0 + a_1(X + \langle m \rangle) + a_2(X + \langle m \rangle)^2 + \cdots + a_n(X + \langle m \rangle)^n \\ &= a_0 + a_1(X + \langle m \rangle) + a_2(X^2 + \langle m \rangle) + \cdots + a_n(X^n + \langle m \rangle) \\ &= (a_0 + a_1X + a_2X^2 + \cdots + a_nX^n) + \langle m \rangle \\ &= f + \langle m \rangle. \end{aligned}$$

Nadalje, $f(\alpha) = 0 + \langle m \rangle$ ako i samo ako $m \mid f$. Stoga, prema teoremu 1.3.2, m je minimalni polinom od α. □

Teorem 1.3.6 (Gaussova lema). *Neka je f polinom u $\mathbb{Z}[X]$ ireducibilan nad $\mathbb{Z}$. Tada je f promatran kao polinom u $\mathbb{Q}[X]$ ireducibilan nad $\mathbb{Q}$.*

Dokaz. Pretpostavimo da f nije ireducibilan nad $\mathbb{Q}$, odnosno da je $f = gh$, gdje su $g, h \in \mathbb{Q}[X]$ te $\deg g, \deg h < \deg f$. Tada postoji $n \in \mathbb{N}$ takav da vrijedi $nf = g'h'$, gdje su $g', h' \in \mathbb{Z}[X]$ i $\deg g' = \deg g$ i $\deg h' = \deg h$. Pretpostavimo da je n najmanji takav broj za koji vrijedi opisano svojstvo. Neka su

$$g' = a_0 + a_1X + \cdots + a_kX^k \quad \text{i} \quad h' = b_0 + b_1X + \cdots + b_lX^l.$$

Ako je $n = 1$, onda je $g = g'$, $h = h'$, odakle slijedi da f nije ireducibilan nad $\mathbb{Z}$, što je kontradikcija s pretpostavkom.

Pretpostavimo sada da je p prosti faktor od n. Tvrdimo da p dijeli sve koeficijente a_i, $i \in \{1, 2, \ldots, k\}$ ili p dijeli sve koeficijente b_j, $j \in \{1, 2, \ldots l\}$. Kada to ne bi vrijedilo, postojale bi vrijednosti i i j za koje vrijedi $p \nmid a_i$ i $p \nmid b_j$. Izaberimo najmanje takve i i j. Koeficijent uz X^{i+j} u $g'h'$ je

$$b_0a_{i+j} + b_1a_{i+j-1} + \cdots + b_ja_i + \cdots + b_{i+j}a_0$$

i po izboru i i j, broj p dijeli svaki član izraza osim b_ja_i, odakle slijedi da p ne dijeli koeficijent uz X^{i+j} polinoma nf. Međutim, f je polinom s cjelobrojnim koeficijentima pa svi koeficijenti od nf moraju biti djeljivi s p.

Bez smanjenja općenitosti, možemo pretpostaviti da p dijeli svaki koeficijent a_i. Tada je $g = pg''$, gdje je g'' polinom nad $\mathbb{Z}$ istog stupnja kao i polinom g'(ili g). Neka je $n = pn_1$. Tada vrijedi $pn_1f = pg''h'$, odnosno $n_1f = g''h'$. Na ovaj način možemo izbaciti sve proste faktore od n te doći do jednadžbe $f = \overline{g}\overline{h}$. Ovdje su $\overline{g}$ i $\overline{h}$ polinomi nad $\mathbb{Z}$, koji su višekratnici početnih polinoma g i h. Stoga je $\deg \overline{g} = \deg g$ i $\deg \overline{h} = \deg h$. Dobivamo kontradikciju s ireducibilnosti od f nad $\mathbb{Z}$. □

Navedimo sada primjer u kojem koristimo Gaussovu lemu.

Primjer 1.3.7. *Pokažimo da je polinom $f(x) = x^3 + 2x^2 - 3x + 5$ ireducibilan nad $\mathbb{Q}$.*

Ako se ovaj polinom može faktorizirati nad $\mathbb{Q}$, onda se, prema Gaussovoj lemi, može faktorizirati i nad $\mathbb{Z}$ te barem jedan od faktora mora biti linearan. Prikažimo zadani polinom f kao umnožak dva polinoma, od kojih je jedan linearan.

$$f(x) = x^3 + 2x^2 - 3x + 5 = (x - a)(x^2 + bx + c)$$

Možemo zaključiti da je $ac = -5$ te da je $a \in \{\pm 1, \pm 5\}$. Provjerimo vrijednosti od $f(a)$ za $a \in \{\pm 1, \pm 5\}$:

a	*-5*	*-1*	*1*	*5*
f(a)	*-55*	*9*	*5*	*165*

Budući da vrijednost $f(a)$ nije 0 niti za jedan $a \in \{\pm 1, \pm 5\}$, zaključujemo da polinom f ne možemo faktorizirati nad $\mathbb{Q}$, odnosno da je f ireducibilan nad $\mathbb{Q}$.

Uz Gaussovu lemu, još jedan bitan kriterij ireducibilnosti je Eisensteinov kriterij.

Teorem 1.3.8 (Eisensteinov kriterij). *Neka je $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ polinom u $\mathbb{Z}[x]$. Prepostavimo da postoji prost broj p takav da*

(i) $p \nmid a_n$,

(ii) $p \mid a_i$, $i = 0, \ldots, n-1$,

(iii) $p^2 \nmid a_0$.

Tada je polinom f ireducibilan nad $\mathbb{Q}$.

Dokaz. Prema Gaussovoj lemi dovoljno je pokazati da je polinom f ireducibilan nad $\mathbb{Z}$. Pretpostavimo da je $f = gh$, gdje su

$$g = b_0 + b_1 X + \cdots + b_r X^r \quad \text{i} \quad h = c_0 + c_1 X + \cdots + c_s X^s$$

te vrijedi $r, s < n$ i $r + s = n$. Budući da je $a_0 = b_0 c_0$, iz (*ii*) slijedi da $p \mid b_0$ ili $p \mid c_0$. Iz (*iii*) znamo da $p^2 \nmid a_0$ pa koeficijenti b_0 i c_0 ne mogu istovremeno biti djeljivi s p. Bez smanjenja općenitosti, neka vrijedi da

$$p \mid b_0 \quad \text{i} \quad p \nmid c_0.$$

Pretpostavimo da p dijeli $b_0, b_1, \ldots, b_{k-1}$, gdje je $1 \leq k \leq r$. Tada vrijedi da je

$$a_k = b_0 c_k + b_1 c_{k-1} + \cdots + b_{k-1} c_1 + b_k c_0.$$

Budući da p dijeli svaki od koeficijenata $a_k, b_0c_k, b_1c_{k-1}, \ldots, b_{k-1}c_1$, slijedi da $p \mid b_kc_0$. No, znamo da $p \nmid c_0$, stoga možemo zaključiti da $p \mid b_k$. Induktivno zaključujemo $p \mid b_r$. Budući da je $a_n = b_rc_s$ imamo da $p \mid a_n$ što je kontradikcija s (i). Ovime smo pokazali da je polinom f ireducibilan.

□

1.4 Polja razlaganja

Još jedna važna cjelina za bolje razumijevanje Galoisove teorije su polja razlaganja. Prije no što ih definiramo, objasnit ćemo što znači da je polinom rascjepiv nad poljem F.

Definicija 1.4.1. *Za polinom f kažemo da je rascjepiv nad poljem F ako se može zapisati kao produkt linearnih faktora iz $F[x]$, odnosno*

$$f = u_0(x - u_1)(x - u_2)\cdots(x - u_n),$$

gdje su $u_i \in F, i \in \{0, 1, \ldots, n\}$.

Definicija 1.4.2. *Neka je K polje i $f \in K[x]$ polinom. Za proširenje polja F od K kažemo da je **polje razlaganja** nad K polinoma f ako je f rascjepiv u $F[x]$ i $F = K(u_1, \ldots, u_n)$, gdje su $u_1, \ldots, u_n$ korijeni od f u F.*

Neka je S skup polinoma u $K[x]$. Za proširenje polja F od K kažemo da je polje razlaganja nad K skupa S ako je svaki polinom iz S rascjepiv u $F[x]$ i F generiran nad K korijenima svih polinoma iz S.

Pogledajmo dva primjera polja razlaganja.

Primjer 1.4.3. *Neka je $f(x) = x^2 - 2$. Polinom f je ireducibilan nad $\mathbb{Q}$. Ako bismo proširili polje $\mathbb{Q}$, polinom bismo mogli zapisati kao $f(x) = (x - \sqrt{2})(x + \sqrt{2})$. Jedini korijeni od f su $\sqrt{2}$ i $-\sqrt{2}$, stoga proširimo polje $\mathbb{Q}$ do polja $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, -\sqrt{2})$. Dobiveno polje $\mathbb{Q}(\sqrt{2})$ je polje razlaganja od $f(x) = x^2 - 2$ nad $\mathbb{Q}$.*

Primjer 1.4.4. *Neka je $f(x) = x^2 + 1$. Polinom f je ireducibilan nad $\mathbb{Q}$, ali je rascjepiv nad $\mathbb{C}$ jer ga možemo zapisati kao $f(x) = (x - i)(x + i)$. No, primijetimo kako polje $\mathbb{C}$ nije najmanje polje nad kojim je polinom f rascjepiv. Proširimo polje $\mathbb{Q}$ do polja $\mathbb{Q}(i)$. Dobiveno polje je polje razlaganja nad $\mathbb{Q}$ polinoma f.*

Dokažimo teorem o egzistenciji polja razlaganja.

Teorem 1.4.5. *Neka je K polje i neka je polinom $f \in K[X]$ stupnja n. Tada postoji polje razlaganja L za f nad K i vrijedi da je $[L : K] \leq n!$.*

Dokaz. Polinom f ima barem jedan ireducibilan faktor g. Ukoliko je $\deg f = 1$, ireducibilan faktor će biti sam polinom f. Bez smanjena općenitosti možemo pretpostaviti da je g normirani polinom. Ako, kao u teoremu 1.3.5, definiramo polje $E_1 = K[X]/\langle g \rangle$ i označimo element $X + \langle g \rangle$ s α, tada je g minimalni polinom od α pa vrijedi $g(\alpha) = 0$. Stoga g ima linearan faktor $Y - \alpha$ u $E_1[Y]$. Dodatno, $[E_1 : K] = \deg g \leq n$. Dalje nastavimo induktivno. Pretpostavimo da za neki $r \in \{1, \ldots, n-1\}$ imamo proširenje E_r od K takvo da f ima bar r linearnih faktora u $E_r[X]$ te da vrijedi

$$[E_r : K] \leq n(n-1)\ldots(n-r+1).$$

Za polinom f vrijedi

$$f = (X - \alpha_1)(X - \alpha_2)\ldots(X - \alpha_r)f_r$$

te $\deg f_r = n - r$. Na sličan način konstruiramo proširenje E_{r+1} od E_r u kojem polinom f_r ima linearan faktor $X - \alpha_{r+1}$ te vrijedi $[E_{r+1} : E_r] \leq n - r$. Zaključujemo da

$$[E_{r+1} : K] = [E_{r+1} : E_r][E_r : K] \leq n(n-1)\ldots(n-r).$$

Dakle, indukcijom možemo zaključiti da postoji polje razlaganja E_n polinoma f nad K i vrijedi $[E_n : K] \leq n!$. □

Dokaz jedinstvenosti polja razlaganja znatno je zahtjevniji te se može pronaći u [6] (str. 258.-261.).

Poglavlje 2

Galoisova teorija

U ovom poglavlju definirat ćemo Galoisovu grupu i Galoisovo proširenje te ćemo dokazati Fundamentalni teorem Galoisove teorije.

Definicija 2.0.1. *Neka je polje L proširenje polja K. Automorfizam α od L se zove K-automorfizam ako vrijedi $\alpha(x) = x$ za svaki $x \in K$. Skup svih K-automorfizama od L zove se Galoisova grupa od L nad K. Oznaka: $Gal(L : K)$.*

Definicija 2.0.2. *Galoisova grupa $Gal(f)$ polinoma f u $K[X]$ definirana je kao $Gal(L : K)$, gdje je L polje razlaganja od f nad K.*

Teorem 2.0.3. *Neka je $L \mid K$ proširenje polja. Tada je skup $Gal(L : K)$ svih K-automorfizama od L podgrupa od Aut L.*

Dokaz. Neka su $\alpha, \beta \in Gal(L : K)$. Za svaki $x \in K$ vrijedi

$$x = \beta^{-1}(\beta(x)) = \beta^{-1}(x) \quad \text{i} \quad \alpha(\beta^{-1}(x)) = \alpha(x) = x.$$

Možemo zaključiti da je $\alpha\beta^{-1} \in Gal(L : K)$. Budući da za sve $\alpha, \beta \in Gal(L : K)$ vrijedi $\alpha\beta^{-1} \in Gal(L : K)$, možemo zaključiti da je $Gal(L : K)$ podgrupa od $AutL$. □

Sada ćemo uvesti koncept koji povezuje potpolja E od L koja sadrže K i podgrupe H grupe $Gal(L : K)$.

Za svako potpolje E polja L definiramo

$$\Gamma(E) = \{\alpha \in AutL : \alpha(z) = z, \ \forall z \in E\},$$

a za svaku podgrupu H grupe $Gal(L : K)$ definiramo

$$\Phi(H) = \{x \in L : \alpha(x) = x, \ \forall \alpha \in H\}.$$

Cilj nam je pokazati da postoji bijekcija između ovako definiranih skupova.

Napomena 2.0.4. *Polje* $\Phi(H)$ *zovemo* ***fiksno polje*** *od* H *u* L.

Teorem 2.0.5. *Neka je* $L \mid K$ *proširenje polja.*

1) Za svako potpolje E *od* L *koje sadrži* K*, skup* $\Gamma(E)$ *je podgrupa od* $Gal(L : K)$.

2) Za svaku podgrupu H *od* $Gal(L : K)$*, skup* $\Phi(H)$ *je potpolje od* L *koje sadrži* K.

Dokaz. 1) Budući da svaki automorfizam iz $\Gamma(E)$ fiksira sve elemente iz E, onda on fiksira i sve elemente iz K jer je $K \subseteq E$. Dakle, $\Gamma(E) \subseteq \mathrm{Gal}(L : K)$.

Neka su $\alpha, \beta \in \Gamma(E)$. Tada za sve $u \in E$ vrijedi

$$\alpha(\beta^{-1}(u)) = \alpha(\beta^{-1}(\beta(u))) = \alpha(u) = u.$$

Time vidimo da je $\alpha\beta^{-1} \in \Gamma(E)$. Dakle, možemo zaključiti da je $\Gamma(E)$ podgrupa od $Gal(L : K)$.

2) Budući da svaki automorfizam u $\mathrm{Gal}(L : K)$ fiksira elemente od K, zaključujemo $K \subseteq \Phi(H)$.

Neka su $x, y \in \Phi(H)$. Tada za sve $\alpha \in H$ vrijedi

$$\alpha(x - y) = \alpha(x) - \alpha(y) = x - y.$$

Možemo zaključiti da je $x - y \in \Phi(H)$.

Ako je $y \neq 0$, za sve $\alpha \in H$ vrijedi

$$\alpha(xy^{-1}) = \alpha(x)\alpha(y^{-1}) = \alpha(x)(\alpha(y))^{-1} = xy^{-1}.$$

Opet možemo zaključiti da je $xy^{-1} \in \Phi(H)$. Dakle, $\Phi(H)$ je potpolje od L.

□

Teorem 2.0.6. *Neka je* K *polje,* L *proširenje polja* K *i* $u \in L \setminus K$*. Ako je* u *korijen polinoma* f *s koeficijentima u* K *i ako je* $\alpha \in Gal(L : K)$*, onda je* $\alpha(u)$ *također korijen polinoma* f.

Dokaz. Neka je $f = a_0 + a_1X + \cdots + a_nX^n$, gdje su $a_0, a_1, \ldots, a_n \in K$. Pretpostavimo da je $f(u) = 0$. Tada vrijedi

$$\begin{aligned} f(\alpha(u)) &= a_0 + a_1\alpha(u) + \cdots + a_n(\alpha(u))^n \\ &= \alpha(a_0) + \alpha(a_1)\alpha(u) + \cdots + \alpha(a_n)\alpha(u^n) \\ &= \alpha(a_0 + a_1u + \cdots + a_nu^n) \\ &= \alpha(0) \\ &= 0. \end{aligned}$$

□

Teorem 2.0.7. *Neka je L proširenje polja K, E potpolje od L koja sadrži K i H podgrupa od Gal*$(L : K)$*. Tada vrijedi*

$$E \subseteq \Phi(\Gamma(E)) \quad i \quad H \subseteq \Gamma(\Phi(H)).$$

Dokaz. Neka je $u \in E$. Budući da je grupa $\Gamma(E)$ skup svih automorfizama od L koji fiksiraju svaki element od E, time je i u fiksiran automorfizmima iz $\Gamma(E)$. To možemo zapisati kao $u \in \Phi(\Gamma(E))$. Dakle, vrijedi $E \subseteq \Phi(\Gamma(E))$.

Neka je $\alpha \in H$. Budući da je polje $\Phi(H)$ skup svih elemenata od L koji su fiksirani svakim elementom od H, time α fiksira svaki element od $\Phi(H)$. Dakle, $H \subseteq \Gamma(\Phi(H))$. □

Propozicija 2.0.8. *Vrijede sljedeće tvrdnje:*

1) $\Gamma\Phi\Gamma = \Gamma$

2) $\Phi\Gamma\Phi = \Phi$

Dokaz. 1) Neka je E potpolje od L koje sadrži K. Iz teorema 2.0.7 znamo da je $E \subseteq \Phi(\Gamma(E))$ odakle slijedi $\Gamma(E) \supseteq (\Gamma\Phi\Gamma)(E)$. S druge strane, znamo da za svaku podgrupu H od $Gal(L : K)$ vrijedi $H \subseteq \Gamma(\Phi(H))$. Kada supstituiramo $\Gamma(E)$ umjesto H dobivamo $\Gamma(E) \subseteq (\Gamma\Phi\Gamma)(E)$. Dakle, dobili smo $\Gamma\Phi\Gamma = \Gamma$.

2) Neka je H podgrupa od $Gal(L : K)$. Iz teorema 2.0.7 znamo da je $H \subseteq \Gamma(\Phi(H))$ odakle slijedi $\Phi(H) \supseteq (\Phi\Gamma\Phi)(H)$. S druge strane, kada supstituiramo $\Phi(H)$ umjesto E u izraz $E \subseteq \Phi(\Gamma(E)$ dobivamo $\Phi(H) \subseteq (\Phi\Gamma\Phi)(H)$. Dakle, vrijedi $\Phi\Gamma\Phi = \Phi$.

□

Teorem 2.0.9. *Neka je L konačno proširenje polja K i G konačna podgrupa od Gal*$(L : K)$*. Tada vrijedi* $[L : \Phi(G))] = |G|$.

Dokaz. Neka je $|G| = m$ i $[L : \Phi(G)] = n$. Pretpostavimo da je $m > n$. Kako je G konačna grupa, možemo G zapisati kao $G = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$, gdje je α_1 identiteta. Neka je $\{z_1, z_2, \ldots, z_n\}$ baza od L nad $\Phi(G)$. Pogledajmo sljedeću matricu:

$$\begin{bmatrix} \alpha_1(z_1) & \alpha_2(z_1) & \cdots & \alpha_m(z_1) \\ \alpha_1(z_2) & \alpha_2(z_2) & \cdots & \alpha_m(z_2) \\ \vdots & \vdots & & \vdots \\ \alpha_1(z_n) & \alpha_2(z_n) & \cdots & \alpha_m(z_n) \end{bmatrix}.$$

Općenito vrijedi, ako imamo $n \times m$ matricu M i vektor $v \in F^m$, preslikavanje $v \mapsto Mv$ je linearan operator iz vektorskog prostora F^m u vektorski prostor F^n. Ukoliko vrijedi da je $n < m$, onda će postojati vektor v za koji vrijedi $Mv = 0$. To slijedi iz teorema o rangu i defektu, budući da je zbroj ranga i defekta linearnog operatora $v \mapsto Mv$ jednak dimenziji

od F^m, tj. jednak je m, a ovdje je $n < m$, a rang je najviše n pa jezgra mora biti netrivijalna. Odnosno, postoje vektori iz K^m za koje vrijedi da je njihova linearna kombinacija jednaka nuli.

Dakle, postoje vektori $u_1, u_2, \ldots, u_m \in L$, barem jedan različit od 0, za koje vrijedi

$$\alpha_1(z_j)u_1 + \alpha_2(z_j)u_2 + \cdots + \alpha_m(z_j)u_m = 0, \tag{2.1}$$

gdje je $j \in \{1, 2, \ldots, n\}$.

Neka je $d \in L$. Kako je $\{z_1, z_2, \ldots, z_n\}$ baza od L nad $\Phi(G)$, postoje elementi $d_1, d_2, \ldots, d_n$ od $\Phi(G)$ za koje vrijedi

$$d = d_1z_1 + d_2z_2 + \cdots + d_nz_n. \tag{2.2}$$

Pomnožimo li n jednakosti (2.1) redom s $d_1, d_2, \ldots, d_n$ dobit ćemo

$$d_j\alpha_1(z_j)u_1 + d_j\alpha_2(z_j)u_2 + \cdots d_j\alpha_m(z_j)u_m = 0, \tag{2.3}$$

gdje je $j \in \{1, 2, \ldots, n\}$. Budući da su svi d_j u $\Phi(G)$ i svi α_i u G, vrijedi $d_j = \alpha_i(d_j)$, za sve i i j. Zato možemo jednakost (2.3) zapisati kao

$$\alpha_1(d_jz_j)u_1 + \alpha_2(d_jz_j)u_2 + \cdots + \alpha_m(d_jz_j)u_m = 0, \tag{2.4}$$

gdje je $j \in \{1, 2, \ldots, n\}$. Ako zbrojimo sve ove jednakosti te koristimo jednakost (2.2), dobit ćemo

$$u_1\alpha_1(d) + u_2\alpha_2(d) + \cdots + u_m\alpha_m(d) = 0. \tag{2.5}$$

Jednakost 2.5 vrijedi za sve $d \in L$ i zato su automorfizmi $\alpha_1, \alpha_2, \ldots, \alpha_m$ linearno zavisni. No, to je kontradikcija jer skup automorfizama $\alpha_1, \alpha_2, \ldots, \alpha_m$ mora biti linearno nezavisan skup. Stoga vrijedi $n \geq m$.

Prepostavimo sada da je $n = [L : \Phi(G)] > m$. Tada postoji podskup $\{z_1, z_2, \ldots, z_{m+1}\}$ od L koji je linearno nezavisan nad $\Phi(G)$. Pogledajmo sljedeću matricu:

$$\begin{bmatrix} \alpha_1(z_1) & \alpha_1(z_2) & \cdots & \alpha_1(z_{m+1}) \\ \alpha_2(z_1) & \alpha_2(z_2) & \cdots & \alpha_2(z_{m+1}) \\ \vdots & \vdots & & \vdots \\ \alpha_m(z_1) & \alpha_m(z_2) & \cdots & \alpha_m(z_{m+1}) \end{bmatrix}.$$

Postoje vektori $v_1, v_2, \ldots, v_{m+1} \in L$, od kojih je barem jedan različit od 0, za koje vrijedi

$$\alpha_j(z_1)v_1 + \alpha_j(z_2)v_2 + \cdots \alpha_j(z_{m+1})v_{m+1} = 0, \tag{2.6}$$

gdje je $j \in \{1, 2, \ldots, m\}$.

Pretpostavimo da su elementi $v_1, v_2, \ldots, v_{m+1}$ izabrani tako da je broj elemenata među njima koji su različiti od 0 najmanji mogući. Bez smanjena općenitosti možemo pretpostaviti da su elementi $v_1, v_2, \ldots, v_r$ različiti od 0 te $v_{r+1} = \cdots = v_{m+1} = 0$. Vrijedi sljedeće:

$$\alpha_j(z_1)v_1 + \alpha_j(z_2)v_2 + \cdots + \alpha_j(z_r)v_r = 0, \tag{2.7}$$

gdje je $j \in \{1, 2, \ldots, m\}$. Kada podijelimo jednakosti (2.7) s v_r dobijemo

$$\alpha_j(z_1)v'_1 + \cdots + \alpha_j(z_{r-1})v'_{r-1} + \alpha_j(z_r) = 0, \tag{2.8}$$

gdje je $j \in \{1, 2, \ldots, m\}$ i $v'_i = v_i/v_r$ za $i \in \{1, 2, \ldots, r-1\}$. Budući da je α_1 identiteta, prva jednakost je oblika

$$z_1v'_1 + \cdots + z_{r-1}v'_{r-1} + z_r = 0. \tag{2.9}$$

Kada bi svi elementi $v'_1, v'_2, \ldots, v'_{r-1}$ pripadali $\Phi(G)$, onda bi skup $\{z_1, z_2, \ldots, z_r\}$ bio linearno zavisan nad $\Phi(G)$, a po pretpostavci to nije moguće. Stoga, barem jedan od elemenata $v'_1, v'_2, \ldots, v'_{r-1}$ ne pripada $\Phi(G)$. Bez smanjenja općenitosti pretpostavimo da $v'_1 \notin \Phi(G)$. Dakle, v'_1 nije fiksiran svim automorfizmima iz G, odnosno, postoji automorfizam u G, na primjer α_2 za koji vrijedi $\alpha_2(v'_1) \neq v'_1$. Primijenimo li α_2 na jednakosti (2.8) dobivamo

$$(\alpha_2\alpha_j)(z_1)\alpha_2(v'_1) + \cdots + (\alpha_2\alpha_j)(z_{r-1})\alpha_2(v'_{r-1}) + \alpha_2\alpha_j(z_r) = 0. \tag{2.10}$$

Budući da je G grupa, skup $\{\alpha_2\alpha_1, \alpha_2\alpha_2, \ldots, \alpha_2\alpha_m\}$ razlikuje se samo u poretku elemenata od skupa $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$. Stoga, možemo promijeniti poredak jednakosti (2.10):

$$\alpha_j(z_1)\alpha_2(v'_1) + \cdots + \alpha_j(z_{r-1})\alpha_2(v'_{r-1}) + \alpha_j(z_r) = 0. \tag{2.11}$$

Oduzmimo sada jednakosti (2.11) i (2.8):

$$\alpha_j(z_1)(v'_1 - \alpha_2(v'_1)) + \cdots + \alpha_j(z_{r-1})(v'_{r-1} - \alpha_2(v'_{r-1})) = 0. \tag{2.12}$$

Neka je $u_i = v'_i - \alpha_2(v'_i)$ za $i = 1, 2, \ldots, r-1$ i $u_i = 0$ za $i = r, r+1, \ldots, m+1$. Tada jednakosti (2.12) možemo zapisati:

$$\alpha_j(z_1)u_1 + \cdots + \alpha_j(z_{r-1})u_{r-1} + \cdots + \alpha_j(z_{m+1})u_{m+1} = 0, \tag{2.13}$$

gdje je $j \in \{1, 2, \ldots, m\}$. Iz $\alpha_2(v'_1) \neq v'_1$ slijedi da nisu svi elementi u_i jednaki 0 te smo uspjeli namjestiti najviše $r-1$ vektora u_i različitih od 0. To je kontradikcija za pretpostavljeno svojstvo elemenata $v_1, v_2, \ldots, v_{m+1}$. Dakle, $[L : \Phi(G)]$ ne može biti veće od m. Stoga vrijedi $[L : \Phi(G)] = m$. □

Da bismo bolje mogli definirati Galoisovo proširenje, uz proširenja polja spomenuta u prvom poglavlju, uvest ćemo još dva proširenja polja - normalno i separabilno proširenje.

Definicija 2.0.10. *Algebarsko proširenje polja F od K je* ***normalno proširenje*** *nad K ako je svaki ireducibilan polinom iz $K[x]$ koji ima barem jedan korijen u F potpuno rascjepiv nad F.*

Definicija 2.0.11. *Neka je L konačno proširenje polja K. Kažemo da je polje N, koje sadrži polje L,* ***normalno zatvorenje*** *od L nad K ako vrijede sljedeće tvrdnje:*

i) N je normalno proširenje od K

ii) ako je E pravo potpolje od N koje sadrži L, onda E nije normalno proširenje od K.

Propozicija 2.0.12. *Neka je L normalno proširenje konačnog stupnja nad poljem K i E potpolje od L koje sadrži K. Tada se svaki K-monomorfizam iz E u L može proširiti u K-automorfizam od L.*

Propozicija 2.0.13. *Neka je L normalno proširenje polja K. Ako su z_1 i z_2 korijeni iz L ireducibilnog polinoma iz $K[X]$, tada postoji K-automorfizam θ od L za koji vrijedi $\theta(z_1) = z_2$.*

Dokazi prethodne dvije propozicije mogu se pronaći u [5].

Teorem 2.0.14. *Neka je L konačno normalno proširenje polja K i E potpolje od L koje sadrži K. Tada je E normalno proširenje od K ako i samo ako je svaki K-monomorfizam od E u L K-automorfizam od E.*

Dokaz. Pretpostavimo da je E normalno proširenje od K. Neka je ρ K-monomorfizam iz E u L i $z \in E$. Neka je $m = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ minimalan polinom od z nad K. Tada vrijedi

$$z^n + a_{n-1}z^{n-1} + \cdots a_1z + a_0 = 0.$$

Primijenimo li ρ na prethodnu jednakost, dobivamo:

$$(\rho(z))^n + a_{n-1}(\rho(z))^{n-1} + \cdots a_1\rho(z) + a_0 = 0.$$

Možemo zaključiti da je $\rho(z)$ također korijen od m u L. No, znamo da je $z \in E$ korijen ireducibilnog polinoma m i budući da je E normalno proširenje, slijedi da je polinom m potpuno rascjepiv nad E. Dakle, $\rho(z) \in E$ te je $\rho(E)$ sadržan u E. Nadalje vrijedi:

$$[\rho(E) : K] = [\rho(E) : \rho(K)] = [E : K] = [E : \rho(E)][\rho(E) : K]$$

te time i da je $\rho(E) = E$. Dakle, ρ je K-automorfizam od E.

Obratno, pretpostavimo da je svaki K-monomorfizam iz E u L K-automorfizam od E. Neka je f ireducibilan polinom iz $K[X]$ čiji je jedan korijen $z \in E$. Da bi E bilo normalno proširenje od K trebamo pokazati da je f potpuno rascjepiv nad E. Budući da je

L normalno proširenje, f je potpuno rascjepiv nad L. Neka je z' neki drugi korijen od f u L. Prema propoziciji 2.0.13, postoji K-automorfizam θ od L za koji vrijedi $\theta(z) = z'$. Neka je θ' restrikcija od θ na E. Tada je θ' K-monomorfizam iz E u L pa je, po pretpostavci, K-automorfizam od E. Dakle, vrijedi

$$z' = \theta(z) = \theta'(z) \in E,$$

odnosno, E je normalno proširenje. □

Definicija 2.0.15. *Neka je K polje i $f \in K[X]$ ireducibilan polinom. Kažemo da je polinom f* ***separabilan nad K*** *ako je svaki korijen od f jednostruk u polju razlaganja od f nad K.*

Ako je F proširenje polja K i $u \in F$ je algebarski nad K, tada kažemo da je u ***separabilan nad*** *K ako je njegov minimalan polinom separabilan nad K.*

Ako je svaki element algebarskog proširenja F od K separabilan nad K, onda kažemo da je F ***separabilno proširenje*** *od K.*

Teorem 2.0.16. *Neka je L konačno separabilno proširenje polja K i neka je E potpolje od L koje sadrži K. Tada je L separabilno proširenje od E.*

Dokaz. Neka je $\alpha \in L$ te neka su m_K i m_E minimalni polinomi od α nad K i E. Pretpostavimo da je m_K separabilan. Koristeći algoritam za dijeljenje polinoma iz $E[X]$ vrijedi da je $m_K = qm_E + r$, odakle slijedi

$$r(\alpha) = m_K(\alpha) - q(\alpha)m_E(\alpha) = 0 - 0 = 0.$$

Ovo je kontradikcija s definicijom minimalnog polinoma m_E, osim za $r = 0$. Dakle, u $E[X]$ vrijedi $m_K = qm_E$.

Ako m_E nije separabilan, onda postoji polinom g stupnja većega ili jednakog 1 koji dijeli m_E i Dm_E, gdje je D operator deriviranja. Budući da je $Dm_K = qDm_E + m_EDq$, slijedi da g dijeli Dm_K, a budući da je $m_K = qm_E$, onda dijeli i m_K. Ovo se može dogoditi samo u slučaju kada m_K ima najmanje jedan višestruki korijen u polju razlaganja, a to je nemoguće. Dakle, m_E je separabilan. □

Definicija 2.0.17. *Konačno proširenje polja K koje je normalno i separabilno zovemo* ***Galoisovo proširenje****.*

Propozicija 2.0.18. *Neka je L Galoisovo proširenje od K i G Galoisova grupa od L nad K. Tada vrijedi*

$$|G| = [L : K].$$

Dokaz prethodne tvrdnje se može pronaći u [5].

Sada ćemo izreći i dokazati lemu koja nam je potrebna za dokaz sljedećeg teorema o Galoisovom proširenju.

Lema 2.0.19. *Za svaki $\rho_i \in Gal(L : K)$, skupovi $\{z_1, z_2, \ldots, z_r\}$ i $\{\rho_i(z_1), \rho_i(z_2), \ldots, \rho_i(z_r)\}$, gdje je $i \in \{1, 2, \ldots, r\}$, su isti.*

Dokaz. Elementi $\rho_j(z_i)$ jednaki su $(\rho_j\rho_i)(z)$, a to je jednako z_k, za neki k jer je $\rho_j\rho_i \in \mathrm{Gal}(L : K)$. Budući da je ρ_j bijekcija, ona permutira elemente $z_1, z_2, \ldots, z_r$. □

Teorem 2.0.20. *Neka je L konačno proširenje od K. Vrijedi da je $\Phi(Gal(L : K)) = K$ ako i samo ako je L Galoisovo proširenje od K.*

Dokaz. Pretpostavimo da je L Galoisovo proširenje od K i neka je $[L : K] = n$. Prema propoziciji 2.0.18 slijedi da je $|Gal(L : K)| = n$. Označimo $\Phi(Gal(L : K))$ s K'. Iz teorema 2.0.7, znamo da je $K \subseteq K'$ te iz teorema 2.0.9 slijedi $[L : K'] = n$. Budući da je $K \subseteq K'$ i $[L : K] = [L : K']$, slijedi da je $K = K'$.

Obratno, pretpostavimo da je $K = K'$. Neka je $Gal(L : K) = \{\rho_1, \rho_2, \ldots, \rho_n\}$. Pretpostavimo da je ρ_1 identiteta. Neka je f ireducibilan polinom iz $K[X]$ koji ima korijen z u L.

Budući da znamo da je $\rho_1(z) = z$, možemo drugačije poredati elemente od $Gal(L : K)$ tako da $\{z, \rho_2(z), \rho_3(z), \ldots, \rho_r(z)\}$ budu sve različite slike od z automorfizama iz $Gal(L : K)$. Uvedimo oznake $\rho_i(z) = z_i$, gdje je $i \in \{1, 2, \ldots, r\}$. Uočimo, vrijedi da je $z_1 = z$.

Neka je sada g polinom oblika

$$(X - z_1)(X - z_2)\cdots(X - z_r) = X^r - s_1X^{r-1} + \cdots + (-1)^r s_r,$$

gdje su koeficijenti $s_1, \ldots, s_r$ oblika

$$\begin{aligned} s_1 &= \sum_{i=1}^{r} z_i \\ s_2 &= \sum_{i \neq j} z_i z_j \\ &\vdots \\ s_r &= z_1 z_2 \ldots z_r. \end{aligned}$$

Koeficijenti s_k, $k \in \{1, 2, \ldots, r\}$ su nepromjenjivi za svaku permutaciju skupa $\{z_1, z_2, \ldots, z_r\}$ pa prema lemi 2.0.19 nisu promjenjivi ni za koji $\rho_j \in \mathrm{Gal}(L : K)$. Stoga je g polinom s koeficijentima iz $\Phi(\mathrm{Gal}(L : K))$ koji se po pretpostavci podudara s K. Znamo da je $z \in L$ korijen ireducibilnog polinoma $f \in K[X]$.

Dokažimo da je polinom g minimalni polinom od z nad K. Pretpostavimo da je polinom $h(X) = a_0 + a_1X + \cdots + a_mX^m$, gdje su $a_0, a_1, \ldots, a_m \in K$ takav da vrijedi

$$h(z) = a_0 + a_1z + \cdots + a_mz^m = 0.$$

Primjenom ρ_j na ovu jednadžbu koeficijenti a_i se ne mijenjaju te dobivamo

$$a_0 + a_1 z_j + \cdots + a_m z_j^m = 0,$$

gdje je $j \in 1, 2, \ldots, r$. Iz ovoga možemo zaključiti da je h djeljiv sa svakim od $X - z_1, \ldots, X - z_r$, odnosno, h je djeljiv s g. Dakle, pokazali smo da je svaki polinom čiji je korijen z djeljiv s g. Stoga je g minimalni polinom od z nad K.

Primjenjujući prethodni zaključak, dobivamo da je polinom f djeljiv s g. Budući da je f po pretpostavci ireducibilan, f je višekratnik od g. Kako se g potpuno razlaže nad L, slijedi da se i f također potpuno razlaže nad L. Štoviše, svi korijeni polinoma g su različiti i stoga je L separabilno normalno proširenje od K.

□

Teorem 2.0.21. *Neka je L Galoisovo proširenje polja K i E potpolje od L koje sadrži K. Ako je $\alpha \in Gal(L : K)$, onda vrijedi*

$$\Gamma(\alpha(E)) = \alpha\Gamma(E)\alpha^{-1}.$$

Dokaz. Uvedimo oznake $E' = \alpha(E)$, $H = \Gamma(E)$ i $H' = \Gamma(E')$. Trebamo pokazati da je $H' = \alpha H \alpha^{-1}$. Neka je $\theta \in H$. Pokažimo da je $\alpha\theta\alpha^{-1} \in H'$. Neka je $z' \in E'$ i z jedinstveni element od E za koji vrijedi $\alpha(z) = z'$. Budući da θ fiksira sve elemente od E, slijedi

$$(\alpha\theta\alpha^{-1})(z') = (\alpha\theta\alpha^{-1}\alpha)(z) = \alpha(\theta(z)) = \alpha(z) = z'.$$

Iz toga zaključujemo da je $\alpha\theta\alpha^{-1} \in H'$. Time smo pokazali da je $\alpha H \alpha^{-1} \subseteq H'$.

Neka je θ' proizvoljni element iz H' i $z \in E$. Tada je $\alpha(z) \in E'$ pa vrijedi da je $\theta'(\alpha(z)) = \alpha(z)$. Nadalje, vrijedi da je

$$(\alpha^{-1}\theta'\alpha)(z) = (\alpha^{-1}\alpha)(Z) = Z,$$

odnosno $\alpha^{-1}\theta'\alpha \in \Gamma(E) = H$. Budući da smo pokazali da je $\alpha^{-1}H'\alpha \subseteq H$, vrijedi da je $H' \subseteq \alpha H \alpha^{-1}$.

□

Teorem 2.0.22 (**Fundamentalni teorem Galoisove teorije**). *Neka je L Galoisovo proširenje polja K konačnog stupnja n.*

1) Za sva potpolja E od L koja sadrže K i sve podgrupe H Galoisove grupe $Gal(L : K)$ vrijedi

$$\Phi(\Gamma(E)) = E, \quad \Gamma(\Phi(H)) = H.$$

Također vrijede i sljedeće jednakosti:

$$|\Gamma(E)| = [L : E], \quad |Gal(L : K)|/|\Gamma(E)| = [E : K].$$

2) Potpolje E je normalno proširenje od K ako i samo ako je $\Gamma(E)$ normalna podgrupa od $Gal(L : K)$. Ako je E normalno proširenje onda je $Gal(E : K)$ izomorfna kvocijentnoj grupi $Gal(L : K)/\Gamma(E)$.

Dokaz. 1) Neka je E potpolje od L koje sadrži K. Budući da je L normalno proširenje od K, ono je polje razlaganja nekog polinoma $f \in K[X]$. Znamo da E sadrži K te time slijedi da je $f \in E[X]$. Dakle, L je normalno proširenje od E. Iz teorema 2.0.16 slijedi da je L separabilno proširenje od E. Dakle L je Galoisovo proširenje polja E pa iz propozicije 2.0.18 slijedi da je $|\Gamma(E)| = [L : E]$. Nadalje, iz teorema 1.2.8 i već spomenutog korolara možemo zaključiti sljedeće:

$$[E : K] = [L : K]/[L : E] = |\mathrm{Gal}(L : K)|/|\Gamma(E)|.$$

Kako znamo da je $\Gamma(E) = \mathrm{Gal}(L : E)$ i da je L Galoisovo proširenje od E, onda iz teorema 2.0.20 slijedi da je

$$\Phi(\Gamma(E)) = E.$$

Još nam preostaje pokazati da vrijedi $\Gamma(\Phi(H)) = H$.

Iz teorema 2.0.7 znamo da je $H \subseteq \Gamma(\Phi(H))$. Označimo $\Gamma(\Phi(H))$ s H'. Iz propozicije 2.0.8 slijedi

$$\Phi(H) = \Phi(\Gamma(\Phi(H))) = \Phi(H').$$

Iz teorema 2.0.9 slijedi $|H| = [L : \Phi(H)] = [L : \Phi(H')] = |H'|$. Zbog $H \subseteq H'$ i konačnosti od $\mathrm{Gal}(L : K)$ slijedi da je $H' = H$. Odnosno, vrijedi tvrdnja:

$$\Gamma(\Phi(H)) = H.$$

2) Pretpostavimo da je E normalno proširenje. Neka je $\alpha \in \mathrm{Gal}(L : K)$ i α' restrikcija od α na E. Tada je α' monomorfizam iz E u L te po teoremu 2.0.14 je to K-automorfizam od E. Budući da $\alpha(E) = \alpha'(E) = E$, po teoremu 2.0.21 slijedi:

$$\Gamma(E) = \Gamma(\alpha(E)) = \alpha\Gamma(E)\alpha^{-1}.$$

Dakle, možemo zaključiti da je $\Gamma(E)$ normalna podgrupa od $\mathrm{Gal}(L : K)$.

Obratno, pretpostavimo da je $\Gamma(E)$ normalna podgrupa od $\mathrm{Gal}(L : K)$. Neka je α_1 K-monomorfizam iz E u L. Iz propozicije 2.0.12 znamo da se K-monomorfizam može proširiti do K-automorfizma α od L. Budući da je $\Gamma(E)$ normalna podgrupa od $\mathrm{Gal}(L : K)$, vrijedi $\alpha\Gamma(E)\alpha^{-1} = \Gamma(E)$, odakle iz teorema 2.0.21 slijedi $\Gamma(\alpha(E)) = \Gamma(E)$.

Budući da je Γ bijekcija, slijedi $\alpha(E) = \alpha_1(E) = E$. Stoga je α_1 K-automorfizam od E. Ovime smo pokazali da je svaki K-monomorfizam iz E u L zapravo K-automorfizam od E. Dakle, iz teorema 2.0.14 slijedi da je E normalno proširenje od K.

Pretpostavimo da je E normalno proširenje i neka je α' restrikcija na E K-automorfizma α od L. Iz teorema 2.0.14 slijedi da je $\alpha' \in \mathrm{Gal}(E : K)$. Definirajmo preslikavanje $\Theta : \mathrm{Gal}(L : K) \to \mathrm{Gal}(E : K)$ na sljedeći način

$$\Theta(\alpha) = \alpha'.$$

Pokažimo da je Θ homomorfizam grupa. Za sve $\alpha_1, \alpha_2 \in \mathrm{Gal}(L : K)$, uz oznake $\Theta(\alpha_1) = \alpha_1'$ i $\Theta(\alpha_2) = \alpha_2'$ te za sve $u \in E$ vrijedi sljedeće:

$$\begin{aligned}([\Theta(\alpha_1)][\Theta(\alpha_2)])(u) &= (\alpha_1'\alpha_2')(u)\\ &= \alpha_1'(\alpha_2(u))\\ &= \alpha_1(\alpha_2(u))\\ &= (\alpha_1\alpha_2)(u)\\ &= (\Theta(\alpha_1\alpha_2))(u).\end{aligned}$$

Dakle vrijedi

$$[\Theta(\alpha_1)][\Theta(\alpha_2)] = \Theta(\alpha_1\alpha_2).$$

Jezgra ovog homomorfizma je skup svih $\alpha \in \mathrm{Gal}(L : K)$ tako da je α' identiteta na E, a to je upravo $\Gamma(E)$. Iz prvog teorema o izomorfizmu slijedi

$$Gal(L : K)/\Gamma(E) \cong Gal(E : K).$$

□

Poglavlje 3

Primjene Galoisove teorije u geometriji

U ovom poglavlju primijenit ćemo teoriju polja u klasičnim konstrukcijskim problemima. Da bismo to mogli učiniti trebamo povezati Euklidsku ravninu s poljem $\mathbb{R}$.

Ako je P_0 potpolje polja $\mathbb{R}$, skup koji se sastoji od svih točaka oblika (x, y), gdje su $x \in P_0$ i $y \in P_0$, zvat ćemo ravnina od P_0 i označavat ćemo istom oznakom. Zamislimo da su jedine dopuštene operacije na tom skupu sljedeće:

(1) (Ravnalo) Kroz bilo koje dvije različite točke iz P_0 možemo povući pravac.

(2) (Šestar) Možemo nacrtati kružnicu čije je središte točka iz P_0 te radijus udaljenost između dviju točaka iz P_0.

Svaka točka koja je presjek dvaju pravca, dviju kružnica ili pravca i kružnice, a dobivena je operacijama ravnalom ili šestarom, kažemo da je konstruirana iz P_0 u jednom koraku. Skup svih takvih točaka označit ćemo s $C(P_0)$. Slično, možemo označiti $P_1 = P_0 \cup C(P_0)$ te općenito

$$P_n = P_{n-1} \cup C(P_{n-1}) \quad n \in \mathbb{N}. \tag{3.1}$$

Dakle, možemo reći da je točka konstruktibilna iz P_0 ako pripada skupu P_n za neki $n \in \mathbb{N}$. Za realan broj c kažemo da se može konstruirati ako se može konstruirati točka $(c, 0)$ s konačno mnogo konstrukcija ravnalom i šestarom koje počinju točkama s cjelobrojnim koordinatama. Kažemo da se točka (x, y) može konstruirati ako i samo ako su obje koordinate konstruktibilni realni brojevi.

Lema 3.0.1. *Neka je P potpolje od $\mathbb{R}$ i neka su L_1 i L_2 dva neparalelna pravca u P te C_1 i C_2 različite kružnice u P. Tada vrijedi sljedeće:*

(1) $L_1 \cap L_2$ je točka u ravnini od P,

(2) $L_1 \cap C_1 = \emptyset$ *ili se sastoji od jedne ili dvije točke u ravnini od* $P(\sqrt{u})$*, za neki* $u \in P,\ u > 0$*,*

(3) $C_1 \cap C_2 = \emptyset$ *ili se sastoji od jedne ili dvije točke u ravnini od* $P(\sqrt{u})$*, za neki* $u \in P,\ u > 0$*.*

Dokaz. (i) Neka su pravci L_1 i L_2 dani jednadžbama $ax + by + c = 0$ i $dx + ey + f = 0$, gdje su $a, b, c, d, e, f \in P$. Rješavanjem sustava ove dvije jednadžbe dobijemo točku presjeka pravaca L_1 i L_2. Točka presjeka je oblika $\left(\frac{bf-ec}{ea-bd}, \frac{cd-af}{ea-bd}\right)$, gdje je $ea - bd \neq 0$ jer su pravci L_1 i L_2 neparalelni. Budući da znamo da su $a, b, c, d, e, f \in P$, izrazi oblika $\frac{bf-ec}{ea-bd}, \frac{cd-af}{ea-bd}$ su također elementi polja. Dakle, dobivena točka je element polja P.

(ii) Neka su pravac i kružnica dani jednadžbama $dx+ey+f = 0$ i $x^2+y^2+ax+by+c = 0$. Pogledajmo slučaj kada je $d = 0$ i $e \neq 0$. Iz jednadžbe pravca dobijemo da je $y = -\frac{f}{e}$. Budući da su $e, f \in P$, slijedi da je $y \in P$. Uvrstimo y u jednadžbu kružnice te dobivamo $x^2 + \left(-\frac{f}{e}\right)^2 + ax + b\left(-\frac{f}{e}\right) + c = 0$. Zapišimo ovu jednadžbu kao $Ax^2 + Bx + C = 0$, gdje je $A = e^2$, $B = ae^2$ i $C = f^2 - bfe + ce^2$. Primijetimo da su $A, B, C \in P$. Kako je $e \neq 0$, onda je i $A \neq 0$. Bez smanjenja općenitosti možemo pretpostaviti da je $A = 1$. Tada dobivamo jednadžbu $x^2 + Bx + C = 0$. Nadopunimo jednadžbu na potpuni kvadrat $\left(x + \frac{B}{2}\right)^2 + C - \frac{B^2}{4} = 0$. Iz ovoga zaključujemo da je ili $L_1 \cap C_1 = \emptyset$ ili $x, y \in P(\sqrt{u})$, gdje je $u = -C + \frac{B^2}{4} \geq 0$.

Pogledajmo sada slučaj kada je $d \neq 0$. Radi jednostavnosti računa, neka je $d = 1$. Izrazimo x iz jednadžbe pravca te dobijemo $x = -ey-f$. Ako je točka $(x, y) \in L_1 \cap C_1$, supstitucijom u jednadžbu kružnice dobivamo

$$(-ey - f)^2 + y^2 + a(-ey - f) + by + c = 0.$$

Ovu jednadžbu možemo zapisati kao $Ay^2 + By + C = 0$, gdje su $A, B, C \in P$. Ako je $A = 0$, onda dobivamo da je $y = -\frac{C}{B}$, gdje su $B, C \in P$. Dakle, zaključujemo da su $x, y \in P$. Ako je $A \neq 0$, bez smanjenja općenitosti možemo pretpostaviti da je $A = 1$. Tada dobivamo jednadžbu $y^2 + By + C = 0$. Nadopunimo jednadžbu na potpuni kvadrat $\left(y + \frac{B}{2}\right)^2 + C - \frac{B^2}{4} = 0$. Iz ovoga zaključujemo da je ili $L_1 \cap C_1 = \emptyset$ ili $x, y \in P(\sqrt{u})$, gdje je $u = -C + \frac{B^2}{4} \geq 0$.

(iii) Neka su dvije kružnice dane jednadžbama $x^2+y^2+ax+by+c = 0$ i $x^2+y^2+dx+ey+f = 0$, gdje su $a, b, c, d, e, f \in P$. Oduzimanjem danih jednadžbi kružnica dobivamo $(a-d)x+(b-e)y+c-f = 0$. Dakle, dobili smo jednadžbu pravca čiji su koeficijenti $a - d, b - e, c - f \in P$. Možemo primijetiti kako problem presjeka dviju kružnica

možemo zapravo svesti na presjek kružnice C_1 ili C_2 i pravca. Dakle, dokaz ove tvrdnje nadalje se svodi na dokaz proveden u (ii).

□

Propozicija 3.0.2. *Za racionalne brojeve vrijede sljedeće tvrdnje:*

1. *svaki racionalan broj je konstruktibilan,*
2. *ako je broj $c > 0$ konstruktibilan, onda se može konstruirati i broj $\sqrt{c}$,*
3. *ako su c i d konstruktibilni brojevi, onda se mogu konstruirati i brojevi $c \pm d$, cd i c/d, tako da konstruktibilni brojevi tvore potpolje od $\mathbb{R}$ koje sadrži racionalne brojeve.*

Dokaz. Pri dokazu ćemo primjenjivati činjenicu da je skup cijelih brojeva $\mathbb{Z}$ konstruktibilan.

1) Zapišimo racionalan broj u obliku $\frac{m}{n}$, gdje su $m, n \in \mathbb{Z}$ i $n \neq 0$.

   Problem konstrukcije $\frac{m}{n}$ svodi se na konstrukciju broja $m\frac{1}{n}$, odnosno konstrukcije brojeva m i $\frac{1}{n}$ te njihovog produkta. Budući da je skup cijelih brojeva konstruktibilan, onda znamo da su brojevi $m, \frac{1}{n}$, a samim time i broj $\frac{m}{n}$, konstruktibilni. Prisjetimo se da se konstrukcija $\frac{1}{n}$ svodi na dijeljenje dužine u zadanom omjeru. Dakle, skup racionalnih brojeva $\mathbb{Q}$ je konstruktibilan.

2) Ova tvrdnja je zapravo jedna od standardnih konstrukcija Euklidske geometrije. Da bismo konstruirali broj $\sqrt{c}$ trebamo jediničnu dužinu.

   Na polupravcu konstruiramo dužinu duljine c te nadodamo dužinu duljine 1, odnosno, konstruiramo dužinu duljine $c + 1$. Nad dužinom $c + 1$ šestarom konstruiramo kružnicu kojoj je dužina duljine $c + 1$ promjer. Nakon toga konstruiramo pravac okomit na početni polupravac na udaljenosti c od početne točke polupravca. Presjek okomitog pravca i kružnice su dvije točke. Udaljenost bilo koje od tih točaka od početnog polupravca je tražena udaljenost $\sqrt{c}$. Dakle, konstruirali smo broj $\sqrt{c}$.

3) Konstrukcija $c \pm d$, cd i c/d se također svodi na standardne konstrukcije Euklidske geometrije (vidi [1]).

□

Teorem 3.0.3. *Ako je realan broj c konstruktibilan, onda je broj c algebarski stupnja 2^n, $n \in \mathbb{N}$ nad poljem $\mathbb{Q}$.*

Dokaz. Iz prethodne propozicije možemo zaključiti da nam je dovoljno raditi s poljem racionalnih brojeva. Dakle, broj c će biti konstruktibilan ako se može konstruirati konačnim brojem konstrukcija ravnalom i šestarom počevši od ravnine racionalnih brojeva. Točke

dobivene ovakvim konstrukcijama bit će presjeci pravaca i kružnica. Također, točke konstrukcije koje tvore pravac ili kružnicu mogu biti točke početne ravnine ili točke dobivene prijašnjim konstrukcijama. Iz leme 3.0.1 znamo da se svaka nova točka tako konstruirana nalazi u ravnini proširenja polja $\mathbb{Q}(\sqrt{u})$ od $\mathbb{Q}$, gdje je $u \in \mathbb{Q}$, $u > 0$ ili drugim riječima, u ravnini proširenja $\mathbb{Q}(v)$ od $\mathbb{Q}$, gdje je $v^2 \in \mathbb{Q}$. Takvo proširenje ima stupanj 1 (odnosno 2^0) ili 2 nad $\mathbb{Q}$, ovisno je li $v \in \mathbb{Q}$. Na sličan se način konstruira iduća točka koja onda leži u ravnini $\mathbb{Q}(v, w) = \mathbb{Q}(v)(w)$, gdje je $w^2 \in \mathbb{Q}(v)$. Za konačan niz konstrukcija ravnalom i šestarom vrijedi:

$$\mathbb{Q} \subset \mathbb{Q}(v_1) \subset \mathbb{Q}(v_1, v_2) \subset \cdots \subset \mathbb{Q}(v_1, \ldots, v_n)$$

gdje je ${v_i}^2 \in \mathbb{Q}(v_1, \ldots, v_{i-1})$ i $[\mathbb{Q}(v_1, \ldots, v_i) : \mathbb{Q}(v_1, \ldots, v_{i-1})] = 1$ ili 2 za $2 \leq i \leq n$. Točka $(c, 0)$ konstruirana na ovaj način leži u ravnini od $P = \mathbb{Q}(v_1, \ldots, v_n)$. Iz teorema 1.2.8 slijedi $[F : \mathbb{Q}]$ je potencija broja 2. Stoga je po teoremu 1.2.8 c algebarski nad $\mathbb{Q}$. Iz $\mathbb{Q} \subset \mathbb{Q}(c) \subset P$ po teoremu 1.2.8 slijedi da $[\mathbb{Q}(c) : \mathbb{Q}]$ dijeli $[P : \mathbb{Q}]$ te je stupanj $[\mathbb{Q}(c) : \mathbb{Q}]$ od c nad $\mathbb{Q}$ potencija broja 2. □

3.1 Problem trisekcije kuta

Teorem 3.1.1. *Nemoguće je trisektirati kut od* $60°$ *ravnalnom i šestarom.*

Dokaz. Imamo kut $3\theta = 60°$. Za svaki kut θ vrijedi:

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

Budući da želimo provjeriti može li se trisektirati kut od $60°$, zaključujemo da je $\theta = 20°$. Pokažimo da broj $\alpha = \cos 20°$ nije konstruktibilan. Imamo $\cos 3\theta = \cos 60° = \frac{1}{2}$. Sada ćemo uvesti supstituciju $\cos\theta = \alpha$.

$$\frac{1}{2} = 4\alpha^3 - 3\alpha$$

Ovo možemo zapisati kao:

$$8\alpha^3 - 6\alpha - 1 = 0$$

Budući da na polinom $f(x) = 8x^3 - 6x - 1$ ne možemo primijeniti Eisensteinov kriterij, definiramo polinom $g(x) = f(x/2) = x^3 - 3x - 1$. Dokažimo najprije da je g ireducibilan nad $\mathbb{Z}$. Ukoliko ne bi bio ireducibilan nad $\mathbb{Z}$, mogao bi se prikazati kao umnožak dvaju polinoma s cjelobrojnim koeficijentima, od kojih je jedan linearan:

$$g(x) = x^3 - 3x - 1 = (x - a)(x^2 + bx + c)$$

Možemo zaključiti da je $ac = -1$ te da je $a \in \{\pm 1\}$. Provjerimo vrijednosti od $g(a)$ za $a \in \{\pm 1\}$:

a	-1	1
g(a)	1	-3

Budući da vrijednost $g(a)$ nije 0 niti za jedan $a \in \{\pm 1\}$, polinom g ne možemo faktorizirati nad $\mathbb{Z}$ te je time g ireducibilan nad $\mathbb{Z}$. Prema Gaussovoj lemi, polinom g je ireducibilan i nad $\mathbb{Q}$. Budući da je polinom g ireducibilan to će značiti da je i polinom f ireducibilan. Stoga je $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$. Po teoremu 3.0.3 slijedi da broj α nije konstruktibilan, a onda ni θ nije konstruktibilan te zaključujemo da nije moguće provesti trisekciju kuta od 60° ravnalom i šestarom.

□

3.2 Problem duplikacije kocke

Teorem 3.2.1. *Nije moguće konstruirati kocku dvostruko većeg volumena od volumena zadane kocke, tj. ne može se duplicirati kocka ravnalom i šestarom.*

Dokaz. Pretpostavimo da je zadana kocka s bridom duljine 1. Želimo ispitati možemo li konstruirati duljinu brida α kocke s volumenom 2. Dakle, želimo da vrijedi $\alpha^3 = 2$. Provjerimo je li polinom $f(x) = x^3 - 2$ ireducibilan koristeći Eisensteinov kriterij.
Broj $p = 2$ je prost i zadovoljava:

(i) $2 \nmid 1$
Broj p ne dijeli vodeći koeficijent a_3.

(ii) $2 \mid 0, 2 \mid -2$
Broj p dijeli koeficijente $a_0,\ a_1$ i a_2.

(iii) $4 \nmid 2$
Broj p^2 ne dijeli koeficijent a_0.

Dakle, polinom f je ireducibilan nad $\mathbb{Q}$. Stoga vrijedi $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$. Nadalje, prema teoremu 3.0.3 broj α nije konstruktibilan. Dakle, nije moguće duplicirati kocku ravnalom i šestarom.

□

3.3 Problem kvadrature kruga

Teorem 3.3.1. *Nije moguće konstruirati kvadrat površine jednake površini zadanog kruga, tj. nije moguća kvadatura kruga ravnalom i šestarom.*

Dokaz. Pretpostavimo da je zadana jedinična kružnica. Želimo konstruirati kvadrat površine $\alpha^2 = \pi$. Odnosno, problem možemo svesti na pitanje, možemo li konstruirati $\sqrt{\pi}$. Kad bi $\sqrt{\pi}$ bio konstruktibilan broj, onda bi π bio konstruktibilan jer $\pi = \sqrt{\pi}^2$. Iz [8] znamo da je π transcedentan, a ne algebarski, a onda je i $\sqrt{\pi}$ također transcedentan. Dakle, prema teoremu 3.0.3 kvadratura kruga nije moguća. □

3.4 Problem konstrukcije pravilnog sedmerokuta

Teorem 3.4.1. *Nije moguće konstruirati pravilni sedmerokut ravnalom i šestarom.*

Dokaz. Konstrukcija mnogokuta ovisi o konstrukciji središnjeg kuta $\theta_n = \frac{2\pi}{n}$, odnosno u našem slučaju kuta $\theta_7 = \frac{2\pi}{7}$. Želimo provjeriti konstruktibilnost broja $\frac{2\pi}{7}$. Broj $\alpha = e^{2\pi i/7}$ zadovoljava jednadžbu $x^7 - 1 = 0$. Primijetimo da je polinom $x^7 - 1 = 0$ reducibilan jer $x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$. Dakle, α poništava polinom $P(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Provjerimo Eisensteinovim kriterijem je li polinom P ireducibilan nad $\mathbb{Q}$. Možemo vidjeti kako polinom P ne zadovoljava Eisensteinov kriterij. Uvedimo supstituciju tako da x zamijenimo s $x + 1$:

$$P(x+1) = (x+1)^6 + (x+1)^5 + (x+1)^4 + (x+1)^3 + (x+1)^2 + (x+1) + 1$$

Nadalje, pojednostavimo dobiveni izraz:

$$P(x+1) = x^6 + 7x^5 + 21x^4 + 35x^3 + 35x^2 + 21x + 7$$

Sada možemo primijeniti Eisensteinov kriterij jer ako dobijemo da je polinom $P(x+1)$ ireducibilan to će značiti da je i polinom P ireducibilan.
Broj $p = 7$ je prost i zadovoljava:

(i) $7 \nmid 1$
Broj p ne dijeli vodeći koeficijent a_6.

(ii) $7 \mid 7, 7 \mid 21, 7 \mid 35$
Broj p dijeli koeficijente a_0, a_1, a_2, a_3, a_4 i a_5.

(iii) $49 \nmid 7$
Broj p^2 ne dijeli koeficijent a_0.

Sada možemo zaključiti da je polinom $P(x+1)$ ireducibilan nad $\mathbb{Q}$, a time i polinom P te slijedi $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 6$. Budući da dobiveni stupanj nije potencija broja 2 po teoremu 3.0.3 slijedi da broj $\frac{2\pi}{7}$ nije konstruktibilan, odnosno da se pravilni sedmerokut ne može konstruirati ravnalom i šestarom. □

Bibliografija

[1] *Konstruktivne metode u geometriji*, 2020, https://web.math.pmf.unizg.hr/nastava/kmg/kmg_predavanja.pdf.

[2] R. Bellovin, *Lectures of Galois theory*, University of Glasgow, Glasgow, 2021.

[3] F. M. Brückler, *Povijest matematike*, PMF - Matematički odsjek, Zagreb, 2020.

[4] L. Goldmakher, *Galois theory - Lecture 12*, https://web.williams.edu/Mathematics/lg5/394/LS12.pdf.

[5] J. M. Howie, *Fields and Galois theory*, Springer, London, 2006.

[6] T. W. Hungerford, *Algebra*, sv. 73, Springer Science & Business Media, San Francisco, 2000.

[7] M. Kazalicki, *Klasične konstrukcije i teorije polja*, https://web.math.pmf.unizg.hr/~mkazal/reprints/konstr.pdf.

[8] I. Stewart, *Galois theory*, Chapman and Hall/CRC, 1990.

[9] B. Širola, *Algebarske strukture*, https://web.math.pmf.unizg.hr/nastava/alg_prof/predavanja/ASpred.pdf.

Sažetak

U ovom diplomskom radu opisana je Galoisova teorija te je ista primijenjena na klasične konstrukcijske probleme u geometriji - trisekciju kuta, duplikaciju kocke, kvadraturu kruga te konstrukciju pravilnog sedmerokuta. Rad se sastoji od tri cjeline. Prvi dio služi kao podsjetnik na važne definicije i teoreme potrebne za bolje razumijevanje same Galoisove teorije. U drugoj cjelini uvodimo Galoisovu teoriju koja se razvila iz klasičnog problema teorije polinomijalnih jednadžbi. Glavna ideja Galoisove teorije je povezati proširenje polja $K \subset F$ s grupom svih automorfizama od F koji fiksiraju elemente polja K, odnosno Galoisovom grupom proširenja polja K. O postojanju bijekcije između ova dva spomenuta skupa govori upravo Fundamentalni teorem Galoisove teorije. U zadnjem, trećem dijelu, ovog rada primijenili smo opisanu teoriju na konstrukcijske probleme i algebarski dokazali kako konstrukcije uistinu nisu moguće.

Summary

In this thesis, Galois theory is described and applied to classical construction problems in geometry - angle trisection, doubling the cube, squaring the circle and construction of a regular heptagon. The work consists of three parts. The first part serves as a reminder of important definitions and theories necessary for a better understanding of Galois theory itself. In the second unit, we introduce the Galois theory, the origin of which begins with a classical problem in the theory of polynomial equations. The main idea of the Galois theory is to connect the field extension $K \subset F$ to the group of all automorphisms of F that fix the elements of the field K, in other words, to the Galois group of the field extension K. The existence of a one-to-one correspondence between these two mentioned sets is exactly what the Fundamental theorem of Galois theory says. In the last, the third part of this paper, we applied the described theory to construction problems and proved algebraically that constructions are truly impossible.

Životopis

Rođena sam 11. 8. 1995. u Zagrebu. Školovanje sam započela u osnovnoj školi Ksavera Šandora Gjalskog u Zagrebu. Nakon završetka osnovne škole, 2010. upisujem opću II. gimnaziju. Po završetku srednjoškolskog obrazovanja, 2014. godine upisujem Preddiplomski sveučilišni studij Matematika na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu pri čemu se 2018. godine prebacujem na Preddiplomski sveučilišni studij Matematika, smjer nastavnički. Godine 2020. stječem titulu sveučilišne prvopristupnice edukacije matematike te iste godine upisujem Diplomski sveučilišni studij Matematika i informatika, smjer nastavnički.