Abel-Ruffinijev teorem

Pavković, Josipa

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Josipa Pavković

ABEL-RUFFINIJEV TEOREM

Diplomski rad

Voditelj rada:
prof.dr.sc. Ozren Perše

Zagreb, veljača 2016.

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

Uvod

U algebri, Abel-Ruffinijev teorem nam govori da ne postoji opće algebarsko rješenje, tj. rješenje u radikalima, za jednadžbe petog ili višeg stupnja. Teorem je dobio ime po Paolu Ruffiniju, koji je dao nepotpuni dokaz 1799., i Niels Henriku Abelu, koji potpuni dokaz objavljuje 1823. godine. Evariste Galois samostalno je dokazao teorem koji je objavljen nakon njegove smrti 1846. godine. Sadržaj teorema je često pogrešno interpretiran. Teorem ne tvrdi da su jednadžbe višeg stupnja nerješive. Štoviše, vrijedi da svaki polinom u polje $\mathbb{C}$ ima rješenja, i to baš onoliko njih koliki je njegov stupanj; to nam tvrdi fundamentalni teorem algebre. Iako ova rješenja ne možemo uvijek izračunati točno u radikalima, mogu se izračunati s proizvoljnom točnošću pomoću numeričkih metoda, kao što su Newton-Raphson ili Laguerrova metoda. Naime, teorem se bavi oblikom kako to rješenje mora imati. Pokazuje se da rješenja jednadžbe višeg stupnja ne možemo uvijek prikazati pomoću koeficijenata jednadžbe s konačnim brojem operacija zbrajanja, oduzimanja, množenja, dijeljenja i korijena.

Opišimo ukratko sadržaj ovog rada. U prvom poglavlju pod nazivom Osnovne algebarske strukture nalazi se uvodno, motivacijsko gradivo algebarskih struktura potrebno za izgradnju temelja Galoisove teorije. U njemu se kreće od izgradnje grupa, definiraju se preslikavanja među grupama te se teorija proširuje do prstena i ideala. U drugom poglavlju poseban naglasak stavit ćemo na prsten polinoma. Vidjeti ćemo da, kada je k polje, svi poznati teoremi koji vrijede u $\mathbb{Z}$, imaju anologon u $k[x]$, štoviše, vidjet ćemo da se svi poznati dokazi mogu prenijeti ovdje. Pojam proširenja polja, kojim se bavimo u trećem poglavlju, je najosnovniji termin koji se proteže kroz ovu čitavu diplomsku radnju. Zbog toga je nastala potreba da se proširenje polja prikaže sa svim svojim najvažnijim svojstvima. Ono pak inducira mnoge pojmove vezane uz razumjevanje i postavljanje Galoisove teorije koja je jedno od glavnih činjenica ovog diplomskog rada. Posebno ćemo proučavati algebarska i separabilna proširenja, koja su ujedno i temelj Galoisove teorije, kojom se opširnije bavimo u četvrtom poglavlju. U petom poglavlju ukratko ćemo prikazati postupak rješavanja jednadžbi trećeg i četvrtog stupnja. Zadnje poglavlje usko se specijalizira na samu bit ovog rada. U njemu se dokazuje Galoisov teorem o korespondenciji rješivosti polinoma u radikalima i rješivosti pripadne Galoisove grupe, te Abel-Ruffinijev teorem.

Poglavlje 1

Osnovne algebarske strukture

1.1 Grupe

Definicija 1.1. *Uređeni par $(G, \cdot)$, pri čemu je G neprazan skup, $a \cdot : G \times G \to G$ binarna operacija, zove se **grupa** ako vrijede sljedeća svojstva (aksiomi grupe):*

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)*

Element e, ili e_G ako želimo posebno naglasiti da je riječ o grupi G, zove se **neutralni element** grupe, ili kraće, **neutral** grupe. Za zadani $x \in G$, element $x^{-1} \in G$ koji zadovoljava gore navedeno treće po redu svojstvo, zove se **inverzni element** od x, ili kraće **inverz** od x. Ako još vrijedi i svojstvo

$$x \cdot y = y \cdot x, \quad \forall x, y \in G \quad \text{(komutativnost)},$$

onda kažemo da je G **komutativna grupa**, a u suprotnom govorimo o **nekomutativnoj grupi**; jednako su u upotrebi i termini **Abelova grupa** za komutativnu grupu, te **neabelova grupa** za nekomutativnu grupu.

Navedimo važan primjer grupe:

Primjer 1.2. *Neka je $E_n = \{1, \ldots, n\}$. Funkcija σ sa skupa E_n u skup E_n koja je bijekcija, zovemo permutacija skupa E_n. Skup $S(E_n)$ svih permutacija nepraznog skupa E_n je grupa u odnosu na kompoziciju funkcija kao binarnu operaciju na skupu $S(E_n)$. Grupu $(S(E_n), \circ)$, ili kraće S_n zovemo simetrična grupa ili grupa permutacija. Spomenimo ovdje još jedan važan pojam. Permutacija $\tau \in S_n$ zove se **transpozicija** ako postoje $1 \leq i, j \leq n, i \neq j$, takvi*

da je $\tau(i) = j, \tau(j) = i$ i $\tau(k) = k$ za sve $k \neq i, j$. Grupa S_n je generirana transpozicijama; tj., svaku se permutaciju $\sigma \in S_n$ može zapisati kao kompoziciju $\sigma = \tau_p \circ \cdots \circ \tau_1$, za neke transpozicije $\tau_1, \ldots, \tau_p$. Kažemo da je σ ***parna permutacija****, ako je broj transpozicija paran, a da je* ***neparna*** *ako je taj broj neparan.*

Primjer 1.3. *Grupa S_n, za $n \geq 3$, nije Abelova jer elementi grupe* (1 2) *i* (1 3) *ne komutiraju;* (1 2) (1 3) = (1 3 2) *i* (1 3) (1 2) = (1 2 3)*.*

Napomena 1.4. *Od sada nadalje, kada je riječ o nekoj grupi $G = (G, \cdot)$, mi pri množenju elemenata u toj grupi nećemo pisati simbol " $\cdot$ " ; tj., ako su $x, y \in G$, onda pišemo xy namjesto $x \cdot y$.*

Ako imamo neki skup G na kojemu je definirana operacija $\cdot : G \times G \to G$, tj. za bilo koje $x, y \in G$ je uvijek i $x \cdot y \in G$, kažemo da je $(G, \cdot)$ **grupoid**. Grupoid u kojem vrijedi i asocijativnost zove se **polugrupa**. Polugrupa koja ima jedinstven neutralni element zove se **monoid**.

Primjer 1.5.

1. *Skup $\mathbb{Q}^\times$, svih ne-nul racionalnih brojeva, s binarnom operacijom $*$ množenja je Abelova grupa. Neutralni element je* 1*. Inverzni element od $r \in \mathbb{Q}^\times$ je $1/r$. Slično, $\mathbb{R}^\times$ i $\mathbb{C}^\times$ su Abelove grupe.*

2. *Skup cijelih brojeva $\mathbb{Z}$ s binarnom operacijom zbrajanja $+$, je Abelova grupa. Neutralni element je* 0*. Inverzni element od $n \in \mathbb{Z}$ je $-n$. Slično $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su Abelove grupe s binarnom operacijom zbrajanja.*

Podskup $H \subseteq G$ je **podgrupa** od G ako je to ujedno i grupa za operaciju koja je definirana na G. Drugim riječima, H je podgrupa od G ako vrijede sljedeća dva uvjeta:

1. $1 \in H$;
2. $(\forall x, y \in H) : \quad xy \in H$;
3. $(\forall x \in H) : \quad x^{-1} \in H$.

Činjenicu da je H podgrupa od G označavamo sa

$$H \leq G.$$

Sljedeći jednostavan rezultat je takozvani "*kriterij podgrupe*".

Propozicija 1.6. *Podskup H je podgrupa grupe G* ***akko*** *vrijedi sljedeći uvjet:*

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

Napomena 1.7. *Svaka grupa G ima barem dvije podgrupe; to su sama G i {e}, njih zovemo* ***trivijalnim*** *podgrupama. Podgrupe koje nisu trivijalne zovemo i* ***pravim*** *podgrupama.*

Primjer 1.8. *1. Četiri permutacije*

$$\boldsymbol{V} = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

čine grupu, iz razloga što je $\boldsymbol{V}$ *podgrupa od* S_4*:* $(1) \in \boldsymbol{V}$*; kako je* $\alpha^2 = (1), \forall \alpha \in \boldsymbol{V}$*, tada je* $\alpha^{-1} = \alpha \in \boldsymbol{V}$*; umnožak bilo koje dvije različite permutacije iz* $\boldsymbol{V}$ *je permutacija iz* $\boldsymbol{V}$*. Lako se pokaže da je* $\boldsymbol{V}$ *Abelova.*

2. Definiramo

$$A_n := \textit{skup svih parnih permutacija u } S_n.$$

Pokazuje se da su A_n *(normalne) podgrupe u simetričnoj grupi* S_n*; one se zovu* ***alternirajuće grupe****. Nadalje, za* $5 \leq n \in \mathbb{N}$*,* A_n *je prosta grupa. Za grupu kažemo da je* ***prosta*** *ako nema netrivijalnih normalnih podgrupa.*

Sada ćemo definirati "skup generatora" koji nam je potreban za razumjevanje pojma "cikličke grupe".

Definicija 1.9. *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; sam skup S zovemo **skup generatora**. Kažemo da je G **konačnogenerirana** grupa ako postoji konačan skup $S = \{x_1, \ldots, x_n\}$ takav da je $G = \langle S \rangle$; u tom slučaju pišemo i $G = \langle x_1, \ldots, x_n \rangle$. Grupa G je **ciklička** ako se može generirati jednim elementom, to jest, ako postoji neki $g \in G$ takav da je $G = \langle g \rangle$; svaki takav g zove se **generator** cikičke grupe G.

Primjer 1.10. *Skup cijelih brojeva* $\mathbb{Z}$ *je aditivna (beskonačna) ciklička grupa s generatorom 1 ili -1.*

Definicija 1.11. *Ako je G grupa, definirajmo njezin* ***red*** *kao*

$$|G| := card(G);$$

tj., red grupe je kardinalni broj skupa G. Kažemo da je grupa G ***konačna grupa*** *ako je* $|G| < \infty$*; inače je G* ***beskonačna grupa****.*

Definicija 1.12. *Neka su G i H dvije grupe. Preslikavanje $f : G \to H$ je **homomorfizam** grupa, ako "čuva strukturu", tj., ako vrijedi*

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

Uvedimo oznaku

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

Nadalje, homomorfizam f koji je još i injekcija naziva se **monomorfizam**, f koji je i surjekcija zovemo **epimorfizam**, a homomorfizam koji je i mono- i epi-,tj., bijektivan homomorfizam, zovemo **izomorfizam**. Za dvije grupe G i H reći ćemo da su *izomorfne*, ako postoji neki izomorfizam među njima; tu činjenicu označavamo sa

$$G \cong H.$$

Posebno, ako je $G = H$, tj., ako imamo homomorfizam $f : G \to G$, onda kažemo da je f **endomorfizam** od G. Skup svih endomorfizama od G označavamo sa $EndG$.
Endomorfizam koji je još i bijekcija zove se **automorfizam** od G. Skup svih automorfizama od G označavamo $AutG$

Korolar 1.13. *Za proizvoljan homomorfizam $f : G \to H$ definirajmo njegovu **jezgru***

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

i njegovu sliku

$$\text{Im } f := \{f(x) | x \in G\}.$$

Definicija 1.14. *Ako je H podgrupa od G i a element od G, tada podskup $aH = \{ax | x \in H\}$ zovemo **lijeva susjedna klasa**, a podskup Ha **desna susjedna klasa** od H u G.*

Sada definiramo važan pojam "normalne podgrupe". Neka je G grupa i neka je H podgrupa grupe G. Pretpostavimo da za sve elemente x od G imamo $xH \subset Hx$ (ili ekvivalentno, $xHx^{-1} \subset H$). Ako umjesto x uvrstimo x^{-1}, dobivamo $H \subset xHx^{-1}$ pa slijedi da je $xHx^{-1} = H$. Stoga je naš uvjet jedank uvjetu $xHx^{-1} = H$, za sve $x \in G$. Podgrupu H koja zadovoljava ovaj uvjet zovemo **normalna**. Ako je K normalna podgrupa od G, uvodimo oznaku $K \triangleleft G$.
Napomenimo ovdje, što je evidentno iz same definicije, da je u komutativnoj grupi svaka podgrupa normalna; zato pojam normalne podgrupe ima smisla samo u nekomutativnim situacijama. Nadalje, primjetimo da su trivijalne podgrupe $\{e\}$ i G, od proizvoljne grupe G, uvijek normalne.

Teorem 1.15. *Neka je G proizvoljna grupa i N neka njezina normalna podgrupa. Tada kvocijentni skup $G/N = \{xN : x \in G\}$ s operacijom*

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

ima strukturu grupe; sada se G/N zove ***kvocijentna grupa*** *od G po N. Nadalje, preslikavanje*

$$\pi = \pi_N : G \to G/N, \quad x \mapsto xN,$$

je epimorfizam grupa sa jezgrom $\operatorname{Ker}\pi = N$*; π zovmo* ***kanonski epimorfizam****, ili* ***kanonska surjekcija****.*

Primjer 1.16. *Kvocijentna grupa $(\mathbb{Z}/m\mathbb{Z}, +)$, tzv.* ***grupa ostataka modulo*** *m, je (konačna) ciklička grupa; obično pišemo $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}$. Gdje smo, za dani $m \geq 0$ i $a \in \mathbb{Z}$,* ***klasu kongruencije*** *$[a]$ od a modulo m definirali kao*

$$[a] = \{b \in \mathbb{Z} : b \equiv a \bmod m\}.$$

Familiju svih klasa kongruencije modulo m označavat ćemo sa $\mathbb{I}_m$ umjesto $\mathbb{Z}/m\mathbb{Z}$.

Iz Teorema 1.15. direktno slijedi:

Korolar 1.17. *Svaka normalna podgrupa $K \triangleleft G$ je jezgra nekog homomorfizma.*

Teorem 1.18. (Prvi teorem o izomorfizmu) *Ako je $f : G \to H$ homomorfizam, tada je*

$$\operatorname{Ker} f \triangleleft G \ \ i \ \ G/\operatorname{Ker} f \cong \operatorname{Im} f.$$

Ako je $\operatorname{Ker} f = K$ *i $\varphi : G/K \to \operatorname{Im} f \leq H$ dana s $\varphi : aK \to f(a)$ tada je φ izomorfizam.*

Sljedeća dva teorema koja navodimo su posljedice Prvog teorema o izomorfizmu.

Teorem 1.19. (Drugi teorem o izomorfizmu) *Ako su H i K podgrupe grupe G takve da je $H \triangleleft G$, tada HK je podgrupa, $H \cap K \triangleleft K$, i*

$$K/(H \cap K) \cong HK/H.$$

Teorem 1.20. (Treći teorem o izomorfizmu) *Ako su H i K normalne podgrupe grupe G takve da $K \leq H$, tada $H/K \triangleleft G/K$ i*

$$(G/K)/(H/K) \cong G/H.$$

Sljedeći rezultat, koji možemo smatrati četvrtim teoremom o izomorfizmu, opisuje podgrupe kvocijentne grupe G/K.

Teorem 1.21. (Teorem o korespodenciji za grupe) *Neka je G grupa, neka je $K \triangleleft G$, i neka je $\pi : G \to G/K$ prirodno preslikavanje. Tada je*

$$S \mapsto \pi(S) = S/K$$

je bijekcija između familije svih podgrupa S od G koje sadrže K i familije svih podgrupa grupe G/K. Ako označimo S/K sa S^*, tada

$$T \leq S \leq G \text{ ako i samo ako } T^* \leq S^* \text{ i tada vrijedi } [S : T] = [S^* : T^*],$$

i

$$T \triangleleft S \text{ ako i samo ako } T^* \triangleleft S^* \text{ i tada vrijedi } S/T \cong S^*/T^*.$$

1.2 Prsteni i ideali

Definicija 1.22. *Uređnu trojku* $(R, +, \cdot)$ *zovemo* ***prsten*** *ukoliko je za operacije zbrajanja* $+ : R \times R \to R$ *i množenja* $\cdot : R \times R \to R$ *ispunjeno sljedeće:*

1. *(R,+) je komutativna grupa, sa neutralom* $0 = 0_R$;
2. $(R, \cdot)$ *je polugrupa, tj. množenje je asocijativno*
3. *Vrijedi distributivnost "množenja prema zbrajanju"*

$$x(y + z) = xy + xz, \quad \forall x, y, z \in R,$$

$$(x + y)z = xz + yz, \quad \forall x, y, z \in R.$$

Element $0 = 0_R$, neutral u grupi $(R, +)$, zvat ćemo **nula** prstena R.
Ako postoji **jedinični element**, ili kraće **jedinica**, $1 = 1_R \in R$ takav da je

$$1 \cdot x = x \cdot 1 = x, \quad \forall x \in R,$$

onda kažemo da je R **prsten s jedinicom**. U nastavku će se pojam prsten odnositi na prsten s jedinicom, a isto tako ćemo s A označavati komutativan prsten. Prsten R je **komutativan prsten** ako je

$$x \cdot y = y \cdot x, \quad \forall x, y \in R;$$

inače govorimo o **nekomutativnom prstenu**.

Definicija 1.23. *Skup* $S \subseteq R$*, gdje je R neki prsten, je* ***podprsten*** *od R ako je* $S = (S, +, \cdot)$ *i sam prsten. Drugim riječima, S je podprsten od R ako vrijede sljedeća dva uvjeta:*

1. $(\forall x, y \in S) : \quad x - y \in S \quad$ *(tj., (S,+) je grupa)*;
2. $(\forall x, y \in S) : \quad x \cdot y \in S \quad$ *(tj., (S,·) je grupoid)*.

Definicija 1.24. *Element* $0 \neq \lambda \in R$ *(tj.,* $0 \neq \rho \in R$*) takav da je*

$$\lambda x = 0 \quad (tj.\ x\rho = 0)\ \ za\ neki\ \ 0 \neq x \in R$$

zove se ***lijevi*** *(tj.* ***desni****)* ***djelitelj nule****.*

R je **integralna domena**, ili kraće **domena**, ako nema ni lijevih ni desnih djelitelja nule. Poznati primjeri komutativnih prstena $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$ su domene; nul-prsten nije domena.

Jedna od specijalnih vrsta prstena su **tijela**; to su prsteni kojima su svi ne-nul elementi invertibilni. Za element $\omega \in R$, gdje je R prsten s jedinicom 1, kažemo da je **invertibilan**, ako $\exists \omega' \in R$ takav da je

$$\omega\omega' = \omega'\omega = 1.$$

Komutativna tijela zovu se **polja**. Primjeri polja su $\mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$.

Sljedeća konstrukcija poopćava konstrukciju polja racionalnih brojeva $\mathbb{Q}$ iz domene cijelih brojeva $\mathbb{Z}$.

Teorem 1.25. *Ako je R domena, tada postoji polje F koje sadrži R kao podprsten. Štoviše, F možemo odabrati tako da, za svaki $f \in F$ postoje $a, b \in R$, $b \neq 0$ i $f = ab^{-1}$.*

Definicija 1.26. *Polje F iz Teoremu 1.25. naziva se **polje razlomaka** od R, a označava s $Frac(R)$.*

Sljedeći pojam, *karakteristika prstena*, posebno je važan u teoriji polja, a definiramo ga na sljedeći način. Neka je R prsten i pretpostavimo da postoji $m \in \mathbb{N}$ takav da je

$$mx = 0, \quad \forall x \in R.$$

Najmanji takav prirodan broj naziva se **karakteristika prstena** R. Ako takav broj ne postoji, tada kažemo da R ima *karakteristiku nula*.

Uvodimo sada pojam ideala.

Definicija 1.27. *Neka je R prsten. Podskup $I \subseteq R$ je **lijevi** (tj. **desni**) **ideal** u R ako su ispunjena sljedeća dva uvjeta:*

1. *I je podprsten od R;*
2. *Za sve $r \in R$ i $x \in I$ je $rx \in I$ (tj. $xr \in I$).*

Gornji uvjet (2) često se simbolički piše kao

$$RI \subseteq I \quad \text{(tj. } IR \subseteq I\text{)}.$$

Podskup $I \subseteq R$ je (*dvostrani*) **ideal** ako je on istovremeno i lijevi i desni ideal. Činjenicu da je I ideal u prestenu R označavamo sa

$$I \trianglelefteq R.$$

Nadalje, reći ćemo da je ideal I od R **pravi ideal** ako je $I \neq R$ i $I \neq \{0\}$, ovdje je sa $\{0\}$ označen **nul-ideal**. U slučaju komutativnog prstena R je

$$ideal \equiv \text{lijevi ideal} \equiv \text{desni ideal}.$$

Uvodimo još neke pojmove.

Definicija 1.28. *Neka je R prsten i I neki ideal prstena R. Skup $S \subseteq R$ je* ***skup generatora*** *od I ako je*

$$I = (S) := \bigcap_{\substack{J \trianglelefteq R \\ S \subseteq J}} J;$$

tj., I je najmanji ideal u R koji sadži skup S. Ideal I je ***konačno generiran*** *ako postoji konačan podskup $S \subseteq R$ takav da je $I = (S)$. Ideal I je* ***glavni ideal*** *ako postoji neki element $r \in R$ takav da je $I = (r)$. Kažemo da je R* ***prsten glavnih ideala****, ili kraće PGI, ako je svaki ideal u R glavni.*

Definirajmo sada pojam homomorfizma prstena.

Homomorfizam prstena je preslikavanje $f : R \to S$ gdje su R i S prsteni, a f preslikavanje koje zadovoljava:

$$f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y), \quad f(1_R) = 1_S,$$

za sve $x, y \in R$. Sa $Hom(R, S)$ označavamo skup svih homomorfizama iz R u S. Homomorfizam f koji je još i injekcija naziva se **monomorfizam**, f koji je i surjekcija zovemo **epimorfizam**, a homomorfizam koji je i mono- i epi-, tj. bijektivan homomorfizam, zovemo **izomorfizam**. Za dva prstena R i S reći ćemo da su *izomorfni*, ako postoji neki izomorfizam f među njima; tu činjenicu označavamo sa

$$R \cong S.$$

Za proizvoljan homomorfizam $f : R \to S$ definirajmo njegovu **jezgru**

$$\operatorname{Ker} f := f^{-1}(\{0_S\}) = \{x \in R | f(x) = 0\},$$

i njegovu **sliku**

$$\operatorname{Im} f := f(R) = \{f(x) | x \in R\}.$$

Propozicija 1.29. *Ako je $f : A \to R$ homomorfizam prstena, tada je* $\operatorname{Ker} f$ *ideal u A i* $\operatorname{Im} f$ *je podprsten od R.*

Korolar 1.30. *Ako je $f : k \to R$ homomorfizam prstena, gdje je k polje i R ne nul-prsten, tada je f injekcija.*

Poglavlje 2

Prsten polinoma

Iako pretpostavljamo da smo upoznati s polinomima, u ovom poglavlju ih uvodimo aksiomatski. Skup svih polinom činit će prsten polinoma i predstavljat će važnu strukturu za proučavanje.

Definicija 2.1. *Ako je R komutativan prsten, tada niz σ u R definiramo sa*

$$\sigma = (s_0, s_1, s_2, \ldots, s_i, \ldots);$$

pri čemu su svi $s_i \in R$, za sve $i \geq 0$. s_i se nazivaju koeficijenti *od σ.*

Da bismo odredili kada su dva niza jednaka, uočimo da je niz σ funkcija $\sigma : \mathbb{N} \to \mathbb{R}$, gdje je $\mathbb{N}$ skup prirodnih brojeva, takvih da $\sigma(i) = s_i$ za sve $i \geq 0$. Prema tome, ako je $\tau = (t_1, t_2, t_3, \ldots, t_i, \ldots)$ niz, tada je $\sigma = \tau$ ako i samo ako je $\sigma(i) = \tau(i)$, za svaki $i \geq 0$.

Definicija 2.2. *Niz $\sigma = (s_0, s_1, s_2, \ldots, s_i, \ldots)$ u komutativnom prstenu R naziva se **polinom** ako postoji neki cijeli broj $m \geq 0$ takav da je $s_i = 0$ za sve $i > m$; tj.,*

$$\sigma = (s_0, s_1, s_2, \ldots, s_m, 0, 0, \ldots).$$

Polinom ima konačno mnogo ne-nul koeficijenata. **Nul-polinom**, u oznaci $\sigma = 0$, je niz $\sigma = (0, 0, 0, \ldots)$.

Definicija 2.3. *Ako je $\sigma = (s_0, s_1, s_2, \ldots, s_n, 0, 0, \ldots) \neq 0$ polinom, tada postoji $s_n \neq 0$ tako da je $s_i = 0$ za sve $i > n$. s_n se zove **vodeći koeficijent** od σ, n se zove **stupanj** od σ (označavama sa $deg(\sigma)$).*

Ako je R komutativan prsten, tada skup svih polinoma s koeficijentima u R označavamo s $R[x]$.

Propozicija 2.4. *Ako je R komutativan prsten, tada je $R[x]$ komutativan prsten koji sadrži R kao podprsten.*

Dokaz. (Skica.) Definiramo zbrajanje i množenje polinoma na sljedeći način: ako je $\sigma = (s_0, s_1, \ldots)$ i $\tau = (t_0, t_1, \ldots)$, tada je

$$\sigma + \tau = (s_0 + t_0, s_1 + t_1, \ldots, s_n + t_n, \ldots)$$

i

$$\sigma\tau = (c_0, c_1, \ldots)$$

gdje je $c_k = \sum_{i+j=k} s_i t_j = \sum_{i=0}^{k} s_i t_{k-i}$. Aksiomi iz definicije komutativnog prstena se rutinski provjeravaju. Podskup $\{(r, 0, 0, \ldots) | r \in R\}$ je podprsten od $R[x]$ kojeg poistovjećujemo s R. □

Lema 2.5. *Neka je R komutativan prsten i neka su σ i $\tau \in R[x]$ ne-nul polinomi.*

1. *Ili je $\sigma\tau = 0$ ili $deg(\sigma\tau) \leq deg(\sigma) + \deg(\tau)$.*
2. *Ako je R domena, tada je $\sigma\tau \neq 0$ i*

$$deg(\sigma\tau) = deg(\sigma) + deg(\tau).$$

3. *Ako je R domena, tada je $R[x]$ domena.*

Dokaz. (Skica.) Neka su $\sigma = (s_0, s_1, \ldots)$ i $\tau = (t_0, t_1, \ldots)$ redom stupnja m i n.

1. Ako je $k > m + n$, tada je svaki član u $\sum_i s_i t_{k-i}$ jednak 0 ($s_i = 0$ ili $t_i = 0$).
2. Svaki član u $\sum_i s_i t_{m+n-i}$ je jednak 0, s mogućom iznimkom $s_m t_n$. Kako je R domena, $s_m \neq 0$ i $t_n \neq 0$ povlače $s_m t_n \neq 0$.
3. Slijedi iz (2.) jer je produkt ne-nul polinoma ne-nul.

□

Definicija 2.6. *Definiramo element $x \in R[x]$ sa*

$$x = (0, 1, 0, 0, \ldots).$$

Propozicija 2.7. *Ako je $\sigma = (s_0, s_1, \ldots, s_n, 0, 0, \ldots)$ tada je*

$$\sigma = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n,$$

gdje je svaki element $s \in R$ jednak polinomu $(s, 0, 0, \ldots)$.

Dokaz.

$$\begin{aligned}\sigma &= (s_0, s_1, \ldots, s_n, 0, 0, \ldots)\\ &= (s_0, 0, 0, \ldots) + (0, s_1, 0, 0, \ldots) + \cdots + (0, 0, \ldots, s_n, 0, \ldots)\\ &= s_0(1, 0, 0, \ldots) + s_1(0, 1, 0, 0, \ldots) + \cdots + s_n(0, 0, \ldots, 1, 0, \ldots)\\ &= s_0 + s_1x + s_2x^2 + \cdots + s_nx^n.\end{aligned}$$

□

Nadalje ćemo upotrebljavati standardne oznake, tj. umjesto

$$\sigma = (s_0, s_1, \ldots, s_n, 0, 0, \ldots)$$

ćemo pisati

$$f(x) = s_0 + s_1x + s_2x^2 + \ldots + s_nx^n.$$

Ako je $f(x) = s_0+s_1x+s_2x^2+\ldots+s_nx^n$, gdje je $s_n \neq 0$ tada se s_0 zove **slobodni koeficijent**, a s_n se zove, kao što smo već rekli, **vodeći koeficijent**. Ako je vodeći koeficijent $s_n = 1$, tada se $f(x)$ zove **normiran**. Svaki polinom osim nul-polinoma ima stupanj. **Konstantan polinom** je ili nul-polinom ili polinom stupnja 0. Polinom stupnja 1, $ax + b, b \neq 0$, se zove **linearan**, polinom stupnja 2 se zove **kvadratan**, stupnja 3 **kuban**, itd.

Korolar 2.8. *Polinomi $f(x) = s_0 + s_1x + s_2x^2 + \ldots + s_nx^n$ i $g(x) = t_0 + t_1x + t_2x^2 + \ldots + t_mx^m$ stupnja n i m su jednaki ako i samo ako je $n = m$ i $s_i = t_i$ za sve i.*

Sada možemo opisati općenitu ulogu varijable x u $f(x)$. Neka je R komutativan prsten, svaki polinom $f(x) = s_0 + s_1x + s_2x^2 + \ldots + s_nx^n \in R[x]$ definira **polinomijalnu funkciju** $f : R \to R$ evaluacijom: Ako je $a \in R$, definiramo $f(a) = s_0 + s_1a + s_2a^2 + \ldots + s_na^n \in R$.

Definicija 2.9. *Neka je k polje. Polje razlomaka od $k[x]$, označava se $k(x)$ i zove **polje racionalnih funkcija** nad k.*

Propozicija 2.10. *Ako je k polje, tada elementi od $k(x)$ imaju oblik $f(x)/g(x)$, gdje su $f(x), g(x) \in k[x]$ i $g(x) \neq 0$.*

Teorem 2.11. (Algoritam dijeljenja) *Neka je R komutativan prsten, i neka su $f(x)$, $g(x) \in R[x]$ polinomi stupnja ≥ 0. Pretpostavimo da je vodeći koeficijent od $g(x)$ invertibilan u R. Tada postoje jedinstveni polinomi $q(x)$,$r(x) \in R[x]$ takvi da je*

$$f(x) = g(x)q(x) + r(x), \quad deg(r(x)) < deg(g(x)).$$

U posebnom slučaju kada je k polje i $f(x)$,$g(x) \in k[x]$ gdje je $g(x) \neq 0$, tada postoji jedinstveni polinomi $q(x)$,$r(x) \in k[x]$ takvi da je $f(x) = g(x)q(x) + r(x)$ i $deg(r(x)) < deg(q(x))$. Odavde slijedi da je $k[x]$ prsten u kojem postoji algoritam dijeljenja.

Definicija 2.12. *Ako je $f(x) \in k[x]$, gdje je k polje, tada definiramo* ***korijen*** *od $f(x)$ u k kao element $a \in k$ takav da je $f(a) = 0$.*

Lema 2.13. *Neka je $f(x) \in k[x]$, gdje je k polje, i neka je $u \in k$. Tada postoji $q(x) \in k[x]$ takav da vrijedi*

$$f(x) = q(x)(x - u) + f(u).$$

Propozicija 2.14. *Ako je $f(x) \in k[x]$, gdje je k polje, tada je a korijen od $f(x)$ u k ako i samo ako $x - a$ dijeli $f(x)$ u $k[x]$.*

Teorem 2.15. *Neka je k polje i neka je $f(x) \in k[x]$. Ako je $f(x)$ stupnja n, tada $f(x)$ ima najviše n korijena u k.*

Definicija 2.16. *Neka su $f(x)$ i $g(x)$ polinomi u $k[x]$, pri čemu je k polje. Polinom $c(x) \in k[x]$ nazivamo* ***zajednički djelitelj*** *polinoma $f(x)$ i $g(x)$ ako $c(x)|f(x)$ i $c(x)|g(x)$. Ako $f(x)$ i $g(x)$ nisu oba 0, definiramo njihov* ***najveći zajednički djelitej****,* nzd*, kao normiran zajednički djelitelj s najvećim stupnjem. Ako je $f(x) = 0 = g(x)$, definiramo njihov* nzd*=0.* Nzd *od $f(x)$ i $g(x)$ se često označava i s (f, g).*

Teorem 2.17. *Ako je k polje i neka su $f(x), g(x) \in k[x]$, tada je njihov* nzd *$d(x)$ linearna kombinacija od $f(x)$ i $g(x)$; tj. postoje $s(x), t(x) \in k[x]$ tako da vrijedi*

$$d(x) = s(x)f(x) + t(x)g(x).$$

Definicija 2.18. *Element p u domeni R je ireducibilan ako nije nula niti invertibilan i ako ne može biti prikazan kao produkt dva neinvertibilna elementa.*

Sada opisujemo ireducibilne polinome $p(x) \in k[x]$, gdje je k polje.

Propozicija 2.19. *Ako je k polje, tada je polinom $p(x) \in k[x]$* ***ireducibilan*** *ako i samo ako je $deg(p) = n \geq 1$ i ne postoji faktorizacija u $k[x]$ oblika $p(x) = g(x)h(x)$ u kojem su oba faktora stupnja manjeg od n.*

Drugim riječima, ako $f(x)$ ireducibilan, tada u faktorizacji $f(x) = g(x)h(x)$ jedan od polinoma $g(x)$ ili $h(x)$ mora biti konstantan. Može se provjeriti da je po Propoziciji 2.19. polinom prvog stupnja ireducibilan.

Korolar 2.20. *Neka je k polje i neka je $f(x) \in k[x]$ kvadratan ili kuban polinom. Tada je $f(x)$ ireducibilan u $k[x]$ ako i samo ako $f(x)$ nema korijena u k.*

Lema 2.21. *Neka je k polje i neka su $p(x), f(x) \in k[x]$ i neka je $d(x) = (p, f)$ njihov* nzd*. Ako je $p(x)$ normiran ireducibilan polinom, tada*

$$d(x) = \begin{cases} 1 & ako\ p(x) \nmid f(x); \\ p(x) & ako\ p(x)|f(x). \end{cases}$$

Definicija 2.22. *Za dva polinoma $f(x)$, $g(x) \in k[x]$, gdje je k polje, kažemo da su* ***relativno prosti*** *ako je njihov* nzd *jedank 1.*

Napomena 2.23. *Za svaki (ne nužno ireducibilan polinom) $f(x)$ sa koeficijentima u bilo kojem polju vrijedi da $f(x)$ ima sve različite nultičke ako i samo ako $nzd(f, f') = 1$, gdje je $f'(x)$ derivacija od $f(x)$.*

Na kraju ovog poglavlja navedimo još jednu posljedicu algoritma dijeljenja koju koristimo u kasnijim dokazima:

Teorem 2.24. *Ako je k polje, tada svaki ideal I u $k[x]$ je glavni ideal. Štoviše, ako je $I \neq \{0\}$, tada postoji normiran polinom takav da generira I.*

Poglavlje 3

Kvocijentni prsteni i proširenje polja

U ovom poglavlju prvo ćemo definirati kvocijentni prsten, a zatim ćemo navesti Prvi teorem o izomorfizmu za prstene. Definirat ćemo pojam proširenja polja k te elemenata koji su algebarski nad k. Dokazat ćemo Kroneckerov teorem koji govori o egzistenciji polja proširenja u kojem ireducibilan polinom ima korijen. Nakon toga definiramo pojam polja razlaganja i iskazujemo teorem koji govori o izomorfizmu konačnih polja.

Ako je R neki prsten i I neki njegov ideal, onda je posebno $(R, +)$ aditivna, komutativna grupa i posebno je $(I, +)$ normalna podgrupa. Tako ima smisla definirati kvocijentnu, aditivnu grupu:

$$R/I = (R, +)/(I, +)$$

Cilj nam je tu aditivnu, komutativnu grupu "organizirati" u prsten.

Teorem 3.1. *Neka je R prsten i I bilo koji njegov ideal. Ako na kvocijentnoj, aditivnoj grupi R/I definiramo množenje iz $R/I \times R/I$ u R/I sa*

$$(a + I)(b + I) := ab + I, \quad a, b \in R$$

onda R/I ima strukturu prstena. Nadalje, preslikavanje

$$\pi =: R \to R/I, \quad a \to a + I$$

*je epimorfizam prstena, zove se **kanonski epimorfizam**, ili kanonska surjekcija.*

Dokaz. (Skica.) Definiramo množenje na aditivnoj Abelovoj grupi R/I s

$$(a + I)(b + I) = ab + I.$$

Da bi vidjeli da je ovo dobro definirana funkcija $R/I \times R/I \to R/I$, pretpostavimo da je $a + I = a' + I$ i $b + I = b' + I$, tj. $a - a' \in I$ i $b - b' \in I$. Moramo pokazati da vrijedi

$(a' + I)(b' + I) = a'b' + I = ab + I$,tj. $ab - a'b' \in I$. Ali

$$ab - a'b' = ab - a'b + a'b - a'b'$$

$$= (a - a')b + a'(b - b') \in I,$$

kao što je traženo. Da bi dokazali da je R/I komutativan prsten, dovoljno je dokazati da vrijedi asocijativnost i komutativnost množenja, distributivnost i da je jedinica $1+I$. Dokazi ovih svojstava su trivijalni. Pokažimo npr. da je množenje u R/I komutativno

$$(a + I)(b + I) = ab + I = ba + I = (b + I)(a + I).$$

Ponovnim zapisivanjem jednadžbe $(a+I)(b+I) = ab+I$ i upotrebljavajući definiciju od π, $a+I = \pi(a)$, dobijemo $\pi(a)\pi(b) = \pi(ab)$. Kako je $\pi(1) = 1+I$, slijedi da je π homomorfizam prstena. Konačno π je surjekcija jer je $a + I = \pi(a)$. □

Definicija 3.2. *Komutativan prsten R/I definiran u Teoremu 3.1. zove se* kvocijentni prsten *od R modulo I ili kraće R mod I.*

Korolar 3.3. *Ako je I ideal u komutativnom prstnu R, tada postoji komutativan prsten A i homomorfizam prstena $\pi : R \to A$ takav da vrijedi $I = \operatorname{Ker}\pi$.*

Dokaz. Ako zaboravimo na množenje, tada je preslikavanje $\pi : R \to R/I$ homomorfizam između aditivnih grupa, te vrijedi

$$I = \operatorname{Ker}\pi = \{r \in R | \pi(a) = 0 + I = I\}.$$

Sada se sjetimo množenja $(a + I)(b + I) = ab + I$; tj. $\pi(a)\pi(b) = \pi(ab)$. Stoga, π je homomorfizam prstena i $\operatorname{Ker}\pi$ je jednaka I bez obzira da li je funkcija π homomorfizam prstena ili homomorfizam aditivnih grupa. □

Teorem 3.4. (Prvi teorem o izomorfizmu) *Ako je $f : R \to A$ homomorfizam prstena, tada je* $\operatorname{Ker} f$ *ideal u R,* $\operatorname{Im} f$ *podprsten od A i*

$$R/\operatorname{Ker} f \cong \operatorname{Im} f$$

Dokaz. Neka je $I = \operatorname{Ker} f$. Već smo vidjeli u Propoziciji 1.29. da je I ideal u R i da je $\operatorname{Im} f$ podprsten od A. Ako zaboravimo na množenje u prstenima, tada je funkcija $\varphi : R/I \to A$, definirana s $\varphi(r + I) = f(r)$, izomorfizam aditivnih grupa. Kako je $\varphi(1 + I) = f(1) = 1$, dovoljno je dokazati da je φ čuva množenje. Ali $\varphi((r + I)(s + I)) = \varphi(rs + I) = f(rs) = f(r)f(s) = \varphi(r + I)\varphi(s + I)$. Stoga je φ homomorfizam. □

Za prstene kao i za grupe, prvi teorem o izomorfizmu stvara izomorfizam iz homomorfizma jednom kada znamo jezgru i sliku. Također nam kaže da ne postoji značajna razlika između kvocijentnog prstena i slike homomorfizma.

Propozicija 3.5. *Neka je k polje i $I = (p(x))$, gdje je $0 \neq p(x) \in k[x]$. Tada su sljedeće tvrdnje ekvivalentne: $p(x)$ je ireducibilan polinom; $k[x]/I$ je polje; $k[x]/I$ je domena.*

Dokaz. Pretpostavimo da je $p(x)$ ireducibilan. Uočimo da je $I = (p(x))$ pravi ideal, stoga je *jedinica* u $k[x]/I$, $1 + I$, različita od nule. Uzmemo neki $f(x) + I \in k[x]/I$, različit od nule. Tada $f(x) \notin I$, tj. $f(x)$ nije višekratnik od $p(x)$, ili $p(x) \nmid f(x)$. Po Lemi 2.21. p i f su relativno prosti i tada po Teoremu 2.17. postoje polinomi s i t takvi da je $sf + tp = 1$. Tada, $sf - 1 \in I$ i vrijedi $1 + I = sf + I = (s + I)(f + I)$. Dakle, svaki ne-nul element u $k[x]/I$ je invertibilan. Jasno je da svako polje je ujedno i domena.
Pretpostavimo sada da je $k[x]/I$ domena. Kada $p(x)$ ne bi bio ireducibilan, tada bi postojala faktorizacija $p(x) = g(x)h(x)$ u $k[x]$ sa $deg(g) < deg(p)$ i $deg(h) < deg(p)$. Iz toga odmah slijedi da su i $g(x) + I$ i $h(x) + I$ različiti od nule u $k[x]/I$. *Nula* u $k[x]/I$ je $0 + I = I$ i $g(x) + I = I$ ako i samo ako $g(x) \in I = (p(x))$; međutim kada bi to vrijedilo, imali bi $p(x)|g(x)$, iz čega slijedi $deg(p) \leq deg(g)$. Produkt

$$(g(x) + I)(h(x) + I) = p(x) + I = I$$

je nula u kvocijentnom prstenu, što je kontradikcija s $k[x]/I$ je domena. Dakle, $p(x)$ mora biti ireducibilan polinom. □

Struktura od R/I zna biti dosta komplicirana, ali za neke specijalne slučajeve izbora prstena R i ideala I, može se lako opisati. Ako na primjer za $p(x)$ uzmemo ireducibilan polinom, sljedeća će nam propozicija dati potpun opis polja $k[x]/(p(x))$.

Propozicija 3.6. *Neka je k polje, neka je $p(x) \in k[x]$ normiran ireducibilan polinom stupnja d, neka je $K = k[x]/I$, gdje je $I = (p(x))$ i neka je $\beta = x + I \in K$.*

1. *K je polje i $k' = \{a + I : a \in K\}$ je potpolje od K izomorfno polju k. Dakle, ako identificiramo k' i k, tada je k potpolje od K.*
2. *β je korijen od $p(x)$ u K.*
3. *Ako je $g(x) \in k[x]$ i β je korijen od $g(x)$, tada $p(x)|g(x)$ su u $k[x]$.*
4. *$p(x)$ je jedinstven normiran ireducibilan polinom u $k[x]$ koji ima β za korijen.*
5. *Niz $1, \beta, \beta^2, \ldots, \beta^{d-1}$ je baza od K kao vektorskog prostora nad poljem k, te je $dim_k(K) = d$.*

Dokaz. 1. Kvocijentni prsten $K = k[x]/I$ je polje po Propoziciji 3.5., zbog pretpostvke da je $p(x)$ ireducibilan polinom. Po Korolaru 1.30. lako se vidi da je restrikcija prirodnog preslikavanja $\varphi = \pi|k : k \to K$, definiranog sa $\varphi(a) = a + I$, izomorfizam sa $k \to k'$.

2. Neka je $p(x) = a_0 + a_1x + \ldots + a_{d-1}x^{d-1} + x^d$, gdje su $a_i \in k$, za svaki i. U $K = k[x]/I$ imamo

$$\begin{aligned} p(\beta) &= (a_0 + I) + (a_1 + I)\beta + \ldots + (1 + I)\beta^d \\ &= (a_0 + I) + (a_1 + I)(x + I) + \ldots + (1 + I)(x + I)^d \\ &= (a_0 + I) + (a_1x + I) + \ldots + (1x^d + I) \\ &= a_0 + a_1x + \ldots + x^d + I \\ &= p(x) + I = I, \end{aligned}$$

   jer je $p(x) \in I = (p(x))$. Ali $I = 0 + I$ je nul element od $K = k[x]/I$, dakle β je korijen od $p(x)$.

3. Ako je $p(x) \nmid g(x)$ u $k[x]$, tada jer je $p(x)$ ireducibilan njihov *nzd* je 1. Tada postoje $s(x), t(x) \in k[x]$ takvi da je $1 = s(x)p(x) + t(x)g(x)$. Kako je $k[x] \subseteq K[x]$, možemo promatrati tu jednadžbu u $K[x]$. Uvrštavanjem β dolazimo do kontradikcije $1 = 0$.

4. Neka je $h(x) \in k[x]$ normiran ireducibilan polinom koji ima β za korijen. Po (3.) imamo da $p(x)|h(x)$. Kako je $h(x)$ ireducibilan, imamo da je $h(x) = cp(x)$ za neku konstantu c. Kako su $h(x)$ i $p(x)$ normirani polinomi, imamo da je $c = 1$ i $h(x) = p(x)$.

5. Svaki element od K ima oblik $f(x) + I$, gdje je $f(x) \in k[x]$. Po algoritmu dijeljenja, postoje polinomi $q(x), p(x) \in k[x]$ takvi da je $f(x) = q(x)p(x) + r(x)$ i ili je $r(x) = 0$ ili $deg(r) < d = deg(p)$. Kako je $f - r = qp \in I$, slijedi da je $f(x) + I = r(x) + I$. Ako je $r(x) = b_0 + b_1x + \ldots + b_{d-1}x^{d-1}$, gdje su $b_i \in k$ za svaki i, tada vidimo, kao u dokazu dijela (2.), da $r(x) + I = b_0 + b_1\beta + \ldots + b_{d-1}\beta^{d-1}$. Stoga $1, \beta, \beta^2, \ldots, \beta^{d-1}$ razapinje K.
   Da dokažemo jedinstvenost, prepostavimo da

$$b_0 + b_1\beta + \ldots + b_{d-1}\beta^{d-1} = c_0 + c_1\beta + \ldots + c_{d-1}\beta^{d-1}.$$

   Definiramo $g(x) \in k[x]$ sa $g(x) = \sum_{i=0}^{d-1}(b_i - c_i)x^i$; ako je $g(x) = 0$, gotovi smo. Ako je $g(x) \neq 0$, tada $deg(g)$ je definiran, i $deg(g) < d = deg(p)$. S druge strane, β je korijen od $g(x)$ pa iz dijela (3.) slijedi $p(x)|g(x)$; stoga, $deg(p) \leq deg(g)$, što je kontradikcija. Slijedi da je $1, \beta, \beta^2, \ldots, \beta^{d-1}$ baza od K kao vektorskog prostora nad k, te slijedi $dim_k(K) = d$.

□

Definicija 3.7. *Neka je K polje koje sadži k kao potpolje, tada K zovemo* ***proširenje*** *od k, i pišemo "K/k je proširenje polja". Kažemo da je proširenje polja K/k* ***konačno proširenje*** *od k ako je K konačnodimenzionalan vektorski prostor nad k. Dimenzija od K, koju označavamo $[K : k]$, zovemo stupanj od K/k.*

Propozicija 3.6.(5) pokazuje nam zašto $[K : k]$ zovemo stupanj proširenja K/k.

Definicija 3.8. *Neka je K/k proširenje polja. Za element $\alpha \in K$ kažemo da je **algebarski nad** k ako postoji ne-nul polinom $f(x) \in k[x]$ takav da je $f(\alpha) = 0$. Ako α nije algebarski nad k kažemo da je **transcendentan nad** k. Ako je svaki element $\alpha \in K$ algebarski nad k, kažemo da je K **algebarsko proširenje** polja k.*

Definicija 3.9. *Neka je K/k proširenje i $\alpha \in K$, tada označimo s $k(\alpha)$ najmanje potpolje od K koje sadrži k i α; $k(\alpha)$ nazivamo potpoljem od K dobiveno **pridruživanjem** α polju k. Općenitije, ako je A podskup od K, definiramo $k(A)$ kao presjek svih potpolja od K koje sadrže $k \bigcup A$; $k(A)$ nazivamo potpoljem od K dobiveno **pridruživanjem** A polju k. Posebno, ako je $A = \{z_1, \ldots, z_n\}$ konačan podskup, možemo $k(A)$ označiti s $k(z_1, \ldots, z_n)$.*

Sada iskazujemo sljedeći važan teorem.

Teorem 3.10. *1. Ako je K/k proširenje polja i $\alpha \in K$ algebarski nad k, tada postoji jedinstven normiran ireducibilan polinom $p(x) \in k[x]$ takav da je $p(\alpha) = 0$. Također vrijedi, ako je $I = (p(x))$, tada je $k[x]/I \cong k(\alpha)$; zaista, postoji izomorfizam*

$$\varphi : k[x]/I \to k(\alpha)$$

takav da $\varphi(x + I) = \alpha$ i $\varphi(c + I) = c$, za svaki $c \in k$.

2. Ako je $\alpha' \in K$ neki drugi korijen polinoma $p(x)$, tada postoji izomorfizam

$$\theta : k(\alpha) \to k(\alpha')$$

takav da $\theta(\alpha) = \alpha'$ i $\theta(c) = c$, za svaki $c \in k$.

Dokaz. 1. Uzmimo u obzir evaluaciju polinoma, homomorfizam prstena $\varphi : k[x] \to K$ definiran s

$$\varphi : f(x) \mapsto f(\alpha).$$

Sada $\operatorname{Im}\varphi$ je podprsten od K koji sadrži sve polinome u α; tj., sve elemente oblika $f(\alpha)$ tako da je $f(x) \in k[x]$. $\operatorname{Ker}\varphi$ je ideal u $k[x]$, po Korolaru 3.3., koji sadrži sve $f(x) \in k[x]$ takve da je $f(\alpha) = 0$. Kako je po Teoremu 2.24., svaki ideal u $k[x]$ glavni ideal, imamo da je $\operatorname{Ker}\varphi = (p(x))$ za neki normiran polinom $p(x)$. Ali $k[x]/(p(x)) \cong \operatorname{Im}\varphi$, koja je domena, pa je $p(x)$ ireducibilan polinom po Propoziciji 3.5.. Ista propozicija nam kaže da je $k[x]/(p(x))$ polje i tada po Prvom teoremu o izomorfizmu vrijedi $k[x]/(p(x)) \cong \operatorname{Im}\varphi$; tj. $\operatorname{Im}\varphi$ je potpolje od K koje sadrži k i α. Kako svako potpolje od K koje sadrži k i α sadrži i $\operatorname{Im}\varphi$, imamo $\operatorname{Im}\varphi = k(\alpha)$. Dokazali smo sve osim jedinstvenosti od $p(x)$ koja slijedi iz Propozicije 3.6(4).

2. Kao i u dijelu (i), postoje izomorfizmi $\varphi : k[x]/I \to k(\alpha)$ i $\psi : k[x]/I \to k(\alpha')$ takvi da je $\varphi(c+I) = c$ i $\psi(c) = c+I$ za svaki $c \in k$; također, $\varphi : x+I \mapsto \alpha$ i $\psi : x+I \mapsto \alpha'$. Kompozicija $\theta = \psi\varphi^{-1}$ je traženi izomorfizam.

□

Definicija 3.11. *Ako je K/k proširenje polja i $\alpha \in K$ je algebarski nad k, tada jedinstveni normiran ireducibilan polinom $p(x) \in k[x]$ takav da je $p(\alpha) = 0$ zovemo* ***minimalni polinom*** *od α nad k, i označavamo ga s*

$$irr(\alpha, k) = p(x).$$

Minimalni polinom $irr(\alpha, k)$ ovisi o polju k. Na primjer, $irr(i, \mathbb{R}) = x^2 + 1$, dok $irr(i, \mathbb{C}) = x - i$. Sljedeći teorem koristan je za dokazivanje teorema indukcijom po stupnju.

Teorem 3.12. *Neka je $k \subseteq E \subseteq K$, gdje je E konačno proširenje od k i K konačno proširenje od E. Tada je K konačno proširenje od k, i*

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

Dokaz. Neka je $A = a_1, \ldots, a_n$ baza od E nad k i neka je $B = b_1, \ldots, b_n$ baza od K nad E, tada je dovoljno dokazati da niz X svih $a_i b_j$ je baza od K nad k.
Da bi pokazali da X razapinje K, uzmemo $u \in K$. Kako je B baza od K nad E, postoje skalari $\lambda_j \in E$ takvi da je $u = \sum_j \lambda_j b_j$. Kako je A baza od E nad k, postoje skalari $\mu_{ji} \in k$ takvi da je $\lambda_j = \sum_i \mu_{ji} a_i$. Stoga, $u = \sum_{ij} \mu_{ji} a_i b_j$, i X razapinje K nad k.
Da pokažemo da je X linearno nezavisan nad k, pretpostavimo da postoje skalari $\mu_{ji} \in k$ takvi da je $\sum_{ij} \mu_{ji} a_i b_j = 0$. Ako definiramo $\lambda_j = \sum_j \mu_{ji} a_i$, tada $\lambda_j \in E$ i $\sum_j \lambda_j b_j = 0$. Kako je B linearno nezavisan nad E, slijedi da je

$$0 = \lambda_j = \sum_i \mu_{ji} a_i$$

za svaki j. Kako je A linearno nezavisan nad k, slijedi da je $\mu_{ji} = 0$, za svaki i i j. □

Sada dokazujemo važan rezultat koji kaže ako je $f(x) \in k[x]$, gdje je k bilo koje polje, tada postoji veće polje K koje sadrži k i sve korijene od $f(x)$.

Teorem 3.13. (Kronecker) *Neka je k polje i $f(x) \in k[x]$, tada postoji K koji sadrži k, tj. k je potpolje od K i $f(x)$ je produkt linearnih polinoma u $K[x]$.*

Dokaz. Dokaz provodimo indukcijom po $deg(f)$. Ako je $deg(f) = 1$, tada je $f(x)$ linearan i možemo odabrati $K = k$. Ako je $deg(f) > 1$, možemo zapisati $f(x) = p(x)g(x)$, gdje je $p(x)$ ireducibilan. Sada iz Propozicije 3.6.(1) slijedi da postoji polje F koje sadrži k i korijen z iz $p(x)$. Stoga, u $F[x]$, mi imamo $p(x) = (x - z)h(x)$ i $f(x) = (x - z)h(x)g(x)$. Indukcijom, postoji polje K koje sadrži F (stoga i k) takvo da $h(x)g(x)$, pa i $f(x)$ je produkt linearnih faktora u $K[x]$. □

Sada ćemo definirati polje razlaganja polinoma.

Definicija 3.14. *Neka je k potpolje polja K i neka je $f(x) \in k[x]$. Kažemo da se polinom f razlaže nad proširenjem K polja k ako se f faktorizira u linearne faktore u $K[x]$, tj. postoji $a \in k$ i $z_1, \ldots, z_n \in K$ takvi da je*

$$f(x) = a(x - z_1) \cdots (x - z_n)$$

*Polje K je **polje razlaganja** za polinom f nad poljem k ako je K najmanje proširenje polja k u kojem se f razlaže.*

Pogledajmo polinom $f(x) = x^2 + 1 \in \mathbb{Q}[x]$. Korijeni od $f(x)$ su $\pm i$, zbog čega se $f(x)$ razlaže nad poljem $\mathbb{C}$; tj., $f(x) = (x - i)(x + i)$ je produkt linearnih polinoma u $\mathbb{C}[x]$. Međutim, $\mathbb{C}$ nije polje razlaganja nad poljem $\mathbb{Q}$, iz razloga što $\mathbb{C}$ nije *najmanje* polje koje sadrži $\mathbb{Q}$ i sve korijene od $f(x)$. Polje razlaganja na $\mathbb{Q}$ je $\mathbb{Q}(i)$; polje razlaganja nad $\mathbb{R}$ je $\mathbb{R}(i) = \mathbb{C}$.

Korolar 3.15. *Neka je k polje, i neka je $f(x) \in k[x]$. Tada postoji polje razlaganja od $f(x)$ nad poljem k.*

Dokaz. Po Kroneckerovom teoremu, postoji proširenje polja K/k takvo da se $f(x)$ razlaže u $K[x]$; $f(x) = a(x - \alpha_1) \cdots (x - \alpha_n)$. Potpolje $E = k(\alpha_1, \ldots, \alpha_n)$ od K je polje razlaganja od $f(x)$ nad k. □

Sada ćemo rješiti problem jedinstvenosti polja razlaganja.

Lema 3.16. *Neka je $f(x) \in k[x]$, gdje je k polje, i neka je E polje razlaganja od $f(x)$ na k. Neka je $\varphi : k \to k'$ izomorfizam polja, neka je $\varphi^* : k[x] \to k'[x]$ izomorfizam*

$$g(x) = a_0 + a_1 x + \ldots + a_n x^n \mapsto g^*(x) = \varphi(a_0) + \varphi(a_1)x + \ldots + \varphi(a_n)x^n,$$

i neka je E' polje razlaganja od $f^*(x)$ nad k'. Tada postoji izomorfizam $\phi : E \to E'$ koji proširuje φ.

Dokaz. Dokaz provodimo indukcijom po $d = [E : k]$. Ako je $d = 1$, tada je $f(x)$ produkt linearnih polinoma u $k[x]$, i slijedi da $f^*(x)$ je također produkt linearnih polinoma u $k'[x]$. Stoga, $E' = k'$, i možemo staviti $\phi = \varphi$.
Za korak indukcije, odaberemo korijen z od $f(x)$ u E koji nije u k', i neka je $p(x) = irr(z, k)$ minimalni polinom od z nad poljem k. Sada $deg(p) > 1$, jer $z \notin k$; po Propoziciji 3.6. $[k(z) : k] = deg(p)$. Neka je z' korijen od $p^*(x) = irr(z', k')$ pripadajući normiran ireducibilan polinom u $k'[x]$. Po Propoziciji 3.10.(2) postoji izomorfizam $\tilde{\varphi} : k(z) \to k'(z')$ koji proširuje φ, takav da $\tilde{\varphi} : z \mapsto z'$.

Možemo promatrati $f(x)$ kao polinom sa koeficijentima u $k(z)$ (jer iz $k \subseteq k(z)$ slijedi $k[x] \subseteq k(z)[x]$). Mi tvrdimo da je E polje razlaganja od $f(x)$ nad $k(z)$; tj.,

$$E = k(z)(z_1, \ldots, z_n),$$

gdje su $z_1, \ldots, z_n$ korijeni od $f(x)/(x - z)$; tada;

$$E = k(z, z_1, \ldots, z_n) = k(z)(z_1, \ldots, z_n).$$

Slično, E' je polje razlaganja od $f^*(x)$ nad $k'(z')$. Ali po Teoremu 3.12. $[E : k(z)] < [E : k]$, pa tvrdnja indukcije daje izomorfizam $\phi : E \to E'$ koji proširuje $\tilde{\varphi}$, pa i φ. □

Teorem 3.17. *Neka je k polje i $f(x) \in k[x]$, tada svaka dva polja razlaganja od $f(x)$ nad poljem k su izomorfna putem izomorfizma koji fiksira k po točkama.*

Dokaz. Neka su E i E' polja razlaganja od $f(x)$ nad k. Ako je φ identiteta na k, tada tvrdnja direktno slijedi iz prethodne leme. □

Poglavlje 4

Galoisova teorija

U ovom poglavlju ćemo objasniti osnovne pojmove i tvrdnje teorije Galoisa.

Definicija 4.1. *Neka je E polje i neka je k potpolje polja E. **Automorfizam** od E je izomorfizam $\sigma : E \to E$. Kažemo da σ **fiksira** k ako vrijedi $\sigma(a) = a$, $\forall a \in k$.*

Primjer 4.2. *Neka je $f(x) = x^2 + 1 \in \mathbb{Q}[x]$. Polje razlaganja od $f(x)$ nad poljem $\mathbb{Q}$ je $E = \mathbb{Q}(i)$. $\mathbb{Q}(i)$ je potpolje polja $\mathbb{C}$ koje se sastoji od svih brojeva oblika $a + bi$, gdje su a i b racionalni brojevi. Kompleksna konjugacija $\sigma : a \mapsto \bar{a}$ je primjer automorfizma od E koji fiksira $\mathbb{Q}$.*

Propozicija 4.3. *Neka je k potpolje polja K, neka je*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in k[x],$$

i neka je $E = k(z_1, z_2, \ldots, z_n) \subseteq K$ polje razlaganja. Ako je $\sigma : E \to E$ automorfizam koji fiksira k, tada σ permutira skup korijena $\{z_1, \ldots, z_n\}$ od $f(x)$.

Dokaz. Ako je r korijen od $f(x)$, tada vrijedi

$$0 = f(r) = r^n + a_{n-1}r^{n-1} + \ldots + a_1 r + a_0.$$

Djelujemo li sa σ na ovu jednadžbu dobivamo:

$$\begin{aligned} 0 &= \sigma(r)^n + \sigma(a_{n-1})\sigma(r)^{n-1} + \cdots + \sigma(a_1)\sigma(r) + \sigma(a_0) \\ &= \sigma(r)^n + a_{n-1}\sigma(r)^{n-1} + \cdots + a_1\sigma(r) + a_0 \\ &= f(\sigma(r)), \end{aligned}$$

zato što σ fiksira k, što po definiciji znači $\sigma(a) = a, \forall a \in k$. Dakle, $\sigma(r)$ je korijen od $f(x)$, prema tome, ako definiramo Z kao skup svih korijena, tj. $Z = \{z_1, \ldots, z_n\}$, tada je $\sigma|Z : Z \to Z$, gdje $\sigma|Z$ je restrikcija. Uočimo da je $\sigma|Z$ injekcija (zato što je σ injekcija). Sada iz definicije permutacije slijedi $\sigma|Z$ je permutacija od Z. □

Definicija 4.4. *Neka je k potpolje polja E. **Galoisova grupa** od E nad poljem k, koju označavamo sa $Gal(E/k)$, je skup svih automorfizama od E koji fiksiraju k. Ako je $f(x) \in k[x]$, i ako je $E = k(z_1, \ldots, z_n)$ polje razlaganja, tada **Galoisova grupa** od $f(x)$ nad poljem k je definirana kao $Gal(E/k)$.*

Napomena 4.5. *Lako se provjerava da je $Gal(E/k)$ grupa sa operacijom kompozicije funkcija, tj. $(Gal(E/k), \circ)$ je grupa.*

Lema 4.6. *Neka je $E = k(z_1, \ldots, z_n)$. Ako je $\sigma : E \to E$ automorfizam koji fiksira k, tj. ako $\sigma \in Gal(E/k)$, i ako $\sigma(z_i) = z_i$, $\forall i$, tada je σ identiteta 1_E.*

Dokaz. Dokazujemo lemu indukcijom po $n \geq 1$. Ako je $n = 1$, tada po Propoziciji 2.10 svaki $u \in E$ ima oblik $u = f(z_1)/g(z_1)$, gdje su $f(x), g(x) \in k[x]$ i $g(z_1) \neq 0$. Kako σ fiksira z_1, kao i koeficijente od $f(x)$ i $g(x)$, slijedi da σ fiksira $u \in E$. Za korak indukcije, stavimo da je $K = k(z_1, \ldots, z_{n-1})$, i uočimo da $E = K(z_n)$, gdje $K(z_n)$ je najmanje potpolje koje sadrži k i $z_1, \ldots, z_{n-1}, z_n$. Sada, korak indukcije je potpuno analogan bazi indukcije, samo što polje k zamjenimo sa poljem K. □

Teorem 4.7. *Ako je $f(x) \in k[x]$ stupnja n, tada je pripadajuća Galoisova grupa $Gal(E/k)$ izomorfna podgrupi od S_n.*

Dokaz. Neka je $X = \{z_1, \ldots, z_n\}$. Ako je $\sigma \in Gal(E/k)$, tada nam Propozicija 4.3. kaže da je restrikcija $\sigma|X$ permutacija od X, prema tome $\sigma|X \in S_X$. Definiramo $\varphi : Gal(E/k) \to S_X$ sa $\varphi : \sigma \mapsto \sigma|X$. Tvrdimo da je ovako definirano preslikavanje i homomorfizam. Pokažimo prvo da je φ homomorfizam. Uočimo da su $\varphi(\sigma\tau)$ i $\varphi(\sigma)\varphi(\tau)$ funkcije sa $X \to X$, stoga one će biti jednake ako se podudaraju za svaki $z_i \in X$. Vidimo da je $\varphi(\sigma\tau) : z_i \mapsto (\sigma\tau)(z_i)$, dok je $\varphi(\sigma)\varphi(\tau) : z_i \mapsto \sigma(\tau(z_i))$, tj. imamo $\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$. Time smo pokazali da je φ homomorfizam. Ostaje nam još pokazati da je φ injekcija. Slika od φ je podgrupa od $S_X \cong S_n$. Jezgra od φ je skup svih $\sigma \in Gal(E/k)$ takvih da je σ identiteta na X; tj. σ fiksira svaki korijen z_i. Kako σ također fiksira k, Lema 4.6. nam daje $Ker\varphi = \{1\}$. Dakle, φ je injekcija. Slijedi tvrdnja teorema. □

Sljedeći cilj nam je odrediti red Galoisove grupe, ali prije toga želimo dobiti neke informacije o izmorfizmu i automorfizmu polja.

Lema 4.8. *Neka je k polje karakteristike 0. Tada svaki ireducibilan polinom $p(x) \in k[x]$ nema nultočke koje se ponavljaju.*

Dokaz. Ako je $p(x) \in k[x]$, ili vrijedi da je $p'(x) = 0$ ili $deg(p') < deg(p)$. Kako je $p(x)$ ireducibilan, znamo da $p(x)$ nije konstanta. Dakle, postoji neki član $a_i x^i$, različit od nule, gdje je $i \geq 1$. Kako je k polje karakteristike 0, očito je $p'(x) \neq 0$. Dakle, $ia_i x^{i-1}$ je član različit od nule u $p'(x)$. Budući da je polinom $p(x)$ ireducibilan, njegovi jedini djelitelji

su konstante ili polinomi istog stupnja; kako je $deg(p') < deg(p)$, njihov jedini zajednički djelitelj je 1, što znači da su $p(x)$ i $p'(x)$ relativno prosti polinomi, tj. $nzd(p, p') = 1$. Po napomenini 2.23 imamo da vrijedi tvrdnja Leme. □

Definicija 4.9. *Neka je E/k algebarsko proširenje. Ireducibilan polinom $p(x)$ je **separabilan** ako su sve njegove nultočke međusobno različite. Proizvoljan polinom $f(x)$ je **separabilan** ako svaki od njegovih ireducibilnih faktora ima međusobno različite nultočke.*

*Za element $\alpha \in E$ kažemo da je **separabilan** ako je α transcendentan nad k ili je α algebarski nad k i njegov minimalni polinom $irr(\alpha, k)$ ima međusobno različite nultočke, tj., $irr(\alpha, k)$ je separabilan polinom.*

*Za proširenje polja E/k kažemo da je **separabilno proširenje** ako je svaki element proširenja separabilan; E/k je **neseparabilno** ako nije separabilno.*

Gornja nam lema kaže da je svako proširenje polja karakteristike 0 separabilno proširenje.

Pitanje separabilnosti proširenja povezano je sa Galoisovom grupom zbog ovog teorema:

Teorem 4.10. *1. Neka je E/k polje razlaganja separabilnog polinoma $f(x) \in k[x]$, neka je $\varphi : k \to k'$ izomorfizam polja, i neka je E'/k' polje razlaganja od $f^*(x) \in k'[x]$ [gdje je $f^*(x)$ dobiven iz $f(x)$ djelovanjem funkcije φ na koeficijente od $f(x)$]. Tada postoji točno $[E : k]$ izomorfizama $\theta : E \to E'$ koji proširuju φ.*

2. Ako je E/k polje razlaganja separabilnog polinoma $f(x) \in k[x]$, tada

$$|Gal(E/k)| = [E : k].$$

Dokaz. 1. Dokaz provodimo indukcijom po $[E : k]$. Ako je $[E : k] = 1$, tada $E = k$ i postoji točno jedno proširenje θ od φ, točnije, sam φ. Ako je $[E : k] > 1$, neka je $f(x) = p(x)g(x)$, gdje je $p(x)$ ireducibilan faktor najvećeg stupnja, recimo, d. Možemo pretpostaviti da je $d > 1$, inače $f(x)$ se razlaže nad poljem k i tada je $[E : k] = 1$. Izaberemo korijen α od $p(x)$ (uočimo da je $\alpha \in E$ zato što je E polje razlaganja od $f(x) = p(x)g(x)$). Ako je $\tilde{\varphi} : k(\alpha) \to E'$ bilo koje proširenje od φ, tada $\varphi(\alpha)$ je korijen α' od $p^*(x)$, po Propoziciji 4.3.; kako je $f^*(x)$ separabilan, $p^*(x)$ ima točno d korijena $\alpha' \in E'$; po Lemi 4.6. i Teoremu 3.10.(2), postoji točno d izomorfizama $\hat{\varphi} : k(\alpha) \to k'(\alpha')$ koji proširuju φ, jedan za svaki α'. Sada je i E polje razlaganja od $f(x)$ nad $k(\alpha)$; jer ako dodamo sve korijene od $f(x)$ u $k(\alpha)$ i dalje dobivamo E, i E' je polje razlaganja od $f^*(x)$ nad $k'(\alpha')$. Kako je $[E : k(\alpha)] = [E : k]/d$, indukcija pokazuje da svaki od d izomorfizama $\hat{\varphi}$ ima točno $[E : k]/d$ proširenja $\theta : E \to E'$. Prema tome, konstruirali smo $[E : k]$ izomorfizama koji proširuju φ. Pokažimo još da su to sigurno jedina proširenja, naime, svaki τ koji proširuje φ ima $\tau|k(\alpha) = \hat{\varphi}$ za neki $\hat{\varphi} : k(\alpha) \to k'(\alpha')$.

2. U dijelu 1., stavimo $k = k'$, $E = E'$ i $\varphi = 1_K$.

□

Propozicija 4.11. *Neka je m pozitivan cijeli broj; ako je k polje, i ako je E polje razlaganja od* $x^m - 1$ *nad k, tada* $Gal(E/k)$ *je Abelova grupa.*

Dokaz. (Skica.) Lagano se pokazuje da je $Gal(E/k)$ izomorfna podgrupi multiplikativne grupe invertibilnih elemenata u $\mathbb{I}_m$, tj. svih $[i]$ takvih da je $(i, m) = 1$. □

Poglavlje 5

Formule i rješivost u radikalima

U ovom poglavlju ćemo interpretirati postojanje formula za nultočke polinoma u terminima potpolja polja razlaganja.

Definicija 5.1. ***Čisto proširenje tipa*** *m je proširenje $k(u)/k$, gdje je $u^m \in k$ za neki $m \geq 1$. Proširenje K/k je* ***radikalno proširenje*** *ako postoji niz polja*

$$k = K_0 \subseteq K_1 \subseteq \dots K_t = K$$

u kojem je svako K_{i+1}/K_i čisto proširenje.

Definicija 5.2. *Neka je $f(x) \in k[x]$ polinom s koeficijentima iz polja k i neka je E polje razlaganja polinoma $f(x)$. Kažemo da je polinom $f(x)$* ***rješiv u radikalima*** *nad poljem k, ako postoji radikalno proširenje*

$$k = K_0 \subseteq K_1 \subseteq \dots \subseteq K_t$$

takvo da je $E \subseteq K_t$.

Dakle, polinom $f(x)$ rješiv je u radikalima, ako postoji radiklano proširenje polja k nad kojim se polinom $f(x)$ razlaže.
Ilustrirati ćemo ovu definiciju s obzirom na klasične formule polinoma stupnja dva, tri i četiri.

Algebarske jednadžbe drugog stupnja

Ako je $f(x) = x^2 + bx + c$, tada kvadratna formula daje rješenja

$$\frac{1}{2}(-b \pm \sqrt{b^2 - 4ac}).$$

Neka je $k = \mathbb{Q}(b, c)$. Definiramo $K_1 = k(u)$, gdje je $u = \sqrt{b^2 - 4c}$. Tada je K_1 radikalno proširenje od k, jer je $u^2 \in k$. Također, iz kvadratne formule slijedi da je K_1 polje razlaganja od $f(x)$. Dakle, $f(x)$ je rješiv u radikalima.

Algebarske jednadžbe trećeg stupnja

Neka je $f(X) = X^3 + bX^2 + cX + d$, i neka je $k = \mathbb{Q}(b, c, d)$.
Uvodimo novu varijablu $X = x - \frac{1}{3}b$.
Jednadžba postaje

$$f(x - \frac{1}{3}b) = x^3 + (c - \frac{1}{3}b)x + \frac{2b^3}{27} - \frac{bc}{3} + d,$$

odnosno,

$$\tilde{f}(x) = x^3 + qx + r,$$

gdje je $q = c - \frac{b^2}{3}$ i $r = \frac{2b^3}{27} - \frac{bc}{3} + d$. Vrijedi da je polje razlaganja E od $f(x)$ jednako polju razlaganja od $\tilde{f}(x)$, jer ako je u korijen od $\tilde{f}(x)$, onda je $u - \frac{1}{3}b$ korijen od $f(x)$. Kubna formula izvodi se na sljedeći način.
Ako je u nultočka od $\tilde{f}(x) = x^3 + qx + r$, pretpostavimo da je

$$u = g + h,$$

gdje su g i h nove nepoznanice. Zamjenom u jednadžbi dobivamo

$$0 = \tilde{f}(u) = \tilde{f}(g + h) = g^3 + h^3 + (3gh + q)u + r.$$

Možemo pretpostaviti da je $3gh + q = 0$; tada je,

$$g^3 + h^3 = -r \quad \text{i} \quad gh = -\frac{1}{3}q.$$

Ako kubiramo zadnju jednakost, dobivamo da g i h zadovoljavaju sustav jednadžbi

$$g^3 + h^3 = -r$$

$$g^3 h^3 = -\frac{1}{27}q^3,$$

rješavjući sustav dobivamo:

$$g^6 + rg^3 - \frac{1}{27}q^3 = 0.$$

Sada nam kvadratna formula daje

$$g^3 = \frac{1}{2}\left(-r + \sqrt{r^2 + \frac{4}{27}q^3}\right) = \frac{1}{2}(-r + \sqrt{R})$$

[uočimo još da je i h^3 rješenje jednadžbe, tj. $h^3 = \frac{1}{2}(-r - \sqrt{R})$]. Postoje tri kubna korijena od g^3: g, ωg i $\omega^2 g$, pri čemu je ω primitivni treći korijen jedinice, tj. $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Zbog jednakosti $gh = -\frac{1}{3}q$, svaki od tih korijena ima svoj "par": $h = -q/(3g)$, $-q/(3\omega g) = \omega^2 h$, i $-q/(3\omega^2 g) = \omega h$.
Pokažimo sada da je $\tilde{f}(x)$ rješiv u radiklima. Definiramo $K_1 = k(\sqrt{R})$, gdje je $R = r^2 + \frac{4}{27}q^3$ i definiramo $K_2 = K_1(\alpha)$, gdje je $\alpha^3 = \frac{1}{2}(-r + \sqrt{R})$. Kubna formula pokazuje da K_2 sadrži korijene $\alpha + \beta$ od $\tilde{f}(x)$, gdje je $\beta = -\frac{q}{3\alpha}$. Konačno, definirmo $K_3 = K_2(\omega)$, gdje je $\omega^3 = 1$. Ostali korijeni od $\tilde{f}(x)$ su $\omega\alpha + \omega^2\beta$ i $\omega^2\alpha + \omega\beta$. Oba dva ta korijena se nalaze u K_3, pa iz toga slijedi $E \subseteq K_3$.

Primjer 5.3. *Neka je $f(x) = x^3 - 15x - 126$, tada je $q = -15$, $r = -126$, $R = 15376$ i $\sqrt{R} = 124$. Stoga, $g^3 = 125$, tako da je $g = 5$. Tada imamo da je $h = -\frac{q}{3g} = 1$. Dakle, korijeni od $f(x)$ su*

$$6, \;\; 5\omega + \omega^2 = -3 + 2i\sqrt{3}, \;\; 5\omega^2 + \omega = -3 - 2i\sqrt{3}.$$

Primjer 5.4. *Kubna formula često nije korisna iz razloga što daje korijene u neprepoznatljivom obliku. Na primjer, neka je*

$$f(x) = (x-1)(x-2)(x+3) = x^3 - 7x + 6.$$

Kubna formula daje

$$g + h = \sqrt[3]{\frac{1}{2}\left(-6 + \sqrt{\frac{-400}{27}}\right)} + \sqrt[3]{\frac{1}{2}\left(-6 - \sqrt{\frac{-400}{27}}\right)}.$$

Vidimo da nije potpuno očito da je $g + h$ realan broj, a kamoli cijeli broj. Postoji druga verzija kubne formule, koja daje korijene u terminima trigonometrijskih funkcija umjesto radikala.

Algebarske jednadžbe četvrtog stupnja

Neka je $f(X) = X^4 + bX^3 + cX^2 + dX + e$, i neka je $k = \mathbb{Q}(b, c, d, e)$. Uvedemo novu varijablu $X = x - \frac{1}{4}b$, jednadžba postaje

$$\tilde{f}(x) = x^4 + qx^2 + rx + s \in k[x].$$

Štoviše, vrijedi da je polje razlaganja E od $f(x)$ jednako polju razlaganja od $\tilde{f}(x)$, jer ako je u korijen od $\tilde{f}(x)$, onda je $u - \frac{1}{4}b$ korijen od $f(x)$. Faktoriziramo $\tilde{f}(x)$ u $\mathbb{C}[x]$:

$$\tilde{f}(x) = x^4 + qx^2 + rx + s = (x^2 + jx + l)(x^2 - jx + m),$$

i određujemo j, l i m. Izjednačavanjem koeficijenata dobijemo jednadžbe

$$l + m - j^2 = q;$$

$$j(m - l) = r;$$

$$lm = s.$$

Prve dvije jednadžbe daju

$$2m = j^2 + q + r/j;$$

$$2l = j^2 + q - r/j.$$

Kada uvrstimo vrijednosti za m i l u treću jednadžbu dobijemo:

$$(j^2)^3 + 2q(j^2)^2 + (q^2 - 4s)j^2 - r^2.$$

Sada nam kubna formula daje j^2, iz čega možemo odrediti m i l, pa stoga i ostale korijene jednadžbe četvrtog stupnja.
Definiramo čista proširenja

$$k = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3,$$

kao što smo definirali u slučaju kubne jednadžbe, tako da je $j^2 \in K_3$. Definiramo $K_4 = K_3(j)$ (tako da su $l, m \in K_4$). Konačno, definiramo $K_5 = K_4(\sqrt{j^2 - 4l})$ i $K_6 = K_5(\sqrt{j^2 - 4m})$. Formula jednadžbe četvrtog stupnja daje $E \subseteq K_6$.

Time smo pokazali da su jednadžbe stupnja dva, tri i četiri rješive u radikalima. Obratno, ako je $f(x)$ polinom rješiv u radikalima, tada postoji formula koja izražava korijene u terminima koeficijenata polinoma.

Poglavlje 6

Abel-Ruffinijev teorem

Ovo poglavlje, Abel-Ruffinijev teorem, usko se specijalizira na samu bit ovog rada. U njemu se dokazuje Galoisov teorem o korespondenciji rješivosti polinoma u radikalima i rješivosti pripadne Galoisove grupe, te Abel-Ruffinijev teorem.

Prije nego iskažemo osnovne teoreme ovog poglavlja navest ćemo neke definicije i činjenice koje koristimo u dokazima tih teorema.

Pretpostavimo da je $k(u)/k$ čisto proširenje tipa 6; tj., $u^6 \in k$. Tada $k(u^3)/k$ je čisto proširenje tipa 2, jer je $(u^3)^2 = u^6 \in k$, i $k(u)/k(u^3)$ je očito čisto proširenje tipa 3. Prema tome, $k(u)/k$ možemo zamijeniti nizom čistih proširenja $k \subseteq k(u^3) \subseteq k(u)$ tipa 2 i tipa 3. Općenito, ako je $k \subseteq k(u)$ tipa m, i imamo umnožak $m = p_1 \cdot \ldots \cdot p_q$, gdje su $p_1, \ldots, p_q$, ne nužno različiti, prosti brojevi, tada možemo zamijeniti $k \subseteq k(u)$ sa

$$k \subseteq k(u^{m/p_1}) \subseteq k(u^{m/p_1 p_2}) \subseteq \ldots \subseteq k(u).$$

Sada iskazujemo osnovni rezultat koji nam omogućava da rješivost u radikalima prikažemo pomoću teorije grupa.

Teorem 6.1. *Neka je E proširenje polja k i neka je B međupolje, $k \subseteq B \subseteq E$. Neka su $f(x), g(x) \in k[x]$; neka je B polje razlaganja od $f(x)$ nad poljem k, a E polje razlaganja od $g(x)$ nad poljem k. Tada je $Gal(E/B)$ normalna podgrupa grupe $Gal(E/k)$, i vrijedi*

$$Gal(E/k)/Gal(E/B) \cong Gal(B/k).$$

Dokaz. Neka je $B = k(z_1, \ldots, z_n)$, gdje su $z_1, \ldots, z_n$ korijeni od $f(x)$ u E. Ako je $\sigma \in Gal(E/k)$, tada po Propoziciji 4.3. σ permutira skup korijena $\{z_1, \ldots, z_n\}$ od $f(x)$, i vrijedi $\sigma(B) = B$. Definiramo $\rho : Gal(E/k) \to Gal(B/k)$ sa $\sigma \mapsto \sigma|B$. Lako se pokaže, kao i u dokazu Teorema 4.7, da je ρ homomorfizam. Jezgra od ρ je skup svih $\sigma \in Gal(E/k)$ takvih da je σ identiteta na B; tj., σ fiksira svaki korijen z_i. Kako σ fiksira i k, po definiciji

Galoisove grupe imamo $\operatorname{Ker}\rho = Gal(E/B)$. Koristeći tvrdnju Korolara 1.17. pokazali smo da je $Gal(E/B)$ normalna podgrupa grupe $Gal(E/k)$. Pokažimo još da je ρ surjektivan: Ako je $\tau \in Gal(B/k)$, tada nam Lema 3.16. kaže da postoji $\sigma \in Gal(E/k)$ koja proširuje τ; tj., $\rho(\sigma) = \sigma|B = \tau$. Sada tvrdnja teorema slijedi iz prvog teorema o izomorfizmu (Teorem 1.18.). □

Lema 6.2.

1. *Ako je $B = k(\alpha_1, \ldots, \alpha_n)$ konačno proširenje polja k, tada postoji konačno proširenje E/B koje je ujedno i polje razlaganja nekog polinoma $f(x) \in k[x]$ (takvo proširenje najmanjeg stupnja zovemo **normalno zatvorenje** od B/k). Štoviše, ako je svaki α_i separabilan nad k, tada se $f(x)$ može odabrati tako da bude separabilan polinom.*

2. *Ako je B radikalno proširenje od k, tada proširenje E/B iz dijela* (1) *je radikalno proširenje od k.*

Dokaz. 1. Iz Teorema 3.10.(1) slijedi da, za svaki i, postoji ireducibilan polinom $p_i(x) = irr(\alpha_i, k)$ u $k[x]$ takav da je $p_i(\alpha_i) = 0$, i postoji polje razlaganja E od $f(x) = p_1(x)\cdots p_n(x)$ koje sadrži B. Ako je svaki α_i separabilan nad k, tada svaki $p_i(x)$ je separabilan polinom, stoga je i $f(x)$ separabilan polinom.

2. Za svaki par korijena α i α' bilo kojeg $p_i(x)$, postoji izomorfizam $\gamma : k(\alpha) \to k(\alpha')$ koji fiksira k i takav da $\alpha \mapsto \alpha'$, jer su oba polja $k(\alpha)$ i $k(\alpha')$ izomorfna s $k[x]/(p_i(x))$. Po Lemi 3.16., svaki takav γ proširuje se do automorfizma $\sigma \in G = Gal(E/k)$. Slijedi da $E = k(\sigma(u_1), \ldots, \sigma(u_t) : \sigma \in G)$. Ako je B/k radikalno proširenje, tada je

$$k \subseteq k(u_1) \subseteq k(u_1, u_2) \subseteq \cdots \subseteq k(u_1, \ldots, u_t) = B,$$

gdje svaki $k(u_1, \ldots, u_{i+1})$ je čisto proširenje od $k(u_1, \ldots, u_i)$; naravno vrijedi, $\sigma(B) = k(\sigma(u_1), \ldots, \sigma(u_t))$ je radikalno proširenje od k za svaki $\sigma \in G$. Sada ćemo pokazati da je E radikalno proširenje od k. Definiramo

$$B_1 = k(\sigma(u_1) : \sigma \in G).$$

Sada ako je $G = \{1, \sigma, \tau, \ldots\}$, tada niz

$$k \subseteq k(u_1) \subseteq k(u_1, \sigma(u_1)) \subseteq k(u_1, \sigma(u_1), \tau(u_1)) \subseteq \ldots \subseteq B_1$$

prikazuje B_1 kao radikalno proširenje od k. Na primjer, ako u_1^m leži u k, tada $\tau(u_1)^m = \tau(u_1^m)$ leži u $\tau(k) = k$, i stoga $\tau(u_1)^m$ leži u $k \subseteq k(u_1, \sigma(u_1))$. Pretpostavimo li, po indukciji, da postoji radikalno proširenje B_i/k koje sadrži $\{\sigma(u_j) : \sigma \in G\}$ za svaki $j \leq i$, definiramo

$$B_{i+1} = B_i(\sigma(u_{i+1}) : \sigma \in G).$$

Lako se vidi da je B_{i+1}/B_i radikalno proširenje: Ako je $u_{i+1}^m \in k(u_1, \ldots, u_i)$, tada $\tau(u_{i+1})^m \in k(\tau(u_1), \ldots, \tau(u_i)) \subseteq B_i$; tada slijedi da B_{i+1} je radikalno proširenje od k. Konačno, kako je $E = B_t$, pokazali smo da je E radikalno proširenje od k.

□

Sljedeća lema nam prevodi naš problem u termine teorije grupa.

Lema 6.3. *Neka je*

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_t$$

radiklano proširenje polja K_0. Pretpostavimo, za svaki $i \geq 1$, K_i je čisto proširenje od K_{i-1} tipa p_i, gdje je $p_i \neq char(K_0)$ prost broj, i da K_0 sadrži sve $p_i - te$ korijene jedinice. Ako K_t je polje razlaganja nad poljem K_0, tada postoji niz podgrupa

$$Gal(K_t/K_0) = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_t = \{1\},$$

takav da svaki G_{i+1} je normalna podgrupa od G_i i G_i/G_{i+1} je ciklička prostog reda p_{i+1}.

Dokaz. Za svaki i, definiramo $G_i = Gal(K_t/K_i)$. Očito je

$$Gak(K_t/K_0) = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_t = \{1\}$$

niz podgrupa. Kako je $K_1 = K_0(u)$, gdje je $u^{p_1} \in K_0$, iz pretpostavki da je $char(K_0) \neq p_1$ i da K_0 sadrži sve $p_1 - ve$ korijene jedinice slijedi da K_0 sadrži primitivni $p_i - ti$ korijen jedinice ω; stoga, K_1 je polje razlaganja separabilnog polinoma $x^{p_1} - u^{p_1}$, čiji su korijeni $u, \omega u, \ldots, \omega^{p_1-1}u$. Sada koristeći tvrdnju Teorema 6.1. vidimo da je $G_1 = Gal(K_t/K_1)$ normalna podgrupa od $G_0 = Gal(K_t/K_0)$ i da vrijedi $G_0/G_1 \cong Gal(K_1/K_0)$. Po Teoremu 4.10.(2), $G_0/G_1 \cong \mathbb{I}_{p_1}$. Ovaj argument se može ponoviti za svaki i. □

Motivirani prethodnom lemom, dajemo sljedeću definiciju.

Definicija 6.4. ***Normalni niz*** *grupe G je konačni niz podgrupa*

$$G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_t = \{1\}$$

*takvih da je G_{i+1} normalna podgrupa od G_i; **faktor-grupe** ovog niza su kvocijentne grupe*

$$G_0/G_1, G_1/G_2, \ldots, G_{n-1}/G_n.$$

Konačna grupa G je rješiva ako sadrži normalni niz podgrupa čije su faktor-grupe prostog reda.

Sada Lemu 6.3. možemo iskazati na sljedeći način: $Gal(K_t/K_0)$ je rješiva grupa ako je K_t radikalno proširenje od K_0 i K_0 sadrži odgovarajuće korijene jedinice.

Primjer 6.5. *1. Pokažimo da je S_4 rješiva grupa. Uočimo niz podgrupa*

$$S_4 \geq A_4 \geq \mathbf{V} \geq W \geq \{1\},$$

gdje je $\mathbf{V}$ grupa iz Primjera 1.8.(1) i W bilo koja podgrupa od $\mathbf{V}$ reda 2. Kako je $\mathbf{V}$ Abelova, tada je W normalna podgrupa od $\mathbf{V}$ reda 2. Sada $|S_4/A_4| = |S_4|/|A_4| = 24/12 = 2$, $|A_4/\mathbf{V}| = |A_4|/|\mathbf{V}| = 12/4 = 3$,$|\mathbf{V}/W| = |\mathbf{V}|/|W| = 4/2 = 2$ i $|W/\{1\}| = |W| = 2$. Budući da je svaka faktor-grupa prostog reda, S_4 je rješiva.

2. *Neabelova prosta grupa G, na primjer, $G = A_5$, nije rješiva. Budući da je jedina normalna podgrupa $\{1\}$, i vrijedi $G/\{1\} \cong G$ nije ciklička prostog reda.*

Lema 6.6. *Neka je k polje i $f(x) \in k[x]$ rješiv u radikalima, tada postoji radikalno proširenje $k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$ takvo da K_t sadrži polje razlaganja E od $f(x)$. Ako svaki K_i/K_{i-1} je čisto proširenje tipa p_i, gdje je p_i prost broj, $p_i \neq char(k)$ i ako k sadrži sve p_i − te korijene jedinice, tada Galoisova grupa $Gal(E/k)$ je kvocijent rješive grupe.*

Dokaz. Postoji niz čistih proširenja prostog tipa,

$$k = K_0 \subseteq K_1 \subseteq K_2 \cdots \subseteq K_t$$

takvih da je $E \subseteq K_t$; po Lemi 6.2., možemo pretpostaviti da je K_t polje razlaganja nekog polinoma iz $k[x]$. Koristeći pretpostavke na k, Lema 6.3. nam kaže da je $Gal(K_t/k)$ rješiva grupa. Kako su i E i K_t polja razlaganja nad k iz Teorema 6.1. nam slijedi $Gal(K_t/k)/Gal(K_t/E) \cong Gal(E/k)$. □

Sada ćemo navesti neka svojstva rješivih grupa.

Propozicija 6.7. *Svaka kvocijentna grupa G/N rješive grupe G je i sama rješiva.*

Dokaz. Neka je $G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_t = \{1\}$ niz podgrupa kao u definiciji rješive grupe. Kako je $N \triangleleft G$, vrijedi da je NG_i podgrupa od G za svaki i i postoji niz podgurpa

$$G = G_0N \geq G_1N \geq \cdots \geq G_tN = N \geq \{1\}.$$

Pokažimo da je takav niz normalan. Imamo zapis,

$$(g_in)G_{i+1}N(g_in)^{-1} \leq g_iG_{i+1}Ng_i^{-1} = g_iG_{i+1}g_i^{-1}N \leq G_{i+1}N;$$

prva nejednakost vrijedi zbog $n(G_{i+1}N)n^{-1} \leq NG_{i+1}N \leq (G_{i+1}N)(G_{i+1}N) = G_{i+1}N$ (jer je $G_{i+1}N$ podgrupa); jednakost vrijedi zbog $Ng_i^{-1} = g_i^{-1}N$ (zbog $N \triangleleft G$; lijeva klasa se podudara s desnom klasom); zadnja nejednakost vrijedi zbog $G_{i+1} \triangleleft G_i$. Iz drugog teorema o izomorfizmu nam slijedi

$$\frac{G_i}{G_i \cap (G_{i+1}N)} \cong \frac{G_i(G_{i+1}N)}{G_{i+1}N} = \frac{G_iN}{G_{i+1}N},$$

gdje druga jednakost vrijedi zbog $G_iG_{i+1} = G_i$. Kako je $G_{i+1} \triangleleft G_i \cap G_{i+1}N$, treći teorem o izomorfizmu nam daje surjekciju $G_i/G_{i+1} \to G_i/[G_i \cap G_{i+1}N]$, pa je i kompozicija surjekcija $G_i/G_{i+1} \to G_iN/G_{i+1}N$. Kako je G_i/G_{i+1} ciklička grupa prostog reda, njena slika je ili ciklička prostog reda ili trivijalna. Stoga, G/N je rješiva grupa. □

Propozicija 6.8. *Svaka podgrupa H rješive grupe G je i sama rješiva.*

Dokaz. Kako je G rješiva, postoji niz podgrupa

$$G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_t = \{1\}$$

gdje je G_i normalna podgrupa od G_{i-1} i G_{i-1}/G_i ciklička, za svaki i. Promotrimo niz podgrupa

$$H = H \cap G_0 \geq H \cap G_1 \geq H \cap G_2 \geq \cdots \geq H \cap G_t = \{1\}.$$

Pokažimo da je to normalan niz. Ako je $h_{i+1} \in H \cap G_{i+1}$ i $g_i \in H \cap G_i$, tada $g_ih_{i+1}g_i^{-1} \in H$, za $g_i, h_{i+1} \in H$; također, $g_ih_{i+1}g_i^{-1} \in G_{i+1}$ budući da je G_{i+1} normalna podgrupa od G_i. Dakle, $g_ih_{i+1}g_i^{-1} \in H \cap G_{i+1}$, iz čega slijedi $H \cap G_{i+1} \triangleleft H \cap G_i$. Sada iz drugog teorema o izomorfizmu nam slijedi

$$(H \cap G_i)/(H \cap G_{i+1}) = (H \cap G_i)/[(H \cap G_i) \cap G_{i+1}] \cong G_{i+1}(H \cap G_i)/G_{i+1}.$$

Uočimo da je zadnja (kvocijentna) grupa podgrupa od G_i/G_{i+1}. Po pretpostavci G je rješiva grupa, i vrijedi da je kvocijentna grupa G_i/G_{i+1} ciklička. Kako jedine podgrupe cikličke grupe C, čiji red grupe je prost broj, su C i $\{1\}$, slijedi da su netrivijalne faktor-grupe $(H \cap G_i)/(H \cap G_{i+1})$ cikličke prostog reda. Dakle, H je rješiva grupa. □

Primjer 6.9. *U Primjeru 6.5. pokazali smo da je S_4 rješiva grupa. Međutim, za $n \geq 5$, simetrična grupa S_n nije rješiva grupa. Pretpostavimo li suprotno, tj., da je S_n rješiva, tada bi svaka njena podgrupa bila rješiva. Ali $A_5 \leq S_5 \leq S_n$, a A_5 nije rješiva.*

Propozicija 6.10. *Ako je $H \triangleleft G$ i ako su H i G/H rješive grupe, tada je G rješiva grupa.*

Dokaz. Kako je G/H rješiva grupa, postoji normalni niz

$$G/H \geq K_1^* \geq K_2^* \geq \cdots K_m^* = \{1\}$$

s faktor-grupama prostog reda. Po teoremu korenspodencije za grupe, postoje podgrupe K_i od G,

$$G \geq K_1 \geq K_2 \geq \cdots \geq K_m = H,$$

takve da $K_i/H = K_i^*$ i $K_{i+1} \triangleleft K_i$, za svaki i. Po trećem teoremu o izomorfizmu slijedi,

$$K_i^*/K_{i+1}^* \cong K_i/K_{i+1}$$

za svaki i i K_i/K_{i+1} je ciklička grupa prostog reda za svaki i. Budući da je H rješiva, postoji normalni niz

$$H \geq H_1 \geq H_2 \geq \cdots \geq H_q = \{1\}$$

s faktor-grupama prostog reda. Spajanjem ova dva niza,

$$G \geq K_1 \geq K_2 \geq \cdots \geq K_m \geq H_1 \geq H_2 \geq \cdots \geq H_q = \{1\},$$

dobili smo normalan niz od G s faktor-grupama prostog reda. □

Sljedeći teorem nam daje glavni kriterij za rješivost polinoma u radikalima:

Teorem 6.11. (Galois) *Neka je $f(x) \in k[x]$, gdje je k polje, i neka je E polje razlaganja od $f(x)$ nad poljem k. Ako je $f(x)$ rješiv u radikalima, tada pripadajuća Galoisova grupa $Gal(E/k)$ je rješiva grupa.*

Napomena 6.12. *Obrat ovog teorem ne vrijedi ako je k karakteristike $p > 0$, ali vrijedi kada je k karakteristike 0.*

Dokaz. U dokazu Leme 6.6, pretpostavili smo da osnovno polje sadrži određene $p_i - te$ korijene jedinice (prosti brojevi p_i su bili tipovi čistog proširenja). Definiramo m kao umnožak svih tih p_i, definiramo E^* kao polje razlaganja polinoma $x^m - 1$ nad poljem E, definiramo $k^* = k(\Omega)$, gdje je Ω skup svih $m - tih$ korijena jedinice u E^*. Sada je E^* polje razlaganja od $f(x)$ nad k^*, i po Propoziciji 6.7. slijedi da je $Gal(E^*/k^*)$ rješiva grupa. Uzmemo li u obzir niz $k \subseteq k^* \subseteq E^*$; po Teoremu 6.1. vrijedi $Gal(E^*/k^*) \triangleleft Gal(E^*/k)$ i

$$Gal(E^*/k)/Gal(E^*/k^*) \cong Gal(k^*/k).$$

Sada po Propoziciji 4.11. $Gal(E^*/k^*)$ je rješiva grupa, a $Gal(k^*/k)$ Abelova, stoga i rješiva. Dakle, $Gal(E^*/k)$ je rješiva po Propoziciji 6.10. Napokon, koristeći ponovno Teorem 6.1., niz $k \subseteq E \subseteq E^*$ zadovoljava pretpostavku da su E i E^* polja razlaganja polinoma u $k[x]$ [E^* je polje razlaganja od $(x^m - 1)f(x)$]. Sada slijedi da je $Gal(E^*/k)/Gal(E^*/E) \cong Gal(E/k)$, pa je $Gal(E/k)$ rješiva grupa kao kvocijent rješivih grupa. □

Neka je k polje i $E = k(y_1, \ldots, y_n)$ polje racionalnih funkcija u n varijabli $y_1, \ldots, y_n$ nad poljem k; tj., $E = Frac(k[y_1, \ldots, y_n])$, polje razlomka prstena polinoma u n varijabli. Opći polinom stupnja n nad poljem k definiramo kao

$$f(x) = (x - y_1)(x - y_2)\cdots(x - y_n) \in Frac(k[y_1, \ldots, y_n])[x].$$

Koeficijente od $f(x) = (x - y_1)(x - y_2)\cdots(x - y_n)$, koje ćemo označavati sa α_i, moguće je zadati eksplicitno:

$$\begin{cases} a_{n-1} &= -\sum_i y_i \\ a_{n-2} &= \sum_{i<j} y_i y_j \\ a_{n-3} &= -\sum_{i<j<k} y_i y_j y_k \\ &\vdots \\ a_0 &= (-1)^n z_1 z_2 \cdots z_n. \end{cases}$$

Uočimo još da je E polje razlaganja od polinoma $f(x)$ nad poljem $K = k(a_0, \ldots, a_{n-1})$, koje proizlazi iz K tako da polju K dodamo sve korijene polinoma $f(x)$, točnije sve $y - ne$.

Galoisov teorem nam je dovoljno jak da dokaže da ne postoji generalizacija kvadratne formule za opći polinom petog stupnja.

Teorem 6.13. (Abel-Rufiini) *Ako je $n \geq 5$, opći polinom stupnja n*

$$f(x) = (x - y_1)(x - y_2)\cdots(x - y_n)$$

nad poljem k nije rješiv u radikalima.

Dokaz. Vidjeli smo da ako je $E = k(y_1, \ldots, y_n)$ polje svih racionalnih funkcija u n varijabli sa koeficijentima iz polja k, i ako je $F = k(a_0, \ldots, a_{n-1})$, gdje su a_i koeficijenti od $f(x)$, tada je E polje razlaganja od $f(x)$ nad poljem F. Želimo pokazati da je $Gal(E/k) \cong S_n$. Općenito vrijedi da ako su A i R domene i $\varphi : A \to R$ izomorfizam, tada $a/b \mapsto \varphi(a)/\varphi(b)$ je izomorfizam $Frac(A) \to Frac(R)$. Posebno, ako je $\sigma \in S_n$, tada postoji automorfizam $\hat{\sigma}$ od $k[y_1, \ldots, y_n]$ definiran sa $\hat{\sigma} : f(y_1, \ldots, y_n) \mapsto f(y_{\sigma 1}, \ldots, y_{\sigma n})$; tj., $\hat{\sigma}$ samo permutira varijable, i $\hat{\sigma}$ se proširuje na automorfizam σ^* od $E = Frac(k[y_1, \ldots, y_n])$. Koristeći Lemu 4.6., vidimo da je $\sigma \mapsto \sigma^*$ injektivno preslikavanje $S_n \to Gal(E/F)$, i tada vrijedi $|S_n| \leq |Gal(E/F)|$. S druge strane, iz Teorema 4.7. vidimo da $Gal(E/F)$ može biti uložen u S_n, što daje suprotnu nejednakost $|Gal(E/F)| \leq |S_n|$. Stoga, $Gal(E/F) \cong S_n$. Ali kako smo pokazali u Primjeru 6.9., S_n nije rješiva grupa za $n \geq 5$. Konačno, iz teorema 6.11. slijedi da $f(x)$ nije rješiv u radikalima. □

Mi znamo da neke polinom stupnja pet u $\mathbb{Q}[x]$ je moguće riješiti pomoću radikala; na primjer, $x^5 - 1$ je rješiv u radikalima, jer je njegova Galoisova grupa Abelova, po Propoziciji 4.11. S druge strane, možemo dati primjer polinoma stupnja pet u $\mathbb{Q}[x]$ koji nisu rješivi u radikalima. Na primjer, $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ nije rješiv u radikalima, jer moguće je pokazati da je njegova Galoisova grupa izomorfna sa S_5.

Bibliografija

[1] S. Lang, *Algebra*, 3d ed., Addison-Wesley, Reading, 1993.

[2] J.J. Rotman,*Advanced Modern Algebra*, Prentice Hall; 1st edition (2002); 2nd printing (2003).

[3] B. Širola, *Algebarske strukture*, Electronic copy found at: `https://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf`

Sažetak

Tema ovog diplomskog rada je Abel-Ruffinijev teorem koji nam govori da ne postoji opće algebarsko rješenje, tj. rješenje u radikalima za jednadžbe petog ili višeg stupnja.
U prvom poglavlju uvodimo neke osnovne definicije potrebne za izgradnju Galoisove teorije, kojom se opširnije bavimo u četvrtom poglavlju. U drugom poglavlju poseban nagalasak stavit ćemo na prsten polinoma. Vidjeti ćemo da, kada je k polje, svi poznati teoremi koji vrijede u $\mathbb{Z}$, imaju anologon u $k[x]$, štoviše, vidjeti ćemo da se svi poznati dokazi mogu prenijeti ovdje. U trećem poglavlju definiramo kvocijentni prsten i uvodimo pojam proširenja polja. U petom poglavlju ukratko ćemo pokazati postupak rješavanja jednadžbi trećeg i četvrtog stupnja. U zadnjem poglavlju dokazuje se Galoisov teorem o korespondenciji rješivosti polinoma u radikalima i rješivosti pripadne Galoisove grupe, te Abel-Ruffinijev teorem.

Summary

The theme of this diploma thesis is Abel-Ruffini theorem which states that there is no general algebraic solution, that is, solution in radicals, to polynomial equations of degree five or higher.
In Chapter 1 we introduce some basic definitions that will be needed to build the foundations of the Galois theory, which we detail in Chapter 4. In Chapter 2 we give a special attention to the ring of polynomials. We are going to see that, when k is a field, virtually all the familiar theorems valid in $\mathbb{Z}$ have polynomial analogs in $k[x]$; moreover, we shall see that the familiar proofs can be generalized. In the third chapter we define quotient ring and introduce the notion of field extension. In Chapter 5 we will briefly show the process of solving equations of the third and fourth degree. In the last chapter we will prove Galois theorem on correspondence between solvability of polynomial in radicals and the corresponding Galois group, and Abel-Ruffini theorem.

Životopis

Moje ime je Josipa Pavković. Rođena sam u Zagrebu 23.03.1991.. Završila sam Osnovnu školu Ivan Cankar, te V. Gimnaziju, također u Zagrebu. Nakon završetka srednje škole, 2009. godine, upisala sam Prirodoslovno matematički fakultet (PMF) u Zagrebu, smjer Matematika. Titulu sveučilišne prvostupnice (baccalaureus) matematike stekla sam 2013. godine, te iste godine upisala diplomski studij Primijenjena matematika na istom fakultetu.