Galoisova teorija

Topić, Dragutina

Master's thesis / Diplomski rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:872806

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Dragutina Topić

GALOISOVA TEORIJA

Diplomski rad

Voditelj rada:
prof. dr. sc. Ozren Perše

Zagreb, 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. _____

Mojim roditeljima

Sadržaj

Uvod

Evariste Galois (1811. – 1832.) je francuski matematičar poznat po svom velikom doprinosu u algebri, točnije smatramo ga osnivačem teorije grupa. Galoisova teorija je „odgovor“ na Abel-Ruffnijev teorem. Abel-Ruffini je tvrdio za jednadžbe stupnja 5 ili višeg da nemaju opće algebarsko rješenje, tj. rješenje u radikalima. Prije nego je dokazano da ne postoji općenito rješenje polinoma 5. stupnja, Joseph – Louis Lagrange se bavio problemom rješavanja polinomijalnih jednadžbi 2., 3. i 4. stupnja. Tvrdio je, da bi jednadžba bila rješiva radikalima, moraju postojati jednostavnije jednadžbe takve da su njihove nultočke ujedno i nultočke početne jednadžbe. Lagrange je također tvrdio da jednadžba ostaje nepromijenjena do na permutaciju njenih nultočki. Galois, potaknut Lagrangeovim idejama, počinje proučavati koji su uvjeti dovoljni da algebarske jednadžbe proizvoljnog stupnja budu rješive radikalima.

Ključni zaključak je da je rješivost radikalima moguća ako i samo ako je grupa automorfizama rješiva, što znači da se grupa može razbiti u jednostavne dijelove čija struktura nam je dobro poznata. Rješavanje jednadžbi 5. stupnja ili višeg drugačije se promatra od jedndžbi stupnja nižeg od 5. Evariste Galois je dao važan doprinos u teoriji grupa, proučavanjem proširenja polja. Ukoliko je dan polinom p s koeficijentima u polju F takav da jednadžba $p(x)$ nema rješenje, tada se polje F može proširiti do polja L, gdje je $\alpha \in L$, te vrijedi $p(\alpha) = 0$.

Ovaj diplomski rad je podijeljen u dva dijela. U prvom dijelu će biti dan kratki podsjetnik na teoriju grupa, Lagrangeov teorem, kvocijentne skupove, te komutativne prstene, polja razlomaka, te polinome. Uvodni dio nam je od velike važnosti kasnije za shvaćanje same Galoisove teorije. U drugom dijelu ćemo se upoznati s Galoisovom teorijom, čiji je originalni naziv teorija jednadžbi. Odmah na početku ćemo definirati Galoisovu grupu. Sama Galoisova teorija daje vezu između algebarskog proširenja E nad poljem k, te pripadne Galoisove grupe $Gal(E/k)$. Navest ćemo nekoliko teorema o Galoisovim grupama čije tvrdnje kažu da su proširenja polja razlaganja nekog polinoma. Na samom kraju ćemo iskazati i dokazati Fundamentalni teorem Galoisove teorije, kao posljedicu cjelokupne analize drugog dijela.

Poglavlje 1

Osnovni pojmovi

U ovom dijelu ćemo se ukratko upoznati s definicijama grupa, prstena, polinoma, te osnovnim tvrdnjama vezanih za njih, što će nam kasnije olakšati shvaćanje Galoisove teorije.

1.1 Grupe

Definicija 1.1.1. ***Grupa*** *je skup G s binarnom operacijom $*$ sa svojstvima*

(i) ***asocijativnosti****, tj. za svaki $x, y, z \in G$*

$$x * (y * z) = (x * y) * z$$

(ii) *postoji element $e \in G$, koji se naziva* ***jedinica****, takav da $e * a = a * e = a$ za sve $a \in G$*

(iii) *svaki $x \in G$ ima* ***inverz****, tj. postoji $x' \in G$ takav da $x * x' = x' * x = e$*

Primjer 1.1.2. *Skup svih permutacija skupa X, oznaka S_X, s binarnom operacijom kompozicije, je grupa koja se naziva simetrična grupa na X. Ako je $X = \{1, 2, \ldots, n\}$, tada umjesto S_X koristimo oznaku S_n.*

Definicija 1.1.3. *Grupa G je* ***Abelova*** *ako je zadovoljeno svojstvo komutativnosti, tj. ako vrijedi*

$$x * y = y * x$$

za sve $x, y \in G$.

Definicija 1.1.4. *Podskup H od grupe G je* ***podgrupa*** *ako vrijedi*

(i) $e \in H$

(ii) *ako su* $x, y \in H$*, onda je* $xy \in H$

(iii) *ako je* $x \in H$*, tada* $x^{-1} \in H$*.*

H je podgrupa od G označavamo s $H \leq G$. Kažemo da je H **prava podgrupa** od G, $H < G$, ako je $H \leq G$, te $H \neq G$.

Definicija 1.1.5. *Ako je* G *grupa i* $a \in G$*, tada* $\langle a \rangle$ *definiran s*

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$$

se naziva ***cikličkom podgrupom*** *od* G *generiranom s* a*. Za grupu* G *kažemo da je* ***ciklička*** *ako postoji* $a \in G$ *tako da vrijedi* $G = \langle a \rangle$*, a nazivamo* ***generatorom****.*

Definicija 1.1.6. *Neka je* G *konačna grupa. Broj elemenata u* G *nazivamo* ***red*** *od* G*, oznaka* $|G|$*.*

Definicija 1.1.7. *Ako je* H *podgrupa grupe* G*, te* $a \in G$*, tada* ***klasa*** aH *je podskup od* G*, gdje je*

$$aH = \{ah : h \in H\}.$$

Klasu definiranu u definiciji obično zovemo ***lijeva klasa****, dok* ***desnu klasu*** *definiramo* $Ha = \{ha : h \in H\}$*.*

Lema 1.1.8. *Neka je* H *podgrupa grupe* G*, te neka su* $a, b \in G$*.*

(i) $aH = bH$ *ako i samo ako* $b^{-1}a \in H$*. Posebno,* $aH = H$ *ako i samo ako* $a \in H$*.*

(ii) *Ako je* $aH \cap bH \neq \emptyset$*, tada* $aH = bH$*.*

(iii) $|aH| = |H|$ *za sve* $a \in G$*.*

Teorem 1.1.9 (Lagrange). *Ako je* H *podgrupa konačne grupe* G*, tada* $|H|$ *je djelitelj od* $|G|$*.*

Dokaz. Neka je $\{a_1H, \ldots, a_tH\}$ familija različitih klasa od H u G. Tada

$$G = a_1H \cup a_2H \cup \cdots \cup a_tH,$$

jer svaki $g \in G$ leži u klasi gH, te $gH = a_i$ za neki i. Štoviše, iz prethodne Leme (ii) slijedi da su klase a_iH disjunktne. Slijedi

$$|G| = |a_1H| + |a_2H| + \cdots + |a_tH|.$$

Iz Leme (iii) znamo da je $|a_iH| = |H|$ za sve i, što nam daje $|G| = t|H|$. □

Definicija 1.1.10. ***Indeks*** *podgrupe H u G, oznaka $[G : H]$, je broj lijevih klasa H u G.*

Indeks $[G : H]$ je upravo broj t iz $|G| = t|H|$, iz dokaza Lagrangeovog teorema, što znači

$$|G| = [G : H]|H|.$$

Dobili smo da je indeks $[G : H]$, također, djelitelj od $|G|$, tj. $[G : H] = |G|/|H|$.

Definicija 1.1.11. *Podrupa K grupe K se naziva* ***normalna podgrupa****, oznaka $K \lhd G$ ako za sve $k \in K$ i $g \in G$ vrijedi $gkg^{-1} \in K$.*

Lema 1.1.12. *Podgrupa K grupe G je normalna podgrupa ako i samo ako $gK = Kg$ za svaki $g \in G$. Stoga, svaka lijeva klasa normalne podgrupe je ujedno i desna klasa.*

Teorem 1.1.13. *Neka G/K predstavlja familiju svih lijevih klasa podgrupe K od G. Ako je K normalna podgrupa, tada je G/K grupa s operacijom*

$$aKbK = abK$$

za sve $a, b \in G$, te je G/K grupa s tom operacijom.

Grupa G/K, iz prethodnog Teorema, se naziva **kvocijentna grupa** G mod K. U slučaju da je G konačna, tada red od $|G/K|$ je indeks $[G : K] = |G|/|K|$.

Primjer 1.1.14. *Ako je $G = \mathbb{Z}$ i $K = \langle m \rangle$, ciklička grupa svih višekratnika od m, tada je $\langle m \rangle$ normalna podgrupa od $\mathbb{Z}$, jer je $\mathbb{Z}$ Abelova grupa. Pripadnu kvocijentnu grupu označimo s $\mathbb{I}_m$, odnosno $\mathbb{I}_m = \mathbb{Z}/\langle m \rangle$.*

Korolar 1.1.15. *Svaka normalna podgrupa $K \lhd G$ je jezgra nekog homomorfizma.*

Dokaz. Definirajmo prirodno preslikavanje $\pi : G \longrightarrow G/K$ s $\pi(a) = aK$. Izraz iz prethodnog teorema $aKbK = abK$ možemo zapisati $\pi(a)\pi(b) = \pi(ab)$, slijedi da je π (surjektivni) homomorfizam. Budaući da je K jednični element u G/K,

$$Ker\pi = \{a \in G : \pi(a) = K\} = \{a \in G : aK = K\} = K,$$

po Lemi 1.1.8.

□

Teorem 1.1.16 (**Prvi teorem o izomorfizmu**)**.** *Ako je $f : G \longrightarrow H$ homomorfizam, tada*

$$Ker\ f \lhd G \qquad i \qquad G/Ker\ f \cong\ Im\ f.$$

Ako je $Kerf = K$ i $\varphi : G/K \longrightarrow Im\ f \leq H$ dana s $\varphi : aK \longmapsto f(a)$, tada je φ izomorfizam.

1.2 Komutativni prsteni

Definicija 1.2.1. ***Komutativni prsten*** *R je skup s dvije binarne operacije, zbrajanje i množenje, takav da*

(i) *R je Abelova grupa s operacijom zbrajanja,*

(ii) ***komutativnost*** *$ab = ba$ za sve $a, b \in R$,*

(iii) ***asocijativnost*** *$a(bc) = (ab)c$ za sve $a, b, c \in R$,*

(iv) *postoji element $1 \in R$ takav da $1a = a$ za sve $a \in R$,*

(v) ***distributivnost*** *$a(b + c) = ab + ac$ za sve $a, b, c \in R$.*

Element 1 u prstenu R se naziva *jedan*, *jedinica* od R, ili *identiteta* u R.

Definicija 1.2.2. *Podskup S komutativnog prstena R je* ***potprsten*** *od R ako vrijedi*

(i) $1 \in S$,

(ii) *ako su $a, b \in S$, onda $a - b \in S$,*

(iii) *ako su $a, b \in S$, onda $ab \in S$.*

Za potprsten S od R koristimo oznaku $S \subseteq R$. Oznaku $S \subsetneq R$ koristimo za prave potprstenove, tj. $S \subseteq R$ i $S \neq R$.

Propozicija 1.2.3. *Potprsten S komutativnog prstena R je također komutativan prsten.*

Definicija 1.2.4. ***Integralna domena*** *ili,kraće,* ***domena*** *je komutativni prsten R takav da zadovoljava sljedeća dva aksioma:*

(i) $1 \neq 0$,

(ii) ***zakon kraćenja za množenje*** *za sve $a, b, c \in R$, ako su $ca = cb$ i $c \neq 0$, tada $a = b$.*

Komutativni prstenovi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$ su integralne domene, dok nulprsten nije.

Definicija 1.2.5. *Neka su a i b elementi u komutativnom prstenu. Tada a* ***dijeli*** *b (ili a je* ***djelitelj*** *od b ili b je* ***višekratnik*** *od a), oznaka $a|b$, ako postoji element $c \in R$ takav da $b = ca$.*

Primjetimo da $a|b$ ne ovisi samo o elementima a i b, već i o samoj okolini R. Na primjer, 3 dijeli 2 u $\mathbb{Q}$, jer $2 = 3 \times \frac{2}{3}$ i $\frac{2}{3} \in \mathbb{Q}$. Međutim, 3 ne dijeli 2 u $\mathbb{Z}$, jer ne postoji broj c takav da $3c = 2$.

Definicija 1.2.6. *Element u iz komutativnog prstena R se naziva **jedinica** ako $u|1$ u R, tj. ako postoji $v \in R$ takav da $uv = 1$. Element v se naziva **inverz** od u, te v se često zapisuje kao u^{-1}.*

Propozicija 1.2.7. *Neka je R domena, te neka su $a, b \in R$ nenul elementi. Tada $a|b$ i $b|a$ ako i samo ako $b = ua$ za neku jedinicu $u \in R$.*

Definicija 1.2.8. ***Polje** F je komutativan prsten u kojem $1 \neq 0$ i svaki nenul element a je jedinica, tj., postoji $a^{-1} \in F$ takav da $a^{-1}a = 1$.*

Neki primjeri polja su $\mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$.
Definicija polja se može izreći u terminima grupe jedinica. Komutativan prsten R je polje ako i samo ako $U(R) = R^{\times}$, nenul elementi iz R. R je polje ako i samo ako $R^{\times}$ je multiplikativna grupa (oznaka $U(R^{\times}) = \emptyset$ zbog pretpostavke $1 \neq 0$). Očito je svako polje F je integralna domena.

Teorem 1.2.9. *Ako je R domena, tada postoji polje F koje sadrži R kao potprsten. Štoviše, F se može izabrati takav da, za svaki $f \in F$, postoje $a, b \in R$, $b \neq 0$, takvi da vrijedi $f = ab^{-1}$.*

F zovemo **polje razlomaka** od R, te označavamo s $F = Frac(R)$.

Definicija 1.2.10. ***Potpolje** polja K je potprsten k od K koji je također polje.*

1.3 Polinomi

U ovom dijelu ćemo ukratko opisati polinome, te neke osnovne pojmove vezane za njih.

Definicija 1.3.1. *Ako je R komutativan prsten, tada **niz** σ u R definiramo s*

$$\sigma = (s_0, s_1, s_2, \dots, s_i, \dots),$$

*gdje se $s_i \in R$, za sve $i \geq 0$, nazivaju **koeficijentima** od σ.*

Da bismo odredili kada su dva niza jednaka, primjetimo da je niz σ realna funkcija $\sigma : \mathbb{N} \longrightarrow R$, gdje je $\mathbb{N}$ skup prirodnih brojeva, definirana s $\sigma(i) = s_i$, za sve $i \geq 0$. Stoga, neka je $\tau = (t_0, t_1, t_2, \dots, t_i, \dots)$, $\sigma = \tau$ ako i samo ako $\sigma(i) = \tau(i)$, za sve $i \geq 0$, tj. $\sigma = \tau$ ako i samo ako $s_i = t_i$, za sve $i \geq 0$.

Definicija 1.3.2. *Niz $\sigma = (s_0, s_1, s_2, \dots, s_i, \dots)$ u komutativnom prstenu R se naziva **polinom** ako postoji prirodan broj $m \geq 0$, tako da $s_i = 0$ za sve $i > m$, tj.*

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

Polinom ima konačno mnogo nenul elemenata. **Nul polinom**, oznaka $\sigma = 0$, je niz $\sigma = (0, 0, 0, \dots)$.

Definicija 1.3.3. *Ako je $\sigma = (s_0, s_1, s_2, \dots, s_n, \dots) \neq 0$ polinom, onda postoji $s_n \neq 0$, te $s_i = 0$, za $i > n$. s_n nazivamo **vodećim koeficijentom** od σ, dok n nazivamo **stupnjom** od σ, oznaka $deg(\sigma)$.*

Nul polinom 0 nema stupanj zato jer nema nenul koeficijenata. Ponekad se stupanj nul polinoma, $deg(0)$, označava s $-\infty$.

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

Propozicija 1.3.4. *Ako je R komutativan prsten, tada je $R[x]$ komutativan prsten koji sadrži R kao potprsten.*

Lema 1.3.5. *Neka je R komutativan prsten, te neka su $\sigma, \tau \in R[x]$ nenul polinomi. Tada vrijedi:*

(i) *Ili je $\sigma\tau = 0$ ili $deg(\sigma\tau) \leq deg(\sigma) + deg(\tau)$,*

(ii) *Ako je R domena, tada $\sigma\tau = 0$ i*

$$deg(\sigma\tau) = deg(\sigma)deg(\tau),$$

(iii) *Ako je R domena, tada je $R[x]$ domena.*

Definicija 1.3.6. *Ako je R komutativan prsten, tada $R[x]$ se naziva **prsten polinoma** nad R.*

Skica dokaza. Definirajmo zbrajanje i množenje polinoma na sljedeći način: Ako je $\sigma = (s_0, s_1, \dots)$ i $\tau = (t_0, t_1, \dots)$, tada

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

i

$$\sigma\tau = (c_0, c_1, c_2, \dots),$$

gdje je $c_k = \sum_{i+j=k} s_i t_j = \sum_{i=0}^{k} s_i t_{k-i}$. Provjera aksioma iz definicije komutativnog prstena je lagana. Podskup $\{(r, 0, 0, \dots) : r \in R\}$ je potprsten od $R[x]$ kojeg identificiramo s R. □

Sad ćemo doći do uvriježenog zapisa polinoma. Element $x \in R[x]$ definiramo s $x = (0, 1, 0, 0, \dots)$.

Lema 1.3.7. **(i)** *Ako je* $\sigma = (s_0, s_1, s_2, \dots)$*, tada*

$$x\sigma = (0, s_1, s_2, s_3, \dots),$$

tj. množenjem s x pomičemo svaki koeficijent za jedno mjesto u desno.

(ii) *Ako je* $n \geq 1$*, tada* x^n *je polinom koji ima svuda 0, osim na n-toj koordinati 1.*

(iii) *Ako je* $r \in R$*, tada*

$$(r, 0, 0, \dots)(s_0, s_1, \dots, s_j, \dots) = (rs_0, rs_1, \dots, rs_j, \dots).$$

Propozicija 1.3.8. *Ako je* $\sigma = (s_0, s_1, s_2, \dots, s_n, \dots)$*, onda*

$$\sigma = s_0 + s_1x + s_2x^2 + \cdots + s_nx^n$$

gdje svaki element $s \in R$ *identificiramo s polinomom* $(s, 0, 0, \dots)$*.*

Od sada možemo koristiti standardni zapis polinoma, tj.

$$f(x) = s_0 + s_1x + s_2x^2 + \cdots + s_nx^n \tag{1.1}$$

umjesto $\sigma = (s_0, s_1, \dots, s_n, 0, 0, \dots)$. U zapisu (1.1), s_0 se naziva **konstantnim članom**, **vodeći koeficijent** je s_n, Ako je vodeći koeficijent $s_n = 1$, tada je $f(x)$ normiran. Svaki polinom, osim nul polinoma, ima stupanj. **Konstantan polinom** je ili nul polinom ili polinom stupnja 0.
Sada možemo opisati standardnu ulogu od x u $f(x)$. Ako je R komutativan prsten, svaki polinom $f(x) = s_0 + s_1x + \cdots + s_nx^n \in R[x]$ definira **polinomijalnu funkciju** $f : R \longrightarrow R$ evaluacijom: Ako je $a \in R$, definiramo $f(a) = s_0 + s_1a + s_2x^2 + \cdots + s_na^n \in R$. Bitno je uočiti da su polinomi i polinomijalne funkcije različite funkcije. Na primjer, ako je R konačan prsten (na primjer, $R = \mathbb{I}_m$), tada postoji samo konačno mnogo funkcija iz R u R, stoga postoji samo konačno mnogo polinomijalnih funkcija. S druge strane, postoji beskonačno mnogo različitih polinoma, na primjer $1, x, x^2, \dots, x^n, \dots$.

Definicija 1.3.9. *Ako je* $f(x) \in k[x]$*, gdje je k polje, tada* ***nultočka*** *od* $f(x)$ *je element* $a \in k$ *takav da* $f(a) = 0$*.*

Propozicija 1.3.10. *Neka je k polje, te neka je* $f(x) \in k[x]$*. Ako* $f(x)$ *ima stupanj n, tada* $f(x)$ *ima najviše n nultočki u k.*

Definicija 1.3.11. *Neka su* $f(x)$ *i* $g(x)$ *polinomi u* $k[x]$*, gdje je k polje, tada* ***zajednički djelitelj*** *je polinom* $c(x) \in k[x]$ *takav da* $c(x)|f(x)$ *i* $c(x)|g(x)$*. Ako* $f(x)$ *i* $g(x)$ *u* $k[x]$ *nisu oba 0, definiramo* ***najveći zajednički djelitelj****, u oznaci nzd, kao normiran zajednički djelitelj s najvećim stupnjem. Ako je* $f(x) = 0 = g(x)$*, definiramo njihov nzd* $= 0$*.*

Definicija 1.3.12. *Element p u domeni R je **ireducibilan** ako p nije 0, niti jedinica, te ako za svaku faktorizaciju $p = uv$ u R, u i v nisu jedinice.*

Na primjer, prosti broj $p \in \mathbb{Z}$ je ireducibilan, kao što je i $-p \in \mathbb{Z}$. Sada ćemo definirati ireducibilne polinome $p(x) \in k[x]$, gdje je k polje.

Propozicija 1.3.13. *Neka je K polje, polinom $p(x) \in k[x]$ je ireducibilan ako i samo ako $deg(p) = n \geq 1$, te ne postoji faktorizacija oblika $p(x) = g(x)h(x)$ u kojoj su oba faktora stupnja manjeg od n.*

Kao što definicija djeljivosti ovisi o prostoru prstena, tako i ireducibilnost polinoma $p(x) \in k[x]$ ovisi o komutativnom prstenu $k[x]$, dakle, o polju k.

Korolar 1.3.14. *Neka je k polje, te neka je $f(x) \in k[x]$ polinom drugog ili trećeg stupnja. Tada $f(x)$ je ireducibilan u $k[x]$ ako i samo ako $f(x)$ nema nultočku u k.*

1.4 Homomorfizmi

Sada ćemo se upoznati s homomorfizmima, te njihovoj primjeni u usporedbi komutativnih prstena.

Definicija 1.4.1. *Neka su A i R komutativni prsteni, **homomorfizam (prstena)** je funkcija $f : A \longrightarrow R$ takva da*

(i) $f(1) = 1$,

(ii) $f(a + a') = f(a) + f(a')$ *za sve* $a, a' \in A$,

(iii) $f(aa') = f(a)f(a')$.

Homomorfizam koji je bijekcija se naziva **izomorfizam**. Komutativni prsteni A i R su **izomorfni**, oznaka $A \cong R$, ako postoji izomorfizam $f : A \longrightarrow R$.

Definicija 1.4.2. *Ako je $f : A \longrightarrow R$ homomorfizam prstena, tada se **jezgra** definira kao*

$$Ker f = \{a \in A : f(a) = 0\},$$

*te **slika***

$$Im f = \{r \in R : r = f(a) \text{ za neki } a \in R\}$$

Definicija 1.4.3. ***Ideal** komutativnog prstena R je podskup I od R takav da*

(i) $0 \in I$,

(ii) *ako* $a, b \in I$*, tada* $a + b \in I$*,*

(iii) *ako je* $a \in I$ *i* $r \in R$*, tada je* $ra \in I$*.*

Prsten R koji se sastoji od samo 0, oznaka $\{0\}$, je uvijek ideal u komutativnom prstenu R. Ideal $I \neq R$ se naziva **pravi ideal**.

Primjer 1.4.4. *Ako su* $b_1, b_2, \ldots, b_n$ *iz* R*, tada skup svih linearnih kombinacija*

$$I = \{r_1 b_1 + r_2 b_2 + \cdots + r_n b_n : r_i \in R \text{ za sve } i\}$$

je ideal u R*. Zapisujemo* $I = (b_1, \ldots, b_n)$ *i zovemo* ***ideal generiran*** *s* $(b_1, \ldots, b_n)$*. Posebno, ako je* $n = 1$

$$I = (b) = \{rb : r \in R\},$$

tada je I *ideal.* (b) *se sastoji od višekratnika od* b *i zove se* ***glavni ideal*** *generiran s* b*. Primjetimo da su* R *i* $\{0\}$ *uvijek glavni ideali, jer* $R = (1)$ *i* $\{0\} = (0)$*.*

Propozicija 1.4.5. *Homomorfizam prstena je* $f : A \longrightarrow R$ *je injekcija ako i samo ako je* $Kerf = \{0\}$*.*

Korolar 1.4.6. *Ako je* $f : k \longrightarrow R$ *homomorfizam prstena, gdje je* k *polje i* R *je nenul prsten, tada je* f *injekcija.*

Teorem 1.4.7. *Ako je* k *polje, tada je svaki ideal* I *u* $k[x]$ *glavni ideal. Štoviše, ako je* $I \neq \{0\}$*, tada postoji normiran polinom koji generira* I*.*

1.5 Kvocijentni prsteni

Neka je I ideal u komutativnom prstenu, te R/I pridružena aditivna kvocijentna grupa. Definirano je prirodno preslikavanje $\pi : R \longrightarrow R/I$ s $\pi(a) = a + I$. Preslikavanje π ima svojstvo: $a + I = b + I$ ako i samo ako $a - b \in I$.

Teorem 1.5.1. *Ako je* I *ideal u komutativnom prstenu* R*, tada aditivna Abelova grupa* R/I *ima strukturu komutativnog prstena tako da je prirodno preslikavanje* $\pi : R \longrightarrow R/I$ *surjektivni homomorfizam prstena.*

Skica dokaza. Definiramo množenje na aditivnoj Abelovoj grupi R/I s

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

Da bismo dokazali da je $R/I \times R/I \longrightarrow R/I$ dobro definirana funkcija, pretpostavimo da je $a + I = a' + I$, te $b + I = b' + I$, što daje $a - a' \in I$, te $b - b' \in I$. Trebamo pokazati da vrijedi $(a' + I)(b' + I) = a'b' + I$, tj. $ab - a'b' \in I$. Dobijemo

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

kako je traženo.

Da bismo potvrdili da je R/I komutativan prsten, dovoljno je pokazati asocijativnost i komutativnost množenja, distributivnost, te da je $1 + I$ jedinica. Dokaz tih svojstava je rutinska, tj. nasljeđena su iz odgovarajućih svojstava iz R. Na primjer, množenje u R/I je komutativno zato jer

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

Ako na jednadžbu $(a + I)(b + I) = ab + I$ primjenimo definiciju od π, tj. $\pi(a) = a + I$, dobijemo $\pi(ab) = \pi(a)\pi(b)$. Jasno je da vrijedi $\pi(1) = 1 + I$, pa slijedi da je π prsten homomorfizama. Na kraju, π je surjekcija zato jer $a + I = \pi(a)$. □

Definicija 1.5.2. *Komutativan prsten R/I konstruiran u prethodnom teoremu se naziva **kvocijentni prsten** od R modulo I.*

U Primjeru 1.1.14. smo aditivnu Abelovu grupu $\mathbb{Z}/(m)$ označili s $\mathbb{I}_m$. Budući da je $\langle m \rangle$ ideal u prstenu $\mathbb{Z}$, $\mathbb{I}_m$ je prsten uz operaciju množenja:

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

Korolar 1.5.3. *Ako je I ideal u komutativnom prstenu R, tada postoje komutativan prsten A i homomorfizam prstena $\pi : R \longrightarrow A$ takav da vrijedi $I = Ker\pi$.*

Teorem 1.5.4 (**Prvi teorem o izomorfizmu**)**.** *Ako je $f : R \longrightarrow A$ homomorfizam prstena, tada $Kerf$ ideal u R, Imf potprsten A, te*

$$R/Kerf \cong Imf.$$

Definicija 1.5.5. *Neka je k polje, presjek svih potpolja k se naziva **prosto polje**.*

Svako potpolje od $\mathbb{C}$ sadrži $\mathbb{Q}$, pa slijedi da prosto polje od $\mathbb{C}$ i $\mathbb{R}$ je $\mathbb{Q}$.

Napomena 1.5.6. *Ako je p prost, može se pokazati da je $\mathbb{I}_p$ polje, koje označavamo s $\mathbb{F}_p$. $\mathbb{F}_p$ zovemo konačno polje s p elemenata.*

Definicija 1.5.7. *Polje k je **karakteristike** 0 ako je pripadno prosto polje izomorfno s $\mathbb{Q}$. Polje k je karakteristike p ako pripadno prosto polje je izomorfno s $\mathbb{F}_p$, konačnim poljem s p elemanata, za neki prosti broj p.*

Polja $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ imaju karakteristike 0, kao i njihova potpolja. Svako konačno polje je karakteristike p, kao i $\mathbb{F}_p(x)$, prsten svih racionalnih funkcija nad $\mathbb{F}_p$.

Propozicija 1.5.8. *Ako je k polje i $I = (p(x))$, gdje je $p(x)$ nenul polinom u $k[x]$, tada su sljedeće tvrdnje ekvivalentne:*

(i) *$p(x)$ je ireducibilan,*

(ii) *$k[x]/I$ je polje,*

(iii) *$k[x]/I$ je domena.*

Struktura od R/I je često kompliciranа, ali specijalan izbor R i I, olakšava opis komutativnog prstena R/I. Na primjer, ukoliko je $p(x)$ ireducibilan polinom, sljedeća propozicija daje potpuni opis polja $k[x]/(p(x))$.

Propozicija 1.5.9. *Neka je k polje, neka je $p(x) \in k[x]$ normiran ireducibilan polinom stupnja d, neka je $K = k[x]/I$, gdje je $I = (p(x))$, te neka je $\beta = x + I \in K$.*

(i) *K je polje i $k' = \{a + I : a \in k\}$ je potpolje od K izomorfno s k. Stoga, ako k' identificiramo s k, tada je k potpolje od K.*

(ii) *β je nultočka od $p(x)$ u K.*

(iii) *Ako je $g(x) \in k[x]$ i β nultočka od $g(x)$, tada $p(x)|g(x)$ u $k[x]$.*

(iv) *$p(x)$ je jedinstven normiran ireducibilan polinom u $k[x]$ čija je β nultočka.*

(v) *Niz $1, \beta, \beta^2, \ldots, \beta^{d-1}$ je baza u K kao vektorskog prostora nad k, te $dim_k(K) = d$.*

Dokaz. **(i)** Kvocijentni prsten $K = k[x]/I$ je polje, po Propoziciji 1.5.8, jer je $p(x)$ ireducibilan. Lako se vidi, koristeći Korolar 1.4.6, da restrikcija prirodnog preslikavanja $\varphi = \pi|k : k \longrightarrow K$ definirana s $\varphi(a) = a + I$ je izomorfizam s $k \longrightarrow k'$.

(ii) Neka je $p(x) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} + x^d$, gdje su $a_i \in k$ za sve i. U $K = k[x]/I$, imamo

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

zato jer $p(x) \in I = (p(x))$. Ali, $I = 0 + I$ neutralni element od $K = k[x]/I$, stoga je β nultočka od $p(x)$.

(iii) Ako $p(x) \nmid h(x)$ u $k[x]$, tada je njihov *nzd* 1, jer $p(x)$ je ireducibilan. Stoga, postoje $s(x), t(x) \in k[x]$ takvi da je $1 = s(x)p(x) + t(x)g(x)$. Budući da je $k[x] \subseteq K[x]$, možemo to promatrati kao jednadžbu u $K[x]$. Evaluacijom u β dobivamo kontradikciju $1 = 0$.

(iv) Neka je $h(x) \in k[x]$ normiran polinom čija je nultočka β. Po dijelu (iii), slijedi $p(x)|h(x)$. Budući da je $p(x)$ ireducibilan, imamo $h(x) = cp(x)$ za neku konstantu c. Budući da su $h(x)$ i $p(x)$ normirani, slijedi da je $c = 1$ i $h(x) = p(x)$.

(v) Svaki element iz K ima oblik $f(x) + I$, gdje je $f(x) \in k[x]$. Po algoritmu dijeljenja, postoje polinomi $q(x), r(x) \in k[x]$ takvi da $f(x) = q(x)p(x) + r(x)$, te ili je $r(x) = 0$ ili je $deg(r) < d = deg(p)$. Budući da je $f - r = qp \in I$, slijedi $f(x) + I = r(x) + I$. Ako je $r(x) = b_0 + b_1\beta + \cdots + b_{d-1}\beta^{d-1}$, gdje su $b_i \in k$ za svaki i, tada kao u dokazu dijela (ii) imamo $r(x) + I = b_0 + b_1\beta + \cdots b_{d-1}\beta^{d-1}$. Dakle, $1, \beta, \beta^2, \ldots, \beta^{d-1}$ razapinju K.
Da bismo dokazali jedinstvenost, pretpostavimo da vrijedi

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

Definiramo $g(x) \in k[x]$ s $g(x) = \sum_{i=0}^{d-1}(b_i - c_i)x^i$. Ako je $g(x) = 0$, gotovi smo. Ako je $g(x) \neq 0$, tada je $deg(g)$ definiran s $deg(g) < d = deg(p)$. S druge strane, β je nultočka od $g(x)$, pa po dijelu (iii) $p(x)|g(x)$. Slijedi $deg(p) \leqslant deg(g)$, time dobivamo kontradikciju. Dakle, $1, \beta, \beta^2, \ldots, \beta^{d-1}$ je baza od K kao vektorskog prostora nad k, te $dim_k(K) = d$.

□

Definicija 1.5.10. *Ako je K polje koje sadrži k kao potpolje, tada K se zove **proširenje** polja k, oznaka K/k.*

Proširenje K polja k je **konačno proširenje** od k ako je K konačnodimenzionalni vektorski prostor nad k. Dimenzija od K, oznaka $[K : k]$, se naziva **red** od K/k.

Definicija 1.5.11. *Neka je K/k proširenja polja. Element $\alpha \in K$ je **algebarski** nad k ako postoji nenul polinom $f(x) \in k[x]$ kojem je α nultočka, inače, α je **transcedentan** na k. Proširenje K/k je **algebarsko** ako je svaki $\alpha \in K$ algebarski nad k.*

Kada za realan broj kažemo da je transcedentan, to obično znači da je transcedentan nad $\mathbb{Q}$.

Propozicija 1.5.12. *Ako je K/k konačno proširenje polja, tada je K/k algebarsko proširenje.*

Definicija 1.5.13. *Ako je K/k proširenje i $\alpha \in K$, tada s $k(\alpha)$ označavamo presjek svih potpolja od K koje sadrže k i α. Polje $k(\alpha)$ zovemo potpolje od K dobiveno **pridruživanjem** α u k.*

Teorem 1.5.14. **(i)** *Ako je K/k proširenje, te $\alpha \in K$ algebarski nad k, tada postoji jedinstven normiran ireducibilan polinom $p(x) \in k[x]$ čija je nultočka upravo α. Štoviše, ako je $I = (p(x))$, tada $k[x]/I \cong k(\alpha)$, tj. postoji izomorfizam*

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

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

(ii) *Ako je α' neka druga nultočka od $p(x)$, tada postoji izomorfizam*

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

definiran s $\theta(\alpha) = \alpha'$ i $\theta(c) = c$ za sve $c \in k$.

Dokaz. **(i)** Promatramo evaluaciju, homomorfizam prstena $\varphi : k[x] \longrightarrow K$ definiran s $\varphi : f(x) \longmapsto f(\alpha)$. Sada Imf je potprsten od K koji se sastoji od svih polinoma u α, tj. svih elemenata oblika $f(\alpha)$ takvih da je $f(x) \in k[x]$. Sada $Kerf$ je ideal u $k[x]$ koji se sastoji od svih $f(x) \in k[x]$ čija je α nultočka. Po Teoremu 1.4.7, svaki ideal u $k[x]$ je glavni ideal, tada vrijedi $Ker\varphi = (p(x))$ za neki normirani polinom $p(x) \in k[x]$. Ali $k[x]/(p(x)) \cong Im\varphi$, pa je i domena, slijedi da je $p(x)$ ireducibilan, po Popoziciji 1.5.8. Ista Propzicija tvrdi da je $k[x]/(p(x))$ polje, pa Prvi teorem o izomorfizmu daje $k[x]/(p(x)) \cong Im\varphi$, tj. $Im\varphi$ je potpolje od K koje sadrži k i α. Budući da svako potpolje od K koje sadrži k i α mora sadržavati i $Im\varphi$, tada imamo $Im\varphi = k(\alpha)$. Dokazali smo sve tvrdnje osim jedinstvenosti $p(x)$, što nam slijedi iz Propozicije 1.5.9 (iv).

(ii) Kao u dijelu (i), postoje izomorfizmi $\varphi : k[x]/I \longrightarrow k(\alpha)$ i $\psi : k[x]/I \longrightarrow k(\alpha')$ takvi da $\varphi(c + I) = c$, te $\psi(c) = c + I$, za sve $c \in k$. Štoviše, $\varphi : x + I \longmapsto \alpha$ i $\psi : x + I \longmapsto \alpha'$. Kompozicija $\theta = \psi\varphi^{-1}$ je traženi izomorfizam.

□

Definicija 1.5.15. *Ako je K/k proširenje polja i $\alpha \in K$ algebarski nad k, tada jedinstveni normiran ireducibilan polinom $p(x) \in k[x]$ čija je α nultočka se naziva* ***minimalnim polinomom*** *od α nad k, oznaka*

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

Tvrdnja sljedećeg teorema će nam biti od velike koristi u glavnom dijelu ovog rada, prvenstveno u određivanju reda Galoisove grupe.

Teorem 1.5.16. *Ako su $k \subseteq E \subseteq K$ polja, gdje su E konačno proširenje od k i K konačno proširenje od E. Tada je K konačno proširenje k, te vrijedi*

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

Teorem 1.5.17 (**Kronecker**). *Ako je k polje, te $f(x) \in k[x]$, tada postoji polje K koje sadrži k kao potpolje, te je $f(x)$ produkt linearnih polinoma u $k[x]$.*

Dokaz. Dokaz ćemo provesti indukcijom po $deg(f)$. Ako je $deg(f) = 1$, tada je $f(x)$ linearna, te možemo izabrati $K = k$. Ako je $deg(f) > 1$, zapisujemo $f(x) = p(x)g(x)$, gdje je $p(x)$ ireducibilan polinom. Po Propoziciji 1.5.9 (i) slijedi da polje F sadrži k, i nultočku z od $p(x)$. Stoga, u $F[x]$ se nalazi $p(x) = (x - z)h(x)$ i $f(x) = (x - z)h(x)g(x)$. Indukcijom, postoji polje K koje sadrži F (time i k) tako da $h(x)g(x)$, dakle $f(x)$ je produkt linearnih faktora iz $K[x]$. □

Definicija 1.5.18. *Neka je k potpolje polja K, te neka je $f(x) \in k[x]$. Kažemo da se $f(x)$* ***razlaže*** *nad K ako*

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

gdje su $z_1, \ldots, z_n$ iz K, $a \in k$ različit od 0.

Ako je $f(x) \in k[x]$ polinom, tada se proširenje polja E/k naziva **poljem razlaganja** od $f(x)$ nad k ako se $f(x)$ razlaže nad E, ali se $f(x)$ ne razlaže ni na jednom pravom potpolju od E. Iz Kroneckerovog teorema sada slijedi:

Korolar 1.5.19. *Neka je k polje, te neka je $f(x) \in k[x]$. Tada postoji polje razlaganja od $f(x)$ nad k.*

Primjer 1.5.20. *Neka je k polje, te neka je $E = k(y_1, \ldots, y_n)$ polje racionalnih funkcija n varijabli $y_1, \ldots, y_n$ nad k, tj. $E = Frac(k[y_1, \ldots, y_n])$ je polje razlomaka prstena polinoma u n varijabli. Općeniti polinom stupnja n se definira kao*

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

Koeficijenti od $f(x) = (x - y_1)(x - y_2) \cdots (x - y_n)$ se mogu izraziti u terminima y-na.

Poglavlje 2

Galoisova teorija

Galoisova teorija analizira vezu između algebarskog proširenja E polja k i pripadajuće Galoisove grupe $Gal(E/k)$.

2.1 Uvod u Galoisovu teoriju

Definicija 2.1.1. *Neka je E polje koje sadrži potpolje k.* ***Automorfizam*** *od E je izomorfizam $\sigma : E \longrightarrow E$. Kažemo da σ* ***fiksira*** *k ako $\sigma(a) = a$ za svaki $a \in k$.*

Primjer 2.1.2. *Neka je $f(x) = x^2 + 1 \in \mathbb{Q}[x]$. Polje razlaganja od $f(x)$ nad $\mathbb{Q}$ je $E = \mathbb{Q}(i)$, a kompleksno konjugiranje $\sigma : a \longmapsto \overline{a}$ je primjer automorfizma od E koje fiksira $\mathbb{Q}$.*

Propozicija 2.1.3. *Neka je k potpolje polja K, neka je*

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

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

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

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

Djelovanjem sa σ na jednadžbu dobije se

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

jer σ fiksira k. Dakle, $\sigma(r)$ je nultočka od $f(x)$. Ako je Z je skup svih nultočki, tada $\sigma|Z : Z \longrightarrow Z$, gdje je $\sigma|Z$ restrikcija. σ je injekcija, pa je i $\sigma|Z$ injekcija, slijedi da je $\sigma|Z$ permutacija od Z.

□

Definicija 2.1.4. *Neka je k potpolje polja E.* ***Galoisova grupa*** *od E nad k, oznaka Gal(E/k), je skup svih automorfizama od E koji fiksiraju k. Ako je $f(x) \in k[x]$, te ako je $E = k(z_1, \ldots, z_n)$ polje razlaganja, tada je* ***Galoisova grupa*** *od $f(x)$ nad k definirana kao $Gal(E/k)$.*

$Gal(E/k)$ je grupa s operacijom kompozicije funkcija.

Lema 2.1.5. *Neka je $E = k(z_1, \ldots, z_n)$. Ako je $\sigma : E \longrightarrow E$ automorfizam koji fiksira k, tj. ako je $\sigma \in Gal(E/k)$, takav da $\sigma(z_i) = z_i$ za sve i, tada je σ identiteta 1_E.*

Dokaz. Lemu ćemo dokazati indukcijom po $n \geq 1$. Ako je $n = 1$, tada je svaki $u \in E$ oblika $u = f(z_1)/g(z_1)$, gdje su $f(x), g(x) \in k[x]$, te $g(z_1) \neq 0$. Budući da σ fiksira z_1 kao i koeficijente od $f(x), g(x)$, σ fiksira i sve $u \in E$. Za korak indukcije, pretpostavimo da je $K = k(z_1, \ldots, z_{n-1})$, i primjetimo da je $E = K(z_n)$, gdje je $K(z_n)$ najmanje potpolje koje sadrži k i $z_1, \ldots, z_{n-1}, z_n$. Ako k zamijenimo s K, slijedi da je korak indukcije analogan s korakom baze.

□

Teorem 2.1.6. *Ako $f(x) \in k[x]$ ima stupanj n, tada pripadna Galoisova grupa $Gal(E/k)$ je izomorfna podgrupi od S_n.*

Dokaz. Neka je $X = \{z_1, \ldots, z_n\}$. Ako je $\sigma \in Gal(E/k)$, tada po Propoziciji 2.1.3 slijedi da je restrikcija $\sigma|X$ permutacija od X, tj. $\sigma|X \in S_X$. Definiramo $\varphi : Gal(E/k) \longrightarrow S_X$ s $\varphi : \sigma \longmapsto \sigma|X$. Da bismo dokazali da je φ homorfizam, primjetimo da su $\varphi(\sigma\tau)$ i $\varphi(\sigma)\varphi(\tau)$ funkcije $X \longrightarrow X$, i jednake su ako se podudaraju u svakom $z_i \in X$. $\varphi(\sigma\tau) : z_i \longmapsto (\sigma\tau)(z_i)$, dok $\varphi(\sigma)\varphi(\tau) : z_i \longmapsto \sigma(\tau(z_i))$, što znači da su iste.

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 permutacija identiteta na X, tj. σ fiksira svaku nultočku $z_i \in X$. σ također fiksira k, pa iz definicije Galoisove grupe, te Leme 2.1.5. slijedi $Ker\varphi = 1$. Slijedi, φ je injekcija, time smo dobili tvrdnju teorema.

□

Primjer 2.1.7. *Ako je $f(x) = x^2 + 1 \in \mathbb{Q}[x]$, tada kompleksno konjugiranje σ je automorfizam od pripadnog polja razlaganja $\mathbb{Q}(i)$ koje fiksira $\mathbb{Q}$ (te izmjenjuje nultočke i i $-i$). Budući da je $Gal(Q(i)/\mathbb{Q})$ podgrupa simetrične grupe S_2, koja ima red 2, slijedi $Gal(\mathbb{Q}(i)/\mathbb{Q}) = \langle\sigma\rangle \cong \mathbb{I}_2$. Trebali bismo shvaćati sve Galoisove grupe $Gal(E/k)$ kao generalizacije kompleksne konjugacije.*

Želimo izračunati red Galoisove grupe, ali prvo ćemo priskrbiti osnovne informacije o izomorfizmima i automorfizmima polja.

Lema 2.1.8. *Neka je k polje karakteristike* 0*, tada svaki ireducibilan polinom* $p(x) \in k[x]$ *ima međusobno različite nultočke.*

Dokaz. Općenito, za proizvoljan polinom (ne nužno ireducibilan) $f(x)$ s koeficijentima u proizvoljnom polju vrijedi $f(x)$ ima sve međusobno različite nultočke ako i samo ako vrijedi $nzd(f, f') = 1$, gdje je $f'(x)$ derivacija od $f(x)$.

Pretpostavimo $p(x) \in k[x]$, tada je ili $p'(x) = 0$ ili $deg(p') < deg(p)$. Budući je $p(x)$ ireducibilan, što znači da nije konstantan, tj. postoji nenul monom $a_i x^i$, gdje $i \geq 1$. Dakle, $ia_i x^{i-1}$ je nenul monom u $p'(x)$, jer je k polje karakteristike 0, te $p'(x) \neq 0$. $p(x)$ je ireducibilan, jedini njegovi djelitelji su konstante ili asocirani polinomi. Budući $p'(x)$ ima manji stupanj od polinoma $p(x)$, slijedi $nzd(p', p) = 1$.

□

Definicija 2.1.9. *Neka je* E/k *algebarsko proširenje. Ireducibilan polinom* $p(x)$ *je* ***separabilan*** *ako ima jednostruke nultočke. Proizvoljan polinom* $f(x)$ *je* ***separabilan*** *ako svaki od njegovih ireducibilnih faktora ima međusobno različite nultočke.*
Element $\alpha \in E$ *je* ***separabilan*** *ako je ili* α *transcedentan nad k ili* α *algebarski nad k, te pripadni minimalni polinom* $irr(\alpha, k)$ *ima međusobno različite nultočke, tj.* $irr(\alpha, k)$ *je separabilan polinom.*
Proširenje polja E/k *se zove* ***separabilno proširenje*** *ako svaki element je separabilan. Kažemo da* E/k *je* ***neseparabilno*** *ako nije separabilno.*

Separabilnost od E/k nam omogućava pronalaženje reda od $Gal(E/k)$.

Teorem 2.1.10. **(i)** *Neka je* E/k *polje razlaganja separabilnog polinoma* $f(x) \in k[x]$*, neka je* $\varphi : k \longrightarrow k'$ *izomorfizam polja, te neka je* E'/k' *polje razlaganja od* $f^*(x) \in k'[x]$ *(gdje je* $f^*(x)$ *dobiven iz* $f(x)$ *djelovanjem s* φ *na koeficijente). Tada postoji točno* $[E : k]$ *izomorfizama* $\phi : E \longrightarrow E'$ *koji proširuju* φ*.*

(ii) *Ako je* E/k *polje razlaganja separabilnog* $f(x) \in k[x]$*, tada*

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

Dokaz. **(i)** Dokaz ćemo provesti indukcijom po $[E : k]$. Ako je $[E : k] = 1$, onda je $E = k$ i postoji samo jedno proširenje Φ od φ, to je sam φ. Ako je $[E : k] > 1$, tada je $f(x) = p(x)g(x)$, gdje je $p(x)$ ireducibilan faktor najvišeg stupnja, npr. d. Pretpostavljamo da je $d > 1$, inače se $f(x)$ razlaže nad k i $[E : k] = 1$. Biramo nultočku α od $p(x)$, primjetimo da je $\alpha \in E$ jer je E polje razlaganja od $f(x) = p(x)g(x)$. Ako je $\tilde{\varphi} : k(\alpha) \longrightarrow E'$ proizvoljno proširenje od φ, tada je $\varphi(\alpha)$ nultočka

α' od $p^*(x)$, po Propoziciji 2.1.3.. Budući je $f^*(x)$ je separabilan, $p^*(x)$ ima točno d nultočki $\alpha' \in E'$. Iz Leme 2.1.5. i tvrdnje (ii) Teorema 1.5.14, postoji točno d izomorfizama $\hat{\varphi} : k(\alpha) \longrightarrow k'(\alpha')$ koji proširuju φ , jedan za svaki α'. Sada je i E polje razlaganja od $f(x)$ nad $k(\alpha)$, jer pridruživanjem svih nultočki od $f(x)$ u $k(\alpha)$ i dalje dobivamo E, te E' je polje razlaganja od $f^*(x)$ nad $k'(\alpha')$. Budući je $[E : k(\alpha)] = [E : k]/d$, indukcijom smo dokazali da svaki od d izomorfizama $\hat{\varphi}$ ima točno $[E : k]/d$ proširenja $\Phi : E \longrightarrow E'$. Konstruirali smo $[E : k]$ izomorfizama koji proširuju φ. Ne postoje druga proširenja, jer svaki τ koji proširuje φ ima $\tau|k(\alpha) = \hat{\varphi}$ za neki $\hat{\varphi} : k(\alpha) \longrightarrow k'(\alpha')$.

(ii) Tvrdnju dokažemo ako u tvrdnji (i) napravimo zamjene $k = k'$, $E = E'$, te $\varphi = 1_k$.

□

Korolar 2.1.11. *Neka je E/k polje razlaganja separabilnog polinoma $f(x) \in k[x]$ stupnja n. Ako je $f(x)$ ireducibilan, onda $n \mid |Gal(E/k)|$.*

Dokaz. Iz prethodnog teorema, $|Gal(E/k)| = [E : k]$. Neka je $\alpha \in E$ nultočka od $f(x)$. Budući je $f(x)$ ireducibilan, tada je $[k(\alpha) : k] = n$ i

$$[E : k] = [E : k(\alpha)][k(\alpha) : k] = n[E : k(\alpha)].$$

□

Kasnije ćemo vidjeti, ako je E/k polje razlaganja separabilnog polinoma, tada E/k je separabilno proširenje.
U sljedećem primjeru ćemo pronaći Galoisovu grupu nekih specifičnih polinoma u $\mathbb{Q}[x]$.

Primjer 2.1.12. **(i)** *Neka je $f(x) = x^3 - 1 \in \mathbb{Q}[x]$. Sada je $f(x) = (x-1)(x^2 + x + 1)$, gdje je $x^2 + x + 1$ ireducibilan. Iz kvadratne formule se vidi da nultočke ω i $\overline{\omega}$ ne leže u $\mathbb{Q}$. Polje razlaganja od $f(x)$ je $\mathbb{Q}(\omega)$, jer je $\omega^2 = \overline{\omega}$, te $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. Tada je $|Gal(\mathbb{Q}(\omega)/\mathbb{Q})| = 2$, po Teoremu 2.1.10 (ii), te ciklička je reda 2. Pripadni netrivijalni element je kompleksno konjugiranje.*

(ii) *Neka je $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. $f(x)$ je ireducibilan s nultočkama $\pm\sqrt{2}$, pa je $E = \mathbb{Q}(\sqrt{2})$ polje razlaganja. Po Teoremu 2.1.10 (ii), $|Gal(E/\mathbb{Q})| = 2$. Svaki element iz E ima jedinstven zapis oblika $a + b\sqrt{2}$, gdje su $a, b \in \mathbb{Q}$. Lako se vidi da je $\sigma : E \longrightarrow E$ definiran s $\sigma : a + b\sqrt{2} \longmapsto a - b\sqrt{2}$ automorfizam od E koji fiksira $\mathbb{Q}$. Stoga, $Gal(E/\mathbb{Q}) = \langle\sigma\rangle$, gdje σ izmjenjuje $\sqrt{2}$ i $-\sqrt{2}$.*

(iii) *Neka je $g(x) = x^3 - 2 \in \mathbb{Q}[x]$. Nultočke od $g(x)$ su α, $\omega\alpha$ i $\omega^2\alpha$, gdje $\alpha = \sqrt[3]{2}$, te ω primitivni treći korijen iz jedinice. Lako se vidi, polje razlaganja od $g(x)$ je $E = \mathbb{Q}(\alpha, \omega)$. Primjetimo,*

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 3[E : \mathbb{Q}(\alpha)], \tag{2.1}$$

jer je $g(x)$ ireducibilan nad $\mathbb{Q}$ (to je polinom stupnja 3 koji nema racionalne korijene). Sada $E \neq \mathbb{Q}(\alpha)$, jer je svaki element iz $\mathbb{Q}(\alpha)$ realan, te kompleksni broj ω nije realan. Stoga, $[E : \mathbb{Q}] = |Gal(E/\mathbb{Q})| > 3$. S druge strane, znamo da $Gal(E/\mathbb{Q})$ je izomorfna podgrupi od S_3, pa imamo $Gal(E/\mathbb{Q}) \cong S_3$.

Propozicija 2.1.13. *Neka je k polje, te neka $p(x) \in k[x]$ ima međusobno različite nultočke. Ako je E/k pripadno polje razlaganja od $p(x)$, $p(x)$ je ireducibilan ako i samo ako $Gal(E/k)$ djeluje tranzitivno na nultočke od $p(x)$.*

Dokaz. Pretpostavimo da je $p(x)$ ireducibilan, te neka su $\alpha, \beta \in E$ nultočke od $p(x)$. Po Teoremu1.5.14 (ii), postoji izomorfizam $\varphi : k(\alpha) \longrightarrow k(\beta)$ takav da je $\varphi(\alpha) = \beta$, i da fiksira k. φ proširuje do automorfizma Φ od E koji fiksira k, tj. $\Phi \in Gal(E/k)$. Sada $\Phi(\alpha) = \varphi(\alpha) = \beta$, pa slijedi da $Gal(E/k)$ djeluje tranzitivno na nultočke.
Obrnuto, pretpostavimo da $Gal(E/k)$ djeluje tranzitivno na nultočke od $p(x)$. Ako je $p(x) = q_1(x) \cdots q_t(x)$ faktorizacija polinoma na ireducibilne u $k[x]$, gdje je $t \geq 2$, biramo nultočku $\alpha \in E$ iz $q_1(x)$, te nultočku $\beta \in E$ iz $q_2(x)$. Po pretpostavci, postoji $\sigma \in Gal(E/k)$ takav da $\sigma(\alpha) = \beta$. σ permutira nultočke iz $q_1(x)$, po Propoziciji 2.1.3. Nadalje, β nije nultočka od $q_1(x)$, jer $p(x)$ nema međusobno različite nultočke, što je u kontradikciji s pretpostavkom. Stoga, $t = 1$, tj. $p(x)$ je ireducibilan. □

Teorem 2.1.14. *Neka je $k \subseteq B \subseteq E$ niz polja, neka su $f(x), g(x) \in k[x]$, neka je B polje razlaganja od $f(x)$ nad k, te neka je E polje razlaganja od $g(x)$ nad k. Tada je $Gal(E/B)$ normalna podgrupa od $Gal(E/k)$ i*

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

Dokaz. Neka je $B = k(z_1, \ldots, z_t)$, gdje su $z_1, \ldots, z_t$ nultočke od $f(x)$ u E. Ako je $\sigma \in Gal(E/k)$, tada σ permutira $z_1, \ldots, z_t$, po Propoziciji 2.1.3, pa je $\sigma(B) = B$. Definiramo $\varphi : Gal(E/k) \longrightarrow Gal(B/k)$ s $\sigma \longmapsto \sigma|B$. Lako se vidi, po Teoremu 2.1.6, φ je homomorfizam i $Ker\varphi = Gal(E/B)$. Slijedi da je $Gal(E/B)$ normalna podgrupa od $Gal(E/k)$. φ je surjekcija, jer ako $\tau \in Gal(B/k)$, onda postoji $\sigma \in Gal(E/k)$ koji proširuje τ, tj. $\varphi(\sigma) = \sigma|B = \tau$. □

Lema 2.1.15. *Ako je $B = k(\alpha_1, \ldots, \alpha_n)$ konačno proširenje polja k, tada postoji konačno proširenje E/B koje je polje razlaganja proizvoljnog polinoma $f(x) \in k[x]$ (takvo proširenje s najmanjim stupnjem se naziva **normalan zatvarač** od B/k). Ako svaki α_i je separabilan nad k, onda možemo odabrati $f(x)$ tako da bude separabilan polinom.*

Dokaz. Po Teoremu 1.5.14(i), postoji ireducibilan polinom $p_i(x) = irr(\alpha_1, k)$ u $k[x]$, za svaki i, takav da $p_i(\alpha_i) = 0$, te polje razlaganja E od $f(x) = p_1(x) \cdots p_n(x)$ sadrži B. Ako je svaki α_i separabilan nad k, tada svaki $p_i(x)$ je separabilan polinom, pa je i $f(x)$ separabilan polinom.

□

2.2 Fundamentalni teorem Galoisove teorije

Definicija 2.2.1. *Ako je E polje i H podskup od Aut(E), tada* ***fiksno polje*** *od H je definirano s*

$$E^H = \{a \in E : \sigma(a) = a \text{ za sve } \sigma \in H\}.$$

Najvažniji primjer fiksnog polja E^H proizlazi kada je H podgrupa od $Aut(E)$, ali ćemo se susreti s primjerima u kojima je samo podskup.

Lako se vidi, ako je $\sigma \in Aut(E)$, onda je $E^\sigma = \{a \in E : \sigma(a) = a\}$ potpolje od E. Nadalje, slijedi da je E^H potpolje od E jer je

$$E^H = \bigcap_{\sigma \in H} E^\sigma.$$

$E = k(y_1, \ldots, y_n)$ smo promatrali kao polje racionalnih funkcija n varijabli s koeficijentima iz polja k, te pripadnim potpoljem $K = k(a_0, \cdots, a_{n-1})$ gdje je

$$f(x) = (x - y_1)(x - y_2)\cdots(x - y_n) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \tag{2.2}$$

općeniti polinom stupnja n nad k. E je polje razlaganja od $f(x)$ nad K, jer ga dobivamo dodavanjem svih nultočki od $f(x)$ u K, odnosno y-na. Simetrična grupa $S_n \leq Aut(E)$, jer svaka permutacija od $y_1, \ldots, y_n$ proširuje se do automorfizma od E, pa se dobije $K = E^{S_n}$. Elementi iz K se često nazivaju simetričnim funkcijama u n varijabli nad k.

Definicija 2.2.2. *Racionalna funkcija $g(x_1, \ldots, x_n)/h(x_1, \ldots, x_n) \in k(x_1, \ldots, x_n)$ je* ***simetrična funkcija*** *ako ostaje nepromijenjena permutacijom varijabli: Za svaki $\sigma \in S_n$, vrijedi $g(x_{\sigma 1}, \ldots, x_{\sigma n})/h(x_{\sigma 1}, \ldots, x_{\sigma n}) = g(x_1, \ldots, x_n)/h(x_1, \ldots, x_n)$.*

Propozicija 2.2.3. *Ako je E polje, onda funkcija $H \longmapsto E^H$, iz podskupa H od Aut(E) u potpolje E, je* ***silazna****: Ako je $H \leq L \leq Aut(E)$, onda je $E^L \subseteq E^H$.*

Dokaz. Ako je $a \in E^L$, onda $\sigma(a) = a$ za sve $\sigma \in L$. Budući da je $H \leq L$, slijedi $\sigma(a) = a$ za sve $\sigma \in H$. Stoga, $E^L \subseteq E^H$. □

Primjer 2.2.4. *Pretpostavimo da je k potpolje od E i $G = Gal(E/k)$. Očito je $k \subseteq E^G$, ali može biti i pravi podskup. Na primjer, neka je $E = \mathbb{Q}(\sqrt[3]{2})$. Ako je $\sigma \in G = Gal(E/\mathbb{Q})$, tada σ fiksira $\mathbb{Q}$, tj. permutira korijene od $f(x) = x^3 - 2$. Druga dva korijena $f(x)$ nisu realna, pa $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Iz Leme 2.1.5 slijedi da je σ identiteta, tj. $E^G = E$. Primjetimo da E nije polje razdjeljivanja od $f(x)$.*

Sljedeći cilj je odrediti stupanj $[E : E^G]$, gdje je $G \leq Aut(E)$. Prvo ćemo uvesti pojam karaktera.

Definicija 2.2.5. ***Karakter*** *grupe G u polju E je homorfizam (grupa) $\sigma : G \to E^\times$, gdje $E^\times$ označava multiplikativnu grupu nenul elemenata polja E.*

Ako je $\sigma \in Aut(E)$, onda restrikcija $\sigma|E^x : E^x \to E^x$ je karakter u E.

Definicija 2.2.6. *Neka je E polje i $G \leq Aut(E)$. Niz $\sigma_1, \cdots, \sigma_n$ karaktera iz G u E je* ***nezavisan*** *ako za proizvoljan izbor $c_1, \cdots, c_n \in E$ i za svaki $x \in G$ vrijedi*

$$\sum_i c_i \sigma_i(x) = 0,$$

tada $c_i = 0$ za sve i.

Propozicija 2.2.7 (**Dedekind**)**.** *Svaki niz $\sigma_1, \cdots, \sigma_n$ različitih karaktera iz grupe G u polju E je nezavisan.*

Dokaz. Tvrdnju ćemo dokazati indukcijom po $n \geq 1$. Dokažimo prvo bazu indukcije, tj. da tvrdnja vrijedi za $n = 1$. Ako je $c\sigma = 0$ za sve $x \in G$, tada je ili $c = 0$ ili $\sigma(x) = 0$. Znamo da $\sigma(x) \neq 0$ jer $Im(\sigma) \subseteq E^x$.

Pretpostavimo da za $n > 1$. Kada karakteri ne bi bili nezavisni, tada bi postojali $c_i \in E$, ne svi jednaki 0, takvi da zadovoljavaju

$$c_1\sigma_1(x) + \cdots + c_{n-1}\sigma_{n-1}(x) + c_n\sigma_n(x) = 0 \tag{2.3}$$

za sve $x \in G$. Možemo pretpostaviti da su svi $c_i \neq 0$, ili se možemo pozvati na induktivnu pretpostavku, te doći do kontradikcije, kako je i traženo. Množenjem s c_n^{-1} ako je potrebno, možemo pretpostaviti da $c_n = 1$. Budući da je $\sigma_n \neq \sigma_1$, postoji $y \in G$ takav da je $\sigma_1(y) \neq \sigma_n(y)$. U jednadžbi (2.3) zamijenimo x s yx, pa dobivamo

$$c_1\sigma_1(y)\sigma_1(x) + \cdots + c_{n-1}\sigma_{n-1}(y)\sigma_{n-1}(x) + \sigma_n(y)\sigma_n(x) = 0,$$

jer je $\sigma_i(yx) = \sigma_i(y)\sigma_i(x)$. Sada množenjem s $\sigma_n(y)^{-1}$ dobijemo jednadžbu

$$c_1\sigma_n(y)^{-1}\sigma_1(y)\sigma_1(x) + \cdots + c_{n-1}\sigma_n(y)^{-1}\sigma_{n-1}(y)\sigma_{n-1}(x) + \sigma_n(x) = 0.$$

Oduzmemo zadnju jednadžbu od jednadžbe (2.3) te dobijemo sumu od $n - 1$ članova

$$c_1[1 - \sigma_n(y)^{-1}\sigma_1(y)]\sigma_1(x) + c_2[1 - \sigma_n(y)^{-1}\sigma_2(y)]\sigma_2(x) + \cdots = 0.$$

Indukcijom dobijemo da svaki od članova $c_i[1 - \sigma_n(y)^{-1}\sigma_i(y)] = 0$. Sada $c_i \neq 0$, pa $\sigma_n(y)^{-1}\sigma_i(y) = 1$ za sve $i < n$. Posebno, $\sigma_n(y) = \sigma_1(y)$, što je u kontradikciji s definicijom od y.

□

Lema 2.2.8. *Ako je $G = \{\sigma_1, \ldots, \sigma_n\}$ skup od n različitih automorfizama polja E, tada vrijedi $[E{:}E^G] \geq n$.*

Dokaz. Pretpostavimo suprotno, neka je $[E : E^G] = r < n$, te neka je $\alpha_1, \ldots, \alpha_r$ baza od E/E^G. Promatramo homogen linearan sustav nad E od r jednadžbi s n nepoznanica:

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_1)x_n &= 0 \\ \sigma_1(\alpha_2)x_1 + \cdots + \sigma_n(\alpha_2)x_n &= 0 \\ \vdots \qquad \vdots \qquad & \vdots \\ \sigma_1(\alpha_r)x_1 + \cdots + \sigma_n(\alpha_r)x_n &= 0. \end{aligned}$$

Budući je $r < n$, imamo manji broj jednadžbi nego varijabli pa postoji netrivijalno riješenje $(c_1, \ldots, c_n)$ u E^n.

Sada ćemo pokazati da $\sigma_1(\beta)c_1 + \cdots + \sigma_n(\beta)c_n = 0$ za bilo koji $\beta \in E^x$, što je u kontradikciji s linearnom nezavisnosti karaktera $\sigma_1|E^\times, \ldots, \sigma_n|E^\times$. Budući je $\alpha_1, \ldots, \alpha_r$ baza od E nad E^G, svaki $\beta \in E$ se može zapisati

$$\beta = \sum_i b_i\alpha_i,$$

gdje je $b_i \in E^G$. Pomnožimo i-ti redak sustava s $\sigma_1(b_i)$ pa dobijemo sustav s i-tim retkom:

$$\sigma_1(b_i)\sigma_1(\alpha_i)c_1 + \cdots + \sigma_1(b_i)\sigma_n(\alpha_i)c_n = 0.$$

Ali, $\sigma_1(b_i) = b_i = \sigma_j(b_i)$ za sve i, j jer je $b_i \in E^G$. Sada i-ti red sustava izgleda:

$$\sigma_1(b_i\alpha_i)c_1 + \cdots + \sigma_n(b_i\alpha_i)c_n = 0.$$

Dodavanjem ostalih jednadžbi i-toj, dobijemo:

$$\sigma_1(\beta)c_1 + \cdots + \sigma_n(\beta)c_n = 0,$$

što je u kontradikciji s nezavisnosti karaktera $\sigma_1, \cdots, \sigma_n$. □

Propozicija 2.2.9. *Ako je $G = \{\sigma_1, \cdots, \sigma_n\}$ podgrupa Aut(E), tada vrijedi*

$$[E : E^G] = |G|. \tag{2.4}$$

Dokaz. Iz Leme 2.2.8 slijedi da je dovoljno dokazati $[E : E^G] \leq |G|$. Pretpostavimo suprotno, neka je $[E : E^G] > n$, te neka je $\{\omega_1, \cdots, \omega_{n+1}\}$ linearno nezavisan skup vektora u E nad E^G. Promatramo sustav od n jednadžbi s $n + 1$ nepoznanica:

$$\begin{aligned} \sigma_1(\omega_1)x_1 + \cdots + \sigma_1(\omega_{n+1})x_{n+1} &= 0 \\ \vdots \qquad \vdots \qquad & \vdots \\ \sigma_n(\omega_1)x_1 + \cdots + \sigma_n(\omega_{n+1})x_{n+1} &= 0. \end{aligned}$$

Tada postoji netrivijalno rješenje $(\alpha_1, \cdots, \alpha_{n+1})$ nad E, nastavljamo s normalizacijom. Izabrat ćemo rješenje $(\beta_1, \ldots, \beta_r, 0, \ldots, 0)$ gdje je r najmanji broj nenul komponenata (pod pretpostavkom da smo reindeksiranjem ω_i dobili niz u kojem nenul komponente dolaze prve). Primjetimo da $r \neq 1$, jer $\sigma_1(\omega_1)\beta_1 = 0$ povlači $\beta_1 = 0$. Množenjem s inverzom, možemo pretpostaviti da je $\beta_r = 1$. Nisu svi $\beta_i \in E^G$, jer bi u tom slučaju redak koji odgovara $\sigma = 1_E$ davao linearnu zavisnost skupa $\{\omega_1, \ldots, \omega_{n+1}\}$. Zadnja pretpostavka je da β_1 ne leži u E^G (možemo postići ako reindeksiramo ω_i). Dakle, postoji σ_k takav da je $\sigma_k(\beta_1) \neq \beta_1$. Budući da je $\beta_r = 1$, originalni sistem ima j-ti redak

$$\sigma_j(\omega_1)\beta_1 + \cdots + \sigma_j(\omega_{r-1})\beta_{r-1} + \sigma_j(\omega_r) = 0. \tag{2.5}$$

Djelujemo sa σ_k na sustav pa dobivamo

$$\sigma_k\sigma_j(\omega_1)\sigma_k(\beta_1) + \cdots + \sigma_k\sigma_j(\omega_{r-1})\sigma_k(\beta_{r-1}) + \sigma_k\sigma_j(\omega_r) = 0.$$

Budući da je G grupa, $\sigma_k\sigma_1, \cdots, \sigma_k\sigma_n$ je samo permutacija od $\sigma_1, \cdots, \sigma_n$. Ako stavimo da je $\sigma_k\sigma_j = \sigma_i$, sustav ima i-ti redak

$$\sigma_i(\omega_1)\sigma_k(\beta_1) + \cdots + \sigma_i(\omega_{r-1})\sigma_k(\beta_{r-1}) + \sigma_i(\omega_r) = 0$$

Oduzimamo i-ti redak iz jednadžbe (2.5) i dobivamo novi sustav s i-tim retkom:

$$\sigma_i(\omega_1)[\beta_1 - \sigma_k(\beta_1)] + \cdots + \sigma_i(\omega_{r-1})[\beta_{r-1} - \sigma_k(\beta_{r-1})] = 0.$$

Budući da je $\beta_1 - \sigma_k(\beta_1) \neq 0$, imamo netrivijalno rješenje početnog sustava u kojem ima manje od r nenul komponenata, što je kontradikcija s pretpostavkom.

□

Sljedeće tvrdnje su potrebne u dokazu fundamentalnog teorema Galoisove teorije.

Teorem 2.2.10. *Ako su G i H konačne podgrupe od $Aut(E)$ takve da je $E^G = E^H$, tada je $G = H$.*

Dokaz. Prvo treba pokazati za $\sigma \in Aut(E)$ da vrijedi: σ fiksira E^G ako i samo ako je $\sigma \in G$. Očigledno, σ fiksira E^G ako je $\sigma \in G$. Pretpostavimo suprotno, da σ fiksira E^G, ali $\sigma \notin G$. Ako je $|G| = n$, onda je

$$n = |G| = [E : E^G],$$

što slijedi iz Propozicije 2.2.9. Budući da σ fiksira E^G, slijedi $E^G \subseteq E^{G\cup\{\sigma\}}$. Po Propoziciji 2.2.3 znamo da vrijedi i obrnuta inkluzija, time dobivamo $E^G = E^{G\cup\{\sigma\}}$. Stoga, iz Leme 2.2.8.

$$n = [E : E^G] = [E : E^{G\cup\{\sigma\}}] \geq |G \cup \{\sigma\}| = n + 1,$$

što daje kontradikciju s $n \geq n + 1$.

Ako je $\sigma \in H$, tada σ fiksira $E^H = E^G$ pa je $\sigma \in G$, stoga $H \leq G$. Obratnu inkluziju dobijemo na isti način, pa slijedi $H = G$.

□

Sljedeći teorem daje karakterizaciju polja razlaganja.

Teorem 2.2.11. *Ako je E/k konačno proširenje sa Galoisovom grupom $G = Gal(E/k)$, onda su sljedeće tvrdnje ekvivalentne.*

(i) *E je polje razlaganja separabilnog polinoma $f[x] \in k[x]$*

(ii) $k = E^G$.

(iii) *Svaki ireducibilan $p(x) \in k[x]$ koji ima jednu nultočku u E je separabilan i razlaže se u $E[x]$.*

Dokaz. (i) $\Longrightarrow$ (ii) Iz tvrdnje (ii) Teorema 2.1.9, $|G| = Gal(E/k)$. Propozicija 2.2.9 daje $|G| = [E : E^G]$, stoga vrijedi

$$[E : k] = [E : E^G].$$

Budući da je $k \leq E^G$, slijedi $[E : k] = [E : E^G][E^G : k]$, pa je $[E^G : k] = 1$ i $k = E^G$.

(ii) $\Longrightarrow$ (iii) Neka je $p(x) \in k[x]$ ireducibilan polinom koji ima nultočku α u E, te neka su $\alpha_1, \ldots, \alpha_n$ različiti elementi skupa $\{\sigma(\alpha) : \sigma \in G\}$. Definiramo $g(x) \in E[x]$ s

$$g(x) = \prod (x - \alpha_i).$$

Sada svaki $\sigma \in G$ permutira α_i, tako da svaki σ fiksira svaki koeficijent od $g(x)$, tj. svaki koeficijent od $g(x)$ leži u $E^G = k$. Stoga je $g(x)$ polinom u $k[x]$ takav da su sve nultočke međusobno različite. Sada $p(x)$ i $g(x)$ imaju zajednički korijen u E, te njihov *nzd* u $E[x]$ nije 1. (tu fali Korolar 3.41). $p(x)$ je ireducibilan, pa mora dijeliti $g(x)$. Slijedi, $p(x)$ ima međusobno različite nultočke, što znači da je separabilan i razlaže se nad E.

(iii) $\Longrightarrow$ (i) Odaberimo $\alpha_1 \in E$ tako da $\alpha_1 \notin k$. Budući je E/k konačno proširenje, α_1 mora biti algebarski nad k. Neka je $p_1(x) = irr(\alpha_1, k) \in k[x]$ minimalan polinom. Po pretpostavci, $p_1(x)$ je separabilan polinom koji se razlaže nad E, te neka je $K_1 \subseteq E$ pripadno polje razlaganja. Ako je $K_1 = E$, dokaz je gotov. Inače, biramo $\alpha_2 \in E$ takav da $\alpha_2 \notin K_1$. Po pretpostavci, postoji separabilan ireducibilan polinom $p_2(x) \in k[x]$ čiji je korijen α_2. Neka je $K_2 \subseteq E$ polje razlaganja od $p_1(x)p_2(x)$, separabilnog polinoma. Ako je $K_2 = E$, dokaz je gotov. Inače, analogno nastavljamo s istom konstrukcijom. Proces se zaustavlja s $K_m = E$ za neki m jer je E/k konačno. Stoga, E je polje razlaganja separabilnog polinoma $p_1(x) \cdots p_m(x)$.

□

Definicija 2.2.12. *Proširenje polja E/k je **Galoisovo proširenje** ako zadovoljava jedan od ekvivalentnih uvjeta iz Teorema 2.2.11.*

Korolar 2.2.13. *Ako je E/k Galoisovo proširenje i ako je B **međupolje**, tj. B je potpolje takvo da $k \subseteq B \subseteq E$, onda je E/B Galoisovo proširenje.*

Dokaz. Znamo da je E polje razlaganja nekog separabilnog polinoma $f(x) \in k[x]$, odnosno $E = k(\alpha_1, \ldots, \alpha_n)$ gdje su $\alpha_1, \ldots, \alpha_n$ nultočke od $f(x)$. Budući je $k \subseteq B \subseteq E$, slijedi $f(x) \in B[x]$ i $E = B(\alpha_1, \ldots, \alpha_n)$ □

Elementarne simetrične funkcije u n varijabli su polinomi, za $j = 1, \ldots, n$, dane s

$$e_j(x_1, \ldots, x_n) = \sum_{i_1 < \cdots < i_j} x_{i_1} \ldots x_{i_j}.$$

Ako su $z_1, \ldots, z_n$ nultočke od $x^n + a_{n-1}x^{n-1} + \cdots + a_0$, onda $e_j(z_1, \ldots, z_n) = (-1)^j a_{n-j}$.

Teorem 2.2.14 (**Fundamentalni teorem simetričnih funkcija**)**.** *Neka je k polje. Svaka simetrična funkcija u $k(x_1, \ldots, x_n)$ je racionalna funkcija u elementarnim simetričnim funkcijama $e_1, \ldots, e_n$.*

Dokaz. Neka je F najmanje potpolje od $E = k(x_1, \ldots, x_n)$ koje sadrži elementarne simetrične funkcije. E je polje razlaganja općenitog polinoma $f(t)$ stupnja n:

$$f(t) = \prod_{i=1}^{n} (t - x_i).$$

Ako je $f(t)$ separabilan polinom, E/k je Galoisovo proširenje. Iz Leme 2.1.5. i Teorema 2.1.6. se lako može provjeriti da vrijedi $Gal(E/F) \cong S_n$. Iz Teorema 2.2.11 slijedi $E^{S_n} = F$. $\theta(x) = g(x_1, \ldots, x_n)/h(x_1, \ldots, x_n)$ leži u E^{S_n}, tj. ostaje nepromijenjena obzirom na permutaciju varijabli. Slijedi, $\theta(x)$ je simetrična funkcija.

□

Definicija 2.2.15. *Ako su A i B potpolja polja E, tada njihova **kompozicija**, oznaka $A \vee B$, je presjek svih potpolja od E koja sadrže $A \cup B$.*

Lako se vidi da je $A \vee B$ najmanje potpolje od E koje sadrži A i B. Na primjer, ako je E/k proširenje s međupoljima $A = k(\alpha_1, \ldots, \alpha_n)$ i $B = k(\beta_1, \ldots, \beta_m)$, tada njihova kompozicija je

$$k(\alpha_1, \ldots, \alpha_n) \vee k(\beta_1, \ldots, \beta_m) = k(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m).$$

Propozicija 2.2.16. (i) *Svako Galoisovo proširenje E/k je separabilno proširenje od k.*

(ii) *Ako je E/k algebarsko proširenje polja i $S \subseteq E$ je proizvoljan, moguće beskonačan, skup separabilnih elemenata, onda je $k(S)/k$ separabilno proširenje.*

(iii) *Neka je E/k algebarsko proširenje, gdje je k polje, te neka su B i C međupolja. Ako su B/k i C/k separabilna proširenja, onda njihova kompozicija $B \vee C$ je također separabilno proširenje od k.*

Dokaz. **(i)** Ako je $\beta \in E$, onda $p(x) = irr(\beta, k) \in k[x]$ je ireducibilan polinom u $k[x]$ koji ima nultočku u E. Iz Teorema 2.2.11 (iii), $p(x)$ je separabilan polinom (koji se razlaže u $E[x]$). Stoga, β je separabilan u k, te E/k je separabilno proširenje.

(ii) Prvo ćemo promatrati slučaj kada je S konačan. Tada je $B = k(\alpha_1, \ldots, \alpha_t)$ konačno proširenje, gdje je svaki α_i separabilan nad k. Iz Leme 2.1.14 (i), postoji proširenje E/B polje razlaganja nekog separabilnog polinoma $f(x) \in k[x]$. Dakle, E/k je Galoisovo proširenje po Teoremu 2.2.11 (i). Iz tvrdnje (i), E/k je separabilno proširenje, odnosno za svaki $\alpha \in E$, polinom $irr(\alpha, k)$ ima međusobno različite nultočke. Posebno, $irr(\alpha, k)$ ima međusobno različite nultočke za sve $\alpha \in B$, te B/k je separabilno proširenje.
Sada ćemo promatrati općeniti slučaj. Ako je $\alpha \in k(S)$, tada postoji konačno mnogo elemenata $\alpha_!, \ldots, \alpha_n \in S$ takvih da je $\alpha \in B = k(\alpha_1, \ldots, \alpha_n)$. Slijedi, B/k je separabilno proširenje, te α je separabilan nad k. Kako je α proizvoljan element iz $k(S)$, slijedi da je $k(S)/k$ separabilno proširenje.

(iii) Iskoristimo tvrdnju (ii) za podskup $S = B \cup C$, jer je $B \vee C = k(B \cup C)$.

□

Sljedeća propozicija određuje kada međupolje B daje Galoisovo proširenje.

Definicija 2.2.17. *Neka je E/k Galosiovo proširenje, ako je B međupolje, tada **konjugat** od B je međupolje oblika*

$$B^\sigma = \{\sigma(b) : b \in B\} \tag{2.6}$$

za neki $\sigma \in Gal(E/k)$.

Propozicija 2.2.18. *Neka je E/k Galoisovo proširenje. Međupolje B nema drugih konjugata osim samog sebe ako i samo ako je B/k Galosiovo proširenje.*

Dokaz. Pretpostavimo da je $B^\sigma = B$ za svaki $\sigma \in G$, gdje je $G = Gal(E/k)$. Neka je $p(x) \in k[x]$ ireducibilan polinom s nultočkom β u B. Budući da je $B \subseteq E$ i E/k je Galoisovo proširenje, $p(x)$ je separabilan polinom i razlaže se u $E[x]$. Ako je $\beta' \in E$ druga nultočka od $p(x)$, tada postoji izomorfizam $\sigma \in G$ takav da je $\sigma(\beta) = \beta'$ (G djeluje tranzitivno na nultočke ireducibilnog polinoma). Stoga, $\beta' = \sigma(\beta) \in B^\sigma = B$, te se $p(x)$ razlaže u $B[x]$. Dakle, B/k je Galoisovo proširenje.

Obrnuto, budući da je B/k polje razlaganja nekog polinom $f(x)$ nad k, imamo $B = k(\alpha_1, \ldots, \alpha_n)$, gdje su $\alpha_1, \ldots, \alpha_n$ sve nultočke od $f(x)$. Znamo da svaki $\sigma \in Gal(E/k)$ permutira nultočke od $f(x)$, pa slijedi da σ preslikava B u samog sebe. □

Sada ćemo pokazati da ako je E/k Galoisovo proširenje, onda su međupolja klasificirana podgrupama od $Gal(E/k)$. Počinjemo s definicijom.

Definicija 2.2.19. *Skup X je **parcijalno uređen skup** ako postoji binarna operacija $x \preccurlyeq y$ koja zadovoljava, za sve $x, y, z \in X$:*

(i) ***Refleksivnost:*** $x \preccurlyeq x$

(ii) ***Antisimetričnost:*** *Ako je $x \preccurlyeq y$ i $y \preccurlyeq x$, tada $x = z$.*

(iii) ***Tranzitivnost:*** *Ako je $x \preccurlyeq y$ i $y \preccurlyeq z$, tada $x \preccurlyeq z$.*

Element c u parcijalno uređenom skupu X je **gornja granica** od $a, b \in X$ ako je $a \preccurlyeq c$ i $b \preccurlyeq c$, dok je element $d \in X$ **najmanja gornja granica** od a, b ako je d je gornja granica i ako je $d \preccurlyeq c$ za sve gornje granice c od a i b. **Donja granica** i **najveća donja granica** se definiraju analogno, samo sa suprotnim nejednakostima.

Definicija 2.2.20. ***Rešetka*** *je parcijalno uređen skup $\mathcal{L}$ u kojem svaki par elemenata $a, b, \in \mathcal{L}$ ima najveću donju granicu $a \wedge b$, te najmanju gornju granicu $a \vee b$.*

Definicija 2.2.21. *Ako su $\mathcal{L}$ i $\mathcal{L}'$ rešetke, funkcija $f : \mathcal{L} \longrightarrow \mathcal{L}'$ je **padajuća (silazna)** ako za $a \preccurlyeq b$ u $\mathcal{L}$ vrijedi $f(b) \preccurlyeq f(a)$ u $\mathcal{L}'$.*

Lema 2.2.22. *Neka su $\mathcal{L}$ i $\mathcal{L}'$ rešetke, te neka je $\varphi : \mathcal{L} \longrightarrow \mathcal{L}'$ bijekcija takva da su φ i φ^{-1} silazne. Tada vrijedi*

$$\varphi(a \wedge b) = \varphi(a) \vee \varphi(b) \qquad i \qquad \varphi(a \vee b) = \varphi(a) \wedge \varphi(b).$$

Dokaz. Budući da su $a, b \preccurlyeq a \vee b$, imamo $\varphi(a \vee b) \preccurlyeq \varphi(a), \varphi(b)$. Tada je $\varphi(a \vee b)$ donja granica od $\varphi(a), \varphi(b)$, pa slijedi $\varphi(a \vee b) \preccurlyeq \varphi(a) \wedge \varphi(b)$.
Za obratnu nejednakost, surjektivnost od φ nam kaže da postoji $c \in \mathcal{L}$ takav da $\varphi(a) \wedge \varphi(b) = \varphi(c)$. Sada je $\varphi(c) = \varphi(a) \wedge \varphi(b) \preccurlyeq \varphi(a), \varphi(b)$. Djelovanjem φ^{-1}, koja je silazna funkcija, dobijemo $a, b \preccurlyeq c$. Stoga, c je gornja granica za a, b, pa $a \vee b \preccurlyeq c$. Dakle, $\varphi(a \vee b) \succcurlyeq \varphi(c) = \varphi(a) \wedge \varphi(b)$. Analogno se dokaže i druga tvrdnja. □

Teorem 2.2.23 (**Fundamentalni teorem Galoisove toerije**). *Neka je E/k konačno Galoisovo proširenje s Galoisovom grupom $G = Gal(E/k)$. Tada vrijedi:*

(i) *Funkcija $\gamma : Sub(Gal(E/k)) \longrightarrow Int(E/k)$, definirana s*

$$\gamma : H \longmapsto E^H,$$

je silazna bijekcija čiji inverz, $\delta : Int(E/k) \longrightarrow Sub(Gal(E/k))$, je silazna bijekcija definirana s

$$\delta : B \longmapsto Gal(E/B)$$

(ii) *Za svaki $B \in Int(E/k)$ i $H \in Sub(Gal(E/k))$ vrijedi*

$$E^{Gal(E/B)} = B \qquad i \qquad Gal(E/E^H) = H.$$

(iii) *Za svaki $H, K \in Sub(Gal(E/k))$ i $B, C \in Int(E/k)$, vrijedi*

$$\begin{aligned} E^{H\vee K} &= E^H \cap E^K, \\ E^{H\cap K} &= E^H \vee E^K, \\ Gal(E/(B \vee C)) &= Gal(E/B) \cap Gal(E/C), \\ Gal(E/(B \cap C)) &= Gal(E/B) \vee Gal(E/C). \end{aligned}$$

(iv) *Za svaki $B \in Int(E/k)$ i $H \in Sub(Gal(E/k))$, vrijedi*

$$[B : k] = [G : Gal(E/B)] \qquad i \qquad [G : H] = [E^H : k].$$

(v) *Ako je $B \in Int(E/k)$, tada je B/k Galoisovo proširenje ako i samo ako je $Gal(E/B)$ normalna podgrupa od G.*

Dokaz. **(i)** Propozicija 2.2.3 nam govori da je γ silazan, također se lako vidi da je δ silazan. Injektivnost od γ je dokazana u Teoremu 2.2.10. Da je γ bijekcija s inverzom δ, dovoljno je dokazati da je $\gamma\delta : Int(E/k) \longrightarrow Int(E/k)$ je identiteta. Ako je B međupolje, onda je $\gamma\delta : B \longmapsto E^{Gal(E/B)}$. Po Kororalu 2.2.13 E/E^B je Galoisovo proširenje, te po Teoremu 2.2.11 $E^{Gal(E/B)} = B$.

(ii) Tvrdnja govori da su $\gamma\delta$ i $\delta\gamma$ su funkcije identiteta, što smo dokazali kroz tvrdnju (i).

(iii) Tvrdnja slijedi iz Leme 2.2.22.

(iv) Po Teoremu 4.7 (ii) i činjenici da je E/B je Galoisovo proširenje, slijedi

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

Stupanj od B/k je indeks pripadne Galoisove grupe od G. Sljedeća tvrdnja slijedi iz prethodne, ako uzmemo $B = E^H$, te iz tvrdnje (ii) dobijemo $Gal(E/E^H) = H$

$$[E^H : k] = [G : Gal(E/E^H)] = [G : H].$$

(v) Iz Teorema 4.16. slijedi da je $Gal(E/B) \lhd G$ kada je B/k je Galoisovo proširenje (B/k i E/k su polja razlaganja polinoma iz $k[x]$).
Obrat, neka je $H = Gal(E/B)$, te neka je $H \lhd G$. Iz tvrdnje (ii), $E^H = E^{Gal(E/B)}$, slijedi da je dovoljno dokazati da je $(E^H)^\sigma = E^H$ za sve $\sigma \in G$, po Popoziciji 2.2.18. Pretpostavimo da je $a \in E^H$, tj. $\mu(a) = a$ za sve $\mu \in H$. Sada iz $H \lhd G$ znamo da je $\mu \in H$ i $\sigma \in G$, tada postoji $\mu' \in H$ takav da $\mu\sigma = \sigma\mu'$ ($\mu' = \sigma^{-1}\mu\sigma$). Slijedi

$$\mu\sigma(a) = \sigma\mu'(a) = \sigma(a),$$

jer je $\mu' = a$. Stoga, $B/k = E^H/k$ je Galoisovo proširenje.

□

Nadalje ćemo zapisati nekoliko korolara i teorema koji su posljedica Fundamentalnog teorema Galoisove teorije.

Teorem 2.2.24. *Ako je E/k Galoisovo proširenje čija Galoisova grupa je Abelova, tada svako međupolje je Galoisovo proširenje.*

Dokaz. Svaka podgrupa Abelove grupe je normalna podgrupa. □

Korolar 2.2.25. *Galoisovo proširenje E/k ima samo konačno mnogo međupolja.*

Dokaz. Konačna grupa $Gal(E/k)$ ima samo konačno mnogo podgrupa. □

Definicija 2.2.26. *Proširenje polja E/k je **jednostavno proširenje** ako postoji $u \in E$ takav da $E = k(u)$.*

Sljedeći teorem nam daje karakterizaciju jednostavnih proširenja.

Teorem 2.2.27 (Steinitz)**.** *Konačno proširenje E/k je jednostavno ako i samo ako ima konačno mnogo međupolja.*

Dokaz. Pretpostavimo da je E/k jednostavno proširenje, tako da $E = k(u)$. Neka je $p(x) = irr(u, k) \in k[x]$ pripadni minimalni polinom. Ako je B proizvoljno međupolje, neka je

$$q(x) = irr(u, B) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} + x^n \in B[x]$$

normiran ireducibilan polinom od u nad B, te definiramo

$$B' = k(b_0, \ldots, b_{n-1}) \subseteq B.$$

Primjetimo da je $q(x)$ ireducibilan polinom nad manjim poljem B'. Sada

$$E = k(u) \subseteq B'(u) \subseteq B(u) \subseteq E,$$

pa je $B'(u) = E = B(u)$. Stoga, $[E : B] = [B(u) : B]$ i $[E : B'] = [B'(u) : B']$. Budući da su oba jednaka $deg(q)$, vrijedi $[E : B] = deg(q) = [E : B']$. Znamo da je $B' \subseteq B$, slijedi $[B : B'] = 1$, tj.

$$B = B' = k(b_0, b_1, \ldots, b_{n-1}).$$

Karakterizirali smo B s koeficijentima $q(x)$, normiranog djelitelja $p(x) = irr(u, k)$ u $E[x]$. $p(x)$ ima samo konačno mnogo normiranih djelitelja, stoga ima samo konačno mnogo međupolja.
Obrnuto, pretpostavimo da E/k ima konačno mnogo međupolja. Ako je k konačno polje, tada znamo da je E/k jednostavno proširenje (uzmimo u kao primitivni element), dakle, možemo pretpostaviti da k nije konačno. Budući da je E/k konačno proširenje, tada postoje elementi $u_1, \ldots, u_n$ takvi da $E = k(u_1, \ldots, u_n)$. Indukcijom po $n \geqslant 1$, dovoljno je dokazati da je $E = k(a, b)$ jednostavno proširenje. Sada postoji beskonačno mnogo elemenata $c \in E$ oblika $c = a + tb$, gdje je $t \in k$, jer je k beskonačan. Budući da postoji konačno mnogo međupolja, stoga postoji konačno mnogo polja oblika $k(c)$. Po principu golubinjaka, koji kaže ako postoji beskonačno golubova u konačno mnogo golubinjaka, tada barem jedan golubinjak sadrži beskonačno mnogo golubova, postoje različiti elementi $t, t' \in k$ takvi da $k(c) = k(c')$ gdje je $c' = a + t'b$. Jasno je da $k(c) \subseteq k(a, b)$. Za obratnu inkluziju, polje $k(c) = k(c')$ sadrži $c - c' = (t - t')b$, tako da $b \in k(c)$ (zato jer $t - t' \neq 0$). Slijedi $a = c - tb \in k(c)$, te $k(c) = k(a, b)$. □

Bibliografija

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

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

Sažetak

Ovaj diplomski rad smo podijelili u dva dijela. U prvom dijelu smo dali kratki podsjetnik na teoriju grupa, Lagrangeov teorem, kvocijentne skupove, te komutativne prstene, polja razlomaka, te polinome. Uvodni nam je bio od velike važnosti kasnije za shvaćanje same Galoisove teorije. U drugom dijelu smo se upoznali s Galoisovom teorijom, čiji je originalni naziv teorija jednadžbi. Odmah na početku smo definirali Galoisovu grupu. Sama Galoisova teorija nam daje vezu između algebarskog proširenja E nad poljem k, te pripadne Galoisove grupe $Gal(E/k)$. Naveli smo nekoliko teorema o Galoisovim grupama čije tvrdnje kažu da su proširenja polja također i polja razlaganja nekog polinoma. Na samom kraju smo iskazali i dokazali Fundamentalni teorem Galoisove teorije, kao posljedicu cjelokupne analize drugog dijela. ◃

Summary

This thesis is divided into two parts. The first part was a brief reminder of the group theory, Lagrange's theorem, quotient groups, and commutative rings, fields fractions, and polynomials. The introductory part was of great importance for the understanding of Galois theory in the second part. In the second part, we got familiar with Galois theory, which original name was the theory of equations. Right at the beginning we defined the Galois group. Galois theory gives connection between algebraic extension E over the field k, and the corresponding Galois group $Gal(E/k)$. We stated some theorems about Galois groups which say that an exstension is a splitting field of a polynomial. At the very end we stated and proved of The fundamental theorem of Galois theory, as a result of the overall analysis of the second part.

Životopis

Rođena sam 04.12.1987. u Travniku, Bosna i Hrcegovina. Osnovnu školu sam završila 2002. u Novalji, te iste godine upisala opću gimnaziju u Pagu. Maturirala sam 2006, godine, te nakon mature upisala Preddiplomski sveučilišni studij Matematika na Prirodoslovno-matematičkom fakultetu. 2013. godine sam stekla titulu sveučilišne prvostupnice, i iste godine upisala diplomski studij Primijenjena matematika na istom fakultetu.