Galoisova grupa polinoma

Preselj, Ana

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Ana Preselj

Galoisova grupa polinoma

Završni rad

Osijek, 2018.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Ana Preselj

Galoisova grupa polinoma

Završni rad

Voditelj: izv. prof. dr. sc. Ivan Matić

Osijek, 2018.

Sadržaj

Sažetak: U ovom završnom radu bavit ćemo se proučavanjem Galoisove grupe polinoma. Pokazati ćemo kako se pronalazi Galoisova grupa određenih polinoma kroz mnoge primjere.

Ključne riječi: Galoisova grupa, polje cijepanja, polinom, Fundamentalni teorem Galoisove teorije, separabilan, ireducibilan, Eisensteineov kriterij

Abstract: In this final work, we will explain the Galois group of polynomial. We will show how to find the Galois group of some polynomials through many examples.

Key words: Galois group, splitting field, polynomial, Fundamental Theorem of Galois theory, separable, irreducible, Eisenstein's Criterion

Uvod

Evariste Galois (1811.-1832.) je bio francuski matematičar koji je uvelike doprinio razvoju algebre. Prvi je uveo pojam grupe, a nakon smrti dobiva priznanje za Galoisovu teoriju nazvanu po njemu.

Ključna ideja Galoisove teorije je povezati proširenje polja $K \subset F$ u grupu svih automorfizama F koji fiksiraju K (Galoisova grupa proširenja). Galoisovo proširenje polja K može se definirati u terminima njegove Galoisove grupe ili u smislu unutarnje strukture proširenja.

Fundamentalni teorem Galoisove teorije navodi da postoji jednoznačna korespondencija između međupolja Galoisovog proširenja (konačno dimenzionalno) i podgrupa Galoisove grupe proširenja. Taj teorem nam omogućuje da prenosimo svojstva i probleme koji uključuju polja, polinome i proširenja polja u pojmove teorije grupa.

Često odgovarajući problem u grupama ima rješenje, zbog čega se može riješiti izvorni problem u teoriji polja. Mi ćemo spominjati ona Galoisova proširenja polja čije su Galoisove grupe konačne cikličke ili rješive.

1. Galoisova grupa polinoma

Definicija 1.1. *Neka je K polje. Galoisova grupa polinoma $f \in K[x]$ nad poljem K je grupa $Aut_K F$, gdje je F polje cijepanja polinoma f nad poljem K.*

Galoisova grupa polinoma f ne ovisi o izboru polja F. Prije određenih primjera prvo ćemo navesti neke korisne činjenice. Kažemo da je podgrupa G simetrične grupe S_n tranzitivna ako za bilo koje $i \neq j$ $(1 \leq i, j \leq n)$, postoji $\sigma \in G$ takav da $\sigma(i) = j$.

Definicija 1.2. *K-automorfizam polja F je automorfizam $\sigma \in AutL$ koji je K-homomorfizam. Skup svih K-automorfizama polja F označavamo s $Aut_K F$ i nazivamo Galoisova grupa proširenja F polja K.*

Definicija 1.3. *Neka je F proširenje polja K tako da je fiksno polje Galoisove grupe $Aut_K F$ K. Tada se kaže da je F Galoisovo proširenje polja K ili Galoisovo nad K.*

Teorem 1.1. ***(Fundamentalni teorem Galoisove teorije)*** *Ako je F konačno dimenzionalno Galoisovo proširenje polja K, onda postoji jednoznačna korespondencija između skupa svih međupolja proširenja i skupa svih podgrupa Galoisove grupe $Aut_K F$ (određeno s $E \mapsto E' = Aut_E F$) tako da:*

(a) Relativna dimenzija dva međupolja jednaka je relativnom indeksu odgovarajuće podgrupe, $Aut_K F$ je reda [F:K].

(b) F je Galoisova nad svakim međupoljem E, ali E je Galoisova nad K ako i samo ako odgovarajuća podgrupa $E' = Aut_E F$ je normalna u $G = Aut_K F$. U tom slučaju je kvocijentna grupa G/E' (izomorfna) Galoisovoj grupi $Aut_K E$ od E nad K.

Teorem 1.2. *Neka je K polje i $f \in K[x]$ polinom s Galoisovom grupom G.*

(a) G je izomorfna podgrupi neke simetrične grupe S_n.

(b) Ako je f (iredubicilan) separabilan polinom stupnja n, onda n dijeli $|G|$ i G je izomorfna tranzitivnoj podgrupi od S_n.

Dokaz:

(a) Ako su $u_1, \ldots, u_n$ različite nultočke od f u nekom polju cijepanja F $(1 \leq n \leq \deg f)$, tada svaki $\sigma \in Aut_K F$ određuje jedinstvenu permutaciju $\{u_1, \ldots, u_n\}$ (ali ne nužno obratno!). Gledati ćemo S_n kao grupu svih permutacija $\{u_1, \ldots, u_n\}$ i provjeriti ćemo je li pridruživanje $\sigma \in Aut_K F$ permutaciji definirano kao monomorfizam $Aut_K F \longrightarrow S_n$ (primijetimo da je F=$K(u_1, \ldots, u_n)$.)

(b) F je Galoisova nad K i $[K(u_1) : K] = n$ =deg$f$. Stoga G ima podgrupu indeksa n prema Fundamentalnom teoremu Galoisove teorije odakle $n \mid |G|$. Za bilo koje $i \neq j$ imamo K-izomorfizam $\sigma : K(u_i) \cong K(u_j)$ takav da $\sigma(u_i) = u_j$. σ se proširuje do K-automorfizma od F, a G je izomorfna tranzitivnoj podgrupi od S_n. $\square$

U nastavku će se Galoisova grupa polinoma f često identificirati s izomorfnom podgrupom S_n i smatrati će se grupom permutacija nultočki od f. Nadalje, prvenstveno ćemo se baviti polinomima $f \in K[x]$ čije su nultočke različite u nekom polju cijepanja. Iz toga slijedi da su ireducibilni elementi separabilni. Polje cijepanja F polinoma f je Galoisovo nad poljem K. Ako se Galoisove grupe takvih polinoma uvijek mogu izračunati onda je moguće izračunati Galoisovu grupu bilo kojeg polinoma.

Korolar 1.1. *Neka je K polje i $f \in K[x]$ ireducibilan polinom drugog stupnja s Galoisovom grupom G. Ako je f separabilan (kao što je uvijek slučaj kada je karakteristika od K različita od 2), onda je $G \cong \mathbb{Z}_2$ inače G=1.*

Iz Teorema 1.2.(b) odmah dolazimo do činjenice da je Galoisova grupa separabilnih polinoma trećeg stupnja ili S_3 ili A_3 (jedina tranzitivna podgrupa od S_3). Kako bi dobili točniji rezultat, uvest ćemo općenitije razmatranje.

Definicija 1.4. *Neka je K polje karakteristike različite od 2 i $f \in K[x]$ polinom stupnja n sa n različitih nultočki $u_1, \dots, u_n$ u nekom polju cijepanja F polinoma f nad poljem K. Neka je*

$$\triangle = \prod_{i<j}(u_i - u_j) = (u_1 - u_2)(u_1 - u_3)\cdots(u_{n-1} - u_n) \in F;$$

diskriminanta od f je D=$\triangle^2$.

Primijetimo da je $\triangle$ element određenog polja cijepanja F, stoga *apriori* $D = \triangle^2$ je također u F.

Propozicija 1.1. *Neka su K, f, F i $\triangle$ kao u Definiciji* 1.4.

(a) Diskriminanta $\triangle^2$ od f zapravo leži u K.

(b) Za svaki $\sigma \in Aut_K F < S_n$, σ je parna (odnosno neparna) permutacija ako i samo ako je $\sigma(\triangle) = \triangle$ (odnosno $\sigma(\triangle) = -\triangle$)

Korolar 1.2. *Neka su K, f, F i $\triangle$ kao u Definiciji* 1.4. *(tako da je F Galoisovo nad poljem K) i gledati ćemo G=$Aut_K F$ kao podgrupu od S_n. U Galoisovoj teoriji potpolje $K(\triangle)$ odgovara podgrupi $G \cap A_n$. Konkretno, G se sastoji od parnih permutacija ako i samo ako $\sigma \in K$.*

Korolar 1.3. *Neka je K polje i $f \in K[x]$ (ireducibilan) separabilan polinom trećeg stupnja. Galoisova grupa od f je S_3 ili A_3. Ako je karateristika različita od 2, onda je Galoisova grupa od f A_3 ako i samo ako je diskriminanta od f kvadrat nekog elementa iz K.*

Ako je bazno polje K potpolje polja realnih brojeva, tada se diskriminanta polinoma trećeg stupnja $f \in K[x]$ može upotrijebiti da otkrijemo koliko realnih nultočki ima f.

Neka je f kao u Korolaru 1.3. Ako je Galoisova grupa od f $A_3 \cong \mathbb{Z}_3$, onda nema međupolja. Ako je riječ o S_3 onda postoje četiri odgovarajuća međupolja $K(\triangle), K(u_1), K(u_2)$ i $K(u_3)$ gdje su u_1, u_2 i u_3 nultočke od f. $K(\triangle)$ odgovara A_3, a $K(u_i)$ odgovara podgrupi $\{(1),(jk)\}(i \neq j,k)$ od S_3 koja je reda 2 i indeksa 3.

Osim u slučaju kada je karakteristika 2, računanje Galoisove grupe separabilnog polinoma trećeg stupnja se svodi na računanje diskriminante i određivanje da li je ona ili nije kvadrat u K. Sljedeća tvrdnja je ponekad korisna.

Propozicija 1.2. *Neka je K polje karakteristike različite od 2 i 3. Ako $f(x) = x^3 + bx^2 + cx + d \in K[x]$ ima tri različite nultočke u nekom polju cijepanja onda je polinom $g(x) = f(x - \frac{b}{3}) \in K[x]$ oblika $x^3 + px + q$ i diskriminanta od f je $-4p^3 - 27q^2$.*

Dokaz:

Neka je F polje cijepanja polinoma f nad poljem K i $u \in F$ je nultočka od f ako i samo ako je $u + \frac{b}{3}$ nultočka od $g = f(x - \frac{b}{3})$. Iz toga slijedi da g i f imaju istu diskriminantu. Provjerimo da je g oblika $x^3 + px + q$ $(p, q \in K)$. Neka su v_1, v_2 i v_3 nultočke od g u F. Onda je $(x - v_1)(x - v_2)(x - v_3) = g(x) = x^3 + px + q$ iz čega slijedi da je

$$v_1 + v_2 + v_3 = 0;$$

$$v_1v_2 + v_1v_3 + v_2v_3 = p;$$

$$-v_1v_2v_3 = q.$$

Budući da je svaki v_i nultočka od g

$$v_i^3 = -pv_i - q \qquad (i = 1, 2, 3).$$

Diskriminanta $\triangle^2$ od g je $-4p^3 - 27q^2$, a to slijedi iz definicije $\triangle^2 = (v_1 - v_2)^2(v_1 - v_3)^2(v_2 - v_3)^2$, gore navedene jednakosti i činjenice da je $(v_i - v_j)^2 = (v_i + v_j)^2 - 4v_iv_j$. $\square$

Primjer 1.1. *Polinom $x^3 - 3x + 1 \in \mathbb{Q}[x]$ je ireducibilan i separabilan jer je $\mathbb{Q}$ karakteristike nula. Diskriminanta je $-4(-3)^3 - 27(-1)^2 = 108 - 27 = 81$ što je kvadrat u $\mathbb{Q}$. Stoga je Galoisova grupa A_3 prema Korolaru 1.3.*

Primjer 1.2. *Ako je $f(x) = x^3 - 3x^2 - x - 1 \in \mathbb{Q}[x]$, onda je $g(x) = f(x - \frac{3}{3}) = f(x - 1) = x^3 - 4x + 2$, koji je ireducibilan po Eisensteinovom kriteriju. Prema Propoziciji 1.2. diskriminanta od f je $-4(-4)^3 - 27(2)^2 = 256 - 108 = 148$ što nije kvadrat u $\mathbb{Q}$. Stoga je Galoisova grupa S_3.*

Sada je vrijeme za polinome četvrtog stupnja nad poljem K. Kao u prethodnom primjeru, baviti ćemo se samo onima $f \in K[x]$ koji imaju različite nultočke u_1, u_2, u_3, u_4 u nekom polju cijepanja F. Prema tome, F je Galoisovo nad poljem K i Galoisova grupa od f može biti grupa permutacija u_1, u_2, u_3, u_4 i podgrupa od S_4. Podskup $V = \{(1), (12)(34), (13)(24), (14)(23)\}$ je normalna podgrupa od S_4, što će biti od velike važnosti u nastavku. Primijetimo da je V izomorfna grupi $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ i $V \cap G$ je normalna podgrupa od $G = Aut_K F < S_4$.

Lema 1.1. *Neka su K, f, F, u_i, V i $G = Aut_K F < S_4$ kao u prethodnom odjeljku. Ako je $\alpha = u_1u_2 + u_3u_4$, $\beta = u_1u_3 + u_2u_4$, $\gamma = u_1u_4 + u_2u_3$ onda potpolje $K(\alpha, \beta, \gamma)$ odgovara normalnoj podgrupi $V \cap G$. Stoga je $K(\alpha, \beta, \gamma)$ Galoisovo nad poljem K i $AutK_K(\alpha, \beta, \gamma) \cong G/(G \cap V)$.*

Dokaz:
Jasno je da svaki element u $G \cap V$ fiksira α, β, γ te stoga i $K(\alpha, \beta, \gamma)$. Kako bi se dovršio dokaz, dovoljno je, s obzirom na Fundamentalni teorem, pokazati da svaki element iz G, a ne iz V ne fiksira barem jedan od elemenata α, β, γ. Na primjer, ako je $\sigma = (12) \in G$ i $\sigma(\beta) = \beta$, onda $u_2u_3 + u_1u_4 = u_1u_3 + u_2u_4$ i $u_2(u_3 - u_4) = u_1(u_3 - u_4)$. Stoga, $u_1 = u_2$ ili $u_3 = u_4$, bilo koji od ovih slučajeva vodi na kontradikciju. Dakle $\sigma(\beta) \neq \beta$. Ostale mogućnosti dobijemo na sličan način. Umjesto provjere svih 20 mogućnosti, dovoljno je uzeti u obzir samo jednog predstavnika iz svakog člana od V u S_4. □

Neka su K, f, F, u_i i α, β, γ definirani kao u Lemi 1.1. Elementi α, β, γ imaju ključnu ulogu u određivanju Galoisove grupe proizvoljnih polinoma četvrtog stupnja. Polinom $(x - \alpha)(x - \beta)(x - \gamma) \in K(\alpha, \beta, \gamma)$ naziva se rastav polinoma trećeg stupnja f. To je zapravo polinom nad poljem K.

Lema 1.2. *Ako je F polje i $f = x^4 + bx^3 + cx^2 + dx + e \in K[x]$ onda je rastav polinoma trećeg stupnja f polinom $x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2 \in K[x]$*

Dokaz:
Neka f ima nultočke $u_1, \ldots, u_4$ u nekom polju cijepanja F. Zatim iz $f = (x-u_1)(x-u_2)(x-u_3)(x - u_4)$ izrazimo b, c, d i e u terminima u_i. Proširimo rastav polinoma trećeg stupnja $(x - \alpha)(x - \beta)(x - \gamma)$ i trebamo naći odgovarajuće supstitucije koristeći definiciju od α, β, γ (Lema 1.1.) i ranije dobivene izraze za b, c, d i e. □

Sada smo u situaciji da izračunamo Galoisovu grupu bilo kojeg (ireducibilnog) separabilnog polinoma $f \in K[x]$ četvrtog stupnja. Budući da je Galoisova grupa G tranzitivna podgrupa od S_4 čiji je red djeljiv s 4 (Teorem 1.2.), G je reda 24, 12, 8 ili 4. Provjerimo da su jedine tranzitivne podgrupe reda 24, 12 i 4 zapravo $S_4, A_4, V(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2)$ i različite cikličke podgrupe reda 4 generirane s 4-ciklusom. Jedna tranzitivna podgrupa od S_4 reda 8 je diedralna grupa D_4 reda 8 dobivena pomoću (1234) i (24). Budući da D_4 nije normalna u S_4 i da je svaka podgrupa reda 8 Sylowljeva 2-podgrupa, iz drugog i trećeg Sylowljevog teorema slijedi da S_4 ima 3 podgrupe reda 8, a svaka je izomorfna D_4.

Propozicija 1.3. *Neka je K polje i $f \in K[x]$ (ireducibilan) separabilan polinom četvrtog stupnja s Galoisovom grupom G (smatra se podgrupom od S_4). Neka su α, β, γ nultočke kubnog polinoma f u nekom polju cijepanja i neka je m=[K(α, β, γ):K]. Tada je:*

(a) *m=6 $\Leftrightarrow$ G=S_4;*

(b) *m=3 $\Leftrightarrow$ G=A_4;*

(c) *m=1 $\Leftrightarrow$ G=V;*

(d) *m=2 $\Leftrightarrow$ $G \cong D_4$ ili $G \cong \mathbb{Z}_4$; u slučaju $G \cong D_4$, f je ireducibilan nad K(α, β, γ), a $G \cong \mathbb{Z}_4$ inače.*

Dokaz:

Budući da je $K(\alpha, \beta, \gamma)$ polje cijepanja kubnog polinoma nad K, jedine mogućnosti za m su 1, 2, 3 i 6. S obzirom na to i argument koji prethodi teoremu, dovoljno je dokazati samo implikacije $\Leftarrow$ u svakom od slučajeva. Koristimo činjenicu da je $m = [K(\alpha, \beta, \gamma) : K] = \mid G/G \cap V \mid$ prema Lemi 1.1. Ako je $G = A_4$, onda je $G \cap V = V$ i $m = \mid G/V \mid = \mid G \mid / \mid V \mid = 3$. Slično, ako je $G = S_4$, onda je $m = 6$. Ako je $G = V$, onda je $G \cap V = G$ i $m = \mid G/G \mid = 1$. Ako je $G \cong D_4$, onda je $G \cap V = V$ budući da je V sadržan u svakoj Sylowljevoj 2-podgrupi od S_4 i $m = \mid G/V \mid = \mid G \mid / \mid V \mid = 2$. Ako je G ciklička grupa reda 4, onda je G generirana s 4-ciklusom čiji kvadrat mora biti u V tako da $\mid G \cap V \mid = 2$ i $m = \mid G/G \cap V \mid = \mid G \mid / \mid G \cap V \mid = 2$. Budući da je f ireducibilan ili reducibilan i $D_4 \not\cong \mathbb{Z}_4$, dovoljno je dokazati da posljednja tvrdnja ne vrijedi. Neka su u_1, u_2, u_3, u_4 nultočke od f u nekom polju cijepanja F i pretpostavimo $G \cong D_4$, tako da $G \cap V = V$. Budući da je V tranzitivna podgrupa i $G \cap V = Aut_{K(\alpha,\beta,\gamma)}F$ (Lema 1.1.), postoji za svaki par $i \neq j$ $(1 \leq i, j \leq 4)$, a $\sigma \in G \cap V$ što inducira izomorfizam $K(\alpha, \beta, \gamma)(u_i) \cong K(\alpha, \beta, \gamma)(u_j)$ tako da $\sigma(u_i) = u_j$ i $\sigma \mid K(\alpha, \beta, \gamma)$ je identiteta. Prema tome, za svaki $i \neq j$, u_i i u_j su nultočke istog ireducibilnog polinoma nad $K(\alpha, \beta, \gamma)$. Slijedi da je f ireducibilan nad $K(\alpha, \beta, \gamma)$. S druge strane, ako je $G \cong \mathbb{Z}_4$, onda je $G \cap V = Aut_{K(\alpha,\beta,\gamma)}F$ reda 2 i nije trazitivna. Stoga za neke $i \neq j$ ne postoji $\sigma \in G \cap V$ tako da je $\sigma(u_i) = u_j$. Budući da je F polje cijepanja nad $K(\alpha, \beta, \gamma)(u_i)$ i $K(\alpha, \beta, \gamma)(u_j)$, ako postoji izomorfizam $K(\alpha, \beta, \gamma)(u_i) \cong K(\alpha, \beta, \gamma)(u_j)$, koji je identiteta na $K(\alpha, \beta, \gamma)$ i šalje u_i u u_j, to bi bila restrikcija nekih $\sigma \in Aut_K(\alpha, \beta, \gamma)F = G \cap V$. Dakle, ne postoji takav izomorfizam, odakle slijedi u_i i u_j ne mogu biti nultočke istog ireducibilnog polinoma nad $K(\alpha, \beta, \gamma)$. Prema tome, f mora biti reducibilan nad $K(\alpha, \beta, \gamma)$. $\square$

Primjer 1.3. *Polinom $f = x^4 + 4x^2 + 2 \in \mathbb{Q}[x]$ je ireducibilan prema Eisensteineovom kriteriju; f je separabilan budući da je $\mathbb{Q}$ karakteristike nula. Koristeći Lemu* 1.2. *dobivamo da je rastav polinoma trećeg stupnja $x^3 - 4x^2 - 8x + 32 = (x-4)(x^2-8)$ tako da je $\alpha = 4$, $\beta = \sqrt{8}$, $\gamma = -\sqrt{8}$ i $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\sqrt{8}) = \mathbb{Q}(2\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ je proširenje od $\mathbb{Q}$ stupnja* 2. *Dakle Galoisova grupa je (izomorfna) D_4 ili $\mathbb{Z}_4$. Supstitucija $z = x^2$ reducira f do z^2+4z+2, lako vidimo da su rješenja $z = -2 \pm \sqrt{2}$; tako da su rješenja od f $x = \pm\sqrt{z} = \pm\sqrt{-2 \pm \sqrt{2}}$. Dakle $f = (x - \sqrt{-2+\sqrt{2}})(x + \sqrt{-2+\sqrt{2}})(x - \sqrt{-2-\sqrt{2}})(x + \sqrt{-2-\sqrt{2}}) = (x^2 - (-2 + \sqrt{2})(x^2 - (-2-\sqrt{2})) \in \mathbb{Q}(\sqrt{2})[x]$.*
Dakle f je reducibilan nad $\mathbb{Q}(\sqrt{2})$ i stoga je Galoisova grupa ciklička reda 4 *prema Propoziciji* 1.3.*(d).*

Primjer 1.4. *Da bi našli Galoisovu grupu polinoma $f = x^4 - 10x^2 + 4 \in \mathbb{Q}[x]$ prvo moramo provjeriti da je f ireducibilan (i stoga i separabilan). Sada f nema nultočaka u $\mathbb{Q}$ i tako nema ni linearnih ili kubičnih faktora. Provjerom pokažimo da f nema kvadratnih faktora u $\mathbb{Z}[x]$. Lako je provjeriti da ne postoje brojevi a,b,c,d takvi da je $f = (x^2 + ax + b)(x^2 + cx + d)$. Tako da je f ireducibilan u $\mathbb{Q}[x]$. Rastav polinoma trećeg stupnja f je $x^3 + 10x^2 - 16x - 160 = (x + 10)(x + 4)(x - 4)$, od kojeg su sva rješenja u $\mathbb{Q}$. Stoga, $m = [\mathbb{Q}(\alpha, \beta, \gamma) : \mathbb{Q}] = 1$ i Galoisova grupa od f je $V(\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2)$ prema Propoziciji* 1.3.

Primjer 1.5. *Polinom $x^4 - 2 \in \mathbb{Q}[x]$ je ireducibilan (i separabilan) prema Eisensteineovom kriteriju. Rastav polinoma trećeg stupnja $x^3 + 8x = x(x + 2\sqrt{2i})(x - 2\sqrt{2i})$ i $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\sqrt{2i})$ je proširenje od $\mathbb{Q}$ stupnja 2. Provjerimo da je $x^4 - 2$ ireducibilan nad $\mathbb{Q}(\sqrt{2i})$ (jer $\sqrt{2}$ i $\sqrt[4]{2} \notin \mathbb{Q}(\sqrt{2i})$). Stoga je Galoisova grupa izomorfna diedralnoj grupi D_4 prema Propoziciji* 1.3.

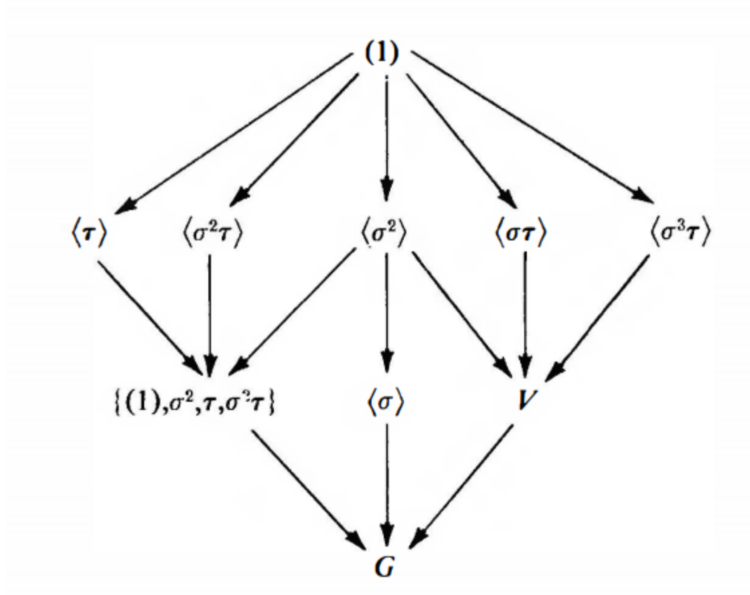
Primjer 1.6. *Promatramo polinom $f = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$. Polinom f je reducibilan nad $\mathbb{Q}$, to jest $f = (x^2 - 2)(x^2 - 3)$. Dakle, Propozicija* 1.3. *ovdje nije primjenjiva. Jasno je da je $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ polje cijepanja polinoma f nad poljem $\mathbb{Q}$ i pošto je f reducibilan nad $\mathbb{Q}(\sqrt{2})$, $[F : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$. Dakle $Aut_{\mathbb{Q}}F$, Galoisova grupa polinoma f je reda 4 prema Fundamentalnom teoremu. Iz dokaza Teorema* 1.2. *i Korolara* 1.1. *slijedi da se $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{2})$ sastoji od dva elementa: neutralni element 1 i σ kao $\sigma(\sqrt{2}) = -\sqrt{2}$. 1 i σ se protežu na $\mathbb{Q}$-automorfizam od F na dva različita načina (ovisno o tome $\sqrt{3} \mapsto \sqrt{3}$ ili $\sqrt{3} \mapsto -\sqrt{3}$). To nam daje četiri različita elementa $Aut_{\mathbb{Q}}F$ (određena pomoću četiri moguće kombinacije: $\sqrt{2} \mapsto \pm\sqrt{2}$ i $\sqrt{3} \mapsto \pm\sqrt{3}$). Budući da je $\mid Aut_{\mathbb{Q}}F \mid = 4$ i svaki od tih automorfizama je reda 2, Galoisova grupa f mora biti izomorfna grupi $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Određivanje međupolja i odgovarajućih podgrupa Galoisove grupe separabilnog polinoma četvrtog stupnja složenije je nego raditi isto to za separabilni polinom trećeg stupnja. Između ostalog može vrijediti $K(u_i) = K(u_j)$, iako je $u_i \neq u_j$ (pogledati prethodni primjer). Ne postoji lagan način za određivanje Galoisove grupe polinoma četvrtog stupnja.*

Primjer 1.7. *Neka je $F \subset \mathbb{C}$ polje cijepanja polinoma $f = x^4 - 2 \in \mathbb{Q}[x]$ nad $\mathbb{Q}$. Ako je u pozitivan realni četvrti korijen od 2, onda su nultočke od f: u, -u, ui, -ui. Da bismo razmatrali Galoisovu grupu $G = Aut_{\mathbb{Q}}F$ od f kao podgrupu S_4, moramo odabrati redoslijed nultočki, recimo $u_1 = u$, $u_2 = -u$, $u_3 = ui$, $u_4 = -ui$. Znamo iz Primjera* 1.5. *da je G jedna od tri podgrupe reda 8 u S_4, od kojih je svaka izomorfna diedralnoj grupi D_4. Uočimo da je kompleksno konjugiranje R-automorfizam od $\mathbb{C}$ koji preslikava $u \mapsto u$, $-u \mapsto -u$, $ui \mapsto -ui$ i $-ui \mapsto ui$. Prema tome, kompleksno konjugiranje inducira $\mathbb{Q}$-automorfizam τ od $F{=}\mathbb{Q}(u, ui)$. Jedan element od S_4 je $\tau = (34)$. Svaka podgrupa reda 8 u S_4 je konjugirana s D_4 (Drugi Sylowljev teorem) i jednostavan račun pokazuje da je jedina koja sadrži* (34)*, podgrupa D generirana s $\sigma = (1324)$ i $\tau = (34)$. Lako je vidjeti da vrijedi $F{=}\mathbb{Q}(u, ui) = \mathbb{Q}(u, i)$, tako da je svaki $\mathbb{Q}$-automorfizam od F potpuno određen svojim djelovanjem na u i na i. Tako se elementi od D mogu opisati ili terminima σ i τ ili njihovim djelovanjem na u i na i. Te informacije su sažete u tablici.*

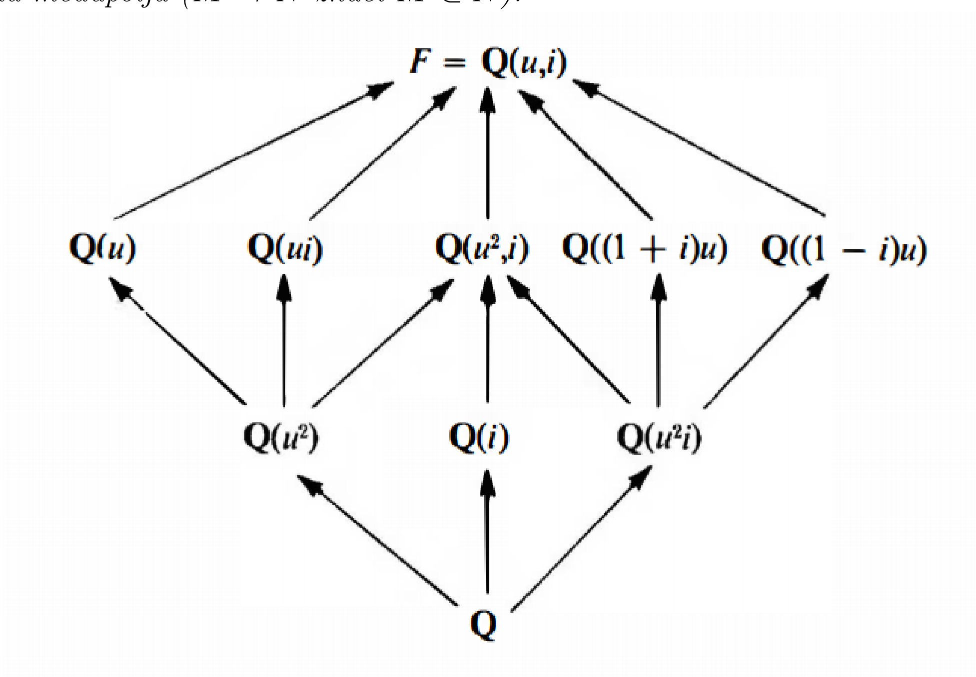
	(1)	(34) τ	(1324) σ	(12)(34) σ^2	(1423) σ^3	(13)(24) $\sigma\tau$	(12) $\sigma^2\tau$	(14)(23) $\sigma^3\tau$
$u \mapsto$	u	u	ui	$-u$	$-ui$	ui	$-u$	$-ui$
$i \mapsto$	i	$-i$	i	i	i	$-i$	$-i$	$-i$

Može se vidjeti da je odnos podgrupa od D i odnos međupolja dan idućim prikazima, pri čemu je:

Podgrupa rešetke ($H \to K$ znači $H < K$):



Rešetka međupolja ($M \to N$ znači $M \subset N$):



Posebne tehnike za računanje Galoisove grupe polinoma stupnja većeg od 4 nad proizvoljnim poljima su prilično rijetke.

Teorem 1.3. *Ako je p prost broj i f ireducibilan polinom stupnja p nad poljem racionalnih brojeva koji ima dvije ne čisto realne nultočke u polju kompleksnih brojeva, onda je Galoisova grupa polinoma f (izomorfna) S_p.*

Dokaz:
Promatrajmo Galoisovu grupu G polinoma f kao podgrupu od S_p. Budući da $p \mid\mid G \mid$ (Teorem 1.2.), G sadrži element σ reda p prema Cauchyjevom teoremu. Kompleksno konjugiranje $(a + bi \mapsto a - bi)$ je $\mathbb{R}$-automorfizam od $\mathbb{C}$ koji fiksira sve realne brojeve. To znači da G sadrži transpoziciju $\tau = (ab)$. Budući da σ možemo zapisati u obliku $\sigma = (aj_2 \cdots j_p)$, neki σ su oblika $\sigma^k = (abi_3 \cdots i_p) \in G$. Promjenom notacije, možemo pretpostaviti $\tau = (12)$ i $\sigma^k = (123 \cdots p)$. Ova dva elementa generiraju S_p. Stoga $G \equiv S_p$. □

Primjer 1.8. *Iz grafa polinoma $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ može se vidjeti da taj polinom ima samo tri realne nultočke. Polinom f je ireducibilan prema Eisensteineovom kriteriju i njegova Galoisova grupa je S_5.*

Još uvijek je otvoreno pitanje postoji li ili ne, Galoisovo proširenje polja $\mathbb{Q}$ s Galoisovom grupom G, za svaku konačnu grupu G. Ako je $G = S_n$, odgovor je potvrdan.

Literatura

[1] Thomas W. Hungerford, *Algebra*, Springer-Verlag New York, 1974.

[2] Hrvoje Kraljević, *Algebra*, Odjel za matematiku, 2007.