Математичка гимназија

Матурски рад
из математике

Увод у теорију Галоа

Ученик
Данило Ранђеловић, IVц

Ментор
др Лука Милићевић

Београд, *27. мај 2024.*

Садржај

1

Увод

Проблем решавања полиномских једначина је највероватније стар колико и сама математика. Све до 19. века, главна тема изучавања алгебре су управо биле полиномске једначине са рационалним коефицијентима. Природно се поставило следеће питање:

Под којим условима се корени произвољне полиномске једначине са рационалним коефицијентима могу представити као алгебарски израз њених коефицијената?

Квадратна формула је позната још од античких времена, а постојање експлицитних формула за нуле полинома степена три и четири је оправдано радом италијанског математичара Лодовика Ферарија и његовог ментора Ђиролама Кардана у књизи *Ars Magna* из 1545. године.

Француски математичар Еварист Галоа је у 19. веку самостално развио алат којим је питање решивости полинома свео на питање решивости група. У овом раду биће речи о напреднијим концептима теорије група и теорије поља са којима се ученици највероватније нису сусрели у оквиру наставе линеарне алгебре, али и о самој теорији Галоа, која успоставља природну везу између поменутих области. Експлоатисаћемо групе симетрија између решења полиномских једначина, а својства тих симетрија ће нам помоћи да боље разумемо природу самих полинома. На крају, даћемо једноставан пример полинома степена 5 чије нуле **не можемо** записати у облику алгебарског израза. Циљ овог рада је да подстакне заинтересоване ученике да истраже нешто о овој теми, служећи се овим радом као сажетим уводом, а касније и као подсетником.

Желео бих да се захвалим свом ментору, др Луки Милићевићу, на конструктивним саветима и пруженој помоћи током израде овог рада.

2

Теорија група

2.1 Уводни појмови

Шта значи да је група *решива*?

Пре него што кренемо да се бавимо главним тврђењем, доказаћемо неколико кључних резултата из теорије група који ће нам помоћи у раду, а успут и мотивисати Галоаов приступ. Бавићемо се искључиво коначним групама, а симбол операције групе ћемо изостављати.

Подсетимо се дефиниције групе:

Дефиниција 2.1. *Група* је скуп G са операцијом $*$ која задовољава следеће аксиоме:

- $(\forall\, x, y \in G)\ x * y \in G$ (*затвореност*)
- $(\forall\, x, y, z \in G)\ x * (y * z) = (x * y) * z$ (*асоцијативност*)
- $(\exists\, e \in G)(\forall\, x \in G)\ e * x = x * e = x$ (*постојање неутралног елемента*)
- $(\forall\, x \in G)(\exists x^{-1} \in G)\ x * x^{-1} = x^{-1} * x = e$ (*постојање инверзног елемента*)

Уколико је операција групе комутативна, тада је група *Абелова*. Ред групе G, у ознаци $|G|$, је број њених елемената.

Дефиниција 2.2. Нека је G група и $H \subseteq G$. Уколико је H такође група, кажемо да је H *подгрупа* групе G, у ознаци $H \leqslant G$.

Подсетимо се да Лагранжова теорема тврди да ред подгрупе дели ред групе. Увешћемо неколико појмова који ће оправдати ову теорему, а успут и доказати тврђења која су неопходна за наставак.

Дефиниција 2.3. Нека је G група и нека је H њена подгрупа. За $g \in G$, скупове

$$gH = \{gh \mid h \in H\}$$
$$Hg = \{hg \mid h \in H\}$$

редом зовемо *леви* и *десни косет* подгрупе H у групи G. Специјално, за $h \in H$ важи $hH = Hh = H$.

Лема 2.4. *Нека је $H \leqslant G$. Тада су различити леви косети групе H дисјунктни.*

Доказ. Претпоставимо да је скуп $aH \cap bH$ непразан. Тада постоје h_1,$h_2 \in H$ такви да важи $ah_1 = bh_2$. Сада је $bH = (ah_1{h_2}^{-1})H = a(h_1{h_2}^{-1}H) = aH$. □

Последица 2.5. Фиксирајмо $H \leqslant G$ и $a \in G$. Тада $aH = bH$ ако и само ако $b \in aH$.

Лагранжова теорема нам говори да је број различитих левих косета подгрупе H у групи G управо $\frac{|G|}{|H|}$. Инспирисани овим, постављамо следеће питање:

Да ли можемо успоставити неку структуру над косетима, тако да дељење групе њеном подгрупом добије смисао?

Испоставља се да је одговор потврдан!

Дефиниција 2.6. Нека је G група и N нека њена подгрупа. Уколико је једнакост $gN = Ng$ задовољена за свако $g \in G$, кажемо да је N *нормална подгрупа* групе G у ознаци $N \trianglelefteq G$. Специјално, $\{e\}$ и G су *тривијалне* нормалне подгрупе G.

Дефиниција 2.7. Нека је $N \trianglelefteq G$. *Количничку групу* G/N (читамо G *mod* N) чини скуп левих косета групе N у групи G, заједно са операцијом $\circ$ дефинисаном са

$$(gN) \circ (hN) = (gh)N$$

за g,$h \in G$.

Зашто је битно да је N баш *нормална* подгрупа G?

Фиксирајмо косете gN и hN. Одаберимо по један произвољан елемент косета gN и hN; нека су то g_1 и h_1. Јасно је да важи

$$g_1h_1N = (g_1N) \circ (h_1N) = (gN) \circ (hN) = ghN$$

Због чега смо сигурни да ова једнакост уопште могућа? Одговор нам даје следеће тврђење:

Тврдња 2.8. *Операција $\circ$ дата у претходној дефиницији је добро дефинисана ако и само ако је N нормална подгрупа G.*

Доказ. Нека је $N \trianglelefteq G$ и притом фиксирајмо $g,h \in G$. Доказаћемо да важи $abN = ghN$ за произвољне $a \in gN$ и $b \in hN$, одакле ће следити један смер тврђења. Постоје $n_1,n_2 \in N$ такви да $a = gn_1$ и $b = hn_2$. Сада је

$$abN = gn_1hn_2N = gn_1hN = gn_1Nh = gNh = ghN$$

Докажимо сада други смер; претпоставимо да је операција заиста добро дефинисана. Фиксирајмо произвољне $g \in G$ и $n \in N$. Важи

$$gN = (eg)N = (eN) \circ (gN) = (N) \circ (gN) = (nN) \circ (gN) = (ng)N$$

Одавде видимо $N = g^{-1}ngN$. Ово је еквивалентно томе да $g^{-1}ng \in N$, одакле N мора бити нормална подгрупа G. □

2.2 Композициони низови

Рецимо да су нам дате групе H и A.

На који начин бисмо пронашли **све** групе G такве да је H нормална подгрупа G, и да је A управо количник G/H? Овај проблем је познат као *екстензиони проблем* (или *проблем проширења*) у теорији група; решење овог проблема би довело до класификације **свих** коначних група. Сам проблем проширења група излази из опсега овог рада, али користићемо приступ сличан поставци проблема.

Кренимо од произвољне коначне групе G. Узмимо неку њену нормалну подгрупу N, а затим и нормалну подгрупу групе N, и тако даље. Под условом да смо избегавали тривијалне нормалне подгрупе, овај поступак ће се завршити у коначно много корака.

Добијени низ нормалних подгрупа се назива *нормални низ* групе G, а ми ћемо посматрати један специјалан тип нормалног низа. Испоставља се да су својства количника суседних чланова нормалног низа један од кључних детаља Галоаове теореме.

Дефиниција 2.9. Коначна група G је *проста* ако и само ако нема нетривијалне нормалне подгрупе.

Дефиниција 2.10. Нека је G коначна група. Низ група $H_0, H_1 \ldots, H_n$ такав да важи

$$\{e\} = H_n \triangleleft H_{n-1} \triangleleft \cdots \triangleleft H_1 \triangleleft H_0 = G$$

и притом да је свака од количничких група H_k/H_{k+1} (за $k = 0, 1, \ldots, n-1$) проста, назива се *композициони низ* групе G. Тада поменуте количничке групе називамо *композиционим факторима*.

Тврдња 2.11. Свака коначна група има композициони низ.

Доказ. Доказ спроводимо индукцијом по $n = |G|$.

Уколико је $n = 1$ или је G проста, тврђење је тривијално; наиме, G је једини члан композиционог низа. Надаље, нека G није проста, а самим тим и нека је $n > 1$.

За $n > 1$, нека је N *максимална* нетривијална нормална подгрупа G. Како је $|N| < |G|$, по индуктивној хипотези N има композициони низ

$$\{e\} = H_k \triangleleft H_{k-1} \triangleleft \cdots \triangleleft H_1 \triangleleft H_0 = N$$

Сада G има композициони низ

$$\{e\} = H_k \triangleleft H_{k-1} \triangleleft \cdots \triangleleft H_1 \triangleleft H_0 = N \triangleleft G$$

□

Примедба 2.12. Група N је *максимална* нормална подгрупа G ако је G/N проста. Приметимо да не мора бити јединствена.

Подсећамо се појма изоморфизма између две групе.

Дефиниција 2.13. Нека су A и B две групе. *Изоморфизам* је бијективно пресликавање $\varphi : A \to B$ које чува структуру групе. Другим речима, φ задовољава

$$\varphi(ab) = \varphi(a)\varphi(b)$$

за свако $a, b \in A$.

Постојање изоморфизма између две групе подразумева чињеницу да су те групе *суштински исте*, односно да имају еквивалентна својства те се могу сматрати истом.

Идеја иза увођења композиционих низова је једноставна. Самим тим што су чланови композиционог низа мање кардиналости од полазне групе, погоднији су за испитивање. Међутим, у случају да посматрана група има више максималних нормалних подгрупа, другачијим одабиром њих можемо добити више различитих композиционих низова.

Следећа теорема, коју наводимо без доказа, говори о томе да су сви композициони низови суштински исти.

Теорема 2.14 (**Жордан-Хелдер**). *Сви композициони низови коначне групе G су еквивалентни. Исте су дужине, а њихови композициони фактори су изоморфни до на пермутацију.*

Следећа дефиниција издваја својство композиционог низа које је наизглед немотивисано, а његов значај ћемо увидети у каснијим поглављима.

Дефиниција 2.15. Група G је *решива* ако и само ако су јој сви композициони фактори Абелове групе.

2.3 Симетричне и алтернирајуће групе

Као посебну класу коначних група уводимо *симетричне групе* које на природан начин енкодирају пермутације неког скупа.

Дефиниција 2.16. *Симетрична група* S_n је скуп свих пермутација скупа од n објеката, заједно са операцијом композиције пермутација.

Еквивалентно, симетричну групу S_n можемо посматрати као скуп свих бијекција које скуп од n елемената сликају у самог себе.

Будући да се пермутације врше на коначном скупу објеката, поједини објекти образују *петље* које даље можемо појединачно анализирати.

Дефиниција 2.17. *Цикл* дужине k, у ознаци $(a_1, a_2, \ldots, a_k)$, је бијекција која елементе a_i слика у a_{i+1} за $1 \leq i \leq k-1$ и елемент a_k у a_1, а остале елементе оставља непромењеним.

Сваку пермутацију $\sigma \in S_n$ можемо написати као производ дисјунктних циклова.

Циклове дужине 2 називаћемо *транспозицијама*, а циклове дужине 3 3-*цикловима*.

Дефиниција 2.18. Нека је $\theta \in S_n$ и $A = \{1, 2, \ldots, n\}$. *Инверзија* пермутације θ је неуређени пар $\{a_i, a_j\} \subseteq A$ такав да $i < j$ али $\theta(a_i) > \theta(a_j)$.

Дефиниција 2.19. *Знак пермутације* σ, у ознаци $\epsilon(\sigma)$, дефинишемо као

$$\epsilon(\sigma) = (-1)^{inv(\sigma)}$$

где је $inv(\sigma)$ број инверзија пермутације σ. Пермутације σ називамо *парним* уколико је $\epsilon(\sigma) = 1$, а *непарним* у супротном.

Може се показати да је знак цикла дужине k једнак $(-1)^{k-1}$. Како је свака пермутација $\sigma \in S_n$ производ дисјунктних циклова, знак пермутације σ је производ знакова њених појединачних циклова.

Следећа лема олакшава рачун приликом композиције пермутација.

Лема 2.20. Нека је $\tau = (a_1, a_2, \ldots, a_k)$ цикл и $\sigma \in S_n$. Тада је

$$\sigma\tau\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k)).$$

Доказ. Означимо са f пермутацију $\sigma\tau\sigma^{-1}$. Довољно је доказати да важи $f(\sigma(a_1)) = \sigma(a_2)$, а ово следи из

$$f(\sigma(a_1)) = \sigma\tau\sigma^{-1}\sigma(a_1) = \sigma\tau(a_1) = \sigma(a_2).$$

□

Последица 2.21. Претходна лема важи и када τ заменимо са произвољним елементом S_n. Довољно је да ту пермутацију напишемо као композицију циклова, а затим и применимо лему на њих.

Дефиниција 2.22. *Алтернирајућа група* A_n је скуп свих *парних* пермутација скупа од n објеката, заједно са операцијом множења пермутација.

Индукцијом се може показати да се свака пермутација $\sigma \in S_n$ може написати као производ транспозиција. Слично, свака пермутација $\sigma \in A_n$ може се написати као производ 3-*циклова*.

Износимо конструктиван доказ следеће теореме која у некој мери оправдава дефиницију са краја претходног поглавља.

Теорема 2.23. Алтернирајућа група A_n је проста за $n \geq 5$.

Доказ. Нека је N било која нормална подгрупа A_n. Служећи се њеном нормалношћу, доказ делимо на неколико случајева:

1. N *садржи неки цикл дужине* 3. Узмимо без умањења општости да $(1, 2, 3) \in N$. Нека је $\sigma \in A_n$ пермутација која задовољава $\sigma(k) = a_k$ за $1 \leq k \leq 3$. Тада $(a_1, a_2, a_3) = \sigma(1, 2, 3)\sigma^{-1} \in N$, под условом да је σ парна пермутација. Међутим, уколико није, довољно је да је компонујемо са транспозицијом нека друга два елемента (а то можемо зато што је $n \geq 5$). Одавде имамо да сваки 3-цикл припада N, што повлачи $N = A_n$.

2. *N садржи елемент са циклом дужине бар* 4. Нека је то без умањена општости $g = (1, 2, \ldots, k)h$. Може се проверити да важи

$$(2, 3, k) = g^{-1}\left[(1, 2, 3)^{-1} g (1, 2, 3)\right] \in N$$

па по првој ставци доказа важи $N = A_n$.

3. *N садржи елемент са бар два цикла дужине* 3. Нека је то без умањења општости $g = (1, 2, 3)(4, 5, 6)h$. Може се проверити да важи

$$(1, 2, 4, 3, 6) = g^{-1}\left[(1, 2, 4)^{-1} g (1, 2, 4)\right] \in N$$

па по другој ставци доказа важи $N = A_n$.

4. *N садржи елемент који је само композиција једног цикла дужине* 3 *и транспозиција.* Нека је то рецимо $g = (1, 2, 3)h$. Тада важи

$$g^2 = (1, 3, 2)$$

па првој ставци доказа поново важи $N = A_n$.

5. *N садржи елемент који је само композиција транспозиција.* Овај елемент је парна пермутација па мора да садржи бар 2 транспозиције. Нека је то рецимо $g = (1, 2)(3, 4)h$. Важи

$$(1, 4)(2, 3) = g\left[(1, 2, 3)^{-1} g (1, 2, 3)\right] \in N$$

Слично, важи и

$$(1, 2, 3, 4, 5) = (1, 4)(2, 3)\left[(1, 2, 5)^{-1}(1, 4)(2, 3)(1, 2, 5)\right] \in N$$

па по другој ставци доказа важи $N = A_n$.

Сада видимо да N мора бити тривијална нормална подгрупа A_n, одакле следи тврђење. □

Последица 2.24. Количнички фактори групе S_n за $n \geq 5$ су Z_2 и A_n. Будући да A_n није Абелова група, **група S_n није решива** за $n \geq 5$.

3

Раширења поља

3.1 Основни појмови

Дефиниција 3.1. *Поље* чине скуп K и операције $+$ и $\cdot$ које су затворене у K, и притом задовољају следећи скуп аксиома:

- $(\forall\, x, y \in K)\ x + y = y + x$
- $(\forall\, x, y, z \in K)\ x + (y + z) = (x + y) + z$
- $(\exists\, 0 \in K)(\forall\, x \in K)\ 0 + x = x$
- $(\forall\, x \in K)(\exists\, \text{-}x \in K)\ x + (\text{-}x) = 0$
- $(\forall\, x, y \in K)\ x \cdot y = y \cdot x$
- $(\forall\, x, y, z \in K)\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $(\exists\, 1 \in K)(\forall\, x \in K)\ 1 \cdot x = x$
- $(\forall\, x \in K \setminus \{0\})(\exists\, x^{-1} \in K)\ x \cdot x^{-1} = 1$
- $(\forall\, x, y, z \in K)\ x \cdot (y + z) = x \cdot y + x \cdot z$

За наше потребе, поље можемо посматрати као скуп у којем можемо да сабирамо, одузимамо, множимо и делимо (али никако нулом).

Дефиниција 3.2. Нека је K поље. *Раширење* поља K је поље L такво да $K \subseteq L$.

Пишемо L/K да назначимо да је L раширење поља K. У том случају, K је *потпоље* поља L.

Посматрајмо полином $p(x) = x^2 - 2$. Његове нуле, $\sqrt{2}$ и $-\sqrt{2}$, очито не припадају пољу $\mathbb{Q}$. Јасно је да ове елементе не можемо тек тако додати у $\mathbb{Q}$, зато што добијени скуп не би формирао поље. Конкретно, елементи

$$3\sqrt{2},\ \sqrt{2} - 16,\ \frac{1+\sqrt{2}}{5}$$

су само неки од елемената који не припадају овом скупу, а морали би по аксиомама поља. Међутим, зашто не бисмо додали **све** овакве елементе у скуп и тиме заиста формирали поље?

Ова идеја је уопштена и формализована кроз следећих неколико дефиниција.

Дефиниција 3.3. Нека је K поље и $X \subseteq K$. Потпоље K *генерисано скупом* X је пресек свих потпоља K која садрже X.

Дефиниција 3.4. Нека је L/K раширење и $Y \subseteq L$. Са $K(Y)$ означавамо потпоље L генерисано скупом $K \cup Y$.

Када је Y коначан скуп а $a_1, a_2, \ldots, a_t$ су његови елементи, поље $K(Y)$ означаваћемо са $K(a_1, a_2, \ldots, a_t)$.

Дефиниција 3.5. Раширење L/K је *просто* уколико постоји $\alpha \in L$ такво да $L = K(\alpha)$.

Дефиниција 3.6. Раширење L/K је *просто радикално* уколико је $L = K(\alpha)$ за неко α које задовољава $\alpha^n = \beta$, за неко $n \in \mathbb{N}$ и $\beta \in K$.

Дефиниција 3.7. Раширење L/K је *радикално* уколико се може добити низом простих радикалних раширења.

Како раширења поља улазе у причу решавања полиномских једначина?

Под *алгебарским изразом* подразумевамо било који израз који се може добити од рационалних константи, применом коначног броја основних рачунских операција и узимањем коначног броја n-тих корена[1].

Овим смо описали сва решења било ког полинома $p \in \mathbb{Q}[X]$ степена мањег од 5 јер управо квадратна, Карданова и Фераријева формула конструишу нуле ових полинома у облику алгебарских израза. Идеја иза увођења раширења поља се сада природно намеће; уколико се нула неког полинома може

[1]Подразумевамо да је $\sqrt[n]{a}$ **било који** комплексан број чији је n-ти степен једнак a.

написати као алгебарски израз, требало би да можемо да конструишемо низ радикалних раширења

$$\mathbb{Q} \subset K_1 \subset K_2 \subset \cdots \subset K_m$$

такав да финално поље K_m садржи све жељене нуле посматраног полинома.

Уводимо неколико стандардних дефиниција и тврђења која су неопходна за даљи рад.

Дефиниција 3.8. Нека је $\alpha \in \mathbb{C}$ и $K \subseteq \mathbb{C}$ поље. Скуп

$$Null(\alpha) = \{p \mid p \in K[X],\ deg(p) > 0,\ p(\alpha) = 0\}$$

називамо *анулирајућим* скупом елемента α, а његове елементе зовемо *анулирајућим полиномима*.

Дефиниција 3.9. Нека је $K \subset \mathbb{C}$ поље. Елемент $\alpha \in \mathbb{C} \setminus K$ је *алгебарски над* K ако и само ако је $Null(\alpha)$ непразан. Уколико је скуп $Null(\alpha)$ празан, кажемо да је α *трансцедентан над* K.

Дефиниција 3.10. Нека је α алгебарски над пољем K. Моничан анулирајући полином елемента α минималног степена називамо *минималним полиномом* елемента α.

Лема 3.11. Минимални полином p елемента α дели сваки елемент $Null(\alpha)$.

Доказ. Претпоставимо супротно; узмимо неки анулирајући полином q елемента α који није дељив са p. Тада постоје полиноми $A(x)$ и $B(x)$ такви да

$$q(x) = p(x)A(x) + B(x)$$

и притом да је B ненула полином степена мањег од $deg(p)$. За $x = \alpha$ добијамо да је $B(\alpha) = 0$, што је у контрадикцији са минималношћу полинома p. □

У складу са дефиницијом 3.9, разликујемо два типа раширења.

Дефиниција 3.12. Раширење L/K је *алгебарско* уколико је сваки елемент поља L алгебарски над K. Раширење је *трансцедентно* ако није алгебарско.

Доказ следеће леме следи директно из дефиниције алгебарских елемената и раширења.

Лема 3.13. Нека је $\alpha \in \mathbb{C} \setminus K$ алгебарски над K. Тада је просто раширење $K(\alpha)/K$ *алгебарско*.

3.2 Степен раширења

Знајући да је L раширење неког поља K, интуиција нам говори да нам нису неопходни сви његови елементи како бисмо га описали. Заиста, елементи овог поља задовољавају велики број полиномних релација са коефицијентима из поља K, што индукује избацивање *сувишних* елемената док нам не остану тачно они који су нам потребни и довољни да опишемо цело поље.

Идеја посматрања таквог генеришућег скупа је заступљена код векторских простора, а како је димензија самог простора битна за његову карактеризацију, увешћемо сличан појам којим описујемо *величину* раширења.

Дефиниција 3.14. Нека је L/K раширење. Посматрајући L као векторски простор над пољем скалара K, димензија овог векторског простора је *степен раширења*, у ознаци $[L : K]$. Раширење L/K је *коначно* уколико му је степен коначан, а *бесконачно* у супротном.

Теорема 3.15. Нека је $K(\alpha)/K$ просто раширење. Разликујемо два случаја:

- *Елемент α је алгебарски над K.* Означимо са p минимални полином α над K, и нека је $n = deg(p)$. Тада је:

  $$B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

  база векторског простора $K(\alpha)$ над K. Специјално, $[K(\alpha) : K] = n$.

- *Елемент α је трансцедентан над K.* Тада су елементи $1, \alpha, \alpha^2, \ldots$ линеарно независни над K.

Доказ. Случајеве доказујемо засебно:

- *Елемент α је алгебарски над K.* Скуп B је линеарно независан због минималности полинома p; заиста, када би постојали $b_0, b_1, \ldots, b_{n-1} \in K$ који нису сви нула, који задовољавају

  $$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1} = 0$$

  полином $q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1}$ би био анулирајући за елемент α и притом степена мањег од n.

- *Елемент α је трансцедентан над K.* Коначан број различитих степена елемента α не може задовољавати нетривијалну полиномну релацију над K због трансцедентности елемента α. Специјално, одавде директно следи да је степен раширења $K(\alpha)/K$ бесконачан.

□

Будући да смо сада окарактерисали проста раширења, можемо да се бавимо и раширењима која су добијена конструкцијом коначног низа простих. Следећу лему ћемо у наставку цитирати више пута, а она повезује степен овако добијеног раширења са степенима њених међураширења.

Лема 3.16 (**Лема о торњу**)**.** Нека су M/L и L/K алгебарска раширења. Тада важи

$$[M : L] = [M : K][K : L]$$

Доказ. Нека су редом $A = \{a_1, a_2, \ldots, a_n\}$ и $B = \{b_1, b_2, \ldots, b_m\}$ базе раширења M/K и K/L. Доказаћемо да је

$$C = \{ab \mid a \in A,\ b \in B\}$$

база раширења M/L. Узмимо $x_{ij} \in K$ такве да

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j x_{ij} = 0$$

Одавде је

$$\sum_{i=1}^{n} a_i \sum_{j=1}^{m} b_j x_{ij} = 0$$

Како су $\{a_i\}$ линеарно независни, мора важити

$$\sum_{j=1}^{m} b_j x_{ij} = 0$$

за свако $i \in \{1, 2, \ldots, n\}$. Из линеарне независности $\{b_j\}$ мора важити и $x_{ij} = 0$ за свако $j \in \{1, 2, \ldots, m\}$, одакле су елементи скупа C линеарно независни. Остаје да докажемо да елементи скупа C генеришу цео скуп M; заиста, произвољно $m \in M$ можемо написати као

$$m = \sum_{i=1}^{n} a_i m_i$$

за $m_i \in K$, а свако m_i као

$$m_i = \sum_{j=1}^{m} b_j t_j$$

за $t_j \in L$, одакле следи тврђење. □

3.3 Разделна поља

Враћајући се на посматрање нула неког полинома $p \in \mathbb{Q}[X]$, подсећамо се дефиниције алгебарске затворености поља, а уводимо нови појам који све нуле тог полинома посматра одједном, као целину.

Дефиниција 3.17. Поље L је *алгебарски затворено* уколико сваки неконстантан полином $p \in L[X]$ има нулу у L.

Основна теорема алгебре тврди да је поље $\mathbb{C}$ алгебарски затворено.

Дефиниција 3.18. Нека је $p \in M[X]$. Кажемо да се p *дели у* M уколико се може написати

$$p(x) = \beta(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n)$$

за неко $n \geq 0$ и $\beta, \alpha_1, \alpha_2, \dots, \alpha_n \in M$.

На почетку овог поглавља смо поменули низ раширења који почев од поља $\mathbb{Q}$ долази до поља K_m у којем се полином p дели. Повучени чињеницом да је $\mathbb{C}$ алгебарски затворено поље, зашто не бисмо тежили томе да нам финално поље K_m буде што приближније пољу $\mathbb{C}$? Испоставља се да бисмо овим поступком добили *превелико* финално поље које губи значајне информације специфичне за нуле посматраног полинома.

Стога, има смисла посматрати оно поље у којем се полином $p \in \mathbb{Q}[x]$ дели, које је минимално по томе што нема право потпоље са истим својством.

Дефиниција 3.19. Нека је $p \in K[X]$ ненула полином. *Разделно поље полинома* p *над* K је раширење M поља K такво да:

- f се дели у M;
- уколико се p дели у L и важи $K \subseteq L \subseteq M$, тада је $L = M$.

Лема 3.20. Нека је $p \in K[X]$ неконстантан полином и $K \subseteq \mathbb{C}$. Означимо са $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ нуле полинома p. Тада је $K(\alpha_1, \dots, \alpha_n)$ његово разделно поље.

Доказ. Јасно је да се полином p дели у $K(\alpha_1, \alpha_2, \dots, \alpha_n)$. Ово поље је минимално, зато што свака нула полинома p мора лежати у разделном пољу. □

Како све нуле полинома морају лежати у његовом разделном пољу, следеће тврђење је евидентно.

Последица 3.21. Разделно поље полинома $p \in A[X] \subseteq B[X]$ је **јединствено** уколико је B алгебарски затворено поље.

Лема 3.22. Нека је $p \in K[X] \subseteq \mathbb{C}[X]$ неконстантан полином и нека су $\alpha_1, \alpha_2, \ldots, \alpha_n$ његове нуле. Тада је сваки елемент раширења $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ алгебарски над K. Специјално, важи

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n) \leq n!$$

Доказ. Раширење $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ можемо конструисати као низ простих раширења

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq K(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Свако међураширење је алгебарско по леми 3.13. Лема о торњу гарантује да је степен раширења $K(\alpha_1, \alpha_2, \ldots, \alpha_n)/K$ коначан, па ово раширење мора бити алгебарско.

Неједнакост важи ако се p дели у K. У супротном, факторишимо p над $K(\alpha_1)$ као $p(x) = (x - \alpha_1)A(x)B(x)$ где је A минимални полином елемента α_2 над $K(\alpha_1)$. Полином A је степена највише $n-1$, па је $[K(\alpha_1, \alpha_2) : K(\alpha_1)] \leq n-1$. Сада је

$$[K(\alpha_1, \alpha_2) : K] = [K(\alpha_1, \alpha_2) : K(\alpha_1)][K(\alpha_1) : K] \leq n(n-1)$$

. Наставимо овај поступак док не додамо све нуле полинома p у раширење. □

Дефиниција изоморфизма између два поља је еквивалентна дефиницији изоморфизма између две групе.

Дефиниција 3.23. Нека су A и B два поља. *Изоморфизам* је бијективно пресликавање $\varphi : A \to B$ које чува структуру поља. Другим речима, φ задовољава

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

као и

$$\varphi(ab) = \varphi(a)\varphi(b)$$

за свако $a, b \in A$. Специјално, за $A = B$, изоморфизам називамо *аутоморфизмом.*

У случају да су коефицијенти полинома p у пољу $K \subseteq \mathbb{C}$, разделно поље смо конструисали служећи се основном теоремом алгебре; нуле овог полинома смо додавали једну по једну док нисмо конструисали комплетно разделно поље.

Важно је напоменути да разделна поља постоје и када не радимо у алгебарски затвореном пољу. Идеја иза доказа егзистенције разделног поља је слична претходној; поново бисмо конструисали низ раширења почев од поља

над којим је полином дефинисан. Међутим, овде губимо слободу одабира редоследа којим додајемо нуле у раширења, па самим тим губимо контролу над изгледом разделног поља. Испоставља се да ово не утиче знатно на структуру добијеног раширења, јер су сва могућа разделна поља датог полинома суштински иста.

Доказ постојања разделног поља полинома у случају где немамо алгебарско затворење почетног поља изостављамо, али наводимо скицу доказа његове јединствености.

Теорема 3.24. Било која два разделна поља полинома $p \in K[X]$ су изоморфна.

Доказ ове теореме може се спровести индукцијом по степену полинома p, посматрањем његових иредуцибилних фактора и узастопним примењивањем следеће леме:

Лема 3.25. Нека је $p \in K[X]$ иредуцибилан полином степена n и нека су α и β његове нуле. Тада постоји изоморфизам између $K(\alpha)$ и $K(\beta)$ који фиксира сваки елемент K.

Доказ. Произвољан елемент $K(\alpha)$ је облика

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}$$

за неке $a_i \in K$, где је $n = deg(p)$. Слично, сваки елемент $K(\beta)$ је облика

$$b_0 + b_1\beta + b_2\beta^2 + \cdots + b_{n-1}\beta^{n-1}$$

за неке $b_i \in K$, где је $n = deg(p)$. Дефинишимо пресликавање $\varphi : K(\alpha) \to K(\beta)$ са

$$\varphi(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}) = a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{n-1}\beta^{n-1}$$

Користећи чињеницу да је $p \in K[X]$ минимални полином α и β, директно се проверава да је ово пресликавање заиста изоморфизам који фиксира сваки елемент поља K. □

Надаље сматрамо да је разделно поље сваког посматраног полинома јединствено.

Лако се проверава да скуп свих аутоморфизама поља L, заједно са операцијом композиције функција, чини групу. Посматрајући раширења L/K, од посебног значаја су нам аутоморфизми поља L који фиксирају сваки елемент поља K.

Дефиниција 3.26. Групу свих аутоморфизама над пољем L означавамо са $Aut(L)$.

Дефиниција 3.27. Нека је L/K раширење. Скуп свих аутоморфизама над пољем L који фиксирају сваки елемент K означавамо са $Aut(L/K)$.

Лема 3.28. Нека је L/K раширење. Тада је $Aut(L/K)$ подгрупа $Aut(L)$.

Доказ. Јасно је да је $Aut(L/K) \subseteq Aut(L)$. Узмимо произвољне аутоморфизме $g, h \in Aut(L/K)$ и произвољно $\alpha \in K$. Приметимо

$$gh^{-1}(\alpha) = g(h^{-1}(\alpha)) = g(\alpha) = \alpha$$

па је $Aut(L/K)$ заиста подгрупа $Aut(L)$. □

С обзиром на то да при дејству било ког аутоморфизма групе $Aut(L/K)$ елементи поља K остају фиксни, а самим тим и полиноми $p \in K[X]$, природно је погледати шта се деси са нулама тог полинома када применимо аутоморфизам на њих.

Лема 3.29. Нека је $f \in K[X]$ ненула полином са разделним пољем L и $\theta \in Aut(L/K)$. Ако је $\alpha \in L$ нула полинома f, онда је то и $\theta(\alpha)$.

Доказ. Напишимо $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, за $a_0, a_1 \ldots, a_n \in K$. Примењивањем θ на обе стране једнакости

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

добијамо

$$\theta(a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) = \theta(0)$$
$$a_n\theta(\alpha^n) + a_{n-1}\theta(\alpha^{n-1}) + \cdots + a_1\theta(\alpha) + a_0 = 0$$
$$a_n\theta(\alpha)^n + a_{n-1}\theta(\alpha)^{n-1} + \cdots + a_1\theta(\alpha) + a_0 = 0$$

Како је лева страна управо $f(\theta(\alpha))$, тврђење следи. □

Имајући претходну лему у виду, елементе $Aut(L/K)$ можемо посматрати као пермутације на скупу свих нула неког полинома $p \in K[X]$.

Као важну последицу леме 3.25 наводимо следеће:

Последица 3.30. Нека је L разделно поље иредуцибилног полинома $p \in K[X]$ и нека су α и β његове нуле. Тада постоји елемент $Aut(L/K)$ који слика α у β.

4

Теорија Галоа

Завршетак претходног поглавља представља мост између теорије група и теорије поља; почевши од полинома и његовог разделног поља, дошли смо до аутоморфизма који пермутује нуле тог полинома. Еварист Галоа је први формализовао ову везу и тиме отворио пут ка проналаску полинома чије нуле нису алгебарски израз рационалних бројева.

Анализираћемо појам *Галоа* раширења, чија својства на кључан начин описују његову групу аутоморфизама.

4.1 Сепарабилност раширења

Уводимо неколико појмова који ће нам помоћи да дефинишемо Галоа раширења, а касније и испитамо њихове карактеристике.

Дефиниција 4.1. Иредуцибилан полином $p \in K[X]$ је *сепарабилан* уколико у свом разделном пољу нема вишеструке нуле, а *несепарабилан* у супротном.

Дефиниција 4.2. Произвољан полином $p \in K[X]$ је *сепарабилан* уколико су му сви иредуцибилни фактори *сепарабилни*, а *несепарабилан* у супротном.

Дефиниција 4.3. Нека је L/K раширење. Елемент $\alpha \in L$ је *сепарабилан* над K уколико му је минимални полином $f \in K[X]$ *сепарабилан*, а *несепарабилан* у супротном.

Дефиниција 4.4. Раширење L/K је *сепарабилно* уколико је сваки елемент поља L *сепарабилан*.

Лема 4.5. Нека су M/L и L/K раширења. Уколико је M/K сепарабилно, тада су и M/L и L/K такође сепарабилна раширења.

Доказ. Сваки елемент $\alpha \in L$ је такође елемент скупа M, па је самим тим сепарабилан над K.

Минимални полином елемента $\alpha \in M$ над L је сепарабилан, зато што дели његов минимални полином над K који је сепарабилан. □

Значај следеће леме је у томе што ограничавањем величине групе аутоморфизама знатно смањујемо њену слободу, а самим тим и олакшавамо њено испитивање.

Лема 4.6. Нека је $K(\alpha)/K$ раширење, и $p \in K[X]$ минимални полином елемента α. Тада је

$$|Aut(K(\alpha)/K)| \leq [K(\alpha) : K]$$

где једнакост важи ако и само ако је p сепарабилан полином који се дели у $K(\alpha)$.

Доказ. Нека је $\theta \in Aut(K(\alpha)/K)$. По леми 3.29 је $\theta(\alpha)$ нула полинома p. Узмимо произвољан аутоморфизам θ поља $K(\alpha)$ који фиксира сваки елемент поља K, и нека је n степен полинома p. Овај аутоморфизам мора да пресликава елементе поља $K(\alpha)$ по правилу

$$\theta(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}) = a_0 + a_1\theta(\alpha) + a_2\theta(\alpha)^2 + \cdots + a_{n-1}\theta(\alpha)^{n-1}$$

одакле видимо да је овај изоморфизам јединствено одређен сликом елемента α. Сада је јасно да оваквих изоморфизама има тачно онолико колико полином p има различитих нула у пољу $K(\alpha)$. Другим речима, важи

$$|Aut(K(\alpha)/K)| \leq deg(p) = [K(\alpha) : K]$$

где се једнакост успоставља када је p сепарабилан полином који се дели у $K(\alpha)$. □

Следећу теорему ћемо користити касније, а наводимо је без доказа.

Теорема 4.7 (**Теорема о примитивном елементу**)**.** Свако коначно сепарабилно раширење је просто. Другим речима, уколико је $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ сепарабилно раширење, постоји β такво да

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(\beta)$$

4.2 Нормалност раширења

Под условом да су посматране нуле α и β полинома присутне у раширењу, претходно поглавље гарантује постојање аутоморфизма који шаље α у β.

Инспирисани овим, уводимо тип раширења налик разделним пољима.

Дефиниција 4.8. Раширење M/K је *нормално* уколико се сваки иредуцибилан полином $f \in K[X]$ са нулом у M дели у M.

Следећа теорема показује праву моћ нормалних раширења.

Теорема 4.9. Раширење L/K је *нормално* и *коначно* ако и само ако је L разделно поље неког полинома $g \in K[X]$.

Доказ. Нека је L/K нормално и коначно раширење. Напишимо $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ за $\alpha_i \in K$, и нека је $f_i \in K[X]$ минималан полином елемента α_i за $i = 1, 2 \ldots, n$. Тврдимо да је L разделно поље полинома $F = f_1 f_2 \ldots f_n$. Сваки f_i је иредуцибилан и има нулу у L; из нормалности раширења L/K се f_i дели у L, а самим тим и полином F такође. Како је поље L генерисано нулама полинома F, мора бити његово разделно поље.

Нека је сада L разделно поље неког полинома $g \in K[X]$. Ово раширење је коначно; остаје да докажемо да је нормално. Доказаћемо да се дат иредуцибилан полином $f \in K[X]$ са нулом у L дели у L.

Нека је M/L раширење поља L такво да је M разделно поље полинома f. Нека су $\alpha, \beta \in M$ нуле овог полинома. Посматрајмо следеће низове раширења:

$$K \subset K(\alpha) \subset L(\alpha)$$

$$K \subset K(\beta) \subset L(\beta)$$

$$K \subset L \subset L(\alpha), L(\beta)$$

Из иредуцибилности полинома f важи $[K(\alpha) : K] = deg(f) = [K(\beta) : K]$. Како је L разделно поље полинома g над K, $L(\alpha)$ је разделно поље полинома g, али овај пут над $K(\alpha)$. Слично је $L(\beta)$ разделно поље полинома g над $K(\beta)$. По леми 3.25 и теореми 3.24 важи $[L(\alpha) : K(\alpha)] = [L(\beta) : K(\beta)]$. Сада, по леми о торњу, важи

$$[L(\alpha) : L][L : K] = [L(\alpha) : K(\alpha)][K(\alpha) : K]$$

$$[L(\beta) : L][L : K] = [L(\beta) : K(\beta)][K(\beta) : K]$$

Одакле је $[L(\alpha) : L] = [L(\beta) : L]$. Узмимо да је α она нула полинома f за коју знамо да је у L, а β било која друга. Важи

$$[L(\beta) : L] = [L(\alpha) : L] = 1$$

одакле $\beta \in L$, па се f заиста дели у L. □

Служећи се лемом 4.6, следеће тврђење се може доказати индукцијом.

Лема 4.10. Нека је L/K нормално раширење. Тада

$$|Aut(L/K)| \leq [L : K]$$

где једнакост важи ако и само ако је раширење L/K нормално и сепарабилно.

4.3 Фиксна поља

Идеја посматрања аутоморфизама поља L који фиксирају његово унапред одређено потпоље се показала као плодоносна. Међутим, зашто не бисмо кренули супротним смером?

Дефиниција 4.11. Нека је L поље и G било која група аутоморфизама над L. Са L^G означавамо *фиксно поље* групе G над пољем L

$$L^G = \{x \in L |\ g(x) = x \text{ за свако } g \in G\}.$$

Лема 4.12. Фиксно поље L^G је заиста поље.

Доказ. Нека су a и b елементи фиксног поља и g произвољан елемент G. Приметимо

$$g(1) = 1$$

$$g(a + b) = g(a) + g(b) = a + b$$

$$g(ab) = g(a)g(b) = ab$$

одакле следи тврђење. □

Теорема која следи нам отвара пут ка даљој класификацији раширења зато што повезује фиксна поља са појмом сепарабилних раширења.

Теорема 4.13. Нека је G коначна група аутоморфизама над пољем L и нека је K фиксно поље групе G. Тада:

- За свако $\alpha \in L$ важи $[K(\alpha) : K] \leq |G|$.
- L/K је сепарабилно раширење.
- $[L : K] \leq |G|$.

Доказ.

- Узмимо произвољно $\alpha \in L$. Нека је

$$B = \{g(\alpha) \mid g \in G\}$$

и полином p дефинисан са

$$p(x) = \prod_{\beta \in B} (x - \beta).$$

Приметимо да сваки аутоморфизам $g \in G$ задовољава $g(B) = B$. Одавде непосредно следи да p остаје фиксан када применимо g на њега, што значи да $p \in K[X]$. Нека је сад $f \in K[X]$ минимални полином α. Како је $p(\alpha) = 0$, важи $f \mid p$, одакле

$$[K(\alpha) : K] = deg(f) \leq deg(p) \leq |G|$$

- Полином f дели сепарабилан полином p, па је и он сам сепарабилан. Другачијим одабиром елемената α добијамо да је L/K сепарабилно раширење.

- Како је $[K(\alpha) : K]$ ограничен одозго (са $|G|$), можемо узети α такво да је $[K(\alpha) : K]$ максимално. Доказаћемо да произвољно $\beta \in L$ припада $K(\alpha)$, одакле ће важити $L = K(\alpha)$. Тада ће жељена тврдња следити из прве.

Прва ставка ове теореме тврди да је β алгебарски над K, као и да је његов минимални полином степена највише $|G|$. Лема о торњу говори да је $[K(\alpha, \beta) : K]$ коначан, што уз другу тврдњу каже да је раширење $K(\alpha, \beta)/K$ сепарабилно.

По теореми о примитивном елементу, можемо изабрати $\omega \in L$ такво да $K(\alpha, \beta) = K(\omega)$. Међутим, применом леме о торњу добијамо

$$[K(\omega) : K] = [K(\omega) : K(\alpha)][K(\alpha) : K]$$

Из максималности $[K(\alpha) : K]$ добијамо $[K(\omega) : K(\alpha)] = 1$, одакле следи $\beta \in K(\alpha)$.

□

4.4 Карактеризација Галоа раширења

У литератури је појам *Галоа* раширења дефинисан као раширење које је истовремено нормално и сепарабилно. Ми ћемо увести алтернативну дефиницију ради лакшег доказивања, а у теореми која следи ћемо навести неколико еквивалентних верзија ове дефиниције.

Дефиниција 4.14. Раширење M/K је *Галоа раширење* уколико је K фиксно поље неке групе $G \leq Aut(M)$.

Теорема 4.15. Нека је L/K раширење. Тада су следеће ставке

1. L/K је Галоа раширење
2. K је фиксно поље групе $Aut(L/K)$
3. $|Aut(L/K)| = [L : K]$
4. L/K је нормално и сепарабилно раширење

међусобно еквивалентне.

Доказ. Доказ спроводимо на следећи начин:

$2 \Rightarrow 1$. По дефиницији 4.14.

$1 \Rightarrow 2, 3$. Нека је $K = L^G$ за неко $G \leq Aut(L)$. По теореми 4.13 важи

$$[L : K] \leq |G|.$$

Слично, по леми 4.10 важи:

$$|G| \leq |Aut(L/K)| \leq [L : K]$$

одакле је $G = Aut(L/K)$ и $|Aut(L/K)| = [L : K]$.

$3 \Leftrightarrow 4$ Важи по леми 4.10.

$3 \Rightarrow 1$. Нека је $G = Aut(L/K)$ и F фиксно поље ове групе. Тада је L/F Галоа раширење, па мора важити $|G| = [L : F]$. Сада је

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

што са лемом о торњу на

$$K \subseteq F \subseteq L$$

завршава доказ. □

Последица 4.16. Нека је L/K Галоа раширење. Једино $H \leq Aut(L)$ за које важи $K = L^G$ је $Aut(L/K)$.

Комбиновањем ове теореме са теоремом 4.9 даје следећи резултат.

Последица 4.17. Раширење L/K је Галоа раширење ако и само ако је L разделно поље неког сепарабилног полинома $p \in K[X]$.

Приметимо да смо дефиницију Галоа раширења упростили, а успут и пронашли начин да их конструишемо на сасвим интуитиван начин. Довољно је да одаберемо **било који** сепарабилан полином над K и узмемо његово разделно поље!

У случају да је L/K Галоа раширење, групу $Aut(L/K)$ означаваћемо са $Gal(L/K)$, а називаћемо је *Галоа групом* овог раширења.

4.5 Основна теорема и Галоа кореспонденција

Сада смо спремни да уведемо споменуту везу коју је Галоа успоставио.

Теорема 4.18 (**Основна теорема теорије Галоа**)**.** Нека је L/K Галоа раширење и $G = Gal(L/K)$. Тада постоји бијекција између свих потпоља поља L и подгрупа групе G.

Доказ. Нека је $A = \{H \mid H \leq G\}$ и $B = \{E \mid K \subseteq E \subseteq L\}$. Доказаћемо да је да је пресликавање $f\colon A \to B$ задато са

$$f(H) = L^H$$

бијекција.

Нека је $E \in B$. Како је L/K Галоа раширење, поље L је разделно поље неког сепарабилног полинома $p \in K[X]$. Међутим, како је и $K \subseteq E$, важи $p \in E[X]$, одакле је и L/E Галоа раширење. Сада је E фиксно поље групе $Aut(L/E) \leq G$, одакле је f сурјекција.

Нека су сада G_1 и G_2 подгрупе групе G са истим фиксним пољем F. Тада је L/F Галоа раширење, одакле по последици 4.16 важи

$$G_1 = Aut(L/K) = G_2$$

што значи да је f заиста бијекција. □

Последица 4.19. Важи $G_1 \leq G_2$ ако и само ако важи $L^{G_2} \subseteq L^{G_1}$.

Надаље, уколико је $F = L^H$, рећи ћемо да поље F и група H *одговарају* једно другом.

Следећа лема продубљује добијену везу уплитањем нормалних подгрупа у причу, и показаће се као кључна у наставку.

Лема 4.20. Нека је L/K Галоа раширење и $G = Gal(L/K)$. Нека је M поље такво да $K \subseteq M \subset L$ и да притом одговара групи $H \leq G$. Тада је M/K Галоа раширење ако и само ако је $H \trianglelefteq G$, и у том случају је $Gal(M/K) = G/H$.

Доказ. Нека је $\sigma \in G$. Ако поље M одговара групи H, тада $\sigma(M)$ одговара групи $\sigma H \sigma^{-1}$, зато што

$$\sigma H \sigma^{-1}(\sigma(M)) = \sigma H(M) = \sigma(M)$$

одакле је H нормална подгрупа групе G ако и само ако $\sigma(M) \subseteq M$ за свако $\sigma \in G$.

Претпоставимо да је H нормална подгрупа G, а самим тим и $\sigma(M) \subseteq M$. Нека су $\sigma_1, \sigma_2 \in G$. По претпоставци, ови аутоморфизми су такође аутоморфизми поља M. Њихова дејства на M су идентички иста ако и само ако $\theta = \sigma_1^{-1}\sigma_2$ фиксира M, односно $\theta \in H$. Када би $\theta \in H$, онда би важило $\sigma_1 H = \sigma_2 H$. Одавде видимо да елементи групе G/H делују различито на поље M. Знајући да су L/K и L/M Галоа раширења, важи $|G| = [L : K]$ и $|H| = [L : M]$. Применом Лагранжове теореме и леме о торњу добијамо

$$|G/H| = [M : K]$$

одакле је $Gal(M/K) = G/H$.

Нека је сада M/K Галоа раширење. По леми о примитивном елементу, постоји $\omega \in M$ такво да $M = K(\omega)$, и то оно ω које је нула неког полинома $p \in K[X]$ који се дели у M. Тада сваки елемент $\sigma \in G$ шаље ω у неку нулу полинома p, одакле је $\sigma(M) = M$. По тврђењу са краја првог пасуса, H мора бити нормална подгрупа G. □

5

Решавање полиномских једначина

5.1 Циклотомична и Кумерова раширења

Решења полиномских једначина тражимо у раширењима поља $\mathbb{Q}$. Надаље подразумевамо да су сва поменута поља управо добијена коначним раширењем поља рационалних бројева[1]. Стављамо акценат на две врсте раширења која играју круцијалну улогу у решавању полиномских једначина.

Дефиниција 5.1. Раширење генерисано n-тим кореном јединице и пољем $\mathbb{Q}$ називамо *циклоτомичним раширењем.*

Теорема 5.2. Нека је n природан број и $p(x) = x^n - 1$. Нека је полазно поље $K \supseteq \mathbb{Q}$, а са L означимо разделно поље полинома p. Тада је L/K Галоа раширење, а његова Галоа група је Абелова.

Доказ. Приметимо да је полином p сепарабилан, па је L/K Галоа раширење. Нека је $\omega = e^{i\frac{2\pi}{n}}$ Свака нула овог полинома је n-ти корен јединице, а како је сепарабилан, свака нула је облика ω^j за $1 \leq j \leq n$.

Нека је $\theta \in Gal(L/K)$. Приметимо да је $\theta(\omega)$ такође нула полинома p, па можемо написати $\theta(\omega) = \omega^k$ за неко $1 \leq k \leq n$. Ово k јединствено одређује аутоморфизам, зато што важи

$$\theta(\omega^j) = \theta(\omega)^j = \omega^{kj}$$

Сада се директно проверава да је $Gal(L/K)$ Абелова група. □

[1]Довољно је да је полазно поље карактеристике нула, али за потребе овог рада подразумевамо да смо почели са $\mathbb{Q}$.

Надовезивањем на циклотомична раширења, следећи тип раширења подразумева да се жељени n-ти корени јединице већ налазе у полазном пољу.

Дефиниција 5.3. Раширење генерисано пољем K, које садржи све n-те корене јединице, и елементом $\sqrt[n]{a}$, где $a \in K$, називамо *Кумеровим раширењем.*

Теорема 5.4. Нека је K поље које садржи све n-те корене јединице. Нека је $a \in K$, и нека је $L = K(\sqrt[n]{a})$. Тада је L/K Галоа раширење, а његова Галоа група је циклична.

Доказ. Нека је $\omega = e^{i\frac{2\pi}{n}} \in K$. Полином $x^n - \alpha$ је сепарабилан, а његове нуле су управо облика $\omega^j \sqrt[n]{a}$ за $1 \leq j \leq n$. Сада је L разделно поље овог полинома, па је L/K Галоа раширење.

Нека је $\theta \in Gal(L/K)$. Слично претходном доказу, важи $\theta(\sqrt[n]{a}) = \omega^k \sqrt[n]{a}$ за неко k. Ово k такође јединствено одређује аутоморфизам, зато што важи

$$\theta(\omega^j \sqrt[n]{a}) = \omega^j \theta(\sqrt[n]{a}) = \omega^{k+j} \sqrt[n]{a}$$

Може се проверити да је $Gal(L/K)$ подгрупа цикличне групе $\mathbb{Z}_n$, па и она сама мора бити циклична, а специјално и Абелова. □

5.2 Решивост полиномских једначина

Имајући у виду све алате које смо развили до сад, време је да се бавимо проблемом из реченице којом смо започели овај рад.

Дефиниција 5.5. Нека је $p \in K[X]$ полином. Полиномска једначина $p(x) = 0$ је *решива* уколико постоји низ поља

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m$$

такав да је свако K_i генерисано пољем K_{i-1} и свим нулама полинома $x^n - a_i$, за неко n и неко $a_i \in K_{i-1}$, и још при услову да K_m садржи разделно поље полинома $p(x)$.

Важно је уочити да немамо информацију о томе да ли је раширење K_m/Q Галоа раширење. Конкретно, не мора да значи да конструисањем низа Галоа раширења добијамо Галоа раширење. Узмимо за пример следећи низ:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt[4]{5})$$

Прво раширење је Галоа зато што је разделно поље полинома $x^2 - 5$. Слично, друго раширење је Галоа зато што је разделно поље полинома $x^2 - \sqrt{5}$.

Међутим, полином $x^4 - 5$ се не дели у $\mathbb{Q}(\sqrt[4]{5})$, али евидентно има две нуле у том пољу. Самим тим, раширење $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$ није нормално раширење, па не може бити ни Галоа!
Лема која следи нам омогућава да заобиђемо овај проблем и докажемо један део Галоаове теореме.

Надаље претпостављамо да је $p(x)$ иредуцибилан полином над пољем $\mathbb{Q}$, иако следећа тврђења важе за сва почетна поља карактеристике нула.

Лема 5.6. Претпоставимо да постоји низ раширења

$$K = K_0 \subset K_1 \subset \cdots \subset K_m$$

такав да је свако K_i генерисано пољем K_{i-1} и свим нулама полинома $x^n - a_i$, за неко n и неко $a_i \in K_{i-1}$. Тада можемо наћи разделно поље M неког иредуцибилног полинома $p \in K[X]$ које садржи сва ова поља, и да се притом M може добити неким низом радикалних раширења.

Доказ. Нека су $\alpha_1, \alpha_2, \ldots, \alpha_m$ они елементи којим су генерисана сва међураширења. Са $k_1, k_2, \ldots, k_m \in \mathbb{N}$ означимо минималне изложиоце такве да $\alpha_i^{k_i} \in K_{i-1}$. Са L_i означимо минимални полином елемента α_i над K, а са M означимо разделно поље полинома $L(x) = L_1(x)L_2(x)\ldots L_m(x)$. Како је L сепарабилан, M/K је Галоа раширење. Нека је $G = Gal(M/K)$ и $|G| = n$.

Како је M/K уједно и нормално раширење, сваки L_i се дели у M. Доказали смо да за било које две нуле сваког L_i можемо пронаћи елемент G који шаље једну у другу. Знајући да сваки L_i остаје фиксан при дејству било ког елемента $\theta \in G$, добијамо да су нуле полинома L_i управо елементи скупа

$$\{\theta(\alpha_i) \mid \theta \in G\}.$$

Сада је јасно да је поље M генерисано управо елементима скупа

$$\{\theta(\alpha_i) \mid \theta \in G,\ i = 1, 2, \ldots, m\}.$$

Дефинишимо поље A_1 као

$$K \subset K(\theta_1(\alpha_1)) \subset K(\theta_1(\alpha_1), \theta_2(\alpha_1)) \subset \cdots \subset K(\theta_1(\alpha_1), \theta_2(\alpha_1), \ldots, \theta_n(\alpha_1)) = A_1.$$

Свако међураширење је радикално, па је зато и A_1/K радикално. Дефинишимо A_i индуктивно преко A_{i-1} на следећи начин

$$A_i = A_{i-1}(\{\theta(\alpha_i) \mid \theta \in G\}).$$

Доказаћемо да за произвољно $\theta \in G$ и неко (довољно велико) $t \in N$, елемент $\theta(\alpha_i)^t$ лежи у A_{i-1}. Из поставке знамо да елемент α_i^t лежи у пољу генерисаним преко $\alpha_1, \alpha_2, \ldots, \alpha_{i-1}$, што значи да можемо пронаћи полиномну релацију $Q(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}) = \alpha_i^t$, где $Q \in A_{i-1}[X_1, X_2, \ldots, X_{i-1}]$. Примењивањем θ на обе стране ове једнакости, уз чињеницу да $\theta(\alpha_k) \in A_{i-1}$ за $1 \leq k \leq i-1$, добијамо да $\theta(\alpha_i)^t$ лежи у A_{i-1}, одакле је раширење A_i/A_{i-1} радикално.

Имајући у виду да је $M = A_m$, тврђење леме следи. □

Теорема која следи је управо Галоаова теорема о решивости полиномских једначина. Иако наводимо њен комплетан облик, доказаћемо само један смер који нам је довољан да испитамо решивост једног полинома.

Теорема 5.7 (**Галоа**)**.** Нека је $p \in K[X]$ иредуцибилан полином.

- Уколико се *нека* нула овог полинома може написати у облику алгебарског израза, онда се *свака* његова нула може написати у облику алгебарског израза.
- Нека је L разделно поље овог полинома. Тада је L/K Галоа раширење, а његова Галоа група је *решива* ако и само ако је једначина $p(x) = 0$ *решива*.

Доказ. Уколико се једна нула може написати у жељеном облику, можемо конструисати низ радикалних раширења:

$$K \subset K_1 \subset K_2 \cdots \subset K_m$$

где је свако међураширење $K_i \subset K_{i+1}$ генерисано нулама полинома облика $x^{n_i} - \alpha_i$ за $\alpha_i \in K_i$.

По леми 5.6 можемо наћи низ радикалних раширења до разделног поља M неког иредуцибилног полинома $g \in K[X]$. Такође, ради једноставности, можемо претпоставити да смо најпре поље K раширили свим n-тим коренима јединице до поља F, за неко довољно велико n (конкретно неким садржаоцем поменутих n_i).

Како је p иредуцибилан, знамо да је M/K Галоа раширење, па можемо применити основну теорему теорије Галоа. Означимо са G Галоа групу овог раширења. Сада, добијени низ радикалних раширења

$$K \subset F \subset L_1 \subset \cdots \subset K_t = M$$

одговара низу група

$$G > G_0 > G_1 > \cdots > G_t = \{e\}.$$

Раширење K/F је циклотомично, а специјално и Галоа, одакле је $G_0 \triangleleft G$ са количничком групом G/G_0 која је Абелова.

Остала раширења $L_i \subset L_{i+1}$ су радикална. С обзиром на то да F садржи све потребне корене јединице, ово су Кумерова раширења, а специјално и Галоа, одакле је $G_i \triangleleft G_{i+1}$ са количничком групом која је Абелова.

Сада видимо да група G има нормални низ чије су количничке групе Абелове. Даљим *уметањем* нормалних група у овај низ добијамо цео композициони низ групе G. Може се показати да се овим *разбијањем* Абелових количничких група до простих количника не ремети услов комутативности[2], односно да су количнички фактори групе G Абелови. Подсетимо се да ово значи да је група G решива!

Нека је сада L разделно поље полинома p. Он је иредуцибилан, па је L/K заиста Галоа раширење. Специјално, важи

$$K \subset L \subset M.$$

Нека је $H = Gal(L/K)$. По основној теореми теорије Галоа, овај низ раширења одговара низу група

$$\{e\} > H > G.$$

Знајући да се M може добити низом циклотомичних и Кумерових раширења почев од поља L, композициони низ групе G можемо *скратити* тако да добијемо композициони низ групе H. Како је G решива, и H мора бити такође. □

Други смер доказа се може спровести коришћењем својстава цикличних група која се појављују баш због конструисања Кумерових раширења.

5.3 Пример нерешивог полинома

Питање решивости полиномских једначина је сведено на питање решивости коначних група. Наводимо пример полинома на којем примењујемо Галоаову теорему и демонстрирамо дејство групе S_n.

Пре него што кренемо са главним доказом, навешћемо три тврђења техничке природе која ће нам олакшати рад. Наводимо само скице њихових доказа.

[2]Наравно, под условом да је група G коначна.

Теорема 5.8 (**Ајзенштајнов критеријум**)**.** Нека је $p \in \mathbb{Z}[X]$ задат са

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

Уколико постоји прост број p који задовољава услове:

- p дели $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$,
- p не дели a_n,
- p^2 не дели a_0,

онда је p иредуцибилан над $\mathbb{Q}$.

Скица доказа 5.9. Претпоставимо супротно; напишимо $p(x) = g(x)h(x)$ за неке $g, h \in \mathbb{Q}[X]$ и распишимо производ по модулу p.

Лема 5.10. Ако је полином $p \in \mathbb{Q}[X]$ степена бар 2 иредуцибилан, тада је и сепарабилан.

Доказ. Претпоставимо да p није сепарабилан. Нека је α нула овог полинома вишеструкости барем 2. Знамо да је $p'(\alpha) = 0$, те како је p минимални полином α над $\mathbb{Q}$ знамо и $p \mid p'$, што је могуће само када је p константан. □

Теорема 5.11 (**Коши**)**.** Нека је p прост број који дели ред групе G. Тада постоји елемент $g \in G$ различит од неутралног елемента, такав да

$$g^p = e.$$

Другим речима, постоји елемент *реда* p.

Скица доказа 5.12. Посматајмо све p-торке $(g_1, g_2, \ldots, g_p) \in G^p$ такве да

$$g_1 g_2 \ldots g_p = e$$

и циклично пермутујмо њихове елементе.

Пређимо сада на главно тврдњу.

Тврдња 5.13. Једначина $x^5 - 4x + 2 = 0$ није решива.

Доказ. Нека је $p(x) = x^5 - 4x + 2$. По Ајзенштајновом критеријуму за $p = 2$, полином p је иредуцибилан, а по леми 5.8 је сепарабилан. Извод полинома p има тачно две реалне нуле, одакле p има највише три реалне нуле.

Међутим, видимо да су вредности $p(-2)$ и $p(1)$ негативне, а вредности $p(0)$ и $p(2)$ позитивне, што говори о томе да p има тачно 3 реалне нуле, и то по

једну на сваком од интервала $(-2, 0)$, $(0, 1)$ и $(1, 2)$. Одавде видимо да има и 2 нуле у скупу $\mathbb{C} \setminus \mathbb{R}$, које су притом конјуговане.

Нека је L разделно поље овог полинома. Тада је $L/\mathbb{Q}$ Галоа раширење, те са G означимо његову Галоа групу. Нека је θ било која нула овог полинома. Знајући да је p иредуцибилан, он је минимални полином елемента α, те $[K(\alpha) : K] = 5$.

По леми о торњу добијамо да 5 дели $[L : K]$ што је уједно и $|G|$. Кошијева лема каже да G садржи елемент елемент g реда 5, а то мора бити управо цикл дужине 5 (лако се доказује да је цикл дужине k баш реда k).

Такође, у Галоа групи се налази комплексна конјугација која је у конотацији пермутација заправо транспозиција. Можемо без умањења општости претпоставити да је у питању $(1, 2)$.

Може се показати да међу пермутацијама

$$g, g^2, g^3, g^4$$

постоји нека која слика 1 у 2 или 2 у 1. Погодним индексирањем, можемо без умањења општости претпоставити да се $(1, 2)$ и $(1, 2, 3, 4, 5)$ налазе у Галоа групи G. По леми 2.20 добијамо

$$(2, 3) = (1, 2, 3, 4, 5)^{-1}(1, 2)(1, 2, 3, 4, 5) \in G.$$

Слично добијамо да се и $(3, 4)$, $(4, 5)$ и $(5, 1)$ налазе у Галоа групи. Остале транспозиције генеришемо на следећи начин:

$$(1, 3) = (2, 3)(1, 2)(2, 3) \in G,$$
$$(1, 4) = (3, 4)(1, 3)(3, 4) \in G,$$
$$(2, 4) = (3, 4)(2, 3)(3, 4) \in G,$$
$$(3, 5) = (4, 5)(3, 4)(4, 5) \in G.$$

Како су све транспозиције над скупом од 5 елемената у овој групи, мора важити $G = S_n$. Међутим, доказали смо да група S_n није решива. Сада, по Галоаовој теореми, ни ова полиномска једначина није решива! □

6

Закључак

У математици постоји велики број тврђења чија је формулација довољно једноставна да могу сваког натерати на размишљање, а да притом немају елегентан доказ. Као школски пример оваквих тврђења можемо узети *Велику Фермаову теорему*, или пак *Бертранов постулат*. Од тренутка када сам наишао на Карданову формулу, која представља велики скок у сложености од квадратне формуле, занимало ме је - има ли тој сложености краја? Срећом, јако брзо сам наишао на одговор, а то тврђење је управо налик поменутим. Чињеница да **не постоји** општа формула за решавање полиномских једначина степена бар 5 је олакшавајућа све док се не запитамо шта стоји иза њеног доказа.

У овом раду смо представили темељан рад посебног француског математичара на приступачан начин и тиме спојили теорију група и теорију поља у једну целину. Заинтересовани читаоци у литератури могу пронаћи још пуно последица, тврђења и алата ове целоукупне теорије.

Желим да се поново захвалим свом ментору, др Луки Милићевићу, на уложеном труду и тежњи да овај рад буде што бољи. Такође, желим да се захвалим свим професорима који су ми улепшали процес учења математике, а успут и научили да будем истрајан у ономе што радим.

Литература

[1] D. S. Dummit and R. M. Foote, **Abstract Algebra**, third edition, John Wiley and Sons, 2004.

[2] J. Rotman, **Galois Theory**, second edition, Universitext, Springer-Verlag, 1998.

[3] M. Mrinal, *Galois theory and the Abel-Ruffini theorem*, `https://math.uchicago.edu/~may/REU2019/REUPapers/Mrinal.pdf`

[4] R. Koch, *Galois theory*, `https://pages.uoregon.edu/koch/Galois.pdf`

[5] T. Leinster, *Galois theory*, `https://www.maths.ed.ac.uk/~tl/gt/gt.pdf`

[6] Dr P.M.H. Wilson, *Galois theory*, `https://www.dpmms.cam.ac.uk/study/II/Galois/Galois.pdf`

[7] S. R. Ghorpade, *Notes on Galois theory*, `https://www.math.iitb.ac.in/~srg/Lecnotes/galois.pdf`

[8] J.S. Milne, *Fields and Galois theory*, `https://eclass.uoa.gr/modules/document/file.php/MATH594/J.S.Milne.pdf`

[9] A. Sjoblom, *The Abel-Ruffini theorem*, `https://umu.diva-portal.org/smash/get/diva2:1845608/FULLTEXT01.pdf`

[10] C. Birkarl, *Galois theory*, `https://dec41.user.srcf.net/h/II_M/galois_theory`