Galoisova teorija

Ivan Novak

31.5.2024.

Za položiti ovu zadaću potrebno je riješiti barem 3 zadatka od 1. do 11. i barem 4 zadatka od 12. do 18., ili barem 6 zadataka od 1. do 11. i barem 3 zadatka od 12. do 18.

Cilj ovog predavanja je objasniti rezultat koji se zove osnovni teorem Galoisove teorije. Za početak ćemo iskazati teorem, a onda redom objašnjavati što znače pojmovi koji se pojavljuju, te dati nekoliko primjera i primjena.

Teorem 1. *Neka je L/K konačno Galoisovo proširenje polja i $G = \mathrm{Gal}(L/K)$ Galoisova grupa tog proširenja. Tada postoji padajuća bijekcija između skupa svih međuproširenja polja L/K i skupa svih podgrupa od G, koja podgrupi $H \leq G$ pridružuje fiksno polje L^H, a njen inverz međupolju $L/M/K$ pridružuje njegov stabilizator $G_M = \mathrm{Gal}(L/M)$. Nadalje, vrijedi*

$$[L : M] = |G_M| \quad i \quad [L : L^H] = |H|.$$

Ovdje smo dužni puno toga definirati. Prisjetimo se prvo definicija osnovnih algebarskih struktura; grupa, prstenova i polja.

Kratki uvod u algebarske strukture

Grupa je uređeni par $(G, \cdot)$, gdje je $\cdot : G \times G \to G$ operacija sa sljedećim svojstvima:

- asocijativnost, tj. $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$, za sve $g_1, g_2, g_3 \in G$;
- postoji neutralni element $e \in G$, za njega vrijedi $g \cdot e = e \cdot g = g$, za svaki $g \in G$;
- svaki $g \in G$ ima inverz g^{-1}, za njega vrijedi $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Ako je operacija $\cdot$ komutativna, tada kažemo da je G komutativna ili Abelova. U tom slučaju operaciju množenja najčešće označavamo s $+$ umjesto $\cdot$, a neutralni element s 0.
Podgrupa H je podskup grupe G koji je grupa s obzirom na istu operaciju $\cdot$, to označavamo s $H \leq G$.
Prsten je uređena trojka $(R, +, \cdot)$, gdje su $+$ i $\cdot$ operacije na skupu R sa sljedećim svojstvima:

- $(R, +)$ je Abelova grupa
- operacija $\cdot$ je asocijativna i postoji neutralni element 1,
- operacija $\cdot$ je distributivna u odnosu na $+$.

Integralna domena je komutativni prsten u kojem vrijedi

$$ab = 0 \implies a = 0 \text{ ili } b = 0.$$

Polje F je komutativni prsten u kojem svaki element $a \neq 0$ ima multiplikativni inverz, odnosno b takav da je $ab = 1$. Možemo kraće reći da je $(F \setminus \{0\}, \cdot)$ komutativna grupa.
Karakteristika polja je najmanji prirodan broj n takav da je $\underbrace{1 + 1 + \ldots + 1}_{n \text{ puta}} = 0$, a ako taj broj ne postoji kažemo da je polje karakteristike 0.

Zadatak 1. Dokažite da je karakteristika polja uvijek prost broj ili 0.

Primjer 2. Vrijedi da su $\mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$ polja, te $\mathbb{Z}$ nije polje, jer 2 nema multiplikativni inverz. Ta polja su karakteristike 0.
Za prost broj p, cijeli brojevi modulo p sa zbrajanjem i množenjem modulo p čine polje s p elemenata karakteristike p, koje označavamo sa $\mathbb{F}_p$.

Proširenja polja

Sada znamo što su grupe i podgrupe, te znamo što su polja.
Sljedeće što trebamo definirati su proširenja polja.

Definicija 3. Ako su L i K polja takva da je K sadržano u L (te su naravno računske operacije u L i K iste), kažemo da je L proširenje od K i pišemo L/K. Ako je M neko proširenje od K sadržano u L, kažemo da je M međuproširenje od L/K i pišemo $L/M/K$.

Primjer 4. Promotrimo skup $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Taj skup je polje, jer svaki element ima multiplikativni inverz (samo "racionaliziramo" razlomke).
To je proširenje od $\mathbb{Q}$. Netrivijalnih međuproširenja od $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ nema.

Izrazito važna činjenica je sljedeća: ako je L/K proširenje polja, onda je L vektorski prostor nad K. To nam omogućava da primjenjujemo linearnu algebru na ta proširenja, što daje puno alata.

Zadatak 2. Dokažite da svako konačno polje ima p^n elemenata za neki prost broj p i neki prirodan broj n.

U našem teoremu spominju se konačna Galoisova proširenja. Definicija konačnog proširenja je jednostavna.

Definicija 5. Za proširenje polja L/K kažemo da je konačno ako je L konačnodimenzionalan vektorski prostor nad K. U tom slučaju, stupanj proširenja definiramo kao dimenziju vektorskog prostora L nad K. Označavamo ga s $[L : K]$.

Primjer 6. Polje $\mathbb{Q}[\sqrt{2}]$ je proširenje stupnja 2 od $\mathbb{Q}$.

Stupnjevi proširenja se lijepo ponašaju pod tornjevima proširenja.

Lema 7. *Ako je $L/M/K$ toranj konačnih proširenja polja, onda je $[L : K] = [L : M][M : K]$.*

Skica dokaza. Ako je $\{\alpha_1, \ldots, \alpha_k\}$ baza za L/M i $\{\beta_1, \ldots, \beta_\ell\}$ baza za M/K, onda umnošci

$$\{\alpha_i \beta_j \mid 1 \leq i \leq k, 1 \leq j \leq \ell\}$$

čine bazu za L/K. □

Zadatak 3. Dopunite prethodni dokaz argumentom da je ovaj skup stvarno baza za L/K.

Algebarska proširenja polja

Treba nam još malo novih riječi.

Definicija 8. Neka je L/K proširenje polja. Kažemo da je $\alpha \in L$ algebarski nad K ako postoji nenul polinom $f(x)$ s koeficijentima u K takav da je $f(\alpha) = 0$. Za L/K kažemo da je algebarsko ako je svaki $\alpha \in L$ algebarski nad K.

Lema 9. *Svako konačno proširenje polja je algebarsko.*

Zadatak 4. Dokažite ovu lemu.

Obrat leme ne vrijedi - npr. polje svih algebarskih brojeva $\overline{\mathbb{Q}}$ je algebarsko nad $\mathbb{Q}$, a nije konačno proširenje.

Definicija 10. Neka je $\alpha \in L$ algebarski nad K. Normirani polinom najmanjeg stupnja koji α poništava zovemo minimalni polinom od α. Lako se vidi da je minimalni polinom jedinstven. Nultočke minimalnog polinoma od α zovemo konjugati od α.

Automorfizmi polja

Sada razumijemo što znači da je proširenje konačno, ali još uvijek ne znamo što znači da je proširenje Galoisovo, te ne znamo što je Galoisova grupa proširenja. To je nešto kompliciranije za definirati. Za početak ćemo definirati grupu automorfizama polja.

Definicija 11. Neka su K i L polja. Za funkciju $\sigma : K \to L$ kažemo da je homomorfizam polja ako vrijedi:

- $\sigma(1) = 1$,
- $\sigma(a + b) = \sigma(a) + \sigma(b)$,
- $\sigma(ab) = \sigma(a)\sigma(b)$.

Ako je $\sigma : K \to K$ homomorfizam koji je bijekcija, kažemo da je σ automorfizam od K.

Dakle, homomorfizam polja je funkcija iz jednog polja u drugo koja poštuje operacije polja. Automorfizam je bijektivni homomorfizam s polja na samog sebe.

Zadatak 5. Dokažite da je svaki homomorfizam polja injekcija. Nađite primjer polja K i homomorfizma $\sigma : K \to K$ koji nije automorfizam.

Automorfizmi su zgodni jer ih možemo komponirati, pa čine grupu uz operaciju kompozicije. Nas zanima nešto generalnija situacija, pa imamo sljedeću definiciju.

Definicija 12. Neka je L/K proširenje polja. Za automorfizam σ od L takav da je $\sigma(k) = k$ za svaki $k \in K$ kažemo da je K-automorfizam. Grupu svih K-automorfizama od L označavamo s $\mathrm{Aut}(L/K)$.

Zadatak 6. Uvjerite se da svi K-automorfizmi od L čine grupu, uz operaciju kompozicije.

Ovime smo zapravo definirali grupu koja nam je od interesa. U teoremu se spominje Galoisova grupa proširenja L/K, a mi smo definirali grupu K-automorfizama od L. No to su zapravo iste grupe, samo što u slučaju kad je L/K Galoisovo proširenje se koristi naziv "Galoisova grupa od L/K" i piše se $\mathrm{Gal}(L/K)$, umjesto $\mathrm{Aut}(L/K)$.
Objasnimo sada zašto nas zanimaju K-automorfizmi od L. Recimo da imamo polinom s koeficijentima u K,

$$a_n x^n + \ldots + a_1 x + a_0,$$

i neka je $\alpha \in L$ njegova nultočka. Tada imamo

$$a_n \alpha^n + \ldots + a_1 \alpha + a_0 = 0.$$

Djelujmo nekim K-automorfizmom σ na tu jednakost, dobivamo

$$a_n \sigma(\alpha)^n + \ldots + a_1 \sigma(\alpha) + a_0 = 0.$$

Drugim riječima, σ permutira nultočke polinoma s koeficijentima u K koje se nalaze u L.

Galoisova proširenja polja

Definicija 13. Kažemo da je proširenje polja L/K Galoisovo ako je separabilno i normalno.

Separabilna proširenja

Sada želimo definirati separabilna proširenja. Dobra vijest je da je teže naći proširenje polja koje nije separabilno nego ono koje je, pa ovo nije veliki zahtjev na proširenja.

Pitanje: Neka su $f(x)$ i $g(x)$ ireducibilni normirani polinomi s racionalnim koeficijentima. Mogu li $f(x)$ i $g(x)$ imati zajedničku nultočku?

Odgovor je NE. Naime, različiti ireducibilni polinomi su relativno prosti, pa po Bezoutovoj lemi možemo pronaći polinome s racionalnim koeficijentima $A(x)$ i $B(x)$ takve da je

$$A(x)f(x) + B(x)g(x) = 1.$$

Ako bi $f(x)$ i $g(x)$ imali zajedničku nultočku t, onda bi uvrštavanjem te nultočke u gornju relaciju dobili $0 = 1$, kontradikcija.

To znači da o normiranim ireducibilnim polinomima s racionalnim koeficijentima možemo razmišljati kao o disjunktnim vrećama algebarskih brojeva (u vrećama su njihove nultočke). Primijetimo i da u odgovaranju na ovo pitanje nismo koristili svojstva racionalnih brojeva, jer Bezoutova lema vrijedi nad proizvoljnim poljima.

Pitanje: Može li neki ireducibilni polinom s racionalnim koeficijentima imati višestruku nultočku?

Odgovor je opet NE. Naime, polinom $f(x)$ ima višestruku nultočku t ako i samo ako $f'(x)$ također ima tu nultočku. Međutim, kako je $f(x)$ ireducibilan i ne dijeli $f'(x)$ jer je $f'(x)$ manjeg stupnja, možemo opet primijeniti Bezoutovu lemu i dobiti $A(x)f(x) + B(x)f'(x) = 1$.

Nažalost, ovdje smo koristili jedno svojstvo polja $\mathbb{Q}$. Naime, gornji argument ne prolazi ako je $f'(x)$ nul-polinom. To se ne može dogoditi ako je karakteristika polja 0, ali može u karakteristici p. Tamo polinom x^p ima derivaciju $px^{p-1} = 0$.
Proširenje polja je separabilno ako se ne događaju ovakvi problemi.

Definicija 14. Konačno proširenje polja L/K je separabilno ako za svaki ireducibilan polinom s koeficijentima iz K koji ima barem jednu nultočku u L vrijedi da mu derivacija nije nulpolinom.

Kao što smo i objasnili, kad god je karakteristika polja jednaka 0, sva proširenja će biti separabilna. Nadalje, kad god je polje K konačno, sva proširenja će biti separabilna. Zato se nećemo dalje zadržavati na ovom pojmu, ali ćemo imati na umu da je ovo bitan uvjet i da nešto može poći po zlu ako ga nemamo.

Zadatak 7. Dokaži da svaki ireducibilan polinom s koeficijentima u $\mathbb{F}_p$ ima derivaciju različitu od nulpolinoma.

Normalna proširenja

Primjer 15. Promotrimo proširenja polja $\mathbb{Q}[\sqrt{2}]$ i $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$ nad $\mathbb{Q}$. Pogledajmo koliko $\mathbb{Q}$-automorfizama ima svako od tih proširenja. Znamo da svaki K-automorfizam $\sigma : L \to L$ permutira nultočke polinoma koje se nalaze u L.
To znači da je u slučaju prvog proširenja $\sigma(\sqrt{2}) = \pm\sqrt{2}$ jer permutira nultočke od $x^2 - 2$. Nadalje vidimo da je slikom od $\sqrt{2}$ određen cijeli σ, pa zaključujemo da imamo 2 automorfizma od $\mathbb{Q}[\sqrt{2}]$.
Promotrimo sada drugi slučaj. Svaki automorfizam mora permutirati nultočke od $x^3 - 2$ koje leže u $\mathbb{Q}[\sqrt[3]{2}]$. Međutim, samo $\sqrt[3]{2}$ leži u tom proširenju. Zaključujemo da svaki automorfizam fiksira $\sqrt[3]{2}$, pa imamo samo jedan automorfizam, identitetu.

Ono što je ovdje pošlo po zlu je da proširenje $\mathbb{Q}[\sqrt[3]{2}]$ nije normalno.

Definicija 16. Neka je L/K algebarsko proširenje. Kažemo da je L/K normalno ako za svaki $\alpha \in L$ vrijedi da su svi njegovi konjugati također u L.

Poanta je sljedeća: da bismo imali dovoljno K-automorfizama od L, moramo imati sve konjugate.
Ekvivalentna definicija bi bila sljedeća.

Definicija 17. Neka je L/K algebarsko pošrenje. Kažemo da je L/K normalno ako svaki ireducibilan polinom s koeficijentima u K koji ima jednu nultočku u L ima sve nultočke u L.

Zadatak 8. Neka je $L/M/K$ toranj proširenja polja. Dokažite: ako je L/K normalno, onda je i L/M normalno, te ako je L/K separabilno, onda su L/M i M/K separabilna.

Galoisova korespondencija

Definicija 18. Neka je G grupa i X skup. Djelovanje grupe G na skup X je preslikavanje $\cdot : G \times X \to X$ koje je kompatibilno s grupovnom operacijom, odnosno $e \cdot x = x$ za sve $x \in G$, te $(gh) \cdot x = g \cdot (hx)$ za sve $g, h \in G$ i $x \in G$.

Djelovanje koje nas zanima je djelovanje Galoisove grupe $\mathrm{Gal}(L/K)$ na polje L, gdje je L/K Galoisovo proširenje.
Za djelovanje G na X, definiramo sljedeće bitne pojmove. Za podgrupu $H \leq G$, definiramo fiksan skup X^H kao skup koji fiksiraju svi elementi od H, odnosno

$$X^H = \{x \in X \mid \sigma(x) = x,\ \forall \sigma \in H\}.$$

Dualno, za podskup $Y \subset X$, definiramo stabilizator od Y kao

$$G_Y = \{\sigma \in G \mid \sigma(x) = x,\ \forall x \in Y\}.$$

Primijetimo da prvo preslikavanje podgrupi daje podskup od X, a drugo ide u suprotnom smjeru.

Zadatak 9. Dokažite da vrijedi $X^{(G_Y)} \supseteq Y$ i $G_{(X^H)} \supseteq H$.

Vratimo se sada na teorem.

Teorem 19. *Neka je L/K konačno Galoisovo proširenje polja i $G = \mathrm{Gal}(L/K)$ Galoisova grupa tog proširenja. Tada postoji padajuća bijekcija između skupa svih međuproširenja polja L/K i skupa svih podgrupa od G, koja podgrupi $H \leq G$ pridružuje fiksno polje L^H, a njen inverz međupolju $L/M/K$ pridružuje njegov stabilizator $G_M = \mathrm{Gal}(L/M)$. Nadalje, vrijedi*

$$[L : M] = |G_M| \quad i \quad [L : L^H] = |H|.$$

Ono što teorem kaže je da je pridruživanje koje međupolju M pridružuje stabilizator G_M padajuća bijekcija u skup svih podgrupa od G, te da je inverz funkcija koja podgrupi H pridružuje fiksno polje L^H.
Ono što nam prethodni zadatak kaže je da svakako vrijedi $L^{(G_M)} \supseteq M$ i $G_{(L^H)} \supseteq H$.
Jedino što nam nedostaje su preostale inkluzije. Zbog konačnosti, dovoljno je dokazati da se kardinalnosti podgrupa i indeksi međupolja poklapaju.
Za to su trebaju sljedeće dvije leme.

Lema 20. *Neka je L/K konačno proširenje. Tada je L/K Galoisovo ako i samo ako postoji točno $[L : K]$ automorfizama od L koji fiksiraju K.*

Lema 21. *Neka je L polje i H neka konačna podgrupa grupe svih automorfizama od L. Tada je $[L : L^H] = |H|$.*

Iz ovih lema direktno slijede preostale dvije inkluzije.
Objasnimo $G_{(L^H)} = H$. Znamo da je L/L^H Galoisovo, pa je iz prve tvrdnje $|G_{(L^H)}| = [L : L^H]$.
Iz druge tvrdnje je $[L : L^H] = |H|$, pa slijedi $G_{(L^H)} = H$.

Zadatak 10. Objasnite preostalu jednakost:

$$L^{(G_M)} = M.$$

Još preostaje objasniti ove dvije leme. Prva od njih nije teška i to je više tehnički rezultat do kojeg bismo lako došli ako bismo definirali još pojmova, pa ćemo to samo uzeti zdravo za gotovo. Druga tvrdnja je teža, ali nije strašna. Svodi se na primjenu linearne algebre. U zadnjem poglavlju nalazi se dokaz te tvrdnje kao zadatak.

Primjena - teorem o primitivnom elementu

Normalno zatvorenje

Ako naše konačno proširenje L/K nije normalno, tada postoji proširenje $L'/L/K$ takvo da je L'/K normalno i konačno. Takvo L' koje je najmanjeg mogućeg stupnja nad K zovemo normalno zatvorenje od L u K. Svaka dva normalna zatvorenja su izomorfna nad L.
Ovu tvrdnju nećemo dokazivati, nego samo koristiti.

Proširenja generirana jednim elementom

Definicija 22. Neka je $\alpha \in L$ algebarski nad K čiji minimalni polinom je stupnja n. Definiramo

$$K(\alpha) = \{f(\alpha)/g(\alpha) \mid f, g \in K[x], g(\alpha) \neq 0\},$$
$$K[\alpha] = \{f(\alpha) \mid f \in K[x]\},$$
$$K_n[\alpha] = \{f(\alpha) \mid f \in K[x], \deg f < n\}.$$

Zadatak 11. Dokažite da su ova tri polja jednaka. Za $K(\alpha) = K[\alpha]$ ćete trebati koristiti Bezoutovu lemu koja kaže da za polinome $f, g \in K[x]$ bez zajedničkih ireducibilnih faktora postoje $A, B \in K[x]$ takvi da je $A(x)f(x) + B(x)g(x) = 1$.

Za proširenje $K(\alpha)/K$ kažemo da je generirano s α. Za α kažemo da je primitivni element proširenja.
Općenitije, ako imamo nekoliko elemenata $\alpha_1, \ldots, \alpha_k$ algebarskih nad K, definiramo $K(\alpha_1, \ldots, \alpha_n)$ kao najmanje polje koje sadrži K i $\alpha_1, \ldots, \alpha_n$. To je polje se sastoji od svih izraza oblika $f(\alpha_1, \ldots, \alpha_n)$, gdje je $f(x_1, \ldots, x_n)$ polinom u n varijabli s koeficijentima u K.

Dokaz teorema o primitivnom elementu

Teorem 23. *Neka je L/K konačno separabilno proširenje, gdje je K beskonačno polje. Tada postoji $\alpha \in L$ takav da je $K(\alpha) = L$.*

Zadatak 12. Dokažimo teorem. Koraci su sljedeći:

1. Kako je L/K konačno, sigurno je $L = K(\alpha_1, \ldots, \alpha_m)$ za neke $\alpha_1, \ldots, \alpha_m \in L$. Dokažite.
2. Dokažite da postoje $c_1, c_2 \in K$ takvi da je $K(\alpha + c_1\beta) = K(\alpha + c_2\beta)$. (Ovdje vam treba normalno zatvorenje $L'/L/K$ da biste mogli primijeniti osnovni teorem Galoisove teorije.)
3. Dokažite da je tada $K(\alpha, \beta) = K(\alpha + c_1\beta)$.

Primjena - dokaz osnovnog teorema algebre

Općenito o algebarskim zatvorenjima

Definicija 24. Za polje C kažemo da je algebarski zatvoreno ako svaki nekonstantan polinom $f \in C[x]$ ima nultočku u C.

Ekvivalentno je da C nema netrivijalnih konačnih proširenja, jer ako bi imali neko proširenje C'/C, onda bi svaki element $\alpha \in C'$ bio nultočka polinoma iz $C[x]$, pa bi bio iz C.

Definicija 25. Neka je K polje. Za polje C/K kažemo da je algebarsko zatvorenje od K ako je C/K algebarsko proširenje i C je algebarski zatvoreno.

Teorem 26. *Za svako polje K postoji njegovo algebarsko zatvorenje. Svaka dva algebarska zatvorenja su K-izomorfna.*

Teorem nećemo dokazivati, ali zapravo nije strašan - ako Zornovu lemu ne smatrate strašnom.

Osnovni teorem algebre

Teorem 27. *Polje $\mathbb{C}$ je algebarsko zatvorenje od $\mathbb{R}$.*

Prije dokaza, navedimo jedan osnovni teorem iz teorije grupa koji ćemo koristiti bez dokaza.

Teorem 28 (Sylowljev teorem)**.** *Neka je G konačna grupa reda $p^r m$, gdje je p prost broj koji ne dijeli m. Tada G ima (ne nužno jedinstvenu) podgrupu reda p^r, koju zovemo p-Sylowljeva podgrupa od G. Nadalje, za svaki $1 \leq \ell < r$, postoji podgrupa od G reda p^ℓ.*

Zadatak 13. Dokažimo teorem korak po korak.

1. Dokažite da je $\mathbb{C}/\mathbb{R}$ algebarsko.
2. Dokažite da $\mathbb{C}$ nema proširenja stupnja 2.
3. Dokažite da svaki polinom s realnim koeficijentima neparnog stupnja ima realnu nultočku.
4. Neka je $L/\mathbb{C}$ netrivijalno algebarsko proširenje, bez smanjenja općenitosti Galoisovo (samo uzmemo normalno zatvorenje). Promotrimo grupu $G = \mathrm{Gal}(L/\mathbb{R})$. To je konačna grupa s $[L : \mathbb{R}] = [L : \mathbb{C}][\mathbb{C} : \mathbb{R}]$ elemenata. Promotrimo njenu 2-Sylowljevu podgrupu H i neka je $M = L^H$ fiksno polje. Dokažite da je $[M : \mathbb{R}]$ neparno.
5. Objasnite kako iz toga slijedi $M = \mathbb{R}$.
6. Koristeći tvrdnju iz 2. koraka dovršite dokaz.

Primjeri

Primjer 29. Za kvadratna proširenja od $\mathbb{Q}$ vrijedi da je svako oblika $\mathbb{Q}(\sqrt{d})$ za $d \in \mathbb{Z}$ kvadratno slobodan. Svako takvo proširenje je Galoisovo. Galoisova grupa ima dva elementa, pa je izomorfna sa $\mathbb{Z}/2\mathbb{Z}$ (nema što drugo biti).

Lema 30 (Kriterij za normalnost preko generatora)**.** *Neka je $L = K(\alpha_1, \ldots, \alpha_n)/K$ proširenje generirano s n elemenata. Tada je L/K normalno ako i samo ako za svaki generator α_i vrijedi da su svi njegovi konjugati u L.*

Primjer 31. Odredimo Galoisovu grupu proširenja $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$, gdje je ω primitivni treći korijen iz jedinice, odnosno broj za koji je $\omega^2 + \omega + 1 = 0$.
Kao prvo, vidimo da je to proširenje Galoisovo, jer se konjugati svakog generatora nalaze u polju. Nadalje, vidimo da je proširenje stupnja 6, jer je

$$[\mathbb{Q}(\sqrt[3]{2}, \omega)] : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}].$$

Drugi broj u umnošku je 2, a prvi sigurno dijeli 3 i nije jednak 1 jer $\sqrt[3]{2} \notin \mathbb{Q}[\omega]$.
Odredimo sada grupu automorfizama. Svaki je određen time gdje se šalju generatori. Za $i \in \{0, 1, 2\}$ i $j \in \{1, 2\}$ označimo sa $[i, j]$ automorfizam koji šalje $\sqrt[3]{2}$ u $\sqrt[3]{2}\omega^i$ i šalje ω u ω^j. Vidimo da je $([i_1, j_1] \circ [i_2, j_2])(\omega) = \omega^{j_1 j_2}$, te je $([i_1, j_1] \circ [i_2, j_2])(\sqrt[3]{2}) = \sqrt[3]{2}\omega^{i_1 + j_1 i_2}$.
Iz toga dobivamo grupovni zakon:

$$[i_1, j_1][i_2, j_2] = [i_1 + j_1 i_2, j_1 j_2].$$

Možemo prepoznati ovo kao podgrupu svih 2×2 matrica modulo 3, ako elementu $[i, j]$ pridružimo matricu $\begin{bmatrix} 1 & 0 \\ i & j \end{bmatrix}$.

Galoisova grupa polinoma

Cijelo vrijeme smo pričali o Galoisovim grupama proširenja. Češće se priča o Galoisovim grupama polinoma, pa definirajmo to.

Definicija 32. Neka je $f(x) \in K[x]$ polinom. Polje cijepanja od $f(x)$ je minimalno proširenje od K koje sadrži sve nultočke od $f(x)$, odnosno minimalno proširenje od K u kojem se $f(x)$ cijepa na linearne faktore.

Teorem 33. *Polje cijepanja polinoma postoji, i svaka dva polja cijepanja su K-izomorfna.*

Jednom kad imamo algebarsko zatvorenje od K, možemo samo gledati polje cijepanja kao potpolje algebarskog zatvorenja generirano svim nultočkama od $f(x)$. Polje cijepanja polinoma je uvijek normalno, jer je to polje generirano svim nultočkama od $f(x)$, pa za svaki generator su svi njegovi konjugati sigurno u polju.

Definicija 34. Galoisova grupa polinoma $f(x) \in K[x]$ je Galoisova grupa njegovog polja cijepanja (pod uvjetom da je to proširenje separabilno).

Zapravo ovo nije ništa manje općenito od generalne Galoisove teorije, jer vrijedi sljedeće.

Teorem 35. *Konačno separabilno proširenje L/K je Galoisovo ako i samo ako je polje cijepanja nekog polinoma $f \in K[x]$.*

Za polje cijepanja L ireducibilnog polinoma f stupnja n iz $K[x]$ vrijedi $[L : K] \mid n!$. Naime, neka su $\alpha_1, \ldots, \alpha_n$ nultočke od f. Tada svaki automorfizam iz Galoisove grupe permutira nultočke, i određen je djelovanjem na tim nultočkama, pa Galoisovu grupu polinoma možemo shvatiti kao podgrupu grupe S_n svih permutacija na n elemenata.
Za "generički" polinom dobit ćemo cijelu grupu S_n. Ali teoretski možemo dobiti i puno manju grupu, na primjer $\mathbb{Z}/n\mathbb{Z}$.

Primjer 36. Odredimo Galoisovu grupu polinoma $x^4 + x^3 + x^2 + x + 1$ nad $\mathbb{Q}$. Nultočke polinoma su $\omega, \omega^2, \omega^3, \omega^4$ gdje je $\omega^5 = 1$. Tada vidimo da je polje cijepanja $\mathbb{Q}[\omega]$, te je svaki automorfizam određen slikom od ω, i dobivamo cikličku grupu s 4 elementa.

Zadatak 14. Neka je $f(x) \in \mathbb{Q}[x]$ ireducibilan polinom stupnja p za neki prost broj p koji ima točno $p - 2$ realne nultočke. Dokažimo da je Galoisova grupa od f jednaka S_p.

1. Dokažite da u Galoisovoj grupi postoji element reda 2, koji djeluje tako da dvije nultočke zamijeni, a ostale fiksira.

2. Dokažite da postoji element koji djeluje kao ciklus duljine p (slobodno koristite teorem da u grupi reda djeljivog s p postoji element reda p).

3. Dokažite da je podgrupa od S_p koja ima element reda 2 i ciklus duljine p nužno cijela S_p. Drugim riječima, imamo brojeve $1, \ldots, p$ poredane jedan za drugim u redu. Dozvoljen potez je ili pomaknuti svaki element za jedan udesno, a zadnji staviti na početak, ili zamijeniti poredak prva dva elementa. Dokaži da možemo od početnog poretka doći do bilo kojeg drugog poretka.

Dokaz ključne tvrdnje

Cilj ovog poglavlja je dokazati sljedeću tvrdnju.

Lema 37. *Neka je L polje i H neka konačna podgrupa grupe svih automorfizama od L. Tada je $[L : L^H] = |H|$.*

Zadatak 15. Prvo ćemo dokazati da ako je L polje i $\sigma_1, \ldots, \sigma_n$ su različiti automorfizmi od L, onda su $\sigma_1, \ldots, \sigma_n$ linearno nezavisni (nad L).

1. Pretpostavimo da je
$$\sum_{i=1}^{k} a_i \sigma_i(x) = 0, \ \forall x \in L,$$
gdje smo uzeli da je k najmanji broj za koji postoji linearna kombinacija k automorfizama koja je 0. Tada su svi $a_i \neq 0$ i $k \neq 1$. Dokažite onda koristeći svojstva automorfizama da za sve x i y vrijede sljedeće dvije jednakosti:
$$\sum_{i=1}^{k} a_i \sigma_i(x)\sigma_i(y) = 0,$$
$$\sum_{i=1}^{k} a_i \sigma_i(x)\sigma_n(y) = 0.$$

2. Iz toga dođite do kontradikcije s minimalnošću broja k.

Zadatak 16. Sada ćemo dokazati da iz prethodnog zadatka slijedi $[L : L^H] \geq |H|$ za svaku konačnu podgrupu grupe automorfizama od L.
Pretpostavimo suprotno, onda postoji baza $b_1, \ldots, b_m$ za L nad L^H, i automorfizmi $\sigma_1, \ldots, \sigma_n$ tako da je $n > m$. Promatranjem sljedećeg sustava m jednadžbi s n nepoznanica dođite do kontradikcije s linearnom nezavisnošću $\sigma_1, \ldots, \sigma_n$:
$$\sum_{i=1}^{n} \sigma_i(b_j) x_i = 0, \ j = 1, \ldots, m.$$

Zadatak 17. Sada ćemo dokazati suprotnu nejednakost, da je $[L : L^H] \leq |H|$.
Pretpostavimo suprotno. Neka su $b_1, \ldots, b_n \in L$ nezavisni nad L^H, te neka su $\sigma_1, \ldots, \sigma_m \in H$, poredani tako da je σ_1 identiteta. Tada je $m < n$.

1. Promotrimo sljedeći sustav sa m jednadžbi i n nepoznanica:
$$\sum_{i=1}^{n} \sigma_j(b_i) x_i = 0, \ j = 1, \ldots, m.$$
Taj sustav ima netrivijalno rješenje $(a_1, \ldots, a_n)$. Promatranjem prve jednadžbe zaključite da nisu svi $a_1, \ldots, a_n \in L^H$.

2. Dokažite: ako je $(a_1, \ldots, a_n)$ rješenje sustava, onda je i $(\sigma(a_1), \ldots, \sigma(a_n))$ rješenje za $\sigma \in H$.

3. Uzmimo netrivijalno rješenje $(a_1, \ldots, a_n)$ s najmanjim brojem nenul elemenata. Bez smanjenja općenitosti, neka su $a_1, \ldots, a_r \neq 0$, i $a_k = 0$ za $k > r$. Nadalje, skaliranjem možemo pretpostaviti da je $a_r = 1$. Kako nisu svi $a_i \in K$, možemo pretpostaviti $a_1 \notin K$. Dakle, imamo rješenje oblika $(a_1, \ldots, a_{r-1}, 1, 0, \ldots, 0)$. Sada iskoristite 2. dio zadatka za neki prikladan $\sigma \in H$, takav da je $(a_1 - \sigma(a_1), \ldots, a_{r-1} - \sigma(a_{r-1}), 1 - \sigma(1), 0, \ldots, 0)$ netrivijalno rješenje s više nula, što je kontradikcija.

Primjena - nema neočekivanih linearnih relacija među korijenima

Sada ćemo uvesti dva nova bitna, a jednostavna pojma iz teorije polja.

Definicija 38. Neka je L/K Galoisovo proširenje polja. Za $\alpha \in L$, definiramo normu od α, u oznaci $N_K^L(\alpha)$, kao

$$N_K^L(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

Slično, definiramo trag od α, u oznaci $T_K^L(\alpha)$, kao

$$T_K^L(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

Vrijedi da je norma multiplikativna, i trag je K-linearan. Nadalje, norma i trag elementa iz L leže u K. To vidimo ovako: ako djelujemo s bilo kojim $\tau \in \mathrm{Gal}(L/K)$ na umnožak $\prod_\sigma \sigma(\alpha)$, samo ćemo permutirati faktore. To znači da je $N_K^L(\alpha)$ invarijantan za $\mathrm{Gal}(L/K)$, pa leži u K.
Trag i norma se lijepo ponašaju pod tornjevima Galoisovih proširenja.

Lema 39. *Neka je $L/M/K$ toranj proširenja takav da su sva Galoisova. Onda je*

$$T_K^L(\alpha) = T_K^M(T_M^L(\alpha)),$$

te analogna tvrdnja vrijedi za normu.

Koristeći ovu lemu možemo riješiti sljedeći zadatak.

Zadatak 18. Cilj zadatka je dokazati sljedeću tvrdnju: neka su $n_1, \ldots, n_k$ različiti kvadratno slobodni cijeli brojevi. Tada su $\sqrt{n_1}, \ldots, \sqrt{n_k}$ linearno nezavisni nad $\mathbb{Q}$.

1. Neka je $L/\mathbb{Q}$ bilo koje Galoisovo proširenje koje sadrži $\sqrt{d}$ za neki $d \in \mathbb{Z}$. Dokažite da je
$$T_{\mathbb{Q}}^L(\sqrt{d}) = 0.$$

2. Pretpostavimo da je
$$a_1 + a_2\sqrt{n_2} + \ldots + a_k\sqrt{n_k} = 0$$
za neke $a_1, \ldots, a_k \in \mathbb{Q}$. Dokažite da je $a_1 = 0$.

3. Dovršite dokaz tvrdnje.

4. Neka su $p_1, \ldots, p_k$ različiti prosti brojevi. Koji je stupanj proširenja $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k})/\mathbb{Q}$? Dokažite da je Galoisova grupa tog proširenja komutativna. Koliko ima međuproširenja?

Ako proširenje L/K nije Galoisovo nego samo separabilno, i dalje možemo definirati N_K^L i T_K^L tako da umjesto svih K-automorfizama od L gledamo sve K-homomorfizme $L \to L'$, gdje je L' normalno zatvorenje od L u K (ili ekvivalentno sve K-homomorfizme $L \to C$, gdje je C/L algebarsko zatvorenje). Za tako definirane normu i trag vrijede ista svojstva koja smo naveli.