

IZRAČUNAVANJE VRIJEDNOSTI TRIGONOMETRIJSKIH FUNKCIJA POMOĆU TEORIJE GALOA

Sažetak: U ovom radu ćemo pokazati računanje vrijednosti broja $\sin 6^\circ$, korištenjem teorije Galoa.

Ključne riječi: Teorija Galoa, nule polinoma, sinus ugla

Summary: In this paper we will show how to calculate $\sin 6^\circ$, by applying Galois theory.

Keywords: Galois theory, roots of polynomial, sine of angle

Uvod

Elementarne metode u trigonometriji nam dopuštaju da pronađemo tačnu vrijednost svih trigonometrijskih funkcija za uglove $9^\circ, 18^\circ$, itd. Međutim, upotrebom teorije Galoa, možemo izračunati $\sin 6^\circ$, pa zatim i vrijednosti ostalih osnovnih trigonometrijskih funkcija (kosinusa, tangensa i kotangensa) za ugao od 6° . Zatim, kombinujući uglove 6° i 9° možemo dobiti vrijednosti trigonometrijskih funkcija i za ugao 3° i mnoge druge.

Osnovne definicije i teoreme u teoriji polja

Ako je K potpolje polja L , onda se kaže da je L proširenje polja K . Svako proširenje L polja K može se shvatiti kao vektorski prostor nad poljem K . Ako je dimenzija tog vektorskog prostora konačna, onda kažemo da je L konačno proširenje polja K , a dimenziju vektorskog prostora L nad poljem K označavamo sa $(L : K)$ i zovemo stepen proširenja L u odnosu na K . Algebarsko proširenje L polja K je proširenje takvo da je svaki element iz L korijen nekog polinoma stepena većeg od nula sa koeficijentima iz K . Svako konačno proširenje je algebarsko.

Ako je K bilo koje potpolje polja C kompleksnih brojeva, onda prema osnovnoj teoremi algebre za svaki polinom $f(x)$ sa

koeficijentima iz K (*oznaka: $f(x) \in K[x]$*) stepena većeg od 0 postoji minimalno potpolje L polja C koje sadrži sve nule polinoma $f(x)$ i samo polje K , pa se u prstenu polinoma sa koeficijentima iz L , polinom $f(x)$ razlaže na linearne faktore. To polje L se naziva polje razlaganja polinoma $f(x)$ u odnosu na K .

Minimalni polinom $f_\alpha(x) \in K[x]$ elementa α iz L je polinom najnižeg stepena pri čemu je najstariji koeficijent jednak jedinici, takav da je element α nula tog polinoma. Ako je $g(x) \in K[x]$ drugi polinom za koji vrijedi $g(\alpha) = 0$, tada $f_\alpha(x) \mid g(x)$.

Neka je L proširenje polja K . Za element α iz L kažemo da je separabilan nad K , ako je α algebarski element nad K , a osim toga minimalni polinom $f_\alpha(x) \in K[x]$ elementa α u odnosu na K ima samo jednostruke nule. Ako je svaki element iz polja L separabilan onda za polje L kažemo da je separabilno. Svako konačno separabilno proširenje polja K je jednostavno tj. postoji $\alpha \in L$ tako da je $L = K(\alpha)$.

Za polje K kaže se da je algebarski zatvoreno ako nema pravih tj. strogih algebarskih proširenja. Za svako polje K postoji algebarski zatvoreno algebarsko proširenje $\bar{K}$ polja K .

Neka su L i M dva proširenja polja K . Izomorfizam (monomorfizam) $\varphi: L \rightarrow M$ zove se relativni izomorfizam (monomorfizam) u odnosu na K , ako ostavlja na miru sve elemente polja K .

Ako je L algebarsko, a M algebarski zatvoreno proširenje polja K , tada postoji relativni monomorfizam $\varphi: L \rightarrow M$ u odnosu na K . Ukoliko je $L = K(\alpha)$ jednostavno algebarsko proširenje polja K , tada takvih relativnih monomorfizama ima upravo onoliko koliko minimalni polinom $f(x) \in K[x]$ elementa α u odnosu na K ima različitih nula (u bilo kom polju razlaganja L' toga polinoma u odnosu na K).

Neka je L algebrasko proširenje polja K . Reći ćemo da je L normalno proširenje polja K , ako je L invarijantno u odnosu na svaki relativni monomorfizam $\varphi: L \rightarrow \bar{L}$ u odnosu na K .

Ako je $f(x) \in K[x]$ separabilan polinom (tj. ako svaki nesvodljiv faktor tog polinoma ima samo jednostruke nule), tada je

polje razlaganja L polinoma $f(x)$ u odnosu na K konačno, normalno i separabilno proširenje polja K . Postoji teorema koja kaže: Konačno algebarsko proširenje L polja K je normalno ako i sako ako je to polje razlaganja nekog polinoma sa koeficijentima iz K .

Relativni automorfizmi polja L u odnosu na K čine grupu u odnosu na kompoziciju morfizama. Ta grupa se naziva Galoova grupa polja L u odnosu na K i označava se sa $Gal(L/K)$. Ta grupa ima upravo $(L:K)$ elemenata i K je polje invarijantna te grupe (tj. elementi polja K ostaju nepromijenjeni pod djelovanjem bilo kojeg elementa iz te grupe). Ako je n broj različitih korijena algebarske jednačine $f(x) = 0$ u polju L , tada je Galoova grupa izomorfna sa nekom podgrupom grupe permutacija od n elemenata.

Neka je K polje karakteristike p , a L (normalno) proširenje polja K . Reći ćemo da je L (normalno) polje radikala nad K , ako postoji niz međupolja $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_r = L$ takav da je K_i polje razlaganja nekog čistog polinoma $f_i(x) = x^{n_i} + a_i \in K_{i-1}$ ($i = 1, 2, \dots, r$) nad K_{i-1} . U tom slučaju kaže se da je polje radikala L nad K zadano nizom međupolja. Svako polje radikala L nad K je konačno i separabilno proširenje polja K . Ako je L normalno polje radikala nad poljem K tada je Galoova grupa rješiva.

Prisjetimo se pojma rješive grupe. Neka je data grupa $(X, +)$. Tada se podgrupa $(X', +)$ te grupe generisana svim elementima oblika $x + y - x - y$, ($x, y \in X$) naziva komutatorska podgrupa grupe $(X, +)$. Komutatorska podgrupa grupe $(X', +)$ označava se sa $(X'', +)$ i naziva komutatorska podgrupa drugog reda grupe $(X, +)$. Rekurzivno se definiše komutatorska podgrupa $(X^{(i)}, +)$ i – tog reda kao komutatorska podgrupa grupe $(X^{(i-1)}, +)$, tj. $X^{(i)} = (X^{(i-1)})'$, s tim što se dogovorom uzima $X^{(0)} = X$. Za grupu $(X, +)$ kažemo da je rješiva ako postoji prirodan broj r takav da je $X^{(r)} = \{0\}$.

Zahtjev da se svi korijeni algebarske jednačine $f(x) = 0$ nad poljem K mogu iz koeficijenata te jednačine dobiti u konačnom broju koraka uzastopnom primjenom operacija sabiranja, oduzimanja, množenja, djeljenja i korjenovanja, može se formulisati i u obliku zahtjeva da sve nule polinoma $f(x)$, a time i L polje razlaganja tog polinoma budu sadržani u nekom polju radikala nad poljem K .

Teorem: Neka je $f(x) \in K[x]$ polinom nad poljem K karakteristike 0. Tada se algebarska jednačina $f(x) = 0$ može riješiti pomoću radikala nad poljem K , ako i samo ako je Galoaova grupa te jednačine (u odnosu na K) rješiva.

Teorem (osnovna teorema Teorije Galoa): Neka je L konačno normalno i seperabilno proširenje polja K , a $G = \text{Gal}(L/K)$. Tada $H \mapsto L_H$, H je podgrupa grupe $G = \text{Gal}(L/K)$, a

$$L_H = \{\alpha \in L, \sigma(\alpha) = \alpha, \sigma \in H\}$$

predstavlja bijektivno preslikavanje skupa svih podgrupa H grupe G na skup svih međupolja L_H ($K \subseteq L_H \subseteq L$). Pri tome je $H = \text{Gal}(L/L_H)$. Osim toga, H je normalna podgrupa grupe $G = \text{Gal}(L/K)$, ako i samo ako je L_H normalno proširenje polja K ; u tom slučaju je $\text{Gal}(L_H/K) \cong G/H$.

Kako izračunati $\sin 6^\circ$

Prvo ćemo pronaći polinom sa racionalnim koeficijentima tako da je $\sin 6^\circ$ njegov korijen.

Primijetimo da je

$$\begin{aligned} \sin 30^\circ &= \sin(5 \cdot 6^\circ) = \sin(3 \cdot 6^\circ) \cos(2 \cdot 6^\circ) + \cos(3 \cdot 6^\circ) \sin(2 \cdot 6^\circ) = \dots = \\ &= 16\sin^5 6^\circ - 20\sin^3 6^\circ + 5\sin 6^\circ \end{aligned}$$

$$= \frac{1}{2}.$$

Oдавде dolazimo do polinoma čiji je korijen $\sin 6^\circ$:

$$p(x) = 32x^5 - 40x^3 + 10x - 1 \quad (1)$$

To je očigledno, da ako je $\sin 6^\circ$ korijen polinoma (1), da su

tada i brojevi $\sin\left(6^\circ + \frac{360}{5} \cdot k\right) = \sin\left(6^\circ + \frac{2\pi}{5} \cdot k\right)$, $k = 1, 2, 3, 4$ korijeni

polinoma (1), jer je $\sin 5 \cdot \left(6^\circ + \frac{360}{5} \cdot k\right) = \sin(30^\circ + 360 \cdot k) = \sin 30^\circ$

$\sin 5 \cdot \left(6^\circ + \frac{2\pi}{5} \cdot k\right) = \sin(30^\circ + 2k\pi) = \sin 30^\circ$. Dakle,

korijeni polinoma (1) su $\sin 6^\circ$, $\sin 78^\circ = \cos 12^\circ$, $\sin 150^\circ = \frac{1}{2}$,
 $\sin 222^\circ = -\cos 48^\circ$, $\sin 294^\circ = -\cos 24^\circ$.

Jedan od ovih korijena je racionalan, pa je polinom (1) reducibilan nad $\mathbb{Q}$ (skup racionalnih brojeva) i ima linearan faktor $x - \frac{1}{2}$. Zbog udobnosti razmatranja, uvodimo novu varijablu $2x = t$. Tada dobijamo polinom

$$\begin{aligned} f(t) &= p\left(\frac{t}{2}\right) = 32\left(\frac{t}{2}\right)^5 - 40\left(\frac{t}{2}\right)^3 + 10\left(\frac{t}{2}\right) - 1 = t^5 - 5t^3 + 5t - 1 = \\ &= (t - 1) \\ t^4 + t^3 - 4t^2 - 4t + 1 &= (t - 1) \cdot g(t) \end{aligned}$$

gdje je

$$g(t) = t^4 + t^3 - 4t^2 - 4t + 1 \quad (2)$$

Korijeni polinoma $g(t)$ su

$$2 \cdot \sin 6^\circ, 2 \cdot \sin 78^\circ = 2 \cdot \cos 12^\circ, 2 \cdot \sin 222^\circ = -2 \cdot \cos 48^\circ, 2 \cdot \sin 294^\circ = -2 \cdot \cos 24^\circ$$

Prema teoremu o racionalnim korijenima polinoma, jedine moguće racionalne nule su 1 i -1, no uvrštavanjem ovih vrijednosti u polinom vidimo da 1 i -1 nisu korijeni polinoma $g(t)$.

Prema tome, polinom $g(t)$ je seperabilan i ireducibilan nad $\mathbb{Q}$. Neka je L polje razlaganja polinoma $g(t)$. Tada je $L = \mathbb{Q}(\sin 6^\circ, \cos 12^\circ, \cos 24^\circ, \cos 48^\circ)$. Izračunajmo stepen proširenja.

Iz teorema spomenutih iznad slijedi da je

$$(\mathbb{Q}(\sin 6^\circ, \cos 12^\circ, \cos 24^\circ, \cos 48^\circ) : \mathbb{Q}) = 4$$

, broj elemenata u pripadnoj Galovoj grupi 4, i da je $L = \mathbb{Q}(\sin 6^\circ, \cos 12^\circ, \cos 24^\circ, \cos 48^\circ)$ jednostavno polje, pošto je polje razlaganja seperabilnog polinoma seperabilno, konačno i normalno algebarsko proširenje.

$$\cos 12^\circ = 1 - 2\sin^2 6^\circ, \cos 24^\circ = 2\cos^2 12^\circ - 1,$$

$$\cos 48^\circ = 2\cos^2 24^\circ - 1, -\sin 6^\circ = 2\cos^2 48^\circ - 1$$

Racionalna transformacija $t \mapsto 2 - t^2$ prevodi

korijene polinoma $g(t)$ u druge korijene. Ova transformacija definiše Q - automorfizam σ polja L tako da

$$\begin{aligned}\sigma(2 \cdot \sin 6^\circ) &= 2 - (2 \cdot \sin 6^\circ)^2 = 2(1 - 2\sin^2 6^\circ) = 2 \cos 12^\circ, \\ \sigma(2 \cdot \cos 12^\circ) &= 2 - (2 \cdot \cos 12^\circ)^2 = 2(1 - 2\cos^2 12^\circ) = -2\cos 24^\circ, \\ \sigma(-2 \cdot \cos 24^\circ) &= 2 - (-2 \cdot \cos 24^\circ)^2 = 2(1 - 2\cos^2 24^\circ) = -2\cos 48^\circ, \\ \sigma(-2 \cdot \cos 48^\circ) &= 2 - (-2 \cdot \cos 48^\circ)^2 = 2(1 - 2\cos^2 48^\circ) = 2 \cdot \sin 6^\circ\end{aligned}\quad (3)$$

Ovdje vidimo da svi korijeni polinoma $g(t)$ pripadaju $g(t)$ pripadaju polju $Q(\sin 6^\circ)$, te da je polje razlaganja polinoma $g(t)$ jednostavno proširenje, tj. $L = Q(\sin 6^\circ)$, Galoaova grupa sadrži 4 elementa $\{1, \sigma, \sigma^2, \sigma^3\}$, gdje je σ automorfizam dat sa (3). Pošto je Galoaova grupa ciklička, to je ona Abelova, a sve Abelove grupe su rješive, pa je Galoaova grupa pridružena polju razlaganja našeg polinoma rješiva, to znači da se njegove nule mogu dobiti pomoću radikala.

Iz Lagranžeove teoreme o redu podgrupe u konačnim grupama slijedi da naša Galoaova grupa od netrivialnih podgrupa može sadržavati samo podgrupe drugoga reda. Svaka grupa mora sadržavati neutralni element, u našem slučaju to je identično preslikavanje. I nakon kraćeg razmatranja zaključujemo da ciklička grupa reda četiri ima tačno jednu pravu podgrupu $H, (H \neq 1, H \neq G)$: $H = \{1, \sigma^2\}, |H| = 2$. Podgrupi H prema osnovnoj teoremi Teorije Galoa odgovara međupolje M takvo da je to maksimalno potpolje u $Q(\sin 6^\circ)$ čiji su elementi invarijantni u odnosu na transformacije iz H , tj u odnosu na transformaciju σ^2 . Na osnovu iste teoreme slijedi da je $(Q(\sin 6^\circ):M) = 2, (M:Q) = 2$. Dakle, međupolje je kvadratno. To znači da svaki elemenat iz $Q(\sin 6^\circ)$ je nula nekog kvadratnog polinoma sa koeficijentima iz M .

Naime, ako je $(L:K)=2$, onda za proizvoljno $\alpha \in L$, elementi $1, \alpha, \alpha^2$ su linearno zavisni, tj. postoje p, q i r iz polja K tako da $p + q\alpha + r\alpha^2 = 0$.

Kvadratni polinom je reducibilan nad M ako i samo ako

elemenat pripada M . Specijalno i za $\sin 6^\circ$ postoji kvadratni polinom sa koeficijentima iz M tako da je $\sin 6^\circ$ nula tog polinoma. Na isti način koeficijenti od ovog kvadratnog polinoma su korijeni kvadratnog polinoma sa racionalnim koeficijentima. Dakle, mi možemo izračunati svaki elemenat polja $Q(\sin 6^\circ)$ rješavajući dvije kvadratne jednačine.

Posmatrajmo elemente α i β u $Q(\sin 6^\circ)$ tako da $\alpha = 2 \sin 6^\circ - 2 \cos 24^\circ = t_1 + \sigma^2(t_1)$, gdje je $t_1 = 2 \sin 6^\circ$, $\beta = t_1 \cdot t_3$, $t_3 = -2 \cos 24^\circ$. To je evidentno da su t_1 i t_3 korijeni kvadratnog polinoma $p(t) = t^2 - \alpha t + \beta$. S druge strane $\sigma^2(\alpha) = \alpha$, $\sigma^2(\beta) = \beta$, tj. α i β su invarijanta u odnosu na σ^2 . Pa pripadaju međupolju M . Zbog toga postoje polinomi sa racionalnim koeficijentima tako da su α i β korijeni tih polinoma.

$$\begin{aligned}\alpha &= 2 \sin 6^\circ - 2 \cos 24^\circ = 2 \sin 6^\circ - 2 \sin 66^\circ = 4 \sin \frac{6-66}{2} \cos \frac{6+66}{2} = -2 \cos 36^\circ = 4 \sin^2 18^\circ - 2 \\ \beta &= 2 \sin 6^\circ \cdot (-2 \cos 24^\circ) = -2(\sin 30^\circ - \sin 18^\circ) = 2 \sin 18^\circ - 1\end{aligned}$$

Vidimo iz ovih relacija da $M = Q(\sin 18^\circ)$. Ovo znači da je $\sin 18^\circ$ korijen kvadratnog polinoma sa racionalnim koeficijentima. Umjesto da računamo α i β kao korijene kvadratnog polinoma, izračunaćemo $\sin 18^\circ$, a onda ćemo izračunati α i β preko $\sin 18^\circ$. Pronađimo kvadratni polinom sa racionalnim koeficijentima za $\sin 18^\circ$. Možemo vidjeti da je $\sin 18^\circ$ nula polinoma $4t^2 + 2t - 1$

. Dakle $\sin 18^\circ = \frac{\sqrt{5}-1}{4}$.

Polinom $4t^2 + 2t - 1$ možemo dobiti iz:

$$\begin{aligned}0 &= \cos 36^\circ - \sin 54^\circ = (1 - 2 \sin^2 18^\circ) - (3 \sin 18^\circ - 4 \sin^3 18^\circ) \\ &= (\sin 18^\circ - 1)(4 \sin^2 18^\circ + 2 \sin 18^\circ - 1)\end{aligned}$$

Sada

$$\alpha = -\frac{1+\sqrt{5}}{2} \qquad \beta = \frac{\sqrt{5}-3}{2}$$

Kvadratni polinom čije su nule $t_1 = 2 \sin 6^\circ$ i $t_1 = -2 \cos 24^\circ$ glasi:

$$t^2 + \frac{1+\sqrt{5}}{2}t - \frac{3-\sqrt{5}}{2} = 0$$

Pozitivni korijen prethodne jednakosti je

$$2\sin 6^\circ = \frac{\sqrt{30-6\sqrt{5}}-\sqrt{5}-1}{4}, \text{ pa je } \sin 6^\circ = \frac{\sqrt{30-6\sqrt{5}}-\sqrt{5}-1}{8}.$$

Literatura

- Hovhannes M. Khudaverdian, *Applying Galois Theory to Elementary Problems*, 2012.
- Veselin Perić, *Algebra II*, Svjetlost, Sarajevo, 1991.