Invarijante konačnih grupa na algebri polinoma

Nikičić, Kristina

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Kristina Nikičić

INVARIJANTE KONAČNIH GRUPA NA ALGEBRI POLINOMA

Diplomski rad

Voditelj rada:
prof.dr.sc. Goran Muić

Zagreb, studeni 2018.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Mojoj obitelji.

Sadržaj

Sadržaj **iv**

Uvod **1**

1 Preliminarni rezultati **2**
1.1 Grupe, prsteni i polja 2
1.2 Prsten polinoma 5

2 Simetrični polinomi **8**
2.1 Simetrični i Newtonovi polinomi 8
2.2 Fundamentalni teorem za simetrične polinome 9
2.3 Konačne matrične grupe 16

Bibliografija **23**

Sažetak **24**

Summary **25**

Životopis **26**

Uvod

Svjedoci smo da je, u modernom svijetu u kojem živimo danas, gotovo sve što nas okružuje podložno promjenama. Često su te promjene drastične i brze te je potrebno znati prilagoditi im se. Upravo zbog toga, posebnu pažnju privlače stvari koje, usprkos užurbanim promjenama u okruženju, ostaju iste. Kako u svakodnevnom životu, tako i u matematici, osobito su zanimljivi oni objekti koji ostaju nepromijenjeni, tj. invarijantni, pri određenim transformacijama. Neki od objekata koji ostaju nepromijenjeni jesu neke od konačnih matričnih grupa. Zato ćemo u ovom radu, vrlo elementarno i ni na koji način potpuno, opisati invarijantnu teoriju konačnih grupa što je ujedno i glavna tema ovog rada.

Rad podijeljen je u dva poglavlja.

U prvom poglavlju, koje se sastoji od dva potpoglavlja, definiramo osnovne pojmove poput pojmova grupa, prsten, polje, monom i polinom te navodimo primjere koji detaljno opisuju sve te pojmove. U ovom poglavlju upoznajemo se i s prstenom polinoma $k[x_1, x_2, \ldots, x_n]$.

U drugom poglavlju, koje je podijeljeno na tri potpoglavlja, proučavamo simetrične polinome i iskazujemo Fundamentalni teorem za simetrične polinome koji je poznat još od vremena Isaaca Newtona[1]. Štoviše, ponudit ćemo i njegov dokaz. Zatim definiramo pojam homogenih komponenti što nas dovodi do pojma „biti invarijantan na“ i do nekoliko važnih propozicija i primjera.

[1]Isaac Newton (1642. - 1717) engleski fizičar, matematičar i astronom

Poglavlje 1

Preliminarni rezultati

Ovo poglavlje predstavit će osnovne teme rada iz kojih se daljnim proučavanjem rodila ideja o invarijatama konačnih grupa na algebri polinoma. Da bismo razumjeli Fundamentalni teorem za simetrične polinome, njegov dokaz te pojam konačnih matričnih grupa i primjere istih, potrebno je poznavati elementarne pojmove iz algebre. S posebnom pozornošću proučavat ćemo skup polinoma u varijablama $x_1, x_2, \ldots, x_n$ i s koeficijentima u polju k, u oznaci $k[x_1, x_2, \ldots, x_n]$, a pokazat ćemo da on ima strukturu prstena, tj. da govorimo o prstenu polinoma $k[x_1, x_2, \ldots, x_n]$.

1.1 Grupe, prsteni i polja

Definicija 1.1.1. Uređeni par $(G, *)$ koji se sastoji od nepraznog skupa G i binarne operacije $* : G \to G$ nazivamo **grupa** ako su ispunjeni sljedeći uvjeti:

1. binarna operacija je asocijativna, tj. vrijedi

$$(a * b) * c = a * (b * c), \qquad za\ svaki \quad a, b, c \in G; \tag{1.1}$$

2. za binarnu operaciju postoji i jednoznačno je određen neutralni element, tj. postoji jedinstveni $e \in G$ sa svojstvom

$$e * a = a * e = a, \qquad za\ svaki \quad a \in G;$$

3. svaki je element invertibilan, tj. za svaki $a \in G$ postoji i jednoznačno je određen $a^{-1} \in G$ sa svojstvom

$$a * a^{-1} = a^{-1} * a = e.$$

Zbog jednostavnosti, umjesto grupa $(G, *)$ često pišemo i govorimo samo grupa G. Ukoliko za svaka dva elementa a, b iz skupa G vrijedi

$$a * b = b * a,$$

tada kažemo da je grupa G **komutativna** ili **Abelova**.
Za grupu G kažemo da je **konačna** ako skup G ima konačno mnogo elemenata. U suprotnom, kažemo da je grupa G beskonačna.
Jednostavan primjer grupe jest uređeni par $(\mathbb{Z}, +)$. Lako se provjeri da je ovo grupa. Skup cijelih brojeva $\mathbb{Z}$ zatvoren je s obzirom na zbrajanje, a asocijativnost zbrajanja je očito zadovoljena. Neutralni element za zbrajanje u skupu $\mathbb{Z}$ jest nula, a inverzan element za zbrajanje je $-a$, $a \in \mathbb{Z}$. S obzirom na to da je skup $\mathbb{Z}$ beskonačan, bila bio ovo beskonačna grupa.
Uz strukturu grupe važno je spomenuti i neke jednostavnije algebarske strukture poput polugrupe. Ukoliko binarna operacija $*$ na skupu G zadovoljava samo svojstvo (1.1) iz Definicije 1.1.1., tada kažemo da je uređeni par $(G, *)$ **polugrupa**. Najjednostavniji primjer polugrupe jest skup prirodnih brojeva $\mathbb{N}$ s binarnom operacijom zbrajanje, tj. uređeni par $(\mathbb{N}, +)$, s kojom se susrećemo još u osnovnoj školi, no tada ju tako ne nazivamo. Ponovno se lako provjeri da je to zaista polugrupa. Skup prirodnih brojeva $\mathbb{N}$ zatvoren je s obzirom na zbrajanje, a asocijativnost zbrajanja prirodnih brojeva je trivijalno zadovoljena.

Budući da sada imamo sve potrebno, možemo definirati pojam prstena.

Definicija 1.1.2. Uređenu trojku $(P, +, \cdot)$ koja se sastoji od nepraznog skupa P i dviju binarnih operacija definiranih na tom skupu nazivamo **prsten** ako su ispunjeni sljedeći uvjeti:

1. $(P, +)$ je komutativna grupa
2. $(P, \cdot)$ je polugrupa
3. dvije su operacije povezane zakonom distribucije, tj. vrijedi

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$
$$(a + b) \cdot c = a \cdot c + b \cdot c,$$

za svaki izbor $a, b, c \in P$.

Prsten P je **komutativni prsten** ukoliko je

$$a \cdot b = b \cdot a, \qquad za\ svaki \quad a, b \in P.$$

U suprotnom, govorimo o nekomutativnom prstenu.
Neutralni element ili neutral, $0 = 0_P$, u komutativnoj grupi $(P, +)$ zovemo *nula prstena* P.
Nadalje, ako u prstenu $(P, +, \cdot)$ postoji neutralan element za operaciju $\cdot$, tj. jedinični element, ili kraće jedinica, $1 = 1_P \in P$, takav da vrijedi

$$1 \cdot a = a \cdot 1 = a, \qquad \forall\, a \in P,$$

onda kažemo da je P *prsten s jedinicom.*

Primjer 1.1.3. *Uređena trojka* $(\mathbb{Z}, +, \cdot)$ *ima strukturu prstena.*

Da bismo pokazali da je $(\mathbb{Z}, +, \cdot)$ *prsten, moramo pokazati da je* $(\mathbb{Z}, +)$ *komutativna grupa, da je* $(\mathbb{Z}, \cdot)$ *polugrupa te da vrijedi svojstvo distributivnosti množenja prema zbrajanju.*
Očito je da je skup $\mathbb{Z}$ *zatvoren s obzirom na zbrajanje i množenje jer, kada zbrojimo dva cijela broja dobijemo ponovno cijeli broj, i, isto tako, pomnožimo li dva cijela broja kao rezultat dobit ćemo cijeli broj. Asocijativnost zbrajanja u skupu cijelih brojeva je trivijalno zadovoljena, a neutralni element za zbrajanje cijelih brojeva jest nula. Nadalje, svaki element u skupu* $\mathbb{Z}$ *ima svoj inverzni element za zbrajanje i to je upravo* $-a$*. Poput asocijativnosti, i komutativnost zbrajanja u skupu cijelih brojeva je trivijalno zadovoljena. Zbog svega navedenoga možemo zaključiti da je* $(\mathbb{Z}, +)$ *komutativna grupa.*
Već smo utvrdili da je skup $\mathbb{Z}$ *zatvoren obzirom na množenje, a trivijalno je zadovoljena i asocijativnost množenja. To znači da je* $(\mathbb{Z}, \cdot)$ *polugrupa.*
Ostaje provjeriti vrijede li distributivnost množenja prema zbrajanju slijeva i zdesna. No, to je očito zadovoljeno pa konačno zaključujemo da je $(\mathbb{Z}, +, \cdot)$ *prsten.*
Dodatno, zbog toga što u skupu cijelih brojeva vrijedi komutativnost množenja, možemo reći da je $(\mathbb{Z}, +, \cdot)$ *komutativni prsten.*
Isto tako, $\mathbb{Z}$ *je prsten s jedinicom jer postoji neutralan element za množenje cijelih brojeva.*

Budući da koeficijente u polinomima izabiremo iz nekog proizvoljnog polja, sljedeći pojam kojeg definiramo jest pojam polja.

Definicija 1.1.4 (**Polje**)**.** Polje je komutativni prsten s jedinicom različitom od nule u kojem svaki ne - nul element ima multiplikativan inverz.

Definicija polja može se izreći i na drugačiji način pa kažemo da je $(P, +, \cdot)$ polje ako su i $(P, +)$ i $(P^*, \cdot)$ komutativne grupe, pri čemu je $P^* = P \backslash \{0\}$, te ako vrijedi distributivnost operacije $\cdot$ prema operaciji $+$.

Važnost polja leži u tome što linearna algebra radi nad svakim poljem pa, iako je kolegij Linearna algebra ograničen na polja $\mathbb{R}$ i $\mathbb{C}$, većina rezultata u linearnoj algebri primjenjiva je i u proizvoljnom polju k. U ovom radu, radit ćemo upravo u tome proizvoljnom polju, a različiti primjeri bit će smješteni u različita polja kao što su polje racionalnih brojeva $\mathbb{Q}$, polje realnih brojeva $\mathbb{R}$ i polje kompleksnih brojeva $\mathbb{C}$.

1.2 Prsten polinoma

Neka je k proizvoljno polje. Prije definicije polinoma u n varijabli s koeficijentima u polju k, definirajmo pojam monoma.

Definicija 1.2.1 (**Monom**)**.** Monom u varijablama $x_1, x_2, \ldots, x_n$ je produkt oblika

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

gdje su svi eksponenti $\alpha_1, \alpha_2, \ldots, \alpha_n$ nenegativni cijeli brojevi. Ukupni stupanj ovog monoma je zbroj $\alpha_1 + \alpha_2 + \cdots + \alpha_n$.

Zapis monoma može se i pojednostaviti. Neka je $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ uređena n - torka nenegativnih cijelih brojeva. Tada definiramo

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

Primjetimo, kada je $\alpha = (0, 0, \ldots, 0)$, tada je $x^\alpha = 0$. Nadalje, označimo spomenuti ukupni stupanj monoma x^α s $|\alpha|$, tj. $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$.

Primjer 1.2.2. *Monom $f(x, y) = x^4y^7$ primjer je monoma u dvije varijable x i y. Ukupni stupanj ovog monoma jest* 11*.*

Nakon definicije i primjera monoma prirodno slijedi definicija polinoma kao konačne linearne kombinacije monoma.

Definicija 1.2.3 (**Polinom**)**.** Polinom f u varijablama $x_1, x_2, \ldots, x_n$ s koeficijentima u polju k je konačna linearna kombinacija (s koeficijentima u k) monoma. Polinom f zapisujemo u obliku

$$f = \sum_\alpha a_\alpha \cdot x^\alpha, \qquad a_\alpha \in k,$$

gdje suma ide po konačnom broju n - torki $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Skup svih polinoma u varijablama $x_1, x_2, \ldots, x_n$ i koeficijentima u k označavamo $k[x_1, x_2, \ldots, x_n]$.

Kada proučavamo polinome s malim brojem varijabli, vrlo često te varijable označavamo s x, y, i z pa tako proučavamo polinome u jednoj, dvije ili tri varijable koji leže u $k[x]$, $k[x, y]$ i $k[x, y, z]$.
Kako bismo se mogli uspješno bavito polinomima potrebno je poznavati i sljedeće pojmove.

Definicija 1.2.4. Neka je $f = \sum_{\alpha} a_\alpha x^\alpha$ polinom u $k[x_1, x_2, \ldots, x_n]$.

1. a_α zovemo **koeficijent** polinoma f
2. Ako je $a_\alpha \neq 0$, tada $a_\alpha x^\alpha$ zovemo **član** polinoma f.
3. **Ukupni stupanj** polinoma f, označen sa $deg(f)$, je maksimum $|\alpha|$ za koeficijente a_α različite on nule. Stupanj nul - polinoma ne definiramo.

Primjer 1.2.5. *Polinom $f(x, y, z) = 3x^4y^3z^2 + \frac{4}{3}y^4z^4 - 5xyz + y^6$ jest polinom u tri varijable x, y, z s koeficijentima iz $\mathbb{Q}$, tj. polinom f leži u $\mathbb{Q}[x, y, z]$. Dani polinom ima 4 člana, a njegov ukupni stupanj je 9.*

Skup $k[x_1, x_2, \ldots, x_n]$ ima algebarsku strukturu prstena i nazivamo ga *prsten polinoma u varijablama $x_1, x_2, \ldots, x_n$ s koeficijentima u polju k.*

Primjer 1.2.6. *Skup $k[x_1, x_2, \ldots, x_n]$ uz operacije zbrajanje i množenje ima algebarsku strukturu prstena.*
To znači da $(k[x_1, x_2, \ldots, x_n], +)$ mora biti komutativna grupa, da $(k[x_1, x_2, \ldots, x_n], \cdot)$ mora biti polugrupa te da mora vrijediti distributivnost množenja prema zbrajanju slijeva i zdesna.
Lako se provjeri da to zaista jest tako.

Za dokaz Fundamentalnog teorema za simetrične polinome potrebno je u skup svih monoma n varijabli uvesti poseban uređaj.
Neka su $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ i $x_1^{\beta_1}x_2^{\beta_2}\cdots x_n^{\beta_n}$ dva monoma. Za prvi monom reći ćemo da je **stariji** od drugoga ako postoji $i \in \{1, 2, \ldots, n\}$ takav da je

$$\alpha_1 = \beta_1, \alpha_2 = \beta_2, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i.$$

Na taj smo način u skup svih monoma n varijabli uveli uređaj koji zovemo leksikografskim uređajem. Leksikografski urediti neki polinom znači svrstati njegove članove po starosti.

Primjer 1.2.7. *Leksikografski uredite polinom*

$$f(x, y, z) = 2x^2y^3z^{10} + 8x^3y^3z^8 - 3x^3y^4z + x^4yz.$$

Promotrimo prvo u svakom od monoma eksponente od x. Najveći eksponent od x jest 4, dok se u ostala tri monoma x pojavljuje s manjim eksponentima. Stoga je x^4yz najstariji član tog polinoma. U drugom i trećem monomu x se pojavljuje s jednakim eksponentom pa sada promatramo eksponente od y koji se u prvom monomu pojavljuje s eksponenetom 3, u drugom monomu također s eksponentom 3, a u trećem s eksponentom 4. Zaključujemo da je treći po redu član polinoma stariji od prva dva člana. Konačno, prvi član polinoma f je najmlađi pa leksikografski uređaj od f glasi:

$$f(x, y, z) = x^4yz - 3x^3y^4z + 8x^3y^2z^8 + 2x^2y^3z^{10}.$$

Dodatno možemo još vidjeti kako najstariji član polinoma ne mora nužno biti i najvećeg stupnja. U ovome primjeru najstariji član polinoma f je stupnja 6, a ukupni stupanj polinoma jest 15.

Prije no što krenemo proučavati simetrične polinome, navest ćemo i sljedeću lemu koja će se pokazati izrazito korisna pri dokazivanju fundamentalnog teorema za simetrične polinome.

Lema 1.2.8. *Neka su $f, g \in k[x_1, x_2, \ldots, x_n]$. Najstariji član produkta $f \cdot g$ tih dvaju polinoma jednak je produktu najstarijih članova polinoma f i g.*

Poglavlje 2

Simetrični polinomi

Nakon uvodnih i zaista elementarnih definicija, teorema i primjera slijedi glavna tema ovoga rada pa ćemo u ovom poglavlju razmotriti simetrične polinome koji su jednostavan primjer invarijatni konačnih grupa.

2.1 Simetrični i Newtonovi polinomi

Definicija 2.1.1 (**Simetrični polinom**). Za polinom $f \in k[x_1, x_2, ..., x_n]$ kažemo da je **simetričan** ako

$$f(x_{i_1}, x_{i_2}, ..., x_{i_n}) = f(x_1, x_2, ..., x_n)$$

za svaku moguću permutaciju $x_{i_1}, x_{i_2}, ..., x_{i_n}$ varijabli $x_1, x_2, ..., x_n$.

Primjer 2.1.2.

1. *Ako je zadan polinom u dvije varijable x i y, $f(x, y) = x+y+2xy$, lako se može provjeriti da je ovaj polinom simetričan. Zamijenimo li mjesta varijablama, tj. permutiramo varijable x i y, dobivamo*

   $$f(y, x) = y + x + 2yx.$$

   Nadalje, možemo pisati

   $$f(y, x) = y + x + 2yx = x + y + 2xy = f(x, y).$$

2. *Ako su varijable x, y i z, onda je i polinom $f(x, y, z) = x^2 + y^2 + z^2$ također simetričan polinom.*

Definicija 2.1.3 (**Osnovni simetrični polinomi**). Za dane varijable $x_1, x_2, ..., x_n$ definiramo polinome $\sigma_1, \sigma_2, ...\sigma_n \in k[x_1, x_2, ..., x_n]$ sljedećim formulama:

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + ... + x_n, \\
&\vdots \\
\sigma_r &= \sum_{i_1<i_2<...<i_r} x_{i_1} \cdot x_{i_2} \cdots x_{i_r}, \\
&\vdots \\
\sigma_n &= x_1 \cdot x_2 \cdots x_n.
\end{aligned}$$

Primjerice, ako je $n = 4$, onda je

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + x_3 + x_4, \\
\sigma_2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4, \\
\sigma_3 &= x_1x_2x_3 + x_2x_3x_4 \\
\sigma_4 &= x_1x_2x_3x_4
\end{aligned}$$

Pomoću definiranih elementarnih simetričnih polinoma, mogu se vrlo lako konstruirati i drugi simetrični polinomi. Ako su zadane varijable x, y, z tada je $\sigma_1 = x+y+z$, $\sigma_2 = xy + xz + yz$ i $\sigma_3 = xyz$. Prema tome možemo zaključiti da je

$$\begin{aligned}
\sigma_2^2 - \sigma_1\sigma_3 &= (xy + xz + yz)^2 - (x + y + z) \cdot (xyz) \\
&= \ldots = x^2y^2 + x^2z^2 + y^2z^2 + x^2yz + xy^2z + xyz^2
\end{aligned}$$

također simetričan polinom. No, ono što je iznenađujuće jest da se, osim ovoga, *svi* simetrični polinomi mogu prikazani na ovakav način i upravo o tome govori Fundamentalni teorem za simetrične polinome.

2.2 Fundamentalni teorem za simetrične polinome

Teorem 2.2.1 (**Fundamentalni teorem za simetrične polinome**). *Za svaki simetrični polinom $f \in k[x_1, x_2, \ldots, x_n]$ postoji jedinstven polinom $g \in k[x_1, x_2, \ldots, x_n]$ takav da je $f(x_1, x_2, \ldots, x_n) = g(\sigma_1, \sigma_2, \ldots, \sigma_n)$, gdje su $\sigma_1, \sigma_2, \ldots, \sigma_n$ elementarni simetrični polinomi.*

Dokaz. Neka je zadan simetričan ne-nul polinom $f \in k[x_1, x_2, \ldots, x_n]$, i neka je njegov vodeći član $LT(f) = ax^\alpha$. Ako je $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, tvrdimo da vrijedi

$$\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n. \tag{2.1}$$

Kako bismo to dokazali, pretpostavimo prvo da je $\alpha_i < \alpha_{i+1}$, za neki i. Neka je β neki novi istaknuti vektor dobiven od α zamjenjivanjem mjesta elementima α_i i α_{i+1}. Možemo pisati $\beta = (\ldots, \alpha_{i+1}, \alpha i, \ldots)$. Budući da je ax^α član polinoma $f(\ldots, x_{i+1}, x_i, \ldots)$, slijedi da je ax^β član polinoma $f(\ldots, x_{i+1}, x_i, \ldots)$. No kako je, po pretpostavci teorema, polinom f simetričan polinom, tako vrijedi

$$f(\ldots, x_{i+1}, x_i) = f(\ldots, x_i, x_{i+1,\ldots})$$

i stoga je $a \cdot x^\beta$ član polinoma f. Ali ovo je nemoguće jer je, prema leksikografskom uređaju, $\beta > \alpha$ pa bi $LT(f)$ bio ax^β, što je u kontradikciji s pretpostavkom da je $LT(f) = ax^\alpha$, te je time tvrdnja (2.1) dokazana.
Neka je

$$h = \sigma_1^{\alpha_1 - \alpha_2} \sigma_2^{\alpha_2 - \alpha_3} \cdots \sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \sigma_n^{\alpha_n}.$$

Kako bismo odredili vodeći član polinoma h, primijetimo prvo da je $LT(\sigma_r) = x_1 x_2 \cdots x_r$ za $1 \leq r \leq n$.
Stoga je

$$\begin{aligned} LT(h) &= LT(\sigma_1^{\alpha_1 - \alpha_2} \sigma_2^{\alpha_2 - \alpha_3} \cdots \sigma_n^{\alpha_n}) \\ &= LT(\sigma_1)^{\alpha_1 - \alpha_2} LT(\sigma_2)^{\alpha_2 - \alpha_3} \cdots LT(\sigma_n)^{\alpha_n} \\ &= x_1^{\alpha_1 - \alpha_2} (x_1 x_2)^{\alpha_2 - \alpha_3} \cdots (x_1 x_2 \cdots x_n)^{\alpha_n} \\ &= x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \\ &= x^\alpha. \end{aligned} \tag{2.2}$$

Slijedi da polinomi f i ah imaju jednak vodeći član i stoga je

$$multideg(f - ah) < multideg(f)$$

kad god je $f - ah \neq 0$.
Sada označimo $f_1 = f - ah$ i primijetimo da je i f_1 simetričan budući da su i f i ah simetrični polinomi.
Zato, ako je $f_1 \neq 0$, možemo ponavljati gornji proces kako bismo dobili $f_2 = f_1 - a_1 h_1$, gdje je a_1 konstanta, a h_1 je produkt osnovnih simetričnih polinoma $\sigma_1, \sigma_2 \ldots, \sigma_n$ različitih potencija.
Nadalje, znamo da je

$$LT(f_2) < LT(f_1), \quad za\ f_2 \neq 0.$$

Nastavimo li ovako, dobit ćemo niz polinoma $f, f_1, f_2, \ldots$ tako da vrijedi

$$multideg(f) > multideg(f_1) > multideg(f_2) > \cdots .$$

Budući da je leksikografski uređaj dobro uređen, navedeni niz mora biti konačan. Međutim, jedini način na koji opisani proces može završiti jest kada je $f_{t+1} = 0$, za neki t. Tada lako slijedi

$$f = ah + a_1h_1 + \cdots + a_th_t,$$

iz čega vidimo da je polinom f prikazan pomoću osnovnih simetričnih polinoma.
Konačno, potrebno je dokazati jedinstvenost. Pretpostavimo da imamo simetrični polinom f kojeg možemo zapisati kao

$$f = g_1(\sigma_1, \sigma_2, \ldots, \sigma_n) = g_2(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Ovdje su g_1 i g_2 polinomi u n varijabli, recimo u varijablama $y_1, y_2, \ldots, y_n$.
Trebamo dokazati da je $g_1 = g_2$ u $k[x_1, x_2, \ldots, x_n]$. Ako stavimo $g = g_1 - g_2$, onda je

$$g(\sigma_1, \sigma_2, \ldots, \sigma_n) = 0$$

u $k[x_1, x_2, \ldots, x_n]$. Jedinstvenost će biti dokazana ako možemo pokazati da je $g = 0$ u $k[y_1, y_2, \ldots, y_n]$. Pretpostavimo suprotno, tj. $g \neq 0$. Ako zapišemo

$$g = \sum_{\beta} a_\beta y^\beta$$

tada je $g(\sigma_1, \sigma_2, \ldots, \sigma_n)$ suma polinoma $g_\beta = a_\beta \sigma_1^{\beta_1}\sigma_2^{\beta_2}\cdots\sigma_n^{\beta_n}$, gdje je $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$.
Nadalje, argument koji smo koristili ranije u (2.2) pokazuje

$$LT(g_\beta) = a_\beta x_1^{\beta_1+\beta_2+\cdots\beta_n} x_2^{\beta_2+\beta_3+\cdots+\beta_n} \cdots x_n^{\beta_n}.$$

Lako se pokaže da je preslikavanje

$$(\beta_1, \beta_2, \ldots, \beta_n) \longmapsto (\beta_1 + \beta_2 + \cdots + \beta_n, \beta_2 + \beta + \cdots + \beta_n, \ldots, \beta_n)$$

injektivno. Zato svi g_β imaju različite vodeće članove. Posebno, izaberemo li β takav da $LT(g_\beta) > LT(g_\gamma)$, za sve $\gamma \neq \beta$,tada će $LT(g_\beta)$ biti veći od svih članova u g_γ. Slijedi da ne postoji ništa s čime se pokrati $LT(g_\beta)$ i stoga $g(\sigma_1, \sigma_2, \ldots, \sigma_n)$ ne može biti nula u $k[x_1, x_2, \ldots, x_n]$. Ova kontradikcija završava dokaz teorema.

□

Dokaz ovog teorema ponudio je Carl Friedrich Gauss[1] 1816. godine kojemu su svojstva simetričnih polinoma bila potrebna za njegov drugi dokaz Osnovnog teorema algebre[2].

Zanimljivo je da dokaz Fundamentalnog teorema za simetrične polinome nudi i algoritam za pisanje simetričnih polinoma u varijablama $\sigma_1, \sigma_2, \ldots, \sigma_n$. Kako bismo uočili kako algoritam funkcionira, promatrat ćemo polinom

$$f(x, y, z) = x^3y + x^3z + xy^3 + xz^3 + y^3z + yz^3 \in k[x, y, z].$$

Za pomoć pri praćenju rada algoritma, napišimo prvo osnovne simetrične polinome u varijablama x, y, z.

$$\begin{aligned}\sigma_1(x, y, z) &= x + y + z\\ \sigma_2(x, y, z) &= xy + xz + yz\\ \sigma_3(x, y, z) &= xyz\end{aligned}$$

Najstariji član polinoma f je $x^3y = LT(\sigma_1^2\sigma_2)$, što daje

$$f_1 = f - \sigma_1^2\sigma_2 = -2x^2y^2 - 5x^2yz - 2x^2z^2 - 5xy^2z - 5xyz^2 - 2y^2z^2.$$

Sada je najstariji član polinoma $-2x^2y^2 = -2LT(\sigma_2^2)$ i stoga je

$$f_2 = f - \sigma_1^2\sigma_2 + 2\sigma_2^2 = -x^2yz - xy^2z - xyz^2.$$

Lako se vidi da je

$$f_3 = f - \sigma_1^2\sigma_2 + 2\sigma_2^2 + \sigma_1\sigma_3 = 0$$

i zato je sljedećim izrazom

$$f = \sigma_1^2\sigma_2 - 2\sigma_2^2 - \sigma_1\sigma_3$$

jedinstveno prikazan polinom f pomoću osnovnih simetričnih polinoma.

Prilikom bavljenja simetričnim polinomima, često je pogodno raditi s onim simetričnim polinomima koji su homogeni.

Definicija 2.2.2. Polinom $f \in k[x_1, x_2, \ldots, x_n]$ je **homogen ukupnog stupnja** k ako je svaki član polinoma f ukupnog stupnja k.

[1] Johann Carl Friedrich Gauss (1977. - 1855.) njemački matematičar i astronom

[2] Svaki polinom $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ stupnja $n \geq 1$ s kompleksnim koeficijentima ima nultočku u $\mathbb{C}$.

Kao primjer, primijetimo da je i-ta osnovna simetrična funkcija σ_i homogena ukupnog stupnja i. Važna je činjenica da se svaki polinom može zapisati na jedinstven način kao suma homogenih polinoma. Primjerice, za dani $f \in k[x_1, x_2, \ldots, x_n]$, neka je f_k suma svih članova polinoma f koji su ukupnog stupnja k. Tada je svaki f_k homogen i $f = \sum_k f_k$. f_k zovemo **homogena komponenta od** f.

Simetrične polinome možemo promatrati u smislu njihovih homogenih komponenti na sljedeći način.

Propozicija 2.2.3. *Polinom $f \in k[x_1, x_2, \ldots, x_n]$ je simetričan ako i samo ako su sve njegove homogene komponente simetrični polinomi.*

Dokaz. Neka je zadan simetričan polinom f i neka je $x_{i_1}, x_{i_2}, \ldots, x_{i_n}$ permutacija od $x_1, x_2, \ldots, x_n$. Ova permutacija nekog člana polinoma f ukupnog stupnja k šalje u neki drugi član polinoma jednakog ukupnog stupnja.
Kako je $f(x_{i_1}, x_{i_2}, \ldots, x_{i_n}) = f(x_1, x_2, \ldots, x_n)$, jer je f simetričan polinom, slijedi da i k-ta homogena komponenta također mora biti simetrična.
Suprotan smjer je trivijalan i time je propozicija dokazana. □

Ova propozicija govori o tome da, kada radimo sa simetričnim polinomima, možemo pretpostaviti da su oni homogeni.
Osim što simetrične polinome možemo prikazati pomoću osnovnih simetričnih polinoma, možemo ih prikazati i pomoću suma potencija ili, kako ih drugačije nazivamo, Newtonovih polinoma.

Definicija 2.2.4 (Sume potencija)**. Sume potencija** ili **Newtonovi polinomi**[3] čine klasu simetričnih polinoma, a oni su:

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n, \\ s_2 &= x_1^2 + x_2^2 + \cdots + x_n^2, \\ &\vdots \\ s_k &= x_2^k + x_2^k + \cdots + x_n^k. \end{aligned}$$

Osim polinoma $s_1, s_2, \ldots, s_k$, uobičajeno je još uzeti i $s_0 = x_1^0 + x_2^0 + \cdots + x_n^0 = n$. Prije nego što pokažemo kako se pomoću Newtonovih polinoma mogu stvarati novi proizvoljni simetrični polinomi, dokazat ćemo Newtonove identitete.

[3]Ovakve polinome prvi je proučavao Albert Girard, a detaljnije ih je opisao Newton u svojoj knjizi "Arithmetica universalis" 1707. godine pa se zbog toga zovu Newtonovi polinomi. Albert Girard (1595. - 1632.) francuski je matematičar najpoznatiji po tome što je prvi ponudio induktivnu definiciju za Fibbonaccijeve brojeve.

Teorem 2.2.5 (Newtonovi identiteti)**.** *Neka su $s_1, s_2, \ldots, s_k$ Newtonovi polinomi od n varijabli. Tada za $k \leq n$ vrijedi:*

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \cdots + (-1)^{k-1}s_1\sigma_{k-1} + (-1)^k \cdot k \cdot \sigma_k = 0,$$

a za $k > n$

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \cdots + (-1)^n s_{k-n}\sigma_n = 0,$$

gdje su $\sigma_1, \sigma_2, \ldots, \sigma_n$ osnovni simetrični polinomi.

Dokaz. Najprije neka je $s_1 = \sigma_1$. Neka je $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ neki monom. Tada polinom koji dobijemo zbrajanjem svih monoma, koji se od zadanoga dobiju svim permutacijama varijabli, označavamo sa

$$S(ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}).$$

Tako je, na primjer, $S(x_1) = \sigma_1, S(x_1, x_2) = 2\sigma_2, S(x_1^k) = s_k$ itd.
Za $1 \leq k \leq n$ lako je vidjeti da vrijedi:

$$\begin{aligned}
s_{k-1}\sigma_1 &= s_k + S(x_1^{k-1}x_2),\\
s_{k-2}\sigma_2 &= S(x_1^{k-i}x_2) + S(x_1^{k-2}x_2x_3),\\
&\vdots\\
s_{k-i}\sigma_i &= S(x_1^{k-i+1}x_2\cdots x_i) + S(x_1^{k-i}x_2\cdots x_ix_{i+1}), i = 3, \ldots, k-2\\
&\vdots\\
s_1\sigma_{k-1} &= S(x_1^2x_2\cdots x_{k-1}) + k\sigma_k.
\end{aligned}$$

Ako sada prvu od tih jednadžbi pomnožimo sa 1, drugu sa -1, treću sa 1, itd. te sve tako dobivene produkte zbrojimo, dobit ćemo:

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \cdots + (-1)^{k-1}s_1\sigma_{k-1} + (-1)^k\sigma_k = 0,$$

a to je prvi Newtonov identitet.
Ako je $k > n$, onda imamo

$$\begin{aligned}
s_{k-1}\sigma_1 &= s_k + S(x_1^{k-1}x_2),\\
s_{k-2}\sigma_2 &= S(x_1^{k-i}x_2) + S(x_1^{k-2}x_2x_3),\\
&\vdots\\
s_{k-i}\sigma_i &= S(x_1^{k-i+1}x_2\cdots x_i) + S(x_1^{k-i}x_2\cdots x_ix_{i+1}), i = 3, \ldots, n-1\\
&\vdots\\
s_{k-n}\sigma_n &= S(x_{k-n+1}x_2\cdots x_n).
\end{aligned}$$

Iz tih jednakosti, na isti način kao prije, dobivamo da vrijedi:

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \cdots + (-1)^n s_{k-n}\sigma_n = 0,$$

čime je dokazan i drugi Newtonov identitet. □

Prije sljedećeg teorema, kojeg ćemo iskazati i dokazati, ono što možemo primijetiti jest da su sume potencija s_k simetrični polinomi. Budući da su oni simetrični, možemo ih iskoristiti kako bismo zapisali nove proizvoljne simetrične polinome. Kako se to točno radi, opisano je sljedećim teoremom, a u njegovu dokazu svoju ulogu će pronaći i Newtonovi identiteti.

Teorem 2.2.6. *Ako je k polje koje sadrži racionalne brojeve, tj. ako $\mathbb{Q} \subseteq k$, onda se svaki simetrični polinom u $k[x_1, x_2, \ldots, x_n]$ može zapisati kao polinom pomoću Newtonovih polinoma, tj. pomoću suma potencija $s_1, s_2, \ldots, s_n$.*

Dokaz. Budući da je, prema Fundamentalnom teoremu za simetrične polinome, svaki simetrični polinom ujedno i polinom u osnovnim simetričnim polinomima, dovoljno je pokazati da su $\sigma_1, \sigma_2, \ldots, \sigma_n$ polinomi u varijablama $s_1, s_2, \ldots, s_n$. U tu svrhu koristit ćemo ranije dokazane Newtonovne identitete.

$$\begin{aligned} s_k - \sigma_1 s_{k-1} + \cdots + (-1)^{k-1}\sigma_{k-1}s_1 + (-1)^n \sigma_n s_{k-n} = 0, &\qquad 1 \leq k \leq n, \\ \mathrm{s}_k - \sigma_1 s_{k-1} + \ldots + (-1)^{n-1}\sigma_{n-1}s_{k-n+1} + (-1)^n \sigma_n s_{k-n} = 0, &\qquad k > n. \end{aligned}$$

Sada indukcijom po k dokazujemo da je σ_k polinom u $s_1, s_2, \ldots, s_n$. Za $k = 1$ tvrdnja vrijedi jer je $\sigma_1 = s_1$.
Ako je tvrdnja točna za $1, 2, 3, \ldots, k-1$, onda Newtonovi identiteti pokazuju da je

$$\sigma_k = (-1)^{k-1}\frac{1}{k}(s_k - \sigma_1 s_{k-1} + \cdots + (-1)^{k-1}\sigma_k s_1). \tag{2.3}$$

Ovdje možemo dijeliti s cijelim brojem k jer je $\mathbb{Q}$ sadržan u polju odakle uzimamo koeficijente.
Tada iz pretpostavke indukcije i gornje jednadžbe zaključujemo da je σ_k polinom u varijablama $s_1, s_2, \ldots, s_n$.

□

Teoremi 2.2.1. i 2.2.6. za posljedicu imaju vrlo zanimljivu činjenicu. Lako se može vidjeti da se svaki osnovni simetrični polinom može zapisati pomoću suma potencija. Vrijedi i obratno. Primjerice,

$$\begin{aligned} s_2 = \sigma_1^2 - 2\sigma_2 \longleftrightarrow \sigma_2 = \frac{1}{2}(s_1^2 - s_2), \\ s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 \longleftrightarrow \sigma_3 = \frac{1}{6}(s_1^3 - 3s_1 s_2 + 2s_3). \end{aligned}$$

2.3 Konačne matrične grupe

U sljedećem dijelu rada, ponudit ćemo definiciju konačnih matričnih grupa i neke osnovne primjere. Zatim ćemo definirati pojam "biti invarijatan na" što će nas dovesti do važne propozicije koja će pokazati koja je zapravo veza između simetričnih polinoma i konačnih matričnih grupa. U ostatku ovoga rada, uvijek ćemo pretpostaviti da polje k sadrži polje racionalnih brojeva $\mathbb{Q}$. Za takva polja kažemo da su ona karakteristike nula.

Definicija 2.3.1. Neka je $GL(n,k)$ skup svih inverznih $n \times n$ matrica s koeficijentima iz polja k.

Lako se pokaže da skup $GL(n,k)$ svih invertibilnih $n \times n$ matrica s koeficijentima iz polja k zajedno s binarnom operacijom množenja matrica ima strukturu grupe. Neka su A i B invertibilne $n \times n$ matrice. Pomnožimo li dvije takve matrice dobit ćemo neku novu $n \times n$ matricu koja će također biti invertibilna. Dakle, produkt AB invertibilnih matrica A i B je također invertibilna matrica. Dalje, znamo da je množenje matrica asocijativno, tj. vrijedi $A(BC) = (AB)C$. Neutralni element za množenje matrica je jedinična $n \times n$ matrica I_n. Matrici A, jer je invertibilna, možemo lako pronaći inverznu matricu A^{-1} i upravo ta matrica A^{-1} jest inverzni element za množenje matrica. Zbog svega navedenoga, zaključujemo da je $(GL(n,k), \cdot)$ grupa. Ona, zbog svoje važnosti, nosi i posebno ime. Uobičajeno je $GL(n,k)$ zvati **opća linearna grupa**.

Definicija 2.3.2. Konačan podskup $G \subset GL(n,k)$ zovemo **konačna matrična grupa** ukoliko je on neprazan i ukoliko je zatvoren s obzirom na množenje matrica. Broj elemenata grupe G zovemo **red grupe** G i označava se s $|G|$.

Kako bi bilo jasnije o čemu se radi, pogledajmo neke primjere konačnih matričnih grupa.

Primjer 2.3.3. *Neki od primjera konačnih matričnih grupa su:*

1. *Neka je $G = \{I\}$. Jasno je da je $\{I\}$ podskup od $GL(n,k)$, a vidimo da se skup sastoji od samo jednog elementa, tj. skup G ima konačno mnogo elemenata. Nadalje, trivijalno su zadovoljena sva svojstva iz Definicije 1.1.1. te G zajedno s binarnom operacijom množenja matrica zaista čini grupu.*

2. *Neka je $G = \{I_n, -I_n\}$ konačna matrična grupa, pri čemu je I_n kvadratna matrica reda n. Očito je da je grupa G zatvorena s obzirom na množenje matrica. Asocijativnost množenja matrica nasljeđuje se iz $GL(n,k)$, a neutralni element jest matrica I_n. Osim što je matrica I_n neutralni element za množenje matrica*

u ovome skupu, ona je ujedno i inverzni element za množenje matrica. Dakle, grupa G ima konačno mnogo elemenata i pokazali smo da ima sva svojstva grupe pa kažemo da je G konačna matrična grupa.

3. *Pretpostavimo da je $A \in GL(n,k)$ matrica takva da je $A^m = I_n$ za neki pozitivni cijeli broj m. Ako je m najmanji mogući takav cijeli broj, onda je lako pokazati da je skup*
$$C_m = \{I_n, A, A^2, \ldots, A^{m-1}\} \subset GL(n,k)$$
*zatvoren s obzirom na množenje matrica i stoga čini konačnu matričnu grupu C_m koju zovemo **ciklična grupa reda** m. Pogledajmo to na konkretnom primjeru. Neka je*
$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in GL(n,k).$$
Množenjem matrice A same sa sobom dva, tri i četiri puta dobivamo da je $A^2 = -I_2, A^3 = -A$ i $A^4 = I_2$. Dakle, najmanji m za kojeg vrijedi $A^m = I_2$ jest 4 pa je tako $C_4 = \{I_2, A, A^2, A^3\}$ ciklična matrična grupa reda 4 u $GL(n,k)$.

4. *Neka je*
$$G = \{\begin{bmatrix} \cos\frac{2k\pi}{n} & -\sin\frac{2k\pi}{n} \\ \sin\frac{2k\pi}{n} & \cos\frac{2k\pi}{n} \end{bmatrix}; 0 \leq k \leq n-1\}$$
konačna grupa od n rotacija.

5. *Važan primjer konačnih matričnih grupa dolazi od permutacija varijabli o čemu smo detaljno pisali u prethodnim podpoglavljima. Neka τ označava permutaciju $x_{i_1}, x_{i_2}, \ldots, x_{i_n}$ varijabli $x_1, x_2, \ldots, x_n$. Budući da je τ određen s onime što on radi indeksima, označit ćemo $\tau(1) = i_1, \tau(2) = i_2, \ldots, \tau(n) = i_n$. Tada odgovarajuću permutaciju pišemo kao $x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}$. Od τ se vrlo jednostavno napravi matrica promatranjem preslikavanja koje $(x_1, x_2, \ldots, x_n)$ preslikava u $(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)})$.Matrica koja predstavlja to preslikavanje označava se M_τ i zovemo ju **permutacijska matrica**. Odatle slijedi da M_τ ima svojstvo da, prilikom množenja matrica, permutira varijable s obzirom na permutaciju τ:*
$$M_\tau \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} x_{\tau(1)} \\ x_{\tau(2)} \\ \vdots \\ x_{\tau(n)} \end{bmatrix}.$$
Pogledajmo kako ovo funkcionira na određenom primjeru.
Promotrimo permutaciju (x,y,z) u (y,z,x). Ovdje je $\tau(1) = 2, \tau(2) = 3$ i

$\tau(3) = 1$ i lako se provjeri da

$$M_\tau \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} y \\ z \\ x \end{bmatrix}.$$

Budući da postoji $n!$ načina na koje možemo permutirati varijable, dobivamo $n!$ permutacijskih matrica. Nadalje, skup svih takvih matrica je zatvoren s obzirom na množenje pa zaključujemo da permutacijske matrice čine konačnu matričnu grupu u $GL(n,k)$ i označavamo ju sa S_n.

Sljedeću propoziciju navodimo bez dokaza.

Propozicija 2.3.4. *Neka je $G \subset GL(n,k)$ konačna matrična grupa. Tada:*

1. *$I_n \in G$*
2. *Ako je $A \in G$, onda $A^m = I_n$ za neki pozitivan cijeli broj m.*
3. *Ako je $A \in G$, onda je i $A^{-1} \in G$.*

Sljedeće što promatramo je kako elementi opće linearne grupe $GL(n,k)$ djeluju na polinome u $k[x_1, x_2, \ldots, x_n]$. Kako bismo pokazali što se i kako odvija, uzmimo da je $A = (a_{ij}) \in GL(n,k)$ i da je $f \in k[x_1, x_2, \ldots, x_n]$. Tada je

$$g(x_1, x_2, \ldots, x_n) = f(a_{11}x_1 + \cdots + a_{1n}x_n, \ldots, a_{n1}x_1 + \cdots + a_{nn}x_n) \tag{2.4}$$

ponovno polinom u $k[x_1, x_2, \ldots, x_n]$. Kako bismo ovo mogli ljepše zapisati, neka $\mathbf{x}$ označava stupčastu matricu varijabli $x_1, x_2, \ldots, x_n$, tj.

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

Sada pomoću množenja matrica možemo jednadžbu (2.4) napisati kao

$$g(\mathbf{x}) = f(A \cdot \mathbf{x}).$$

Primjerice, uzmimo polinom $f(x,y) = x^2 + xy + y^2 \in \mathbb{R}[x,y]$ i

$$A = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \in GL(2, \mathbb{R}).$$

Tada

$$\begin{aligned} g(x,y) = f(A\cdot\mathbf{x}) &= f(\frac{x-y}{\sqrt{2}}, \frac{x+y}{\sqrt{2}}) \\ &= (\frac{x-y}{\sqrt{2}})^2 + \frac{x-y}{\sqrt{2}}\cdot\frac{x+y}{\sqrt{2}} + (\frac{x+y}{\sqrt{2}})^2 \\ &= \frac{3}{2}x^2 + \frac{1}{2}y^2. \end{aligned}$$

Osobito je zanimljiva činjenica da ponekad ovaj proces daje isti polinom s kojim smo počeli. Na primjer, uzmemo li $h(x,y) = x^2 + y^2$ i koristimo gornju matricu A, onda se lako provjeri da je

$$h(\mathbf{x}) = h(A\cdot\mathbf{x}).$$

U ovakvim slučajevima kažemo da je h invarijantan na A. Upravo to dovodi nas do sljedeće fundamentalne definicije.

Definicija 2.3.5. Neka je $G \subset GL(n,k)$ konačna matrična grupa. Tada je polinom $f(\mathbf{x}) \in k[x_1, x_2, \ldots, x_n]$ **invarijanta na** G ako

$$f(\mathbf{x}) = f(A\cdot\mathbf{x}), \quad \textit{za sve } A \in G.$$

Skup svih invarijantnih polinoma označava se $k[x_1, x_2, \ldots, x_n]^G$.

Najosnovniji primjer invarijanti konačnih matričnih grupa jesu simetrični polinomi.

Primjer 2.3.6. *Ako razmatramo grupu $S_n \subset GL(n,k)$) permutacijskih matrica, onda je očito da*

$$k[x_1, x_2, \ldots, x_n]^{S_n} = \{\textit{svi simetrični polinomi u } k[x_1, x_2, \ldots, x_n]\}.$$

Prema Fundamentalnom teoremu za simetrične polinome, znamo da simetrične polinome možemo prikazati pomoću osnovnih simetričnih polinoma s koeficijentima u k. Stoga možemo pisati:

$$k[x_1, x_2, \ldots, x_n]^{S_n} = k[\sigma_1, \sigma_2, \ldots, \sigma_n].$$

Odatle slijedi da se svaka invarijanta može zapisati pomoću konačno mnogo invarijanti (osnovnih simetričnih polinoma). Dodatno, znamo da je prikaz pomoću osnovnih simetričnih polinoma jedinstven pa je naše znanje o invarijantama S_n vrlo izričito.

Jedan od ciljeva invarijatne teorije jest ispitati ponašaju li se sve invarijante $k[x_1, x_2, \ldots, x_n]^G$ lijepo kao one u prethodnom primjeru. U ovome radu se to neće detaljnije obrađivati pa bez dokaza navodimo nekoliko propozicija.

Propozicija 2.3.7. *Neka je $G \subset GL(n,k)$ konačna matrična grupa. Tada je skup $k[x_1, x_2, \ldots, x_n]^G$ zatvoren s obzirom na zbrajanje i oduzimanje te sadrži konstantne polinome.*

U prvom poglavlju pokazali smo da $k[x_1, x_2, \ldots, x_n]$ ima strukturu prstena. Primijetimo sada da je i $k[x_1, x_2, \ldots, x_n]^G$ također prsten. Štoviše, $k[x_1, x_2, \ldots, x_n]^G$ je potprsten od $k[x_1, x_2, \ldots, x_n]$.

Ranije u ovome poglavlju vidjeli smo da su homogene komponente simetričnih polinoma isto simetrične. U tom smislu sada primjećujemo da isto vrijedi za invarijante bilo koje konačne matrične grupe.

Propozicija 2.3.8. *Neka je $G \subset GL(n,k)$ konačna matrična grupa. Tada je polinom $f \in k[x_1, x_2, \ldots, x_n]$ invarijanta na G ako i samo ako su sve njegove homogene komponente invarijante na G.*

Lema 2.3.9. *Neka je $G \subset GL(n,k)$ konačna matrična grupa i neka su $A_1, A_2, \ldots, A_m \in G$ takve da svaka od njih može biti zapisana kao*

$$A = B_1 B_2 \cdots B_t,$$

*gdje je $B_i \in \{A_1, A_2, \ldots, A_m\}$ za svaki i (kažemo da $A_1, A_2, \ldots, A_m$ **generiraju** G). Tada je $f \in k[x_1, x_2, \ldots, x_n]$ u $k[x_1, x_2, \ldots, x_n]^G$ ako i samo ako je*

$$f(\boldsymbol{x}) = f(A_1 \cdot \boldsymbol{x}) = \cdots = f(A_m \cdot \boldsymbol{x}).$$

Konačno, sada možemo navesti i detaljno opisati nekoliko primjera prstena invarijanti.

Primjer 2.3.10. *Uzmimo za primjer konačnu matričnu grupu*

$$V_4 = \{ \begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix} \} \subset GL(2,k).$$

Vrlo često se ova grupa naziva Kleinova[4] *četvorna grupa. Oznaku V_4 koristimo iz razloga što je "četiri" na njemačkom jeziku "vier". Lako se provjeri da matrice*

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

[4]Felix Klein (1849. - 1925.) njemački je matematičar poznat po svom radu na teoriji grupa, kompleksnoj analizi i neeuklidskoj geometriji, a poseban doprinos dao je povezivanju geometrije i teorije grupa.

generiraju V_4. Tada prethodna lema ukazuje na to da je polinom $f(x,y)$ invarijanta na V_4 ako i samo ako

$$f(x,y) = f(-x,y) = f(x,-y).$$

Zapišemo li f kao $f = \sum_{ij} a_{ij}x^iy^j$ prvi od gornja dva uvjeta možemo razmotriti ovako:

$$\begin{aligned} f(x,y) = f(-x,y) &\iff \sum_{ij} a_{ij}x^iy^j = \sum_{ij}(-x)^iy^j \\ &\iff \sum_{ij} a_{ij}x^iy^j = \sum_{ij}(-1)^i a_{ij}x^iy^j \\ &\iff a_{ij} = (-1)^i a_{ij} \text{ za svaki } i,j \\ &\iff a_{ij} = 0 \text{ za } i \text{ neparan.} \end{aligned}$$

Slijedi zaključak da se x uvijek pojavljuje s parnom potencijom. Slično, uvjet $f(x,y) = f(x,-y)$ ukazuje na to da se y pojavljuje uvijek na parnu potenciju. Stoga možemo pisati

$$f(x,y) = g(x^2,y^2)$$

za jedinstven polinom $g(x,y) \in k[x,y]$. Obratno, svaki polinom f ovakvog oblika je očito invarijanta na V_4. To pokazuje da je

$$k[x,y]^{V_4} = k[x^2,y^2].$$

Dakle, svaka invarijanta od V_4 se može na jedinstven način zapisati kao polinom pomoću dvije homogene invarijante x^2 i y^2. Posebno, invarijate Kleinove četvorne grupe se uvelike ponašaju kao simetrični polinomi.

Primjer 2.3.11. *Za konačnu matričnu grupu koja se ponaša manje lijepo od Kleinove četvorne grupe možemo promatrati cikličnu grupu $C_2 = \{\pm I_2\} \subset GL(2,k)$ reda 2. U ovome slučaju, invarijanta se satoji od polinoma $f \in k[x,y]$ za koje je $f(x,y) = f(-x,-y)$. To je ekvivalentno sljedećem uvjet:*

$$f(x,y) = \sum_{ij} a_{ij}x^iy^j,$$

pri čemu je $a_{ij} = 0$ kad god je zbroj $i+j$ neparan broj.
To znači da je f invarijanta na C_2 ako i samo ako su eksponenti od x i y iste parnosti, tj. ili su oba parna ili su oba neparna. Dakle, monom x^iy^j, koji se pojavljuje u polinomu f, možemo zapisati u obliku

$$x^iy^j = \begin{cases} x^{2k}y^{2l} = (x^2)^k(y^2)^l, & \text{ako su } i,j \text{ parni} \\ x^{2k+1}y^{2l+1} = (x^2)^k(y^2)^l xy & \text{ako su } i,j \text{ neparni.} \end{cases}$$

Ovo znači da je svaki monom u f, stoga i sam f, polinom u homogenim invarijantama x^2, y^2 i xy. To možemo pisati i ovako:

$$k[x,y]^{C_2} = k[x^2, y^2, xy].$$

Primijetimo također da su potrebne sve tri invarijante kako bismo generirali $k[x,y]^{C_2}$.

Bibliografija

[1] David Cox, John Little, Donal O'Shea. *Ideals, varieties and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer - Verlag, New York, 1992.

[2] Boris Pavković, Darko Veljan. *Elementarna matematika I* Tehnička knjiga, Zagreb, 1992.

Sažetak

U ovome radu proučavamo invarijante konačnih matričnih grupa. Kao najosnovniji primjer takvih invarijanti javljaju se simetrični polinomi u n varijabli s koeficijentima iz proizvoljnog polja k. Upravo te simetrične polinome detaljno proučavamo, a dokazujemo i Fundamentalni teorem za simetrične polinome. Pristup proučavanju ovih tema jest elementara i ni na koji način potpun.

Summary

In this thesis, we study invariants of a finite matrix groups. The most basic example of such invariants is given by symmetric polynomials in n variables with coefficients in arbitraty field k. Furthermore, we prove The fundamental theorem of symmetric polynomials. Our treatment is elementary and by no means complete.

Životopis

Rođena sam 18. prosinca 1994. godine u Slavonskom Brodu. Izrazito sretno djetinjstvo provela sam u Slavonskom Kobašu gdje 2001. godine uspisujem Osnovnu školu "Dr. Stjepan Ilijašević", Područna škola Slavonski Kobaš. Istu završavam s odličnim uspjehom te 2009. godine upisujem Jezičnu gimnaziju u sklopu Gimnazije "Matija Mesić" u Slavonskom Brodu. Godine 2013. završavam četvrti razred gimnazije s odličnim uspjehom te polažem državnu maturu s vrlo dobrim uspjehom. Iste godine upisujem preddiplomski sveučilišni studij Matematika, nastavnički smjer na Matematičkom odsjeku Prirodoslovno - matematičkog fakulteta Sveučilišta u Zagrebu. Nakon završenog navedenog preddiplomskog studija, 2016. godine upisujem diplomski sveučilišni studij Matematika, nastavnički smjer na istome odsjeku. Od 2003. godine aktivna sam članica Kulturno umjetničkog društva "Matija Gubec" iz Slavonskog Kobaša, a od 2013. godine bavim se volonterskim radom u Kreativnoj udruzi mladih "Limes" iz Slavonskog Kobaša.