Hilbertov teorem o nulama

Sesar, Katarina

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni prijediplomski studij matematike

Katarina Sesar

Hilbertov teorem o nulama

Završni rad

Osijek, 2023.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni prijediplomski studij matematike

Katarina Sesar

Hilbertov teorem o nulama

Završni rad

Mentor: prof. dr. sc. Ivan Matić

Osijek, 2023.

Sažetak

Teme istražene u ovom radu spadaju u domenu komutativne algebre, obuhvaćajući i aspekte homološke algebre. Komutativna algebra čvrsto je povezana s algebarskom geometrijom, što predstavlja motivaciju za razvoj određenih koncepata unutar komutativne algebre. Osim toga, ovo je područje gdje se rezultati dobiveni proučavanjem tih koncepata mogu primijeniti u praksi. Iako su odnosi između geometrijskih objekata i matematičkih jednadžbi koje ih opisuju proučavani tijekom stoljeća, specifična povezanost između ovih dvaju područja nije bila potpuno jasna sve do sredine 19. stoljeća. U tom vremenskom razdoblju, David Hilbert je igrao ključnu ulogu svojim rezultatima, uključujući teorem o bazi, teorem o nulama, koncept polinomijalne strukture poznate kao Hilbertova funkcija i teorem o sizigiji. Ovi rezultati su postavili temelje komutativne algebre.

Ovaj rad započinje analizom afinih algebarskih skupova, a zatim se bavi idealima, s posebnim fokusom na koordinatne prstene, k-algebre konačnog tipa i maksimalne ideale. Završno poglavlje istražuje temu "malog" i "velikog" Hilbertovog teorema o nulama te se bavi njihovim aspektima.

Ključne riječi

Hilbertov teorem o nulama, algebra, Hilbertov teorem o bazi, afini algebarski skupovi, maksimalni ideali u prstenovima polinoma

Hilbert's Nullstellensatz

Abstract

The topics covered in this text belong to the commutative algebra domain, including homological algebra elements. Commutative algebra is closely linked to algebraic geometry, which serves as motivation for the development of certain concepts within commutative algebra. Moreover, this is an area where results obtained by studying these concepts can be practically applied. Although the relationship between geometric objects and the mathematical equations that describe them has been studied for centuries, the specific connection between these two fields discussed here was not fully recognized until the mid-nineteenth century. During that period, David Hilbert's results, including the basis theorem, the nullstellensatz, the polynomial structure known as Hilbert's function, and the syzygy theorem, played a crucial role in laying the foundations of commutative algebra.

This paper begins with an analysis of affine algebraic sets, followed by a discussion of ideals, with a particular focus on coordinate rings, finite-type k-algebras, and maximal ideals. The final chapter explores the topic of the "small" and "big" Hilbert nullstellensatz theorems and delves into their aspects.

Keywords

Hilbert's zero theorem, algebra, Hilbert's basis theorem, affine algebraic sets, maximal ideals in rings of polynomials

Sadržaj

Uvod

David Hilbert (Slika 1), istaknuti njemački matematičar, ostavio je dubok i važan doprinos u nekoliko matematičkih disciplina tijekom svoje karijere. Njegovi značajni radovi obuhvaćaju širok spektar matematičkih područja, a jedan od njegovih ranih doprinosa je "Hilbertov teorem o konačnosti" koji je objavio 1888. godine. Ovaj teorem predstavlja bitan korak u razvoju komutativne algebre.

Prije Hilbertovog teorema, matematičar Paul Gordan (Slika 2) već je formulirao teorem o konačnoj generiranosti prstena invarijanti binarnih formi. Međutim, Gordanova metoda uključivala je vrlo složene izračune i primjenjivala se samo na funkcije s dvije varijable. Hilbert je prepoznao potrebu za inovativnim pristupom ovom problemu i razvio "Hilbertov teorem o bazi". Ovaj teorem donosi konkretnu i apstraktnu izjavu o tome da je svaki ideal u prstenu polinoma s više varijabli, $k[X_1, \ldots, X_n]$, konačno generiran nad poljem k. To znači da postoji konačan skup osnovnih polinoma koji, korištenjem određenih operacija, može generirati sve ostale polinome iz tog ideala. Hilbert je dokazao ovu tvrdnju koristeći matematičku indukciju, čime je stvorio temelje za buduća istraživanja u algebri.

Važno je napomenuti da Hilbertova metoda ne pruža algoritam za generiranje ovih osnovnih polinoma za dani ideal, već samo potvrđuje njihovo postojanje. Ova ideja o bazama i idealima igra ključnu ulogu u razumijevanju struktura u komutativnoj algebri i ima brojne primjene u različitim matematičkim kontekstima.

Preusmjerimo se sada na Hilbertov teorem o nulama, jedno od njegovih najpoznatijih postignuća. Ovaj teorem predstavlja kamen temeljac za razumijevanje i rješavanje sustava polinomijalnih jednadžbi. Često ga nazivamo i Hilbertovim teoremom o nulama, a proizlazi iz dubokog proučavanja matematičke strukture polinoma i njihove veze s geometrijskim objektima.

Hilbertov teorem o nulama datira iz sredine 19. stoljeća, kada su matematičari počeli istraživati veze između algebarskih sustava jednadžbi i geometrijskih figura. U tom razdoblju, David Hilbert, iznimno utjecajan matematičar svoga vremena, istraživao je fundamentalna pitanja u području komutativne algebre i algebarske geometrije.

Hilbertov teorem o nulama nije samo matematički rezultat, već i duboko konceptualno otkriće koje je preokrenulo naše razumijevanje veza između algebarskih struktura i geometrijskih entiteta. Ovaj teorem pruža ključne uvide u način na koji se geometrijske točke i oblici povezuju sa sustavima polinomijalnih jednadžbi, otvarajući vrata širokom spektru

primjena u matematici i povezanim znanostima.

U nastavku ovog rada, detaljnije ćemo istražiti Hilbertov teorem o nulama, razumjeti njegove osnove, istražiti njegove posljedice i proučiti značajne primjene u različitim granama matematike.

Slika 1: David Hilbert

Slika 2: Paul Gordan

1 Afini algebarski skupovi

U ovom poglavlju ćemo promotriti "teorem skupa nultočaka", koji predstavlja ključni koncept algebarske geometrije nad poljima. U tradicionalnoj koordinatnoj geometriji u dvije ili tri dimenzije, susrećemo različite objekte kao što su kružnice, koje se mogu opisati kao skup nultočaka polinoma $f(X,Y) = X^2 + Y^2 - 1$ u $\mathbb{R}^2$, ili hiperboloidi, koji su skup nultočaka polinoma $f(X,Y,Z) = X^2 + Y^2 - Z^2 - 1$ u trodimenzionalnom prostoru $\mathbb{R}^3$. Ovi objekti služe kao primjeri afinih algebarskih skupova.

Dakle, formalnije, neka je $\{f_i(a_1,\ldots,a_n)\}_{i\in S}$ neki skup polinoma u n varijabli s realnim koeficijentima, indeksiranim nekim (konačnim ili beskonačnim) skupom S. **Pravi afini algebarski skup** $V(S)$ definiramo s

$$V(S) := \{(a_1,\ldots,a_n) \in \mathbb{R}^n : f_i(a_1,\ldots,a_n) = 0 \text{ za svaki } i \in S\}.$$

To jest, $V(S)$ je skup zajedničkih nultočaka svih polinoma u S, a često se naziva **pravim algebarskim skupom**. Slično se može definirati **kompleksni algebarski skup** kao skup zajedničkih nultočaka u $\mathbb{C}^n$ neke familije polinoma S u n varijabli $X_1,\ldots,X_n$ s **kompleksnim** koeficijentima. Ako je S konačan skup, recimo $S = \{f_1,\ldots,f_k\}$ obično pišemo $V(S)$ kao $V(f_1,\ldots,f_k)$. Dobiva se, kao što će biti objašnjeno kasnije, da se svi algebarski skupovi, realni ili kompleksni, mogu definirati i koristeći samo konačno mnogo polinoma [4, poglavlje 1.2 Affine Algebraic Sets].

Jasno je da ako je f polinom oblika

$$f(X_1,\ldots,X_n) = \sum_{i\in T} g_i(X_1,\ldots,X_n) f_i(X_1,\ldots,X_n),$$

gdje je T bilo koji konačni podskup od S, a g_i bilo koji polinom u $X_1,\ldots,X_n$, tada će f identički nestati na algebarskom skupu $V(S)$. Tada se može postaviti obrnuto pitanje: Pretpostavimo da neki polinom $f(X_1,\ldots,X_n)$ identički nestaje na $V(S)$. Može li se ustvrditi da je f kombinacija nekih $f_i \in S$?

Pojasnit ćemo ovu konceptualnu dilemu kroz trivijalan primjer kako bismo ilustrirali zašto očekivanje da svaki polinom koji identički nestaje na nekom algebarskom skupu može biti izražen kao umnožak drugih polinoma nije uvijek ispravno. Uzmimo polinom drugog stupnja $F(X) := X^2$ kao naš primjer te analizirajmo njegov algebarski skup $V(F)$ u realnom

prostoru $\mathbb{R}$.

$V(F)$ u stvarnosti predstavlja samo jednu točku, odnosno 0. Ovaj algebarski skup sadrži sve točke u ravnini koje zadovoljavaju uvjet $F(X) = 0$, što u ovom slučaju znači da je jedini element skupa $V(F)$ točka 0. Sada, promotrimo polinom X prvog stupnja. Jasno je da će X identički nestati na skupu $V(F)$ jer će svaka točka u skupu $V(F)$ imati koordinate 0, te će biti $F(0) = 0$.

No, ključna poanta ovdje je da polinom X prvog stupnja nikada ne može biti izražen kao umnožak $g(X)F(X)$, gdje je $g(X)$ bilo koji drugi polinom. Razlog za to leži u činjenici da je polinom $F(X)$ drugog stupnja. Pokušamo li pronaći polinom $g(X)$ takav da $X = g(X)F(X)$, primijetit ćemo da to nije moguće jer će $F(X)$ sadržavati kvadratnu komponentu, dok je X linearna funkcija. Ova konkretna situacija ilustrira da očekivanje da svaki polinom koji identički nestaje na nekom algebarskom skupu može biti rastavljen na umnožak drugih polinoma nije uvijek ispravno.

Ovaj primjer također vrijedi i kada zamijenimo realni prostor $\mathbb{R}$ kompleksnim prostorom $\mathbb{C}$. Drugim riječima, ova ograničenja su prisutna i u realnom i u kompleksnom prostoru. Važno je napomenuti da je X^2 zapravo kvadratni monom, što može stvoriti zabludu da se polinom X može dobiti kao umnožak drugih polinoma. Ipak, ovaj primjer naglašava da takva pretpostavka nije uvijek točna i da se moramo nositi s određenim ograničenjima u algebarskoj geometriji [4, 1.2 Affine Algebraic Sets].

Ovaj trivijalan primjer ističe složenost analize algebarskih skupova i potrebu za preciznim razumijevanjem struktura polinoma i algebarskih skupova kako bismo razvili dublje uvide u algebarsku geometriju.

Hipoteza 1.1. [4, Conjecture 1.1] Pretpostavimo da polinom f s realnim (odnosno kompleksnim) koeficijentima, u n varijabli, identički nestaje na algebarskom skupu $V(S) \subset \mathbb{R}^n$, (odnosno $\subset \mathbb{C}^n$). Zatim, tvrdimo da postoji pozitivan cijeli broj r takav da je

$$f^r = g_1 f_1 + \cdots + g_k f_k,$$

gdje su g_i neki polinomi s realnim (odnosno kompleksnim) koeficijentima, i $f_i \in S$.

Prvo ispitajmo ovu pretpostavku u konkretnom slučaju, na primjeru u nastavku. Uzmimo $V(F) \subset \mathbb{R}^2$ gdje je $F(X, Y) = X^2 + Y^2$. Jasno, $V(F)$ je samo jedna točka (0,0), ishodište. Polinom X identički nestaje na $V(F)$. Međutim, može se lako provjeriti da niti jedan X^r

od X ne može biti višekratnik F.

Promotrimo ovaj isti primjer nad skupom kompleksnih brojeva $\mathbb{C}$. Sada, $V(F) \subset \mathbb{C}^2$ postaje veliki skup. Zapravo $V(F) = \{(a, \pm ia) : a \in \mathbb{C}\}$ je par (kompleksnih) pravaca u $\mathbb{C}^2$. Ovo je bolji oblik što pokazuje sljedeći primjer.

Primjer 1.1. *[4, poglavlje 1.2 Affine Algebraic Sets] Može se pokazati da ako je polinom f s kompleksnim koeficijentima identički jednak nuli na $V(F) \subset \mathbb{C}^2$, gdje je $F(X, Y) = X^2 + Y^2$, tada f mora biti djeljiv s F.*

2 Ideali

Promotrimo koncept ideala u kontekstu polinoma i algebre nad poljem k, gdje je k proizvoljno polje. Za svaki podskup Z od k^n, gdje n označava broj varijabli, definiramo **ideal** $I(Z)$ u prstenu polinoma $k[X_1, \ldots, X_n]$ kao:

$$I(Z) = \{f \in k[X_1, \ldots, X_n] : f(a_1, \ldots, a_n) = 0 \text{ za svaki } (a_1, \ldots, a_n) \in Z\}.$$

Ovaj ideal sastoji se od svih polinoma koji identički nestaju na skupu Z. Stoga ga nazivamo idealom od Z.

Sada, za proizvoljan skup S podskupa prstena $k[X_1, \ldots, X_n]$, možemo definirati odgovarajući **algebarski podskup** $V(S)$ nad poljem k na sljedeći način:

$$V(S) = \{(a_1, \ldots, a_n) \in k^n : f(a_1, \ldots, a_n) = 0 \text{ za svaki } f \in S\}.$$

Primijetimo da je $V(S) = V(\langle S \rangle)$[1] tako da su svi algebarski skupovi skupovi nultočaka nekih ideala, a mogli bismo smatrati samo algebarske skupove $V(I)$ za $I \subset k[X_1, \ldots, X_n]$ idealom. Zapravo, preciznije je:

Propozicija 2.1 (**Hilbertov teorem o bazi**). *[4, Proposition 2.4] Ako je k polje, a $I \subset k[X_1, \ldots, X_n]$ ideal, tada je I konačno generiran, to jest $I = \langle f_1, \ldots, f_m \rangle$ za neke polinome f_i, $1 \leq i \leq m$.*

Konkretno, svaki algebarski skup je skup zajedničkih nultočaka konačno mnogo polinoma, jer za bilo koji podskup $S \subset k[X_1, \ldots, X_n]$ vrijedi

$$V(S) = V(\langle S \rangle) = V(\langle f_1, \ldots, f_m \rangle) = V(f_1, \ldots, f_m).$$

Dokaz. Slučaj $n = 1$ je jednostavan jer za prsten polinoma u jednoj varijabli $k[X]$, možemo podijeliti polinom f s drugim polinomom g stupnja $deg\ g = d$ i dobiti ostatak r takav da je ili $r = 0$ ili $deg\ r < d$. Znamo da je $k[X]$ domena glavnih ideala, no to ne vrijedi za $n \neq 2$. □

[1] $\langle S \rangle$ – ideal generiran sa S

2.1 Koordinatni prstenovi, k-algebre konačnog tipa

Sada možemo preciznije istražiti geometrijsko značenje kvocijenata prstenova polinoma. Pretpostavimo da imamo algebarski skup Z u k^n. Svaki polinom $f(X_1, \ldots, X_n)$, možemo interpretirati kao funkciju s k-vrijednostima u k^n, evaluacijom u točki $p = (a_1, \ldots, a_n)$. Napravimo li restrikciju od f na podskup $Z \subset k^n$ dobivamo funkciju definiranu na Z. No, različiti polinomi $f,\ g \in k[X_1, \ldots, X_n]$ mogli bi na kraju rezultirati istom funkcijom na Z ako i samo ako $f - g$ identički nestaje na Z. Odnosno, ako i samo ako je $\overline{f} = \overline{g}$ u $k[X_1, \ldots, X_n]/I(Z)$. Drugim riječima, f i g će dati iste vrijednosti na Z ako i samo ako je $f - g \in I(Z)$. Stoga, kvocijentni prsten $k[X_1, \ldots, X_n]/I(Z)$ predstavlja prsten funkcija definiranih na Z, koje su zapravo restrikcije polinoma na k^n. Ovaj kvocijentni prsten često nazivamo prstenom **k-regularnih funkcija** ili **k-koordinatnim prstenom** od Z, te označavamo s $k[Z]$.

Važno je napomenuti da ako je I pravi ideal u $k[X_1, \ldots, X_n]$, tada je njegov presjek sa skupom konstantnih polinoma jednak $\{0\}$. Zato kvocijentni prsten $k[X_1, \ldots, X_n]/I$ sadrži k kao podprsten te postaje k-algebra. Ovi kvocijentni prstenovi oblika $B = k[X_1, \ldots, X_n]/I$, gdje je I pravi ideal, često nazivamo **k-algebrama konačnog tipa**. Klase ekvivalencije X_i u B obično označavamo s x_i radi praktičnosti i nazivamo **koordinatnim funkcijama**.

Jasno je da je $\overline{f(X_1, \ldots, X_n)} = f(x_1, \ldots, x_n)$ prema definiciji množenja i zbrajanja u B, i stoga ti x_i generiraju B kao k-algebru, tj. svaki element od B može se napisati kao polinom u x_i s koeficijentima od k. Važno je napomenuti da neki od ovih polinoma u x_i mogu biti nula jer, ako je $f(X_1, \ldots, X_n) \in I$, tada je po definiciji, klasa ekvivalencije $\overline{f(X_1, \ldots, X_n)} = 0$ u B, tj. $f(X_1, \ldots, X_n) = 0$. Obrnuto, ako je $f(X_1, \ldots, X_n) = 0$, tada je $f \in I$. Dakle I je upravo skup 'ograničenja' ili 'relacija' koje mjere odstupanje prstena B od prstena polinoma $k[X_1, \ldots, X_n]$. Prsten B označavamo s $k[x_1, \ldots, x_n]$, a mala slova nas podsjećaju da, za razliku od prstena polinoma $k[X_1, \ldots, X_n]$, mogu postojati netrivijalni odnosi između x_i u $k[x_1, \ldots, x_n]$.

Kao primjer, ako uzmemo ideal $I = (X^2 - 2)$ u $\mathbb{Q}[X]$, tada u prstenu $\mathbb{Q}[X]/I = \mathbb{Q}[x]$, dobivamo $x^2 = 2$. Ovaj prsten (koji je zapravo polje) također označavamo s $\mathbb{Q}[\sqrt{2}]$ i predstavlja najmanje potpolje $\mathbb{R}$ koje sadrži $\mathbb{Q}$ i $\sqrt{2}$. Slično, u $\mathbb{R}$-algebri konačnog tipa $\mathbb{R}[X]/(X^2 + 1)$ (koja je zapravo $\mathbb{R}[i] = \mathbb{C}$), imamo $i^2 + 1 = 0$. S druge strane, budući da je π transcendentan, prsten $\mathbb{Q}[\pi]$ (definiran kao najmanja $\mathbb{Q}$-podalgebra od $\mathbb{R}$ koja sadrži π) izomorfan je prstenu polinoma $\mathbb{Q}[X]$.

Lema 2.1. *[4, Lemma 2.6] Ako je B k-algebra konačnog tipa, tada je dimenzija B kao k-vektorskog prostora (u oznaci $dim_k B$) prebrojiva.*

Dokaz. Prema definiciji, $B = k[x_1, \ldots, x_n]$ za neki n. Budući da je svaki element u B polinom od x_i s koeficijentima u k, to je (ne nužno jedinstvena) konačna k-linearna kombinacija monoma

$$\{{x_1}^{i_1} {x_2}^{i_2} \cdots {x_n}^{i_n} : i_j \in \mathbb{N}\}$$

koji je prebrojiv skup S. Skup S sadrži bazu, koja je stoga također prebrojiv skup.

□

2.2 Maksimalni ideali

Pretpostavimo da su svi prstenovi komutativni s jedinicom. U kontekstu komutativnih prstenova, ideal I u prstenu A nazivamo **maksimalnim idealom** ako ispunjava dva ključna uvjeta:

- I je pravi ideal, što znači da nije jednak cijelom prstenu A,
- I nije sadržan ni u jednom drugom pravom idealu.

Sada ćemo dokazati tvrdnju da je svaki pravi ideal I prstena A sadržan u nekom maksimalnom idealu. Promotrimo familiju Σ svih pravih ideala koji sadrže I. Ova familija nije prazna jer znamo da ideal I pripada familiji Σ. Sada ćemo primijeniti koncept parcijalnog uređaja na familiju Σ i pokazati da svi lanci (bilo koji potpuno uređen podskup familije Σ) ima gornju granicu, koja također pripada familiji Σ.

Neka je $\{J_\alpha\}_{\alpha\in\Gamma}$ bilo koji potpuno uređeni podskup od familije Σ. Želimo dokazati da je $\cup_{\alpha\in\Gamma} J_\alpha$ također pravi ideal koji pripada familiji Σ. Prvo primijetimo da je $\cup_{\alpha\in\Gamma} J_\alpha$ pravi ideal jer je unija pravih ideala i ostaje unija pravih ideala.

Sada trebamo pokazati da je $\cup_{\alpha\in\Gamma} J_\alpha$ sadržan u nekom maksimalnom idealu. Budući da je svaki J_α pravi ideal koji sadrži I, $\cup_{\alpha\in\Gamma} J_\alpha$ također sadrži I. To znači da je $\cup_{\alpha\in\Gamma} J_\alpha$ u familiji Σ, jer smo pretpostavili da Σ sadrži sve prave ideale koji sadrže I.

Sada, prema Zornovoj lemi, svaki potpuno uređeni skup u familiji Σ ima gornju granicu u familiji Σ, koja je maksimalni ideal koji također sadrži ideal I. Ovo znači da svaki pravi ideal I prstena A može biti sadržan u nekom maksimalnom idealu, čime je tvrdnja dokazana.

Napomena 2.1. Ovaj dokaz koristi Zornovu lemu, koja je ekvivalentna aksiomu izbora u teoriji skupova i igra ključnu ulogu u teoremima vezanim uz postojanje maksimalnih ideala u komutativnim prstenovima.

Lema 2.2. *[4, Lemma 3.6] Za polje k, sljedeći uvjeti su ekvivalentni:*

(i) Svaki polinom $f(X)$ pozitivnog stupnja u $k[X]$ ima nultočku u k, tj. postoji $\alpha \in k$ takav da je $f(\alpha) = 0$.

(ii) Svaki polinom $f(X)$ pozitivnog stupnja je produkt linearnih faktora. Stoga je svaka nultočka od $f(X)$ u k.

(iii) Jedini ireducibilni polinomi pozitivnog stupnja su linearni polinomi.

(iv) I je maksimalni ideal u $k[X]$ ako i samo ako je $I = (X - \alpha)$ za neki $\alpha \in k$.

*Polje k nazivamo **algebarski zatvorenim poljem** ako i samo ako zadovoljava bilo koji od gornja četiri ekvivalentna uvjeta.*

Propozicija 2.2. *[4, Proposition 3.8] Neka je $k \subset K$ proširenje polja takvo da je K k-algebra konačnog tipa. Pretpostavimo da je k neprebrojiv skup. Tada je K algebarsko proširenje od k.*

Dokaz. Prema Lemi 2.1, dimenzija vektorskog prostora $dim_k K$ je prebrojiva, s obzirom na pretpostavku o skupu K. Svaki element iz skupa k sigurno je algebarski nad skupom k. Neka je sada α bilo koji element iz skupa K koji nije u skupu k, to jest $\alpha \in K \backslash k$. Promotrimo skup:

$$S = \{(\alpha - a)^{-1} : a \in k\}.$$

Ovaj skup ima smisla jer za svaki a iz k izraz $(\alpha - a)$ nije jednak nuli. Također, svi elementi ovog skupa su različiti. Stoga, kardinalnost skupa S je ista kao kardinalnost skupa k, odnosno S je neprebrojiv podskup skupa K.

Stoga, ne mogu svi elementi skupa S biti k-linearno nezavisni, jer bi u suprotnom taj skup mogao biti proširen na k-vektorski prostor koji bi također bio neprebrojiv, a to je u suprotnosti sa činjenicom da je dimenzija vektorskog prostora K prebrojiva. Dakle, postoje neki ne-nul elementi $\{\lambda_i\}_{i=1}^n \in k$ takvi da je

$$\lambda_1(\alpha - a_1)^{-1} + \cdots + \lambda_n(\alpha - a_n)^{-1} = 0.$$

Množenjem ove relacije s $\prod_{i=1}^{n}(\alpha - a)^{-1}$ dobija se polinomijalna relacija $f(\alpha) = 0$ s koeficijentima u k.

Dakle, α je algebarski nad k. □

Napomena 2.2. Ovaj dokaz pokazuje da elementi koji nisu iz skupa k i pripadaju skupu K moraju biti algebarski nad skupom k, jer bi inače neprebrojivost skupa K dovela do neprebrojivosti dimenzije vektorskog prostora K, što je suprotno pretpostavci da je $dim_k K$ prebrojiva.

3 Hilbertov teorem o nulama

Hilbertov Nullstellensatz, ili Hilbertov teorem o nulama, predstavlja klasični rezultat od izuzetne važnosti u komutativnoj algebri i algebarskoj geometriji. Važno je napomenuti da ovaj teorem vrijedi samo kada koristimo osnovno polje $\mathbb{C}$, odnosno polje kompleksnih brojeva, ili općenito algebarski zatvoreno polje. U stvari, kada se koristi polje $\mathbb{C}$, možemo ga smatrati izvanrednom generalizacijom fundamentalnog teorema algebre. Postoje dvije verzije Hilbertovog Nullstellensatz-a koje su poznate kao "Mali Nullstellensatz" i "Veliki Nullstellensatz". Izvorna verzija ovog teorema prvi put se pojavila u Hilbertovom radu iz 1893. godine o potpunim sustavima invarijanata. Hilbert je ovaj teorem nazvao trećim općim teoremom u teoriji algebarskih funkcija, nadovezujući se na teoreme I i III iz svojeg rada iz 1890. godine o teoriji algebarskih formi. Ovi teoremi danas su poznati kao Hilbertov teorem o bazi i Hilbertov teorem o sizigiji.

Prije nego što uvedemo nove pojmove, iskazat ćemo i dokazati neke pomoćne tvrdnje koje će nam biti od koristi.

U nastavku, neka je k naše polje koje je **neprebrojivo i algebarski zatvoreno** (npr. $k = \mathbb{C}$).

3.1 Maksimalni ideali u prstenovima polinoma

Primijetimo da je polje $\mathbb{C}$ neprebrojivo algebarski zatvoreno polje. S druge strane, polja $\overline{\mathbb{Q}}$ i $\overline{\mathbf{F}}_p$ nisu neprebrojiva.

Sada možemo dublje analizirati maksimalne ideale u prstenu polinoma $k[X_1, \ldots, X_n]$. Imamo koristan rezultat koji se često naziva "mali teorem o nulama", iako je ekvivalentan kasnijem "velikom teoremu o nulama".

Propozicija 3.1 (**Hilbertov teorem o nulama I**). *[4, Proposition 4.1] Neka je k kao što je ranije opisano. Tada je ideal $I \subset k[X_1, \ldots, X_n]$ maksimalan ako i samo ako je $I = (X_1 - a_1, \ldots, X_n - a_n)$ za neke $a_1, \ldots, a_n \in k$. Drugim riječima, maksimalni ideali su u bijektivnoj korespondenciji s točkama iz k^n.*

Dokaz. Za slučaj jedne varijable $n = 1$, rezultat je prikazan u (iv) Leme 2.2.

Prvo, uvjerimo se da su svi ideali $I = (X_1 - a_1, \ldots, X_n - a_n)$ doista maksimalni. Za ovo trebamo utvrditi da je A/I polje, gdje je $A = k[X_1, \ldots, X_n]$. Ako je $f(X_1, \ldots, X_n)$ bilo koji polinom u A, možemo ga zapisati kao $f((X_1 - a_1) + a_1, \ldots, (X_n - a_n) + a_n)$. Sada bilo koja

potencija $((X_i - a_i) + a_i)^{n_i}$ može biti napisana u obliku $(X_i - a_i)h_i + a_i^{n_i}$ (prema binomnom poučku), gdje je h_i polinom u X_i. Razvojem u Taylorov red dobivamo

$$f(X_1, \ldots, X_n) = f(a_1, \ldots, a_n) + \sum_{i=1}^{n} g_i(X_1, \ldots, X_n)(X_i - a_i),$$

gdje su $g_i \in A$ neki polinomi. Drugi član na desnoj strani je očigledno u idealu $I = (X_1 - a_1, \ldots, X_n - a_n)$. Ovo pokazuje da je svaki element u $A = k[X_1, \ldots, X_n]$ kongruentan elementu $f(a_1, \in, a_n) \in k \pmod{I}$. Također element $a \in k \subset A$ je jasno kongruentan samo sebi $\pmod{I}$, i nijednom drugom elementu od k (budući da je $I \cap k = \{0\}$). Stoga je A/I samo polje k, a I je maksimalan.

Kako bismo dokazali obratnu tvrdnju, potrebne su nam algebarske pretpostavke na k. Neka je $I \subset A = k[X_1, \ldots, X_n]$ maksimalni ideal. Tada je po definiciji A/I k-algebra konačnog tipa, sadrži k i polje je (prema [4], Lemma 3.1). Označimo ga s K. Stoga je K proširenje polja k. Prema [4] Corollary 3.9, $K = k$.

Označavajući klase ekvivalencije od X_i sa $\overline{X_i} \in K = A/I$, slijedi da je $\overline{X_i} = a_i \in k$ za svaki $i = 1, \ldots, n$. Kažemo li da je $\overline{X_i} = a_i$ u K, to po definiciji znači da je $X_i - a_i \in I$ za sve i. Dakle, ideal $(X_1 - a_1, \ldots, X_n - a_n)$ je sadržan u idealu I. Međutim, vidjeli smo ranije da je ideal $(X_1 - a_1, \ldots, X_n - a_n)$ maksimalan. Stoga mora biti jednak I, koji je pravi ideal (budući da je maksimalni ideal). Ovime smo dokazali tvrdnju. □

Korolar 3.1. *[4, Corollary 4.3] Neka je k kao ranije, a $\{f_i\}_{i=1}^m$ neki skup polinoma u $A = k[X_1, \ldots, X_n]$. Tada je algebarski skup $V(f_1, \ldots, f_m)$ prazan ako i samo ako postoje polinomi $h_i \in A$ za $i = 1, \ldots, m$ takvi da je $\sum_{i=1}^m h_i f_i = 1$.*

Dokaz. Promotrimo ideal $J = (f_1 \ldots, f_m)$. Tada je ili J pravi ideal ili je $J = A$. Da je J pravi ideal, prema [4, Lemma 3.1], slijedilo bi da je $J \subset I$ za neki maksimalni ideal I. Prema Propoziciji 3.1, $I = (X_1 - a_1, \ldots, X_n - a_n)$. Stoga bi svaki element od J bio oblika $\sum_{i=1}^n g_i(X_i - a_i)$, i iščezavao bi u točki $(a_1, \ldots, a_n)$.

Posebno $V(J) = V(f_1, \ldots, f_m)$ bi sadržavao $(a_1, \ldots, a_n)$ i bio bi neprazan skup. Stoga je $J = A$ te je $1 \in J = (f_1, \ldots, f_m)$. Drugim riječima, $V(f_1, \ldots, f_m) = \emptyset$ implicira
$1 = \sum_{i=1}^m h_i f_i$ za neki $h_i \in A$.

Suprotno je očito (iz $1 \neq 0$). □

Primijetimo koliko je bitno da je k algebarski zatvoreno za gornji zaključak jer, na primjeru $V(X^2 + 1) \subset \mathbb{R}$, vidimo da je skup prazan, ali nije moguće pomnožiti $X^2 + 1$ s bilo

kojim polinomom h iz $\mathbb{R}[X]$ kako bismo dobili 1.

Nakon što smo duboko uronili u svijet algebarske teorije i istražili razne algebarske strukture, napokon smo stigli do ključnog trenutka. Sada ćemo uvesti veliki Hilbertov teorem o nulama, temeljno dostignuće koje objedinjuje sve prethodno izložene algebarske koncepte. Ovaj teorem ima duboke posljedice i primjene u matematici i drugim znanstvenim disciplinama.

Teorem 3.1 (**Hilbertov teorem o nulama II**). *[4, Theorem 4.4] Neka je k neprebrojivo i algebarski zatvoreno. Ako polinom $f \in A = k[X_1, \ldots, X_n]$ identički nestaje u svim točkama iz $V(I)$ za neki ideal $I \subset A$, tada je $f^r \in I$ za neki r.*

Dokaz. Prema Hilbertovom teoremu o bazi, neka je $I = (f_1, \ldots, f_m)$. Ako je $f = 0$, nema se što dokazivati, pa pretpostavimo da je $f \neq 0$. Trik je dodati dodatnu varijablu i "invertirati f" (ovo nazivamo Rabinowitchev trik). Doista, svi polinomi u A mogu se smatrati elementima većeg prstena $B = k[X_1, \ldots, X_{n+1}]$. Promotrimo ideal $J \subset B$ generiran elementima $f_i(X_1, \ldots, X_n)$ za $1 \leq i \leq m$ i dodatnim elementom $X_{n+1}f(X_1, \ldots, X_n) - 1$. Tvrdimo da je $V(J) \subset k^{n+1}$ prazan. Da nije tako, postojala bi točka $(a_1, \ldots, a_{n+1}) \in V(J)$. Budući da bi svi $f_i = f_i(X_1, \ldots, X_n)$ morali nestati u ovoj točki, slijedilo bi da je $(a_1, \ldots, a_{n+1}) \in V(J)$. Također, kako bi $X_{n+1}f - 1$ morao nestati u ovoj točki, imali bismo $a_{n+1}f(a_1, \ldots, a_n) = 1$. Ali onda, budući da f identički nestaje na $V(I)$ i $(a_1, \ldots, a_n) \in V(I)$, imamo $f(a_1, \ldots, a_n) = 0$. Stoga je $a_{n+1} \cdot 0 = 1$, tj. $0 = 1$, čime smo došli do kontradikcije, to jest tvrdnja je dokazana.

Dakle, prema Korolaru 3.1 (primijenjenom na $J \subset B$), moraju postojati polinomi $h_i(X_1, \ldots, X_{n+1}) \in B$ takvi da:

$$1 = h_{m+1}(X_1, \ldots, X_{n+1})(X_{n+1}f(X_1, \ldots, X_n) - 1) + \sum_{i=1}^{m} h_i(X_1, \ldots, X_{n+1})f_i(X_1, \ldots, X_n).$$

Gornji identitet vrijedi u prstenu polinoma

$$B = k[X_1, \ldots, X_n].$$

Zamjena $X_i = X_i$ za $1 \leq i \leq n$ i $X_{n+1} = 1/f$ u ovom identitetu daje nam identitet u polju $k(X_1, \ldots, X_n)$, budući da je $f \neq 0$. Ova zamjena uklanja prvi član te dobivamo

$$1 = \sum_{i=1}^{m} h_i(X_1, \ldots, X_n, \frac{1}{f})f_i(X_1, \ldots, X_n)$$

kao identitet u $k(X_1, \ldots, X_n)$. Jasno, korištenjem dovoljno velike potencije f^r kao zajedničkog nazivnika na desnoj strani, (možemo uzeti i da je r = maksimum stupnjeva od X_{n+1} svih h_i), i unakrsnim množenjem, imamo

$$f^r = \sum_{i=1}^{m} P_i(X_1, \ldots, X_n) f_i(X_1, \ldots, X_n),$$

gdje su $P_1, \ldots, P_m$ neki polinomi. Ovaj posljednji identitet vrijedi u polju $k(X_1, \ldots, X_n)$, a obje strane identiteta su u $A = k[X_1, \ldots, X_n]$. Budući da se A nalazi kao podprsten u $k(X_1, \ldots, X_n)$, identitet vrijedi u A. Stoga je $f^r = \sum_i P_i f_i \in I$ to je i trebalo pokazati.

□

Literatura

[1] D. Hilbert, *Ueber die Theorie der algebraischen Formen*, Math Ann. 36 (1890), 473–534, 1890.

[2] D. Hilbert, *Ueber die vollen Invariantensysteme*, Math. Ann. 42 (1893), 313–373, 1893.

[3] H. Kraljević, Algebra, skripta, Osijek, 2007. (javno dostupno na: `https://web.math.pmf.unizg.hr/~hrk/nastava/2006-07/algebra_Osijek_2006_7.pdf`)

[4] V. Pati, *Hilbert's Nullstellensatz and the Beginning of Algebraic Geometry*, Resonance, 36-57, 1999.