

Izreki o ničlah

Jon Mikoš

Mentor: dr. Jakob Cimprič

1 Uvod

Področje geometrije nam podaja mnogo zanimivih, težkih in globokih vprašanj. V iskanju odgovorov pogosto postavimo probleme v drug kontekst, kjer uporabimo tehnike in metode iz na videz nepovezanih področij matematike. Nas bo zanimala povezava med algebro ter geometrijo, preko katere se lahko nato razvijejo dodatna orodja za obravnavo samih problemov.

2 Hilbertov izrek o ničlah

Pogosto si predstavljamo, da geometrijski objekti živijo v neki abstraktni ravnini oziroma v nekem *afinem prostoru*. Na tem prostoru vpeljemo koordinate, s čimer postane afin prostor izomorfen K^n . Pri tem je K polje, iz katerega izbiramo vrednosti za koordinate. S tem lahko enačimo geometrijski objekt s podmnožico A v prostoru K^n .

Na drugi strani povezave želimo imeti algebrski objekt, ki bi določal in bi bil določen z množico $A \subseteq K^n$. Veliko podatkov o nekem prostoru lahko dobimo iz funkcij, ki so definirane na njem. Nas bodo zanimale funkcije oblike $K^n \rightarrow K$ in omejili se bomo na najbolj primerne za algebrsko povezavo – polinome. Povezava, ki jo tvorimo, je naslednja. Množici $A \subseteq K^n$ priredimo ideal $I(A) \triangleleft K[x_1, \dots, x_n]$ vseh polinomov, ki so enaki 0 povsod na A . V obratno smer, idealu $J \triangleleft K[x_1, \dots, x_n]$ priredimo množico $V(J) \subseteq K^n$, ki je množica vseh skupnih ničel polinomov v J . Množice $A \subseteq K^n$, ki so skupne ničle polinomov, si zaslužijo posebno ime.

Definicija 2.1. Množica $A \subseteq K^n$ je *algebrska množica*, če obstaja podmnožica $B \subseteq K[x_1, \dots, x_n]$, da je A množica skupnih ničel polinomov v B . Torej, $A = V(B)$ za nek $B \subseteq K[x_1, \dots, x_n]$.

Opomba 2.2. Kadar želimo poudariti, s katerim baznim poljem delamo, pišemo $I_K(A)$ in $V_K(J)$.

Kadar imamo korespondenco med dvema tipi objektov, bodo eni izmed zanimivih tisti, ki se ne spremenijo, če jih preslikamo na drugo stran in nazaj. Poglejmo najprej tiste množice $A \subseteq K^n$, za katere je $V(I(A)) = A$. Katere točke se sploh nahajajo v $V(I(A))$ za poljubno $A \subseteq K^n$? Znotraj $V(I(A))$

se nahajajo tiste točke $(a_1, \dots, a_n)$, za katere velja naslednje: če je polinom $f \in K[x_1, \dots, x_n]$ enak 0 povsod na A , je enak 0 tudi v $(a_1, \dots, a_n)$. Množice $A \subseteq K^n$, za katere je $V(I(A)) = A$, bodo potem take, ki so že množica skupnih ničel polinomov – algebraične množice. Dodatna lepa lastnost algebraičnih množic je, da lahko iz njih dobimo zelo uporabno topologijo na prostoru K^n . Če vzamemo za zaprte množice natanko algebraične množice, dobimo *topologijo Zariskega* na prostoru K^n .

Poglejmo si sedaj, za katere ideale $J \triangleleft K[x_1, \dots, x_n]$ je $I(V(J)) = J$. Znotraj ideala $I(V(J))$ bodo poleg polinomov iz J tudi polinomi, ki so enaki 0 povsod, kjer imajo polinomi iz J skupne ničle. Kot primer denimo, da J vsebuje polinom f , oblike $f = g^k$ za nek $g \in K[x_1, \dots, x_n]$. Potem bodo v $I(V(J))$ tudi polinomi $g, g^2, \dots, g^{k-1}$, saj so njihove ničle enake ničlam polinoma f . Torej, da bo $I(V(J)) = J$, mora za J veljati, da če je $g^k \in J$, je tudi $g \in J$. Po definiciji idealov so potem vse potence polinoma g v idealu J . Taki ideali imajo tudi posebno ime.

Definicija 2.3. Naj bo $J \triangleleft K[x_1, \dots, x_n]$ ideal. *Radikal* ideala J je ideal $\sqrt{J} = \{f \in K[x_1, \dots, x_n] \mid \exists m \in \mathbb{N} : f^m \in J\}$. Ideal J je *radikalni*, če je $\sqrt{J} = J$.

Seveda so tudi drugi primeri, kako je $I(V(J))$ lahko večji od J . Kadar imamo opravka s poljubnim poljem K , o ničlah polinomov ne moremo veliko povedati. Zato se omejimo na tista polja, kjer vemo čim več o ničlah – *algebraično zaprta* polja. Standardni primer algebraično zaprtega polja je polje kompleksnih števil $\mathbb{C}$. Za algebraično zaprta polja je zgornji način, kako je $I(V(J))$ lahko večji od J , celo edini. To dejstvo je glavni del *Hilbertovega izreka o ničlah*.

Izrek 2.4 (Hilbertov izrek o ničlah). *Naj bo K algebraično zaprto polje in $J \triangleleft K[x_1, \dots, x_n]$ ideal.*

1. $I(V(J)) = J$, natanko tedaj ko je J radikalni.
2. Vedno je $I(V(J)) = \sqrt{J}$.

Posledica 2.5. $\sqrt{J}$ je presek vseh praidealov, ki vsebujejo J . Dovolj je, da vzamemo presek minimalnih praidealov izmed teh, ki vsebujejo J .

3 Realni izrek o ničlah

Seveda si ne moremo predstavljati vseh geometrijskih objektov, kot da so vloženi v prostor $\mathbb{C}^n$, in velikokrat je zelo naravno, da so vloženi v *evklidski prostor* $\mathbb{R}^n$. Ker je $\mathbb{R}$ seveda polje, imamo še vedno isto korespondenco med množicami v $\mathbb{R}^n$ in ideali polinomov v $\mathbb{R}[x_1, \dots, x_n]$. Smo pa izgubili Hilbertov izrek o ničlah, saj $\mathbb{R}$ ni algebraično zaprto polje.

Primer 3.1. Naj bo J ideal, generiran s polinomom $f(x, y) = x^2 + y^2$. Njegovi elementi so torej polinomi oblike $(x^2 + y^2) \cdot g(x, y)$, kjer je $g(x, y) \in \mathbb{R}[x, y]$ poljuben polinom. Hitro tudi premislimo, da je ideal J radikalni.

Jasno je $(0, 0) \in \mathbb{R}^2$ edina skupna ničla polinomov v J , zato je $V(J) = \{(0, 0)\}$. V tej točki sta tudi polinoma $g(x, y) = x$ in $h(x, y) = y$ enaka 0,

torej sta vsebovana v $I(V(J))$. Ker sta g in h polinoma prve stopnje, nista oblike $(x^2 + y^2) \cdot g(x, y)$. V primerjavi s kompleksnim primerom tudi nobena njuna potenca ni vsebovana v idealu J , torej smo pokazali, da je v tem primeru $J = \sqrt{J}$ strogo vsebovan v $I(V(J))$. $\diamond$

Zato Hilbertov izrek o ničlah za polje realnih števil $\mathbb{R}$ res ne drži. Ampak še vedno bi radi imeli vsaj neko različico izreka o ničlah, saj brez njega korespondenca ni pretirano uporabna.

Ko smo prešli na polje realnih števil $\mathbb{R}$, smo izgubili algebraično zaprtost. V zameno smo pa dobili novo orodje, ki ga pri poljubnih algebraično zaprtih poljih nimamo, in to je *linearna urejenost*.

Definicija 3.2. *Linearno urejeno polje* $(K, \leq)$ je polje K skupaj z linearno urejenostjo $\leq$, ki je usklajena s seštevanjem in množenjem. Torej, za vse $x, y, z \in K$ velja:

- $x \leq y \Rightarrow x + z \leq y + z$,
- $(0 \leq x) \wedge (0 \leq y) \Rightarrow 0 \leq xy$.

Pomembna lastnost, ki jo dobimo iz linearne urejenosti polja $\mathbb{R}$, je, če je vsota kvadratov enaka 0, so vsi elementi enaki 0. Torej, iz $\sum_{i=1}^n x_i^2 = 0$ sledi $x_i = 0$ za vse $i = 1, \dots, n$. Ta lastnost ne velja samo za realna števila, temveč tudi za na primer polje racionalnih števil $\mathbb{Q}$, polje realnih algebraičnih števil $\mathbb{R}_{\text{alg}}$ ter polje realnih racionalnih funkcij $\mathbb{R}(x)$. Zato bi pri izpeljavi realnega izreka o ničlah radi uporabljali le lastnosti realnih števil, ki veljajo tudi za ostale navedene primere. Torej, radi bi se izognili uporabi *polnosti*, moči množice realnih števil itd. S tem bo dobljeni izrek veljal za več kot samo polje realnih števil $\mathbb{R}$.

Lastnost, da se kolobar ali ideal „obnaša“ kot polje realnih števil $\mathbb{R}$, lahko zapišemo takole.

Definicija 3.3. Naj bo R poljuben komutativen kolobar z enico. Pravimo, da je kolobar R *realen*, če za poljubne $x_1, \dots, x_n \in R$ velja

$$\sum_{i=1}^n x_i^2 = 0 \Rightarrow x_1 = \dots = x_n = 0.$$

Ideal $J \triangleleft R$ je *realen*, če za poljubne $x_1, \dots, x_n \in J$ velja

$$\sum_{i=1}^n x_i^2 \in J \Rightarrow x_1, \dots, x_n \in J.$$

Opomba 3.4. Izkaže se, da so vsi realni ideali radikalski. Poleg tega, kolobar R je realen natanko takrat, ko R nima *nilpotentov* in so vsi njegovi minimalni praideali realni. [4, Lema 2.9]

S tem seveda nismo pokrili vseh malenkosti in potrebnih lastnosti v kasnejši izpeljavi, je pa to že dovolj, da povemo *realni izrek o ničlah*.

Definicija 3.5. Naj bo $J \triangleleft \mathbb{R}[x_1, \dots, x_n]$ ideal v kolobarju polinomov. *Realni radikal* $\sqrt[\mathbb{R}]{J}$ ideala J je najmanjši realni ideal, ki vsebuje J .

Poleg tega se da eksplisitno zapisati, katere elemente vsebuje $\sqrt[\mathbb{R}]{J}$, kar pride prav pri kasnejši uporabi.

Trditev 3.6. *Naj bo $J \triangleleft \mathbb{R}[x_1, \dots, x_n]$. Potem je njegov realni radikal $\sqrt[\mathbb{R}]{J}$ natanko presek vseh realnih praidealov, ki vsebujejo J , ter je oblike*

$$\sqrt[\mathbb{R}]{J} = \{f \in \mathbb{R}[x_1, \dots, x_n] \mid \exists m, k \in \mathbb{N}, \exists f_1, \dots, f_m \in \mathbb{R}[x_1, \dots, x_n] : f^{2k} + \sum_{i=1}^m f_i^2 \in J\}.$$

Z besedami, polinom $f \in \mathbb{R}[x_1, \dots, x_n]$ je element $\sqrt[\mathbb{R}]{J}$, če obstaja vsota kvadratov $\sum_{i=1}^m f_i^2$, da če jo prištejemo neki sodi potenci polinoma f , dobimo element ideala J .

Izrek 3.7 (Realni izrek o ničlah [2, str. 84-86]). *Naj bo $J \triangleleft \mathbb{R}[x_1, \dots, x_n]$ ideal.*

1. $J = \mathbb{I}_{\mathbb{R}}(\mathbb{V}_{\mathbb{R}}(J))$, natanko tedaj ko je J realen.
2. Vedno je $\mathbb{I}_{\mathbb{R}}(\mathbb{V}_{\mathbb{R}}(J)) = \sqrt[\mathbb{R}]{J}$.

To se ujema s primerom 3.1, kjer smo opazili, da $\sqrt{J}$ ne pokrije vseh polinomov v $\mathbb{I}_{\mathbb{R}}(\mathbb{V}_{\mathbb{R}}(J))$. Iz opombe 3.4 lahko izpeljemo, da je to zato, ker niso vsi praideali realni, torej bo $\sqrt[\mathbb{R}]{J}$ kvečjemu večji od $\sqrt{J}$. S tem dobimo $\sqrt{J} \subseteq \sqrt[\mathbb{R}]{J} = \mathbb{I}_{\mathbb{R}}(\mathbb{V}_{\mathbb{R}}(J))$.

4 Kvaternionski izrek o ničlah

V primerjavi s Hilbertovim in realnim izrekom o ničlah je kvaternionski izrek precej novejši. Ni toliko motiviran z uporabo pri geometriji kot z željo po večji splošnosti, kot je bilo takrat znano. Osrednji objekt je seveda algebra kvaternionov $\mathbb{H}$, katere pomembne lastnosti lahko povzamemo takole: $\mathbb{H}$ je 4-razsežna realna algebra z deljenjem, katere center je $\mathbb{R}$.

Za zapis kvaternionskega izreka o ničlah je potrebno najprej razmisliti, kaj so sploh polinomske funkcije nad kvaternioni. Pri definiciji polinomskih funkcij se namreč moramo odločiti, ali bodo spremenljivke komutirale med sabo ter s kvaternioni ali ne. Odločitev nam da dva, na videz nepovezana kolobarja polinomskih funkcij nad $\mathbb{H}$.

Če vzamemo komutirajoče spremenljivke, dobimo kolobar $\mathbb{H}_c[x_1, \dots, x_n]$. Če vzamemo nekomutirajoče spremenljivke, dobimo kolobar $\mathbb{H}[x_1, \dots, x_n]$, ki je na nek način „prava“ posplošitev polinomskih funkcij na nekomutativne kolobarje. Kako točno so polinomske funkcije v obeh kolobarjih definirane, izpustimo.

Presenetljivo dejstvo je, da sta si ta dva kolobarja polinomskih funkcij skoraj povsem enaka. Namreč, kljub temu da v $\mathbb{H}_c[x_1, \dots, x_n]$ spremenljivke komutirajo in v $\mathbb{H}[x_1, \dots, x_n]$ ne, obstaja izomorfizem med obema, le treba je izbrati primerno število spremenljivk v vsakem. Konkretno, obstaja izomorfizem $\Phi: \mathbb{H}[x_1, \dots, x_n] \rightarrow \mathbb{H}_c[x_{ij} \mid i = 1, \dots, n, j = 1, 2, 3, 4]$. [1, Izrek 5]

S tem izomorfizmom lahko pokažemo, da smemo evaluacijo polinomske funkcije $f \in \mathbb{H}[x_1, \dots, x_n]$ v točki iz $\mathbb{H}^n$ zamenjati z evaluacijo funkcije $\Phi(f)$ v točki iz $\mathbb{R}^{4n}$. Kot posledico dobimo bijektivno korespondenco med ideali v kolobarju $\mathbb{H}[x_1, \dots, x_n]$ ter ideali v kolobarju $\mathbb{R}[x_{ij} \mid i = 1, \dots, n, j = 1, 2, 3, 4]$. S tem dobimo idejo, da bi kvaternionski izrek o ničlah dokazali tako, da bi ga prevedli na realnega.

Po tem premisleku lahko zapišemo kvaternionske analoge definicij in izrekov v ostalih dveh primerih. Kvaternionski analogi so kar enaki realnim, kjer smo polje $\mathbb{R}$ zamenjali z algebro $\mathbb{H}$ ter kvadriranje za množenje s konjugirano funkcijo.

Definicija 4.1. Naj bo $f \in \mathbb{H}[x_1, \dots, x_n]$ poljubna. *Konjugirana funkcija* $\bar{f}$ je taka funkcija, za katero je $\bar{f}(x_1, \dots, x_n) = \overline{f(x_1, \dots, x_n)}$. Da se pokazati, da je $\bar{f}$ tudi polinomska funkcija, torej element kolobarja $\mathbb{H}[x_1, \dots, x_n]$.

Definicija 4.2. Ideal $J \triangleleft \mathbb{H}[x_1, \dots, x_n]$ je *kvaternionski*, če za poljubne polinomske funkcije $f_1, \dots, f_n \in \mathbb{H}[x_1, \dots, x_n]$ velja

$$\sum_{i=1}^n f_i \bar{f}_i \in J \Rightarrow f_1, \dots, f_n \in J.$$

Definicija 4.3. Naj bo $J \triangleleft \mathbb{H}[x_1, \dots, x_n]$ ideal v kolobarju polinomskih funkcij nad $\mathbb{H}$. *Kvaternionski radikal* ideala J je

$$\sqrt[n]{J} = \{f \in \mathbb{H}[x_1, \dots, x_n] \mid \exists m, k \in \mathbb{N}, \exists f_1, \dots, f_m \in \mathbb{H}[x_1, \dots, x_n] : \\ (f \bar{f})^k + \sum_{i=1}^m f_i \bar{f}_i \in J\}$$

V primerjavi z realnim radikalom bomo tukaj ekspliciten zapis vzeli kot definicijo in je posledica izreka o ničlah, da je $\sqrt[n]{J}$ res najmanjši kvaternionski ideal, ki vsebuje J .

Izrek 4.4 (Kvaternionski izrek o ničlah [1, Izrek 9]). *Naj bo $J \triangleleft \mathbb{H}[x_1, \dots, x_n]$ ideal.*

1. $J = I_{\mathbb{H}}(V_{\mathbb{H}}(J))$, natanko takrat ko je J kvaternionski.
2. Vedno je $I_{\mathbb{H}}(V_{\mathbb{H}}(J)) = \sqrt[n]{J}$.

Opomba 4.5. Čeprav $\mathbb{H}$ ni polje, sta definiciji $I_{\mathbb{H}}(A)$ kot ideal polinomskih funkcij, ki so enake 0 povsod na A , ter $V_{\mathbb{H}}(J)$ kot množica skupnih ničel še vedno ustrezni.

Za konec lahko še dokončamo analog trditve 3.6.

Posledica 4.6 (Alon, Paran [1, Posledica 11]). *Kvaternionski radikal $\sqrt[n]{J}$ je presek vseh kvaternionskih praidealov, ki vsebujejo J .*

Literatura

- [1] G. Alon, E. Paran, *A Quaternionic Nullstellensatz*, arXiv:1911.10595 [math.RA].
- [2] J. Bochnak, M. Coste, M-F. Roy, *Real Algebraic Geometry*, Ergebnisse der Mathematik und ihrer Grenzgebiete / A Series of Modern Surveys in Mathematics **36**, Springer-Verlag, New York, 1998.
- [3] M. Brešar, *Undergraduate Algebra*, Springer Undergraduate Mathematics Series, Springer-Verlag, New York, 2019.
- [4] T.Y. Lam, *An Introduction to Real Algebra*, v: Rocky Mountain Journal of Mathematics, **14(4)**, The Rocky Mountain Mathematics Consortium, jesen 1984, str. 767–814.