Realna polja

Glavačević, Ana

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

Ana Glavačević

Realna polja

Završni rad

Osijek, 2018.

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

Ana Glavačević

Realna polja

Završni rad

Mentor: izv.prof. dr. sc. Ivan Matić

Osijek, 2018.

Sažetak

U ovome radu pisat ćemo o realnim poljima. U uvodnom dijelu navest ćemo definiciju prstena, njegova osnovna svojstva te pojmove poput djelitelj nule, grupa invertibilnih elemenata, polje, proširenje polja, algebarski zatvoreno polje, izomorfizam.

Nadalje, u drugom dijelu opisat ćemo uređena polja, prokomentirati postojanje beskonačno velikih brojeva te objasniti arhimedsko polje. Nakon toga ćemo definirati realno polje i iskazati i dokazati bitne teoreme, leme i propozicije vezane uz takvo polje. Također, reći ćemo nešto i o postojanju homomorfizama.

Ključne riječi:

uređaj na polju, uređeno polje, arhimedsko polje, valuacijski prsten, realno polje, realno zatvoreno polje, realni zatvarač, ireducibilan polinom, Sturmov niz, promjena predznaka u nizu, izomorfizam, homomorfizam.

Summary

In this term paper we write about real fields. In introduction we cite the definition of the ring, it's elementary characteristics and terms as divisor of zero, integral domain, group of invertible elements, field, extension field, algebraically closed field, isomorphism.

Furthermore, in the second part we describe the ordered fields, comment on the existence of infinitely large numbers and explain the archimedean field. After that we define the real field and we state and prove theorems, lemma and propositions related to such a field. We also say something about the existence of homomorphisms.

Key words:

an ordering of field, ordered field, archimedean field, valuation ring, real field, real close field, real closure, irreducible polynomial, Sturm sequence, variation of signs in the sequence, isomorphism, homomorphism.

Sadržaj

Uvod

Polja su jedna od osnovnih algebarskih strukutura. Pojavljuju se u analizi, u algebri, u teoriji brojeva te u mnogim drugim granama matematike. U ovom završnom radu bazirat ćemo se na proučavanje realnih polja.

Ispitivati ćemo svojstva realnih polja, navesti bitne tvrdnje i primjere nekih realnih polja te prokomentirati postojanje homomorfizama. Kako bi smo mogli započeti rad na ovu temu moramo uvesti i poznavati neke od osnovnih pojmova, kao što su: prsten, karakteristika prstena, polje, proširenje polja, algebarsko proširenje, algebarski zatvoreno polje, algebarski zatvarač, izomorfizam.

Definicija 1. *Neprazan skup $R = (R, +, \cdot)$ zovemo prsten ukoliko je za operacije zbrajanja $+ : R \times R \to R$ i množenja $\cdot : R \times R \to R$ ispunjeno sljedeće:*

1. *$(R, +)$ je komutativna grupa sa neutralnim elementom $0 = 0_R$*
2. *$(R, \times)$ je polugrupa, tj. množenje je asocijativno*
3. *Vrijedi distributivnost množenja prema zbrajanju, tj.*

$$x \cdot (y + z) = xy + xz, \text{ za svaki } x, y, z \in R$$

$$(x + y) \cdot z = xz + yz, \text{ za svaki } x, y, z \in R.$$

Element $0 = 0_R$ zvat ćemo nula prstena R. Ako postoji jedinični element, ili kraće jedinica, $1 = 1_R \in R$ takav da je

$$1 \cdot x = x \cdot 1 = 1, \text{ za svaki } x \in R$$

onda kažemo da je R prsten s jedinicom.

Prsten R je komutativan ako

$$x \cdot y = y \cdot x, \text{ za svaki } x, y \in R,$$

inače govorimo o nekomutativnom prstenu.

Definicija 2. *Elemet $0 \neq \lambda \in R$ (tj. $0 \neq p \in R$) takav da je*

$$\lambda x = 0 \text{ (tj. } xp = 0) \text{ za neki } 0 \neq x \in R$$

zove se lijevi (tj. desni) djelitelj nule. R je integralna domena ako nema ni lijevih ni desnih djelitelja nule.

Definicija 3. *Element $\omega \in R$, gdje je R prsten s jedinicom, je invertibilan ako postoji $\omega' \in R$ takav da je*

$$\omega\omega' = \omega'\omega = 1,$$

koristit ćemo oznaku

$$R^\times = \textit{grupa invertibilnih elemenata u } R.$$

Definicija 4. *Prsten R je tijelo ili prsten s dijeljenjem ako je svaki ne-nul element u R invertibilan, tj. ako je:*

$$R^\times = R \setminus \{0\}.$$

Komutativno tijelo zove se polje.

Sljedeći pojam, karakteristike prstena, posebno je važan u teoriji polja.

Definicija 5. *Neka je R prsten i neka postoji $m \in \mathbb{N}$ takav da je*

$$mx = 0, \textit{ za svaki } x \in R.$$

Definiramo karakteristiku prstena R sa

$$\textit{char } R = \textit{minimalan takav } m,$$

ako m uopće postoji. U suprotnom, R je karakteristike 0.

Definicija 6. *Neka je K polje koje sadrži potpolje k. Polje K tada zovemo proširenje polja k i označavamo K/k.*

Definicija 7. *Neka je K/k proširenje polja. Kažemo da je element $\alpha \in K$ algebarski nad k ako postoji neki ne-nul polinom $f(x) \in k[x]$ takav da je $f(\alpha) = 0$. Ako α nije algebarski, kažemo da je transcendentan nad k. Za proširenje K/k kažemo da je algebarsko ako je svaki $\alpha \in K$ algebarski nad k.*

Definicija 8. *Polje K nazivamo algebarski zatvoreno ako svaki nekonstantni polinom $f(x) \in K[x]$ ima korijen u K. Algebarski zatvarač polja k je algebarsko proširenje $\overline{k}$ od k koje je algebarski zatvoreno.*

Definicija 9. *Neka su R i S dva prstena. Preslikavanje $f : R \to S$ je homomorfizam prstena ukoliko je i aditivno i multiplikativno, tj. ako vrijedi*

$$f(x+y) = f(x) + f(y) \textit{ i } f(xy) = f(x)f(y), \textit{ za svaki } x, y \in R,$$

te ako je

$$f(1_R) = f(1_S).$$

Homomorfizam f koji je i injekcija zovemo monomorfizam, f koji je i surjekcija zovemo epimorfizam. Homomorfizam koji je i injekcija i surjekcija zovemo izomorfizam.

1 Uređena polja

Neka je K polje. Uređaj na K je podskup P od K koji ima sljedeća svojstva:

1. Za $x \in K, x \in P$ ili $x = 0$ ili $-x \in P$ i ove tri mogućnosti se međusobno isključuju. Drugim riječima, K je disjunktna unija od P, $\{\emptyset\}$ i $-P$.

2. Ako su x, $y \in P$ onda je $x + y \in P$ i $xy \in P$.

Možemo reći da je polje K uređeno podskupom P i P zovemo skupom pozitivnih elemenata.

Pretpostavimo da je K uređeno skupom P. Budući da je $1 \neq 0$ i $1 = 1^2 = (-1)^2$, vidimo da je $1 \in P$. Iz svojstva 2. slijedi da je $1 + 1 + \cdots + 1 \in P$ pa je K karakteristike 0. Ako je $x \in P$ i $x \neq 0$, onda $xx^{-1} = 1 \in P$ implicira da je $x^{-1} \in P$.

Neka su $x, y \in K$. Definiramo $x < y$ (ili $y > x$) što znači da je $y - x \in P$. Ako je $x < 0$, kažemo da je x negativan. To znači da je $-x$ pozitivan. Može se lako vidjeti uobičajeni odnos nejednakosti:

$x < y$	i	$z > 0$	implicira	$xz < yz$
$x < y$	i	$y < z$	implicira	$x < z$
$x < y$	i	$x, y > 0$	implicira	$\frac{1}{y} < \frac{1}{x}$.

Definiramo $x \leq y$ što znači $x < y$ ili $x = y$. Tada $x \leq y$ i $y \geq x$ povlači da je $x = y$.

Ako je K udređeno i $x \in K$, $x \neq 0$, onda je x^2 pozitivan jer je $x^2 = (-x)^2$ ili je $x \in P$ ili je $-x \in P$. Takav zbroj kvadrata je pozitivan ili 0.

Neka je E polje. Tada je produkt sume kvadrate u E suma kvadrata. Ako su $a, b \in E$ sume kvadrata i $b \neq 0$, tada je a/b suma kvadrata.

Prva tvrdnja je očigledna, također i druga iz izraza $a/b = ab(b^{-1})^2$.

Ako je E polje karakteristike različite od 2 i -1 je suma kvadrata u E, tada je svaki element $a \in E$ suma kvadrata jer je $4a = (1 + a)^2 - (1 - a)^2$.

Ako je K polje s uređajem P i F potpolje, tada očito, $P \cap F$ definira uređaj na F koji zovemo inducirani uređaj.

Primjetimo da se naša dva aksioma 1. i 2. primjenjuju u prstenu. Ako je A uređen prsten s $1 \neq 0$, jasno je da A ne može imati djelitelja nule i može se proširiti uređaj na A na polje kvocijenata na očigledan način: razlomak A je pozitivan ako se može pisati u obliku a/b za $a, b \in A$ i $a, b > 0$. Može se lako vidjeti da se na ovaj način dobiva uređaj na polju kvocijenata.

Primjer 1. *Definiramo uređaj na prstenu polinoma $R[t]$ realnih brojeva. Polinom*

$$f(t) = a_n t^n + \cdots + a_0$$

pri čemu je $a_n \neq 0$, je pozitivan ako je $a_n > 0$. Aksiomi se mogu jednostavno provjeriti. Imamo na umu da je $t > a$ za svaki $a \in \boldsymbol{R}$. Takav t je beskonačno velik u odnosu na $\boldsymbol{R}$. Postojanje beskonačno velikih(ili malih) elemenata uređenih polja je glavna karakteristika koja polja razlikuje od podpolja realnih brojeva.

Prokomentirati ćemo postojanje beskonačno velikih brojeva.

Neka je K uređeno polje i neka je F podpolje s induciranim uređajem. Kao obično, stavimo da je $\mid x \mid = x$ ako je $x > 0$ i $\mid x \mid = -x$ ako je $x < 0$. Kažemo da je element α iz K beskonačno velik nad F ako je $\mid \alpha \mid \geq x$ za svaki $x \in F$. Kažemo da je beskonačno mal nad F ako $0 \leq \mid \alpha \mid < \mid x \mid$ za svaki $x \in F$, $x \neq 0$. Vidimo da je α beskonačno velik ako i samo ako je α^{-1} beskonačno mal. Kažemo da je K arhimedsko nad F ako K nema elemenata koji su beskonačno veliki nad F. Međupolje F_1, takvo da je $K \supset F_1 \supset F$, je maksimalno arhimedsko nad F u K ako je arhimedsko nad F i ne postoji drugo međupolje sadržano u F_1 koje je arhimedsko nad F. Ako je F_1 arhimedsko nad F i F_2 arhimedsko nad F_1, onda je F_2 arhimedsko nad F. Stoga po Zornovoj lemi uvijek postoji maksimalno arhimesko podpolje F_1 od K nad F. Kažemo da je F maksimalno arhimedsko polje u K ako je maksimalno arhimedsko nad sobom u K.

Neka je K uređeno polje i F potpolje. Neka je σ skup elemenata iz K koji nisu beskonačno veliki nad F. Jasno je da je σ prsten i da za bilo koji α iz K imamo da je α ili $\alpha^{-1} \in \sigma$. Stoga σ zovemo valuacijski prsten koji sadrži F. Neka je m ideal svih $\alpha \in K$ koji su beskonačno mali nad F. Tada je m jedinstven maksimalan ideal od σ jer svaki element u σ, koji nije u m, ima inverz u σ. σ zovemo valuacijski prsten dobiven uređajem na K/F.

Propozicija 1. *Neka je K uređeno polje i F podpolje. Neka je σ valuacijski prsten dobiven uređajem K/F i neka je m njegov maksimalan ideal. Tada je σ/m realno polje.*

Dokaz: U suprotnom, mogli bismo napisati

$$-1 = \sum \alpha_i^2 + a$$

pri čemu $\alpha_i \in \sigma$ i $a \in m$. Kako je $\sum \alpha_i^2$ pozitivno i α je beskonačno mali, takva relacija je očito nemoguća.

□

2 Realna polja

Za polje K kažemo da je realno ako -1 nije suma kvadrata u K. Za polje K kažemo da je realno zatvoreno ako je realno i ako je bilo koje algebarsko proširenje polja K koje je realno jednako K. Drugim riječima, K je maksimalno realno polje u algebarskom zatvaraču.

Propozicija 2. *Neka je K realno polje.*

(i) Ako $a \in K$, onda je $K(\sqrt{a})$ ili $K(\sqrt{-a})$ realno polje. Ako je a suma kvadrata u K, onda je $K(\sqrt{a})$ realno polje. Ako $K(\sqrt{a})$ nije realno polje, onda je $-a$ suma kvadrata u K.

(ii) Ako je f ireducibilan polinom neparnog stupnja n u $K[X]$ i ako je α nultočka od f, onda je $K(\alpha)$ realno polje.

Dokaz: Neka je $a \in K$. Ako je a kvadrat u K, tada je $K(\sqrt{a}) = K$ i stoga je realno polje prema pretpostavci. Pretpostavimo da a nije kvadrat u K. Ako $K(\sqrt{a})$ nije realno polje, tada postoje $b_i, c_i \in K$ takvi da

$$\begin{aligned} -1 &= \sum (b_i + c_i\sqrt{a})^2 \\ &= \sum (b_i^2 + 2c_i b_i \sqrt{a} + c_i^2 a). \end{aligned}$$

Pošto je $\sqrt{a}$ stupnja 2 nad K, slijedi

$$-1 = \sum b_i^2 + a \sum c_i^2.$$

Ako je a suma kvadrata u K, dobili smo kontradikciju. U svakom slučaju, zaključujemo da

$$-a = \tfrac{1+\sum b_i^2}{\sum c_i^2}$$

je kvocijent sume kvadrata i da je $-a$ suma kvadrata. Stoga je $K(\sqrt{a})$ realno polje pa je dokazana prva tvrdnja.

Prema drugoj tvrdnji, pretpostavimo da $K(\alpha)$ nije realno polje. Tada pišemo

$$-1 = \sum g_i(\alpha)^2$$

pri čemu su polinomi g_i u $K(X)$ stupnja koji je manji ili jednak $n-1$. Postoji polinom h u $K[X]$ takav da

$$-1 = \sum g_i(X)^2 + h(X)f(X).$$

Suma od $g_i(X)^2$ ima paran stupanj i ovaj stupanj mora biti > 0, inače je -1 suma kvadrata u K. Ovaj stupanj je $\leq 2n-2$. Kako f ima neparni stupanj n, slijedi da h ima neparan stupanj koji je $\leq n-2$. Ako je β nultočka od h onda znamo da je -1 suma kvadrata u $K(\beta)$. Kako je stupanj polinoma h manji od stupnja polinoma f, dokaz je završen.

□

Neka je K realno polje. Realno zatvoreno polje L koje je algebarsko nad K zovemo realni zatvarač.

Teorem 1. *Neka je K realno polje. Tada postoji realni zatvarač od K. Ako je R realno zatvoreno polje, onda R ima jedinstveni uređaj. Pozitivni elementi su kvadrati od R. Svaki pozitivni element je kvadrat i svaki polinom neparnog stupnja u $R[X]$ ima nultočku u R. Imamo $R^a = R(\sqrt{-1})$.*

Dokaz: Prema Zornovoj lemi, naše polje K je sadržano u nekom realnom zatvorenom polju koje je algebarsko nad K. Neka je R realno zatvoreno polje. Neka je P skup ne-nul elemenata iz R koji su sume kvadrata. Tada je P zatvoren na operacije zbrajanja i množenja. Prema Propoziciji 2., svaki element skupa P je kvadrat u R i za $a \in R$, $a \neq 0$, imamo da je $a \in P$ ili $-a \in P$. Takav P definira uređaj. Nadalje, prema Propoziciji 2., svaki polinom neparnog stupnja nad R ima nultočku u R. □

Korolar 1. *Neka je K realno polje i a element polja K koji nije suma kvadrata. Tada postoji uređaj na K u kojem je a negativan.*

Dokaz: Polje $K(\sqrt{-a})$ je realno prema Propoziciji 1. i stoga ima uređaj kao podpolje realnog zatvarača. U tom uređaju $-a > 0$ i zato je a negativan.

□

Propozicija 3. *Neka je R polje takvo da $R \neq R^a$ ali $R^a = R(\sqrt{-1})$. Tada je R realno i stoga je realno zatvoreno polje.*

Dokaz: Neka je P skup elemenata iz R koji su kvadrati i $\neq 0$. Tvrdimo da je P uređaj na R. Neka je $a \in R$, $a \neq 0$. Pretpostavimo da a nije kvadrat u R. Neka je α nultočka od $X^2 - a = 0$. Tada je $R(\alpha) = R(\sqrt{-1})$ i stoga postoje $c, d \in R$ takvi da je $\alpha = c + d\sqrt{-1}$. Tada je

$$\alpha^2 = c^2 + 2cd\sqrt{-1} - d^2.$$

Pošto su $1, \sqrt{-1}$ linearno nezavisni nad R, slijedi da je $c = 0$ (zbog $a \notin R$) i stoga je $-a$ kvadrat.

Sada ćemo dokazati da je suma kvadrata kvadrat. Zbog jednostavnosti, pišemo $i = \sqrt{-1}$. Budući da je $R(i)$ je algebarski zatvoreno polje, za $a, b \in R$ možemo pronaći $c, d \in R$ tako da je $(c + di)^2 = a + bi$. Tada je $a = c^2 - d^2$ i $b = 2cd$. Stoga

$$a^2 + b^2 = (c^2 + d^2).$$

kao što je pokazano.

Ako $a \in R$, $a \neq 0$, tada a i $-a$ ne mogu biti kvadrati u R. Stoga je P je uređaj i naša propozicija je dokazana.

□

Teorem 2. *Neka je R realno zatvoreno polje i $f(X)$ polinom u $R[X]$. Neka su $a, b \in R$ i pretpostavimo da je $f(a) < 0$ i $f(b) > 0$. Tada između a i b postoji c takav da je $f(c) = 0$.*

Dokaz: Kako je $R(\sqrt{-1})$ algebarski zatvoreno polje, slijedi da se f cijepa u produkt ireducibilnih faktora prvog ili drugog stupnja. Ako je $X^2 + \alpha X + \beta$ ireducibilan ($\alpha, \beta \in R$) tada je suma kvadrata, preciznije

$$\left(X + \frac{\alpha}{2}\right)^2 + \left(\beta - \frac{\alpha^2}{4}\right),$$

te moramo imati $4\beta > \alpha^2$ jer smo pretpostavili da je naš faktor ireducibilan. Zato je promjena predznaka od f posljedica promijene predznaka linearnog faktora koji je trivijalno provjeren kao korijen koji se nalazi između a i b.

□

Lema 1. *Neka je K podpolje uređenog polja E. Neka je $\alpha \in E$ algebarski nad K i nultočka polinoma*

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

sa koeficijentima u K. Tada vrijedi $\mid \alpha \mid \leq 1 + \mid a_{n-1} \mid + \cdots + \mid a_0 \mid$.

Dokaz: Ako je $\mid \alpha \mid \leq 1$, tvrdnja je očita. Ako je $\mid \alpha \mid > 1$, $\mid \alpha \mid^n$ pišemo u obliku nižeg stupnja, dijelimo sa $\mid \alpha \mid^{n-1}$ i na taj način smo dokazali lemu.

□

Primijetimo da lema implicira kako element koji je algebarski nad uređenim poljem ne može biti beskonačno velik u odnosu na to polje.

Neka je $f(X)$ polinom sa koeficijentima u realnom zatvorenom polju R te pretpostavimo da f nema višestruke nultočke. Neka su $u < v$ elementi iz R. Prema Sturmovom nizu za f nad intervalom $[u, v]$ mislimo na niz polinoma

$$S = \{f = f_0, f' = f_1, \ldots, f_m\}$$

koji imaju slijedeća svojstva:
1. Posljednji polinom f_m je konstanta različita od nule.
2. Ne postoji točka $x \in [u, v]$ takva da $f_j(x) = f_{j+1}(x) = 0$ za bilo koji $0 \leq j \leq m - 1$.
3. Ako $x \in [u, v]$ i $f_j(x) = 0$ za neki $j = 1, \ldots, m - 1$, onda $f_{j-1}(x)$ i $f_{j+1}(x)$ imaju suprotne predznake.
4. Za svaki $j = 0, \ldots, m$ vrijedi da je $f_j(u) \neq 0$ i $f_j(v) \neq 0$.

Za bilo koji $x \in [u, v]$ koji nije nultočka nekog polinoma f_i sa $W_s(x)$ označavamo broj promjena predznaka u nizu

$$\{f(x), f_1(x), \ldots, f_m(x)\},$$

te $W_s(x)$ zovemo promjena predznaka u nizu.

Teorem 3 (Sturmov teorem)**.** *Broj nultočki od f između u i v je jednak $W_s(u) - W_s(v)$ za bilo koji Sturmov niz S.*

Dokaz: Primjećujemo da ako je $\alpha_1 < \alpha_2 < \cdots < \alpha_r$ uređeni niz nultočki polinoma f_j u $[u, v]$ za $j = 0, \ldots, m-1$, tada je $W_s(x)$ konstanta na otvorenom intervalu između navedenih nultočki, prema Teoremu 2. Stoga je dovoljno dokazati da ako postoji točno jedan element α takav da $u < \alpha < v$ i α nultočka nekog f_j, tada je $W_s(u) - W_s(v) = 1$ ako je α nultočka od f i 0 inače. Pretpostavimo da je α nultočka nekog f_j, za $1 \leq j \leq m-1$. Tada $f_{j-1}(\alpha), f_{j+1}(\alpha)$ imaju suprotne predznake prema svojstvu 3. i ti predznaci se ne mijenjaju kada α zamijenimo sa u ili v. Stoga je promjena predznaka u

$$\{f_{j-1}(u), f_j(u), f_{j+1}(u)\} \text{ i } \{f_{j-1}(v), f_j(v), f_{j+1}(v)\}$$

ista, naime jednaka 2. Ako α nije nultočka od f, zaključujemo da

$$W_S(u) = W_S(v)$$

Ako je α nultočka od f, tada $f(u)$ i $f(v)$ imaju suprotne predznake, ali $f'(u)$ i $f'(v)$ imaju iste predznake, naime, predznak od $f'(\alpha)$. U ovom slučaju,

$$W_S(u) = W_S(v) + 1.$$

To dokazuje naš teorem.

□

Lako je napraviti Sturmov niz za polinome bez višestrukih nultočki. Pomoću Euklidovog algoritma, pišemo

$$\begin{aligned} f &= g_1 f' - f_2, \\ f_2 &= g_2 f_1 - f_3, \\ &\vdots \\ f_{m-2} &= g_{m-1} f_{m-1} - f_m, \end{aligned}$$

koristeći $f' = f$. Kako f, f' nemaju zajedničkih faktora, posljednji član ovog niza je konstanta različita od nule. Ostala svojstva Sturmova niza mogu se lako provjeriti jer ako dva uzastopna polinoma u nizu imaju zajedničku nulu, tada su svi nula, što je kontradikcija činjenici da posljednji član nije.

Korolar 2. *Neka je K uređeno polje, f ireducibilan polinom nad K čiji je stupanj veći ili jednako* 1. *Broj nultočki od f u dva realna zatvarača od K koji inducira dani uređaj na K je isti.*

Dokaz: Uzmemo dovoljno veliki pozitivni v i dovoljno veliki negativni u iz K tako da sve nultočke od f i su sve nultočke polinoma u Sturnovom nizu između u i v, prema Lemi 1. Tada je $W_s(u) - W_s(v)$ potpuni broj nultočki od f u bilo kojem realnom zatvaraču od K koji inducira dani uređaj.

□

Teorem 4. *Neka je K uređeno polje i neka su R, R' realni zatvarači od K, čiji uređaji induciraju određeni uređaj na K. Tada postoji jedinstveni izomorfizam $\sigma : R \to R'$ nad K i taj izomorfizam čuva uređaj.*

Dokaz: Pokažimo prvo da s obzirom na konačno potproširenje E od R nad K postoji ulaganje od E u R' nad K. Neka je $E = K(\alpha)$, te neka je

$$f(X) = Irr(\alpha, K, X).$$

Tada je $f(\alpha) = 0$ i posljedica Sturmova teorema (Korolar 2.) pokazuje da f ima nultočku β u R'. Stoga postoji izomorfizam od $K(\alpha)$ na $K(\beta)$ nad K, preslikavanje α na β.

Neka su $\alpha_1, \ldots, \alpha_n$ različite nultočke od f u R i neka su $\beta_1, \ldots, \beta_m$ različite nultočke od f u R'. Kažemo

$$\alpha_1 < \cdots < \alpha_n \text{ u uređaju na } R,$$

$$\beta_1 < \cdots < \beta_m \text{ u uređaju na } R'.$$

Tvrdimo da je $m = n$ i da možemo izabrati ulaganje σ od $K(\alpha_1, \ldots, \alpha_n)$ u R' tako da je $\sigma\alpha_i = \beta_i$ za vrijednost $i = 1, \ldots, n$. Doista, neka je γ_i element od R takav da

$$\gamma_i^2 = \alpha_{i+1} - \alpha_i \text{ za } i = 1, \ldots, n-1$$

i neka je $E_1 = K(\alpha_1, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_{n-1})$. Prema viđenom, postoji ulaganje σ od E_1 u R' i tada je $\sigma\alpha_{i+1} - \sigma\alpha_i$ kvadrat u R'. Stoga je

$$\sigma\alpha_1 < \cdots < \sigma\alpha_n.$$

Ovo dokazuje da je $m \geq n$. Prema simetriji, slijedi da je $m = n$. Štoviše, uvjet $\sigma\alpha_i = \beta_i$ za $i = 1, \ldots, n$ određuje utjecaj σ na $K(\alpha_1, \ldots, \alpha_n)$. Zaključujemo da σ čuva uređaj. Neka je $y \in K(\alpha_1, \ldots, \alpha_n)$ i $0 < y$. Neka $y \in R$ takav da $\gamma^2 = y$. Tada postoji ulaganje od

$$K(\alpha_1, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_{n-1}, \gamma)$$

u R' nad K koje mora inducirati σ na $K(\alpha_1, \ldots, \alpha_n)$ i koje je takvo da je $\sigma\gamma$ kvadrat, stoga je > 0, kao što je zaključeno.

Koristeći Zornovu lemu, sada je jasno da imamo izomorfizam sa R u R' nad K. Ovaj izomorfizam čuva uređaj zato što preslikava kvadrate u kvadrate.

□

Propozicija 4. *Neka je K uređeno polje, K' proširenje takvo da ne postoji relacija*

$$-1 = \sum_{i=1}^{n} \alpha_i \alpha_i^2$$

za $i \in K, a_i > 0$ i $\alpha K'$. Neka je L polje dobiveno iz K' pridruživanjem kvadrata korijena svih pozitivnih elemenata od K. Tada je L realno polje.

Dokaz: U suprotnom, postoji relacija

$$-1 = \sum_{i=1}^{n} \alpha_i \alpha_i^2$$

za $a_i \in K, a > 0$ i $\alpha_i \in L$. (Možemo uzeti da je $a_i = 1$.) Neka je r najmanji cijeli broj takav da možemo napisati relaciju sa α_i u potpolju od L

$$K'(\sqrt{b_1}, \ldots, \sqrt{b_r})$$

za $b_j \in K, b_j > 0$. Pišemo

$$\alpha_i = x_i + y_i\sqrt{b_r}$$

sa $x_i, y_i \in K'(\sqrt{b_1}, \ldots, \sqrt{b_{r-1}})$. Tada

$$\begin{aligned} -1 &= \sum a_i(x_i + y_i\sqrt{b_r})^2 \\ &= \sum a_i(x_i^2 + 2x_iy_i\sqrt{b_r} + y_i^2 b_r). \end{aligned}$$

Prema hipotezi, $\sqrt{b_r}$ ne pripada $K'(b_1, \ldots, \sqrt{b_{r-1}})$. Stoga je

$$-1 = \sum a_i x_i^2 + \sum a_i b_r y_i^2,$$

u kontradikciji s minimalnom vrijednosti r.

□

Teorem 5. *Neka je K uređeno polje. Postoji realni zatvarač R od K koje inducira dani uređaj na K.*

Dokaz: Uzmimo da je $K' = K$ kao u Propoziciji 4. Tada je L realno polje i sadržano u realnom zatvaraču.

□

Korolar 3. *Neka je K uređeno polje i K' proširenje polja. Kako bi postojao uređaj na K' koje inducira dani uređaj na K, nužno je i dovoljno da ne postoji relacija*

$$-1 = \sum_{i-1}^{n} a_i a_i^2$$

za $a_i \in K, a_i > 0$ i $\alpha_i \in K'$.

Dokaz: Ako ne postoji takva relacija, tada Propozicija 4. navodi da je polje L sadržano u realnom zatvaraču, čiji uređaj inducira uređaj na K' i dani uređaj na K, po želji.

□

Primjer 2. *Neka je $\mathbb{Q}^a$ polje algebarskih brojeva. Odmah vidimo da $\mathbb{Q}$ ima samo jedan uređaj, obični uređaj. Stoga su bilo koja dva realna zatvarača od $\mathbb{Q}$ u $\mathbb{Q}^a$ izomorfna, pomoću jedinstvenog izomorfizma. Realni zatvarači od $\mathbb{Q}$ u $\mathbb{Q}^a$ su točno ta podpolja od $\mathbb{Q}^a$ koja imaju konačan stupanj unutar $\mathbb{Q}^a$. Neka je K konačno realno proširenje polja $\mathbb{Q}$, sadržano u $\mathbb{Q}^a$. Element α iz K je suma kvadrata u K ako i samo ako je svaki konjugirani realni broj α pozitivan, ili ekvivalentno, ako i samo ako je svaki konjugirani α u jednom od realnih zatvarača od $\mathbb{Q}$ u $\mathbb{Q}^a$ pozitivan.*

3 Realne nule i homomorfizmi

Baš kao što je razvijena teorija o proširenju homomorfizama u algebarski zatvoreno polje, želimo razviti teoriju za vrijednosti u realno zatvorenom polju. Jedan od glavnih teorema je slijedeći:

Teorem 6. *Neka je k polje te $K = k(x_1 \ldots, x_n)$ konačno proširenje. Pretpostavimo da je K uređeno polje. Neka je R_k realni zatvarač od k koji inducira isti uređaj na k kao što je K. Tada postoji homomorfizam.*

$$\varphi : k[x_1, \ldots, x_n] \to R_k$$

nad k.

Primjenom Teorema 6., dobivamo:

Korolar 4. *Poput zapisa u teoremu, neka je $y_1, \ldots, y_n \in k[x]$ i pretpostavimo da je*

$$y_1 < y_2 < \cdots < y_m$$

zadani uređaj na K. Tada možemo izabrati φ takav da je

$$\varphi y_1 < \cdots < \varphi y_m.$$

Dokaz: Neka je $\gamma_i \in K^a$ takav da je $\gamma^2 = y_{i+1} - y_i$. Tada na $K(\gamma_1, \ldots, \gamma_{m-1})$ postoji uređaj koji inducira zadani uređaj na K. Primjenjujemo teorem na prstenu

$$k[x_1, \ldots, x_n, \gamma^{-1}, \ldots, \gamma_{m-1}^{-1}, \gamma_1, \ldots, \gamma_{m-1}].$$

□

Korolar 5. *(Artin). Neka je k realno polje koje ima samo jedan uređaj. Neka je $f(X_1, \ldots, X_n) \in k(X)$ racionalna funkcija koja ima svojstvo da za sve $(a) = (a_1, \ldots, a_n) \in R_k^{(n)}$ za koje je $f(a)$ definirano, vrijedi $f(a) \geq 0$. Tada je $f(X)$ suma kvadrata u $k(X)$.*

Dokaz: Pretpostavimo da je naš zaključak netočan. Prema Korolaru 4., postoji uređaj na k(X) u kojem je f negativna. Primjenjujemo Korolar 4. na prsten

$$k[X_1, \ldots, X_n, h(X)^{-1}]$$

gdje je $h(X)$ nazivnik polinoma $f(X)$. Možemo pronaći homomorfizam φ ovog prstena u R_k takav da je $\varphi(f) < 0$. Ali

$$\varphi(f) = f(_1, \ldots, \varphi X_n).$$

je kontradikcija. Neka je $a_i = \varphi(X_i)$ kako bi zaključili dokaz.

□

Lema 2. *Neka je R realno zatvoreno polje i neka je R_0 potpolje koje je algebarski zatvoreno u R (tj. takvo da je svaki element od R koji se ne nalazi u R_0 transcendentan nad R). Tada je R realno zatvoreno.*

Dokaz: Neka je $f(X)$ ireducibilan polinom nad R_0. Cijepa se u R na linearne i kvadratne faktore. Njegovi koeficijenti u R su algebarski nad R_0 i stoga se nalaze u R. Zato je $f(X)$ sam po sebi linearan, ili kvadratno ireducibilan preko R_0. Pomoću teorema srednje vrijednosti, možemo pretpostaviti da je f pozitivno definiran, tj. $f(a) > 0$ za svaki $a \in R_0$. Bez smanjenja općenitosti, možemo pretpostaviti da je $f(X) = X^2 + b^2$ za neki $b \in R_0$. Bilo koji korijen ovog polinoma dati će $\sqrt{-1}$ i zato je jedino algebarsko proširenje od R_0 $R_0(\sqrt{-1})$. To dokazuje da je R_0 realno zatvoreno.

□

Neka je R_K realni zatvarač od K koji inducira zadani uređaj na K. Neka je R_0 algebarski zatvarač od k u R_K. Prema lemi, R_0 je realno zatvoreno.

Promatramo polje $R_0(x_1, \ldots, x_n)$. Ako možemo dokazati naš teorem za prsten $R_0[x_1, \ldots, x_n]$ i pronaći homomorfizam

$$\psi : R_0[x_1, \ldots, x_n] \to R_0,$$

tada uzimamo da je $\sigma : R_0 \to R_K$ izomorfizam nad k (koje postoji prema Teoremu 5) i uzimamo da je $\varphi = \sigma \circ \psi$ kako bi riješili naš problem nad k.

Zatim, neka je F međupolje, $K \supset F \supset k$, takvo da je K stupnja transcendentnosti 1 nad F. Neka je R_K realni zatvarač od K koji čuva uređaj i neka je R_F realni zatvarač od F sadržan u R_K. Ako znamo naš teorem za proširenje dimenzije 1, tada možemo pronaći homomorfizam

$$\psi : R_F[x_1, \ldots, x_n] \to R_F.$$

Napominjemo da polje $k(\psi x_1, \ldots, \psi x_n)$ ima stupanj transcendentnosti koji je manji ili jednak $n-1$ i da je realno, pošto je sadržano u R_F. Stoga smo induktivno reducirani na slučaj kada K ima dimenziju 1 i kao što je prethodno viđeno, kada je k realno zatvoreno.

Naša tvrdnja se može tumačiti geometrijski. Možemo pisati da je $K = R(x, y)$ za x transcendentno nad R i (x, y) zadovoljavajući neki ireducibilni polinom $f(X, Y) = 0$ u $R[X, Y]$. Ono što u suštini želimo dokazati je to da postoji beskonačno mnogo točaka na krivulji $f(X, Y) = 0$ sa koordinatama koje leže na R, tj. beskonačno mnogo realnih točaka.

Glavna ideja je pronaći neke točke $(a, b) \in R^2$ takve da je $f(a, b) = 0$ ali da je $D_2 f(a, b) \neq 0$. Tada možemo koristiti teorem srednje vrijednosti. Vidimo da $f(a, b+h)$ mijenja predznak kada se h mijenja iz malog pozitivnog u veliki negativni element od R. Ako uzmemo da je $a' \in R$ blizu a, tada $f(a', b + h)$ također mijenja predznak za mali h i stoga je $f(a', Y)$ ima nulu u R za sve a' dovoljno blizu a. Na ovaj način dobivamo beskonačno mnogo nula.

Kako bi pronašli točku, uzimamo u obzir da je polinom $f(x, Y)$ poput polinoma jedne varijable Y sa koeficijentima u $R(x)$. Bez smanjenja općenitosti možemo pretpostaviti da taj polinom ima glavni vodeći koeficijent 1. Pravimo Sturmov niz za ovaj polinom, na primjer

$$\{f(x, Y), f_1(x, Y), \ldots, f_m(x, Y)\}.$$

Neka je d stupanj od f. Ako pomoću $A(x) = (a_{d-1}(x), \ldots, a_0(x))$ označavamo koeficijente od $f(x, Y)$, tada prema Euklidovom algoritmu, vidimo da koeficijenti polinoma u Sturmovom nizu mogu biti izraženi kao racionalne funkcije

$$\{G_v(A(x))\}$$

za polinome $a_{d-1}(x), \ldots, a_0(x)$. Neka je

$$v(x) = 1 \pm a_{d-1}(x) \pm \cdots \pm a_0(x) + s,$$

gdje je s pozitivni cijeli broj, a predznaci su odabrani tako da svaki član polinoma u ovoj sumi daje pozitivni doprinos. Neka je $u(x) = -v(x)$, i uzmimo s takav da ni u ni v nije korijen bilo kojeg polinoma u Sturmovom nizu za f.

Lema 3. *Neka je R realno zatvoreno polje i $\{h_i(x)\}$ konačan skup racionalnih funkcija jedne varijable sa koeficijentima u R. Pretpostavimo da je racionalno polje $R(x)$ uređeno na neki način, tako da svaki $h_i(x)$ ima predznak uz sebe. Tada postoji beskonačno mnogo posebnih vrijednosti c od x u R takvih da je $h_i(c)$ definirano i ima isti predznak kao $h_i(x)$ za svaki i.*

Dokaz: S obzirom na brojnike i nazivnike racionalnih funkcija, možemo pretpostaviti bez smanjenja općenitosti da su h_i polinomi. Tada pišemo

$$h_i(x) = \alpha \prod (x - \lambda) \prod p(x),$$

gdje je prvi produkt proširen nad sve korijene λ od h_i u R te drugi produkt nad pozitivno definitne kvadratne faktore nad R. Za bilo koji $\xi \in R$, $p(\xi)$ je pozitivan. Stoga je dovoljno pokazati da su predznaci od $(x - \lambda)$ očuvani za svaki λ zamjenom beskonačno mnogo vrijednosti α za x. Uređujemo sve vrijednosti od λ i od x i dobivamo

$$\cdots < \lambda_1 < x < \lambda_2 < \cdots$$

gdje su mogući λ_1 ili λ_2 izostavljeni ako je x veći ili manji nego bilo koji λ. Bilo koja vrijednost α od x u R izabrana između λ_1 i λ_2 zadovoljit će zahtjeve leme.

□

Kako bi primijenili lemu za postojanje naše točke, uzmimo da se neke racionalne funkcije $\{h_1(x)\}$ sastoje od svih koeficijenata $a_{d-1}(x), \ldots, a_0(x)$, svih racionalne funkcija $G_v(A(x))$, i svih vrijednosti $f_j(x, u(x))$, $f_j(x, v(x))$ čije promjene predznaka zadovoljavaju Sturmov teorem. Tada pronalazimo beskonačno mnogo posebnih vrijednosti α od x u R koje su sačuvale predznake tih racionalnih funkcija. Tada polinomi $f(\alpha, Y)$ imaju korijene u R i za sve osim konačnog broja od α, ti korijeni daju umnožak 1.

Stvar je jednostavnog načina shvaćanja da za sve osim konačnog broja točaka na krivulji, elementi $x_1, \ldots, x_n$ leže na lokalnom prstenu homomorfizma $R[x, y] \to R$ preslikavanje (x, y) u (a, b) tako da je $f(a, b) = 0$, ali $D_2 f(a, b) \neq 0$. Na ovaj način dobivamo homomorfizam

$$R[x_1, \ldots, x_n] \to R,$$

time dokazujući Teorem 6.

Teorem 7. *Neka je k realno polje, $K = k(x_1, \ldots, x_n, y) = k(x, y)$ je konačno generirano proširenje takvo da su $x_1, \ldots, x_n$ algebarski neovisni nad k te je y algebarski nad $k(x)$. Neka je $f(X, Y)$ ireducibilan polinom u $k[X, Y]$ takav da je $f(x, y) = 0$. Neka je R realno zatvoreno polje koje sadrži k i pretpostavimo da ondje postoji $(a, b) \in R^{n+1}$ tako da je $f(a, b) = 0$ ali*

$$D_{n+1} f(a, b) \neq 0.$$

Tada je K realno.

Dokaz: Neka su $t_1, \ldots, t_n$ algebarski nezavisni nad R. Induktivno, možemo zadati uređaj na $R(t_1, \ldots, t_n)$ tako da je svaki t_1 beskonačno mali s obzirom na R. Neka je R' realni zatvarač od $R(t_1, \ldots, t_n)$ koji čuva uređaj. Neka je $u_i = a_i + t_i$ za svaki $i = 1, \ldots, n$. Tada $f(u, b + h)$ mijenja predznak za mali h pozitivan i negativan u R i stoga $f(u, Y)$ ima korijen u R'. Kako je f ireducibilan, izomorfizam sa $k(x)$ na $k(u)$ koji preslikava x_1 na u_i proširuje se na ulaganje od $k(x, y)$ u R' i stoga je K realno polje.

□

Literatura

[1] Serge Lang, Algebra: Graduate Texts in Mathematics, Springer-Verlag, New York, 2002.

[2] Boris Širola, Algebarske strukture: Prsteni, polja i algebre, PMF –Matematički odjel, Zagreb, 2008.