



UNIVERZITET U NOVOM SADU  
PRIRODNO-MATEMATIČKI  
FAKULTET  
DEPARTMAN ZA  
MATEMATIKU I INFORMATIKU



Olja Cvetinović

# KONSTRUKCIJA ALGEBARSKOG ZATVORENJA

-master rad-

Mentor dr Petar Marković

Novi Sad, 2026.

# Sadržaj

|                                                   |    |
|---------------------------------------------------|----|
| Uvod                                              | 3  |
| 1 Osnovni pojmovi teorije prstena i teorije polja | 4  |
| 1.1 Prsteni, ideali i polja                       | 4  |
| 1.2 Proširenja polja i polja razlaganja           | 12 |
| 1.3 Separabilnost i savršena polja                | 20 |
| 2 Konstrukcija algebarskog zatvorenja             | 28 |
| Zaključak                                         | 37 |
| Literatura                                        | 38 |

# Uvod

Teorija polja predstavlja jednu od najznačajnijih oblasti apstraktne algebre i ima važnu ulogu u proučavanju algebarskih jednačina i teorije Galoa. Jedan od osnovnih pojmova ove teorije jeste pojam algebarski zatvorenog polja. Ovakva polja imaju značajnu ulogu u teoriji polinoma, jer omogućavaju potpuno rastavljanje svakog polinoma na linearne činioce. Za svako polje postavlja se prirodno pitanje postojanja algebarski zatvorenog algebarskog proširenja koje ga sadrži. Takvo proširenje naziva se algebarsko zatvorenje datog polja. Postoji više različitih pristupa dokazu postojanja algebarskog zatvorenja proizvoljnog polja. Jedan od njih zasniiva se na iterativnom konstruisanju unije polja razlaganja odgovarajućih polinoma. Cilj ovog rada jeste da se prikaže konstrukcija algebarskog zatvorenja polja korišćenjem količničkih prstena polinoma, svojstava separabilnih proširenja i Zornove leme. U prvom poglavlju predstavljeni su osnovni pojmovi teorije prstena i teorije polja. Najpre su uvedeni pojmovi prstena, ideala i polja, zatim su obrađena proširenja polja i polja razlaganja, kao i pojmovi separabilnih i savršenih polja. Ovi rezultati predstavljaju osnovu za razumevanje konstrukcije koja se razmatra u nastavku rada.

# Poglavlje 1

## Osnovni pojmovi teorije prstena i teorije polja

U ovom poglavlju uvodimo osnovne pojmove i rezultate teorije prstena i teorije polja koji će biti korišćeni u nastavku rada. Osnovni pojmovi i rezultati iz teorije prstena, kao i osnovna svojstva prstena polinoma, obrađeni su prema [3, 2, 4]. Pojmovi i rezultati koji se odnose na proširenja polja i polja razlaganja obrađeni su prema [6, 2], dok su pojmovi i rezultati koji se odnose na savršena polja uglavnom preuzeti iz [5, 3].

### 1.1 Prsteni, ideali i polja

**Definicija 1.1** *Prsten* je algebarska struktura  $(R, +, \cdot)$  sa dve binarne operacije  $+$  i  $\cdot$  takva da:

1.  $(R, +)$  je Abelova grupa,
2.  $(R, \cdot)$  je polugrupa,
3. važi zakon distributivnosti: za svako  $x, y, z \in R$

$$(x + y)z = xz + yz,$$

$$x(y + z) = xy + xz.$$

Kažemo da je  $R$  komutativan ako je  $\cdot$  komutativna operacija. Kažemo da je  $R$  prsten sa jedinicom ako postoji neutralni element za množenje i obeležavamo ga sa 1. Neutralni element za sabiranje obeležavamo sa 0.

**Definicija 1.2** *Neprazan podskup  $T$  prstena  $R$  je **potprsten** prstena  $R$  akko je  $(T, +|_{T^2}, \cdot|_{T^2})$  prsten.*

Trivijalni potprsteni prstena  $R$  su sam prsten  $R$  i nula prsten  $(\{0\}, +, \cdot)$ . Ako je  $T$  potprsten prstena  $R$ , pišaćemo  $T \leq R$ , a ako je u pitanju pravi potprsten, koristićemo  $T < R$ .

**Tvrđenje 1.3** *Neka je  $R$  prsten i neka je  $S \subseteq R$ . Tada je  $S$  potprsten od  $R$  ako i samo ako je  $S \neq \emptyset$  i za svaka  $x, y \in S$  važi  $x - y \in S$  i  $xy \in S$ .*

*Dokaz.* Ako je  $S$  potprsten od  $R$ , onda je  $S$  zatvoren za oduzimanje i množenje, pa za svaka  $x, y \in S$  važi  $x - y \in S$  i  $xy \in S$ .

Obrnuto, neka je  $S \neq \emptyset$  i neka za svaka  $x, y \in S$  važi  $x - y \in S$  i  $xy \in S$ . Iz  $x - x = 0$  sledi  $0 \in S$ , a iz  $0 - x = -x$  sledi  $-x \in S$  za svako  $x \in S$ . Zatim, za  $x, y \in S$  imamo  $x - (-y) = x + y \in S$ . Asocijativnost i distributivnost očigledno važe. Dakle,  $S$  je potprsten od  $R$ .

□

**Tvrđenje 1.4** *Neka je  $R$  prsten i neka je  $\{R_i\}_{i \in I}$  familija njegovih potprstena. Tada je  $\bigcap_{i \in I} R_i$  takođe potprsten od  $R$ .*

*Dokaz.* Neka je  $S = \bigcap_{i \in I} R_i$ . Pošto je svaki  $R_i$  potprsten, skup  $S$  je neprazan, jer  $0 \in R_i$  za svako  $i \in I$ , pa je  $0 \in S$ . Neka su  $x, y \in S$ . Tada za svako  $i \in I$  važi  $x, y \in R_i$ . Pošto je  $R_i$  potprsten, imamo  $x - y \in R_i$  i  $xy \in R_i$  za svako  $i \in I$ . Prema tome,  $x - y \in S$  i  $xy \in S$ . Prema kriterijumu za potprsten,  $S$  je potprsten od  $R$ .

□

**Definicija 1.5** *Neka su dati prsteni  $R = (R, +, \cdot)$  i  $S = (S, \oplus, *)$ . Preslikavanje  $\varphi : R \longrightarrow S$  je **homomorfizam** prstena  $R$  u prsten  $S$  ako i samo ako je ispunjeno (za svako  $a, b \in R$ ):*

$$\varphi(a + b) = \varphi(a) \oplus \varphi(b)$$

i

$$\varphi(a \cdot b) = \varphi(a) * \varphi(b).$$

Ako je  $\varphi$  bijektivno preslikavanje, onda je to **izomorfno preslikavanje** prstena  $R$  na prsten  $S$ , a za prstene  $R$  i  $S$  kažemo da su izomorfni, u notaciji  $R \cong S$ .

**Definicija 1.6** Potprsten  $I$  prstena  $R$  je *levi ideal* ako za svako  $r \in R$  i svako  $a \in I$  važi  $ra \in I$ . Analogno,  $I$  je *desni ideal* ako za svako  $r \in R$  i svako  $a \in I$  važi  $ar \in I$ . Potprsten  $I$  je *ideal* ako je istovremeno levi i desni ideal. U tom slučaju pišemo  $I \triangleleft R$  i kažemo da je  $I$  ideal prstena  $R$ .

**Definicija 1.7** Ideal  $I \triangleleft R$  je **pravi** akko  $I \neq R$ . Ideal  $I \triangleleft R$  je **netrivijalan** akko  $I \neq \{0\}$  i  $I \neq R$ .

**Definicija 1.8** Skup svih invertibilnih elemenata prstena  $R$  označava se sa  $R^*$  i definiše se sa

$$R^* = \{a \in R \mid \exists b \in R \text{ takav da je } ab = ba = 1\}.$$

**Tvrđenje 1.9** Ideal  $I$  prstena sa jedinicom  $R$  je pravi akko  $I \cap R^* = \emptyset$ .

*Dokaz.* ( $\Rightarrow$ ) Neka je  $I \neq R$ . Pretpostavimo suprotno, tj. da postoji  $a \in I \cap R^*$ . Onda  $1 = a \cdot a^{-1} \in I$ , pa stoga i  $r = r \cdot 1 \in I$  za svako  $r \in R$ . Odatle dobijamo  $I = R$  što je kontradikcija sa pretpostavkom da je  $I$  pravi ideal.

( $\Leftarrow$ ) Pretpostavimo da je  $I \cap R^* = \emptyset$ . Ako bi bilo  $I = R$ , tada bi  $1 \in I$ , a kako je  $1 \in R^*$ , sledilo bi  $I \cap R^* \neq \emptyset$ , što je kontradikcija.  $\square$

**Definicija 1.10** Neka je  $R$  prsten i  $I \triangleleft R$ . Ideal  $I$  je **maksimalan ideal** ako važi  $I \neq R$  i za svaki ideal  $J$  takav da  $I \subseteq J \subseteq R$  važi  $J = I$  ili  $J = R$ .

**Definicija 1.11** Levi (desni) ideal, odnosno ideal, generisan skupom  $X$  je najmanji u smislu inkluzije levi, desni ideal, odnosno ideal, koji sadrži  $X$ .

Ideali generisani jednoelementnim skupom su **glavni ideali**. Prsten čiji su svi ideali glavni naziva se **domen glavnih ideala**.

**Definicija 1.12** Neka je  $R$  prsten i  $I \triangleleft R$ . Za  $R/I = \{r + I : r \in R\}$  definišemo operacije  $+$  i  $\cdot$  na sledeći način:

$$(r + I) + (s + I) = (r + s) + I \quad \text{i} \quad (r + I) \cdot (s + I) = rs + I.$$

**Tvrđenje 1.13** Ako je  $R$  prsten i  $I \triangleleft R$ , onda je  $(R/I, +, \cdot)$  prsten, tzv. **faktor ili količnički prsten**.

*Dokaz.* Očigledno je da je  $(R/I, +)$  Abelova grupa. Pokazaćemo prvo dobru definisanost. Neka je

$$r_1 + I = r_2 + I \quad tj. \quad r_1 - r_2 \in I,$$

$$s_1 + I = s_2 + I \quad tj. \quad s_1 - s_2 \in I.$$

Sada

$$\begin{aligned} r_1 s_1 - r_2 s_2 &= r_1 s_1 - r_1 s_2 + r_1 s_2 - r_2 s_2 \\ &= r_1(s_1 - s_2) + (r_1 - r_2)s_2 \in I. \end{aligned}$$

Dalje proveravamo asocijativnost.  $((r+I)(s+I))(t+I) = (rs+I)(t+I) = (rst+I) = (r+I)(st+I) = (r+I)((s+I)(t+I))$ .

Pokaćemo levu distributivnost. Desna se pokazuje analogno.  $(r+I)((s+I)+(t+I)) = (r+I)((s+t)+I) = (r(s+t)+I) = (rs+rt+I) = (rs+I) + (rt+I) = (r+I)(s+I) + (r+I)(t+I)$

□

**Definicija 1.14** *Polje je komutativan prsten sa jedinicom u kome svaki nenula element ima multiplikativni inverz. Ekvivalentno,  $(R \setminus \{0\}, \cdot)$  je grupa.*

**Definicija 1.15** *Neka je  $F$  polje. Neprazan podskup  $K$  od  $F$  je **potpolje** polja  $F$  ako je  $K$  potprsten od  $F$  i ako svaki nenula element iz  $K$  ima multiplikativni inverz u  $K$ .*

**Tvrđenje 1.16** *Nenula komutativan prsten sa jedinicom je polje ako nema netrivialnih ideala.*

*Dokaz.*

( $\Rightarrow$ ) Neka je  $R$  polje i neka je  $I \triangleleft R$ . Ako je  $I \neq \{0\}$ , postoji  $a \in I$  takav da je  $a \neq 0$ . Kako je  $R$  polje, element  $a$  ima inverz  $a^{-1} \in R$ . Tada je  $1 = aa^{-1} \in I$ , pa za svako  $r \in R$  važi  $r = r \cdot 1 \in I$ . Dakle,  $I = R$ . Sledi da  $R$  nema netrivialnih ideala.

( $\Leftarrow$ ) Pretpostavimo da  $R$  nema netrivialnih ideala. Neka je  $a \in R$ ,  $a \neq 0$ . Glavni ideal  $\langle a \rangle$  je različit od nula ideala, pa zbog pretpostavke mora biti  $\langle a \rangle = R$ . Kako je  $1 \in R$ , postoji  $b \in R$  takav da je  $1 = ab$ . Dakle, svaki nenula element  $a \in R$  ima multiplikativni inverz. Pošto je  $R$  komutativan prsten sa jedinicom, sledi da je  $R$  polje. □

**Tvrđenje 1.17** *Neka je  $R$  komutativan prsten sa jedinicom i neka je  $I$  ideal prstena  $R$ . Tada je količnički prsten  $R/I$  polje ako i samo ako je  $I$  maksimalan ideal prstena  $R$ .*

*Dokaz.*

( $\Rightarrow$ ) Pretpostavimo da je  $R/I$  polje. Pokazaćemo da je  $I$  maksimalan ideal.

Neka je  $J$  ideal prstena  $R$  takav da važi  $I \subseteq J \subseteq R$ . Po teoremi o korespondenciji između ideala prstena  $R$  koji sadrže  $I$  i ideala količničkog prstena  $R/I$ , idealu  $J$  odgovara ideal

$$J/I = \{a + I \mid a \in J\}$$

u prstenu  $R/I$ . Pošto je  $R/I$  polje, njegovi jedini ideali su  $\{I\} = \{0_{R/I}\}$  i  $R/I$ . Dakle, postoje samo dve mogućnosti.

Ako je  $J/I = \{I\}$ , onda za svaki  $a \in J$  važi  $a + I = I$ , odnosno  $a \in I$ . Iz ovoga sledi da je  $J = I$ .

Ako je  $J/I = R/I$ , onda za svako  $a \in R$  važi  $a + I \in J/I$ , pa postoji  $b \in J$  takav da  $a + I = b + I$ . To znači da je  $a - b \in I \subseteq J$ . Pošto je i  $b \in J$ , zaključujemo da je  $a = (a - b) + b \in J$ . Dakle,  $J = R$ .

Prema tome, između  $I$  i  $R$  ne postoji nijedan drugi ideal, pa je  $I$  maksimalan ideal.

( $\Leftarrow$ ) Pretpostavimo sada da je  $I$  maksimalan ideal. Pokazaćemo da je  $R/I$  polje.

Neka je  $a + I \in R/I$ , pri čemu  $a + I \neq I$ , tj.  $a \notin I$ . Posmatrajmo ideal

$$I + \langle a \rangle = \{x + ra \mid x \in I, r \in R\},$$

gde je  $\langle a \rangle$  glavni ideal generisan elementom  $a$ . Pošto je  $a \notin I$ , imamo  $I \subsetneq I + \langle a \rangle$ . Kako je  $I$  maksimalan ideal, mora važiti  $I + \langle a \rangle = R$ . Otuda postoji element  $i \in I$  i element  $r \in R$  takvi da je  $i + ra = 1$ . Prelaskom na količnički prsten dobijamo  $(i + I) + (ra + I) = 1 + I$ . Pošto je  $i \in I$ , važi  $i + I = I$ , pa je  $(ra) + I = 1 + I$ . Kako je  $(ra) + I = (r + I)(a + I)$ , dobijamo  $(r + I)(a + I) = 1 + I$ . Dakle, element  $r + I$  je multiplikativni inverz elementa  $a + I$ . Pošto svaki nenulti element količničkog prstena  $R/I$  ima multiplikativni inverz, zaključujemo da je  $R/I$  polje.

Stoga je

$$R/I \text{ polje} \iff I \text{ je maksimalan ideal.}$$

**Definicija 1.18** *Prsten polinoma* nad  $F$  po promenljivoj  $X$ , označen sa  $F[X]$ , jeste skup svih izraza oblika  $f(X) = a_n X^n + \dots + a_1 X + a_0$ , gde su  $a_n, \dots, a_0 \in F$ .

**Definicija 1.19** Neka su  $f(X) = a_0 + a_1 X + \dots + a_m X^m$  i  $g(X) = b_0 + b_1 X + \dots + b_n X^n$  polinomi iz  $F[X]$ . Njihov zbir je polinom  $f(X) + g(X) = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k) X^k$ , gde koeficijente koji nisu definisani uzimamo kao nule.

**Definicija 1.20** Neka su  $f(X) = \sum_{i=0}^m a_i X^i$  i  $g(X) = \sum_{j=0}^n b_j X^j$  polinomi iz  $F[X]$ . Njihov proizvod je polinom  $f(X)g(X) = \sum_{k=0}^{m+n} c_k X^k$ , gde je  $c_k = \sum_{i+j=k} a_i b_j$ .

**Definicija 1.21** Za polinom  $f(X) = a_0 + a_1 X + \dots + a_n X^n \in F[X]$ , gde je  $a_n \neq 0$ , broj  $n$  zovemo **stepen polinoma**  $f$  i označavamo sa  $\deg f$ , a  $a_n$  zovemo **vodeći koeficijent** polinoma  $f$ . Polinom  $f$  je **moničan** ako mu je vodeći koeficijent jednak 1.

**Definicija 1.22** Neka je  $F$  polje. Polinom  $f(X) \in F[X]$  naziva se **nesvodljivim** ako je nekonstantan i ne može se zapisati kao proizvod dva polinoma manjeg stepena.

**Definicija 1.23** Polinomi  $f, g \in F[X]$  su **asocirani** ako postoji invertibilni element  $u \in F[X]$  takav da je  $f = ug$ .

**Tvrđenje 1.24 (Algoritam deljenja polinoma)** Neka je  $F$  polje i neka su  $f, g \in F[X]$ , pri čemu je  $g \neq 0$ . Tada postoje jedinstveni polinomi  $q, r \in F[X]$  takvi da važi  $f = qg + r$ , gde je  $r = 0$  ili  $\deg r < \deg g$ .

*Dokaz.* Dokazaćemo prvo postojanje. Dokaz izvodimo indukcijom po  $\deg f$ . Ako je  $\deg f < \deg g$ , uzimamo  $q = 0$  i  $r = f$ , pa tvrdnja važi. Pretpostavimo sada da je  $\deg f \geq \deg g$ . Neka su  $a$  i  $b$  vodeći koeficijenti polinoma  $f$  i  $g$ , redom. Pošto je  $F$  polje, postoji  $b^{-1} \in F$ . Posmatrajmo polinom  $f_1 = f - ab^{-1} X^{\deg f - \deg g} g$ . Zbog izbora koeficijenta  $ab^{-1}$  vodeći članovi se poništavaju, pa je  $\deg f_1 < \deg f$ . Prema induktivnoj pretpostavci, postoje  $q_1, r \in F[X]$  takvi da je  $f_1 = q_1 g + r$ , gde je  $r = 0$  ili  $\deg r < \deg g$ . Zato je  $f = ab^{-1} X^{\deg f - \deg g} g + f_1 = (ab^{-1} X^{\deg f - \deg g} + q_1)g + r$ .

Dakle, za  $q = ab^{-1}X^{\deg f - \deg g} + q_1$  dobijamo  $f = qg + r$ , gde je  $r = 0$  ili  $\deg r < \deg g$ .

Ostaje da pokažemo jedinstvenost. Pretpostavimo da je  $f = qg + r = q'g + r'$ , gde je  $r = 0$  ili  $\deg r < \deg g$ , i  $r' = 0$  ili  $\deg r' < \deg g$ . Tada je  $(q - q')g = r' - r$ . Ako je  $q \neq q'$ , tada je  $q - q' \neq 0$ , pa je  $\deg((q - q')g) = \deg(q - q') + \deg g \geq \deg g$ . Sa druge strane, iz uslova za ostatke sledi da je  $r' - r = 0$  ili  $\deg(r' - r) < \deg g$ . U oba slučaja dobijamo kontradikciju. Zato mora biti  $q = q'$ , a iz jednakosti  $qg + r = qg + r'$  sledi  $r = r'$ . Prema tome, polinomi  $q$  i  $r$  su jedinstveni.  $\square$

**Tvrđenje 1.25** *Ako je  $F$  polje, tada je prsten polinoma  $F[X]$  domen glavnih ideala.*

*Dokaz.* Neka je  $I$  proizvoljan ideal prstena  $F[X]$ . Ako je  $I = \{0\}$ , tada je očigledno  $I = \langle 0 \rangle$ , pa je  $I$  glavni ideal.

Pretpostavimo da je  $I \neq \{0\}$ . Tada u  $I$  postoji nenulti polinom. Među svim nenultim polinomima iz  $I$  izaberimo polinom  $f(X)$  najmanjeg stepena. Pokazaćemo da je  $I = \langle f(X) \rangle$ . Pošto je  $f(X) \in I$  i  $I$  je ideal, sledi da za svaki polinom  $h(X) \in F[X]$  važi  $h(X)f(X) \in I$ , odnosno  $\langle f(X) \rangle \subseteq I$ . Neka je sada  $g(X) \in I$ . Kako je  $F$  polje, u prstenu  $F[X]$  važi algoritam deljenja, pa postoje jedinstveni polinomi  $q(X), r(X) \in F[X]$  takvi da je

$$g(X) = q(X)f(X) + r(X),$$

gde je ili  $r(X) = 0$  ili  $\deg r(X) < \deg f(X)$ . Pošto su  $g(X)$  i  $q(X)f(X)$  elementi ideala  $I$ , sledi da je

$$r(X) = g(X) - q(X)f(X) \in I.$$

Ako bi bilo  $r(X) \neq 0$ , tada bi  $r(X)$  bio nenulti polinom iz  $I$  čiji je stepen manji od stepena polinoma  $f(X)$ , što je u suprotnosti sa izborom polinoma  $f(X)$ . Prema tome, mora biti  $r(X) = 0$ , pa je  $g(X) = q(X)f(X)$ , odnosno  $g(X) \in \langle f(X) \rangle$ . Dakle, važi  $I \subseteq \langle f(X) \rangle$ . Kako je već pokazano da je  $\langle f(X) \rangle \subseteq I$ , zaključujemo da je  $I = \langle f(X) \rangle$ .

Pošto je ideal  $I$  bio proizvoljan, sledi da je svaki ideal prstena  $F[X]$  glavni. Prema tome,  $F[X]$  je domen glavnih ideala.  $\square$

**Tvrđenje 1.26** *Neka je  $F$  polje i neka je  $f(X) \in F[X]$ . Tada je ideal  $\langle f \rangle$  maksimalan u  $F[X]$  ako i samo ako je  $f(X)$  nesvodljiv polinom.*

*Dokaz.*

( $\Rightarrow$ ) Pretpostavimo da je  $\langle f \rangle$  maksimalan ideal u  $F[X]$ . Pokazaćemo da je  $f(X)$  nesvodljiv. Pretpostavimo suprotno, da je  $f(X)$  svodljiv. Tada postoje polinomi  $g(X), h(X) \in F[X]$  takvi da je  $f(X) = g(X)h(X)$ , pri čemu ni  $g(X)$  ni  $h(X)$  nisu invertibilni elementi prstena  $F[X]$ . Pošto  $g(X)$  deli  $f(X)$ , imamo  $\langle f \rangle \subseteq \langle g \rangle$ . Kako  $g(X)$  nije invertibilan, važi  $\langle g \rangle \neq F[X]$ . Takođe, pošto  $h(X)$  nije invertibilan, polinomi  $f(X)$  i  $g(X)$  nisu asociirani, pa je  $\langle f \rangle \neq \langle g \rangle$ . Dakle,

$$\langle f \rangle \subsetneq \langle g \rangle \subsetneq F[X],$$

što je u suprotnosti sa činjenicom da je  $\langle f \rangle$  maksimalan ideal. Prema tome,  $f(X)$  mora biti nesvodljiv.

( $\Leftarrow$ ) Pretpostavimo sada da je  $f(X)$  nesvodljiv u  $F[X]$ . Neka je  $I$  ideal takav da važi

$$\langle f \rangle \subseteq I \subseteq F[X].$$

Pošto je  $F[X]$  prsten glavnih ideala, postoji polinom  $g(X) \in F[X]$  takav da je  $I = \langle g \rangle$ . Iz  $\langle f \rangle \subseteq \langle g \rangle$  sledi da  $g(X)$  deli  $f(X)$ , odnosno postoji polinom  $h(X) \in F[X]$  takav da je  $f(X) = g(X)h(X)$ . Kako je  $f(X)$  nesvodljiv, jedan od polinoma  $g(X)$  ili  $h(X)$  mora biti invertibilan. Ako je  $g(X)$  invertibilan, tada je

$$I = \langle g \rangle = F[X].$$

Ako je  $h(X)$  invertibilan, tada su  $f(X)$  i  $g(X)$  asociirani, pa je

$$I = \langle g \rangle = \langle f \rangle.$$

Dakle, ne postoji ideal strogo između  $\langle f \rangle$  i  $F[X]$ , pa je  $\langle f \rangle$  maksimalan ideal.  $\square$

**Definicija 1.27** (a) Relacija  $\leq$  na skupu  $S$  je **relacija parcijalnog uređenja** ako je refleksivna, tranzitivna i antisimetrična.

(b) Parcijalno uređenje je **totalno uređenje** ako važi, za sve  $s, t \in S$ , ili je  $s \leq t$  ili je  $t \leq s$ .

(c) **Gornje ograničenje** podskupa  $T$  parcijalno uređenog skupa  $(S, \leq)$  je element  $s$  takav da važi  $t \leq s$  za sve  $t \in T$ .

(d) **Maksimalni element** parcijalno uređenog skupa  $S$  je element  $s$  takav da ako za svako  $s' \in S$  važi  $s \leq s'$ , onda  $s = s'$ .

Sledeća lema nam je potrebna za dokazivanje glavnog rezultata, jer obezbeđuje postojanje maksimalnog elementa među pravim idealima. Više detalja o njoj može se naći u [2].

**Lema 1.28** (*Zornova lema*) *Neka je  $(S, \leq)$  parcijalno uređenje gde svaki totalno uređeni podskup ima gornju granicu u  $S$ . Tada  $S$  ima maksimalni element.*

**Posledica 1.29** *Svaki neprazan komutativni prsten sa jedinicom  $A$  ima maksimalni ideal među pravim idealima.*

*Dokaz.* Neka je  $S$  skup svih pravih ideala u  $A$ , parcijalno uređen inkluzijom. Ako je  $T \subseteq S$  totalno uređen skup ideala, onda je  $J = \bigcup_{I \in T} I$  ponovo ideal. Treba da pokažemo da za proizvoljne elemente  $x, y \in J$  i  $a \in A$  važi  $x - y, ax \in J$ . Za  $x, y \in J$  postoje  $I_1, I_2 \in T$  tako da  $x \in I_1, y \in I_2$ . Pošto je  $T$  totalno uređen skup važi ili  $I_1 \subseteq I_2$  ili  $I_2 \subseteq I_1$ . Pretpostavimo da važi  $I_1 \subseteq I_2$ . To znači da i  $x \in I_2$ , što implicira da  $x - y \in I_2 \subseteq J$ . Isto važi za  $ax$  za svako  $a \in A$ .  $J$  je pravi ideal jer kad bi  $1 \in J$  tada bi moralo da važi i da  $1 \in I$  za neki ideal  $I \in T$ , pa  $I$  ne bi bio pravi. Stoga je  $J$  gornje ograničenje za  $T$ . Sada, na osnovu Zornove leme zaključujemo da  $S$  ima maksimalni ideal, koji je maksimalni ideal za  $A$ .  $\square$

## 1.2 Proširenja polja i polja razlaganja

**Definicija 1.30** *Polje  $K$  je **proširenje (ekstenzija)** polja  $F$ , u oznaci  $K/F$ , akko je  $F$  potpolje polja  $K$ .*

Lako se pokazuje da, ako je polje  $K$  ekstenzija polja  $F$ , tada je  $(K, +)$  vektorski prostor nad poljem  $F$ . Pošto je  $K$  vektorski prostor nad  $F$ , možemo posmatrati njegovu dimenziju.

**Definicija 1.31** *Dimenziju vektorskog prostora  $K$  nad  $F$  nazivamo **stepenom ekstenzije** polja  $K$  nad poljem  $F$  i označavamo je sa  $[K : F]$ . Ako je  $[K : F] < \infty$ , kažemo da je  $K$  **konačna ekstenzija** polja  $F$ , a u suprotnom kažemo da je  $K$  **beskonačna ekstenzija** polja  $F$ .*

**Definicija 1.32** *Neka su  $F$  i  $K$  polja,  $F \leq K$  i  $\alpha \in K$ . Tada je  $F[\alpha]$  najmanji potprsten u  $K$  koji sadrži  $F \cup \{\alpha\}$ . Kažemo da je  $F[\alpha]$  prsten generisan elementom  $\alpha$  i  $F[\alpha] = \{f(\alpha) : f(x) \in F[x]\}$ .*

Važno je uočiti da  $F[\alpha]$  u opštem slučaju nije polje. Najmanje polje koje sadrži  $F \cup \{\alpha\}$  označavamo sa  $F(\alpha)$  i nazivamo poljem generisanim elementom  $\alpha$  nad  $F$ . Pri tome važi  $F[\alpha] \subseteq F(\alpha)$ .

**Tvrđenje 1.33** *Neka je  $F$  potpolje polja  $E$  i neka je  $S \subseteq E$ . Tada presek svih potprstena polja  $E$  koji sadrže  $F$  i  $S$  predstavlja najmanji potprsten od  $E$  koji sadrži  $F$  i  $S$ .*

*Dokaz.* Neka je  $R = \bigcap_{\substack{A \subseteq E \\ F \cup S \subseteq A}} A$ . Pošto je presek potprstena ponovo potprsten,  $R$  je potprsten od  $E$ . Za svako  $A$  koje učestvuje u preseku važi  $F \cup S \subseteq A$ , pa je  $F \cup S \subseteq R$ . Ako je  $B$  bilo koji potprsten od  $E$  koji sadrži  $F$  i  $S$ , onda je  $B$  jedan od potprstena koji učestvuju u preseku, pa je  $R \subseteq B$ . Dakle,  $R$  je najmanji potprsten od  $E$  koji sadrži  $F$  i  $S$ .  $\square$

**Definicija 1.34** *Potprsten  $R$  iz prethodne teoreme nazivamo **potprstenom generisanim nad  $F$  skupom  $S$**  i označavamo ga sa  $F[S]$ . Ako je  $S = \{\alpha_1, \dots, \alpha_n\}$ , tada umesto  $F[S]$  pišemo  $F[\alpha_1, \dots, \alpha_n]$ .*

**Lema 1.35** *Potprsten  $F[S]$  sastoji se od svih elemenata polja  $E$  koji se mogu zapisati u obliku konačne sume*

$$\sum a_{i_1, \dots, i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n},$$

gde su  $a_{i_1, \dots, i_n} \in F$ ,  $\alpha_i \in S$  i  $i_j \in \mathbb{N}_0$ .

*Dokaz.* Označimo sa  $R$  skup svih elemenata polja  $E$  koji se mogu zapisati u navedenom obliku. Pokazaćemo da je  $R = F[S]$ .

Najpre, jasno je da  $R$  sadrži polje  $F$ , jer za svaki  $a \in F$  važi  $a = a\alpha_1^0 \cdots \alpha_n^0$ . Takođe, svaki element skupa  $S$  pripada skupu  $R$ , jer za  $\alpha_j \in S$  možemo napisati  $\alpha_j = 1 \cdot \alpha_j$ .

Pokazaćemo da je  $R$  potprsten od  $E$ . Neka su

$$x = \sum a_{i_1, \dots, i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}, y = \sum b_{j_1, \dots, j_n} \alpha_1^{j_1} \cdots \alpha_n^{j_n}$$

elementi skupa  $R$ . Tada je  $x - y$  ponovo konačna suma istog oblika, jer su koeficijenti iz  $F$  zatvoreni za sabiranje. Kod množenja  $x \cdot y$ , proizvod dva člana oblika

$$a_{i_1, \dots, i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}, b_{j_1, \dots, j_n} \alpha_1^{j_1} \cdots \alpha_n^{j_n}$$

jednak je

$$a_{i_1, \dots, i_n} b_{j_1, \dots, j_n} \alpha_1^{i_1+j_1} \cdots \alpha_n^{i_n+j_n},$$

koji je ponovo element istog oblika. Dakle,  $R$  je potprsten polja  $E$  koji sadrži  $F$  i skup  $S$ . Po definiciji generisanog potprstena,  $F[S]$  je najmanji potprsten od  $E$  koji sadrži  $F$  i  $S$ . Pošto je  $R$  jedan takav potprsten, važi  $F[S] \subseteq R$ .

Sa druge strane, neka je  $T$  proizvoljan potprsten od  $E$  koji sadrži  $F$  i  $S$ . Kako je  $T$  zatvoren za množenje, on sadrži sve elemente oblika

$$\alpha_1^{i_1} \cdots \alpha_n^{i_n}.$$

Pošto je  $T$  zatvoren za množenje skalarima iz  $F$  i za sabiranje, on sadrži sve konačne sume oblika

$$\sum a_{i_1, \dots, i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}.$$

Dakle, svaki takav potprsten  $T$  sadrži  $R$ , pa posebno i njihov presek. Prema tome,  $R \subseteq F[S]$ .

Odavde dobijamo  $R = F[S]$ , čime je dokaz završen.  $\square$

**Tvrđenje 1.36** *Neka je  $F$  potpolje polja  $E$  i neka je  $S \subseteq E$ . Tada presek svih potpolja polja  $E$  koja sadrže  $F$  i  $S$  predstavlja najmanje potpolje polja  $E$  koje sadrži  $F$  i  $S$ .*

*Dokaz.* Dokaz je analogan dokazu tvrđenja 1.33. Naime, presek proizvoljne familije potpolja je ponovo potpolje. Ako označimo taj presek sa  $F(S)$ , onda očigledno važi  $F \subseteq F(S)$  i  $S \subseteq F(S)$ . Sa druge strane,  $F(S)$  je sadržano u svakom potpolju polja  $E$  koje sadrži  $F$  i  $S$ . Dakle,  $F(S)$  je najmanje potpolje polja  $E$  koje sadrži  $F$  i  $S$ .  $\square$

**Definicija 1.37** *Potpolje  $F(S)$  nazivamo **potpoljem generisanim nad  $F$  skupom  $S$** . Ako je  $S = \{\alpha_1, \dots, \alpha_n\}$ , tada umesto  $F(S)$  pišemo  $F(\alpha_1, \dots, \alpha_n)$ .*

Dakle, prsten  $F[\alpha_1, \dots, \alpha_n]$  sastoji se od svih elemenata polja  $E$  koji se mogu izraziti kao polinomi po elementima  $\alpha_1, \dots, \alpha_n$  sa koeficijentima iz  $F$ , dok se polje  $F(\alpha_1, \dots, \alpha_n)$  sastoji od svih elemenata polja  $E$  koji se mogu izraziti kao količnik dva takva polinoma.

**Definicija 1.38** *Neka je  $K$  proširenje polja  $F$ . Element  $\alpha$  polja  $K$  je **algebarski element** nad poljem  $F$  ako je nula nekog polinoma sa koeficijentima iz polja  $F$ ; u suprotnom je **transcedentan element** nad poljem  $F$ .*

*Polje  $K$  je algebarsko proširenje polja  $F$  ako je svaki njegov element algebarski nad  $F$ .*

**Tvrđenje 1.39** *Svako konačno proširenje je i algebarsko.*

*Dokaz.* Neka je  $[K : F] = n$ . Uzmimo proizvoljan element  $\alpha \in K$ . Pokazaćemo da je  $\alpha$  algebarski nad  $F$ .

Pretpostavimo suprotno, odnosno da ne postoji nekonstantan polinom  $f(x) \in F[x]$  takav da je  $f(\alpha) = 0$ . To znači da za svaki izbor koeficijenata  $c_0, c_1, \dots, c_m \in F$ , koji nisu svi jednaki nuli, važi

$$c_m \alpha^m + \dots + c_1 \alpha + c_0 \neq 0.$$

Posebno, za  $m = n$  dobijamo da za svaku netrivialnu linearnu kombinaciju elemenata  $1, \alpha, \alpha^2, \dots, \alpha^n$  važi

$$c_0 + c_1 \alpha + \dots + c_n \alpha^n \neq 0.$$

Prema tome, elementi  $1, \alpha, \alpha^2, \dots, \alpha^n$  su linearno nezavisni nad poljem  $F$ . Međutim,  $K$  je vektorski prostor nad  $F$  dimenzije  $n$ , pa ne postoji skup od više od  $n$  linearno nezavisnih vektora u  $K$ . Skup  $1, \alpha, \alpha^2, \dots, \alpha^n$  sadrži  $n + 1$  elemenata i linearno je nezavisan, što je kontradikcija sa činjenicom da je

$$\dim_F K = n.$$

Dakle, naša pretpostavka je bila pogrešna. Mora postojati nekonstantan polinom  $f(x) \in F[x]$  takav da je  $f(\alpha) = 0$ . Zato je  $\alpha$  algebarski nad  $F$ . Pošto je  $\alpha \in K$  bio proizvoljan, sledi da je proširenje  $K/F$  algebarsko.  $\square$

**Tvrđenje 1.40** *Neka su  $F \subseteq K \subseteq E$  proširenja polja. Ako su  $K/F$  i  $E/K$  konačne ekstenzije, tada je i  $E/F$  konačna ekstenzija i važi*

$$[E : F] = [E : K][K : F].$$

*Dokaz.* Neka je  $\{e_1, \dots, e_m\}$  baza prostora  $E$  nad  $K$ , a  $\{k_1, \dots, k_n\}$  baza prostora  $K$  nad  $F$ . Tada je  $m = [E : K]$  i  $n = [K : F]$ . Pokazaćemo da je skup  $\{e_i k_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$  baza prostora  $E$  nad  $F$ .

Neka je  $x \in E$ . Pošto je  $\{e_1, \dots, e_m\}$  baza prostora  $E$  nad  $K$ , postoje elementi  $a_1, \dots, a_m \in K$  takvi da je  $x = a_1 e_1 + \dots + a_m e_m$ . Kako je  $\{k_1, \dots, k_n\}$  baza prostora  $K$  nad  $F$ , svaki element  $a_i \in K$  može se

zapisati u obliku  $a_i = b_{i1}k_1 + \cdots + b_{in}k_n$ , gde su  $b_{ij} \in F$ . Zamenom ovih izraza dobijamo

$$x = \sum_{i=1}^m \sum_{j=1}^n b_{ij} e_i k_j.$$

Odavde sledi da svaki element iz  $E$  može biti predstavljen kao linearna kombinacija elemenata skupa  $\{e_i k_j\}$  sa koeficijentima iz  $F$ . Dakle, ovaj skup generiše vektorski prostor  $E$  nad  $F$ .

Sada pokažimo da su elementi skupa  $\{e_i k_j\}$  linearno nezavisni nad  $F$ . Pretpostavimo da važi

$$\sum_{i=1}^m \sum_{j=1}^n a_{ij} e_i k_j = 0,$$

gde su  $a_{ij} \in F$ . Grupisanjem po elementima baze  $\{e_1, \dots, e_m\}$  dobijamo

$$\sum_{i=1}^m e_i \left( \sum_{j=1}^n a_{ij} k_j \right) = 0.$$

Pošto su  $e_1, \dots, e_m$  linearno nezavisni nad  $K$ , sledi da je  $\sum_{j=1}^n a_{ij} k_j = 0$  za svako  $i$ . Ali su  $k_1, \dots, k_n$  linearno nezavisni nad  $F$ , pa je  $a_{ij} = 0$  za sve  $i, j$ .

Dakle, elementi  $e_i k_j$  su linearno nezavisni nad  $F$  i čine bazu prostora  $E$  nad  $F$ . Ova baza ima  $mn$  elemenata, pa je  $[E : F] = mn$ . Kako je  $m = [E : K]$  i  $n = [K : F]$ , dobijamo

$$[E : F] = [E : K][K : F].$$

□

**Definicija 1.41** *Neka je  $F$  polje, neka je  $E$  proširenje polja  $F$  i neka je  $\alpha \in E$  algebarski element nad  $F$ . **Minimalni polinom** elementa  $\alpha$  nad poljem  $F$  je jedinstven moničan nesvodljiv polinom  $p_\alpha(X) \in F[X]$  takav da važi*

$$p_\alpha(\alpha) = 0.$$

**Tvrđenje 1.42** *Neka je  $L/F$  algebarsko proširenje i neka je  $S \subseteq L$ . Tada važi*

$$F[S] = F(S).$$

*Dokaz.* Dovoljno je pokazati da je  $F[S]$  polje. Neka je  $a \in F[S]$ ,  $a \neq 0$ . Kako je  $L/F$  algebarsko proširenje, element  $a$  je algebarski nad  $F$ . Neka je

$$p_a(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$$

minimalni polinom elementa  $a$  nad  $F$ . Pošto je  $a \neq 0$ , važi  $c_0 \neq 0$ , pa iz jednakosti  $p_a(a) = 0$  dobijamo

$$a^{-1} = -c_0^{-1} (a^{n-1} + c_{n-1}a^{n-2} + \cdots + c_1) \in F[S].$$

Dakle,  $F[S]$  je polje. Kako je  $F[S] \subseteq F(S)$  i  $F(S)$  najmanje potpolje koje sadrži  $F$  i  $S$ , sledi da je  $F(S) \subseteq F[S]$ . Prema tome,

$$F[S] = F(S).$$

□

**Teorema 1.43 (Kronekerova teorema)** *Neka je  $F$  polje i neka je  $f(X) \in F[X]$  nesvodljiv polinom. Tada postoji minimalno proširenje polja  $E/F$  takvo da polinom  $f(X)$  ima koren u  $E$ .*

*Dokaz.* Posmatrajmo ideal  $\langle f \rangle$  u prstenu polinoma  $F[X]$ . Kako je  $f(X)$  nesvodljiv polinom, ideal  $\langle f \rangle$  je maksimalan u  $F[X]$ . Zbog toga je količnički prsten  $E = F[X]/\langle f \rangle$  polje. Neka je  $\alpha = X + \langle f \rangle$  slika polinoma  $X$  u količničkom prstenu  $E$ . Pošto je  $f(X) \in \langle f \rangle$ , u količničkom prstenu važi  $f(\alpha) = 0$ . Dakle,  $\alpha$  je koren polinoma  $f(X)$  u polju  $E$ .

Ostaje da pokažemo da je  $E$  minimalno proširenje polja  $F$  sa ovom osobinom. Neka je  $K/F$  proizvoljno proširenje polja i neka je  $\beta \in K$  koren polinoma  $f(X)$ . Definišimo preslikavanje

$$\varphi : F[X] \rightarrow K$$

sa  $\varphi(g(X)) = g(\beta)$ . Ovo je homomorfizam prstena koji je identičko preslikavanje na  $F$ . Pošto je  $f(\beta) = 0$ , važi  $\langle f \rangle \subseteq \ker \varphi$ . Kako je  $\langle f \rangle$  maksimalan ideal, a  $\ker \varphi \neq F[X]$ , sledi da je  $\ker \varphi = \langle f \rangle$ . Prema Prvoj teoremi o izomorfizmu važi

$$F[X]/\langle f \rangle \cong \text{Im } \varphi.$$

Kako je  $F[X]/\langle f \rangle$  polje, a  $\text{Im } \varphi$  je sa njim izomorfno, sledi da je  $\text{Im } \varphi$  takođe polje. Pri tome je  $\text{Im } \varphi = F[\beta]$ . Kako je  $\beta$  algebarski nad  $F$ , važi

$F[\beta] = F(\beta)$ . Budući da je  $F(\beta)$  najmanje potpolje polja  $K$  koje sadrži  $F$  i koren  $\beta$  polinoma  $f(X)$ , zaključujemo da je  $E = F[X]/\langle f \rangle$ , do na izomorfizam, minimalno proširenje polja  $F$  u kome polinom  $f(X)$  ima koren.  $\square$

**Tvrđenje 1.44** *Neka su  $\alpha$  i  $\beta$  nule moničnog nesvodljivog polinoma  $p(X) \in F[X]$ . Tada postoji izomorfizam polja  $\Phi : F[\alpha] \longrightarrow F[\beta]$  takav da je  $\Phi|_F = \text{id}_F$  i  $\Phi(\alpha) = \beta$ .*

*Dokaz.* Pošto je  $p(X)$  moničan nesvodljiv polinom iz  $F[X]$ , on je minimalni polinom i za  $\alpha$  i za  $\beta$  nad poljem  $F$ . Definišemo preslikavanje  $\Phi : F[\alpha] \longrightarrow F[\beta]$  tako što za svaki  $f(X) \in F[X]$  stavljamo

$$\Phi(f(\alpha)) = f(\beta).$$

Pokazaćemo da je  $\Phi$  dobro definisano. Neka su  $f(X), g(X) \in F[X]$  takvi da je  $f(\alpha) = g(\alpha)$ . Tada je  $(f - g)(\alpha) = 0$ , pa minimalni polinom  $p(X)$  deli  $f(X) - g(X)$ . Kako je  $p(X)$  takođe minimalni polinom elementa  $\beta$  i  $p(X)$  deli  $f(X) - g(X)$ , sledi da je  $(f - g)(\beta) = 0$ . Dakle,  $f(\beta) = g(\beta)$ , što pokazuje da je preslikavanje  $\Phi$  dobro definisano.

Za  $f(X), g(X) \in F[X]$  važi

$$\Phi(f(\alpha) + g(\alpha)) = f(\beta) + g(\beta)$$

i

$$\Phi(f(\alpha)g(\alpha)) = f(\beta)g(\beta),$$

pa je  $\Phi$  homomorfizam polja. Za svaki  $a \in F$  važi  $\Phi(a) = a$ , pa je  $\Phi|_F = \text{id}_F$ . Pošto je  $\beta$  generator polja  $F[\beta]$  nad poljem  $F$ , svaki element polja  $F[\beta]$  može se zapisati u obliku  $f(\beta)$ , za neki polinom  $f(X) \in F[X]$ . Međutim, prema definiciji preslikavanja  $\Phi$  važi

$$\Phi(f(\alpha)) = f(\beta).$$

Dakle, za proizvoljan element  $f(\beta) \in F[\beta]$  postoji element  $f(\alpha) \in F[\alpha]$  takav da je  $\Phi(f(\alpha)) = f(\beta)$ . Prema tome, svaki element polja  $F[\beta]$  pripada slici preslikavanja  $\Phi$ , pa je  $\Phi$  surjektivno. Kako je  $\Phi$  homomorfizam polja, njegovo jezgro je  $\{0\}$ , pa je  $\Phi$  injektivno. Prema tome,  $\Phi$  je izomorfizam polja i važi

$$F[\alpha] \cong F[\beta].$$

$\square$

**Definicija 1.45** *Neka je  $F$  polje i  $f(x) \in F[x]$  nekonstantan polinom. Kažemo da je  $K$  **polje razlaganja polinoma**  $f(x)$  nad  $F$  ako je  $K$  minimalno polje u kom se  $f(x)$  razlaže na linearne faktore.*

**Tvrđenje 1.46** *Neka je  $F$  polje i neka je  $f(X) \in F[X]$  nekonstantan polinom. Tada postoji polje razlaganja polinoma  $f(X)$  nad poljem  $F$ .*

*Dokaz.* Neka je

$$f(X) = f_1(X) \cdots f_m(X)$$

faktorizacija polinoma  $f(X)$  na nesvodljive faktore u prstenu  $F[X]$ . Prema Kronekerovoj teoremi postoji minimalno proširenje  $F_1/F$  u kome polinom  $f_1(X)$  ima koren. Označimo taj koren sa  $\alpha_1$ . Tada se u polju  $F_1$  polinom  $f(X)$  može zapisati u obliku

$$f(X) = (X - \alpha_1)g_1(X),$$

gde je  $g_1(X) \in F_1[X]$ . Ako se polinom  $g_1(X)$  ne razlaže na linearne faktore u polju  $F_1$ , tada postoji nesvodljiv faktor tog polinoma stepena većeg od 1. Na taj faktor ponovo primenjujemo Kronekerovu teoremu i dobijamo proširenje  $F_2/F_1$  u kome taj faktor ima koren. Nastavljajući ovaj postupak dobijamo lanac proširenja

$$F \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r$$

takav da polinom  $f(X)$  u polju  $F_r$  ima sve svoje nule. Ovaj postupak se mora završiti nakon konačno mnogo koraka, jer polinom  $f(X)$  ima konačno mnogo nula, najviše  $\deg f$ .

Neka je  $A$  skup svih nula polinoma  $f(X)$  u polju  $F_r$  i neka je  $K = F(A)$ . Tada  $K$  sadrži polje  $F$  i sve nule polinoma  $f(X)$ , pa se u njemu polinom  $f(X)$  razlaže na proizvod linearnih faktora. Ako je  $L$  bilo koje proširenje polja  $F$  u kome se polinom  $f(X)$  razlaže na linearne faktore, tada  $L$  sadrži sve elemente skupa  $A$ . Zbog toga važi

$$K = F(A) \subseteq L.$$

Dakle,  $K$  je najmanje proširenje polja  $F$  u kome se polinom  $f(X)$  razlaže na linearne faktore. Prema tome,  $K$  je polje razlaganja polinoma  $f(X)$ .  $\square$

### 1.3 Separabilnost i savršena polja

**Definicija 1.47** Karakteristika prstena  $R$ , u oznaci  $\text{char}(R)$ , je najmanji pozitivan ceo broj  $m$  takav da je  $m \cdot a = 0$  za svaki element  $a$  prstena  $R$ , ukoliko takav broj postoji. Ako takav broj ne postoji kažemo da je  $R$  karakteristike 0.

**Tvrđenje 1.48** Karakteristika polja je ili 0 ili prost broj.

*Dokaz.* Neka je  $F$  polje. Ako ne postoji prirodan broj  $n \geq 1$  takav da je  $n \cdot 1_F = 0$ , onda je po definiciji  $\text{char}(F) = 0$ .

Pretpostavimo sada da postoji najmanji prirodan broj  $n \geq 1$  takav da je  $n \cdot 1_F = 0$ . Tada je  $\text{char}(F) = n$ . Pokazaćemo da  $n$  mora biti prost broj. Pretpostavimo suprotno, da je  $n$  složen broj. Tada postoje prirodni brojevi  $a, b < n$  takvi da je  $n = ab$ . Tada važi

$$0 = n \cdot 1_F = (ab) \cdot 1_F = (a \cdot 1_F)(b \cdot 1_F).$$

Pošto je  $F$  polje, ono nema delioce nule. Zato iz  $(a \cdot 1_F)(b \cdot 1_F) = 0$  sledi da je  $a \cdot 1_F = 0$  ili  $b \cdot 1_F = 0$ . Ali to je nemoguće, jer su  $a$  i  $b$  manji od  $n$ , a  $n$  je najmanji prirodan broj za koji važi  $n \cdot 1_F = 0$ . Dobijamo kontradikciju, pa  $n$  ne može biti složen broj. Dakle, ako je karakteristika polja različita od nule, ona mora biti prost broj. Prema tome,  $\text{char}(F) = 0$  ili je  $\text{char}(F) = p$ , gde je  $p$  prost broj.  $\square$

Neka je  $R$  nenulti komutativni prsten. U prstenu  $R$  važi binomna formula:

$$(a + b)^m = a^m + \binom{m}{1} a^{m-1} b + \binom{m}{2} a^{m-2} b^2 + \cdots + b^m.$$

Ako je  $p$  prost broj, tada za svako  $r$ , gde je  $1 \leq r \leq p - 1$ , važi da  $p$  deli binomni koeficijent

$$\binom{p}{r} = \frac{p!}{r!(p-r)!},$$

jer deli brojilac, a ne deli imenilac. Prema tome, ako prsten  $R$  ima karakteristiku  $p$ , za svako  $a, b \in R$  važi

$$(a + b)^p = a^p + b^p.$$

Dakle, preslikavanje

$$\varphi : R \longrightarrow R, \quad \varphi(a) = a^p,$$

jeste homomorfizam prstena karakteristike  $p$ . Ovo preslikavanje naziva se **Frobenijusov endomorfizam** prstena  $R$ . Ako je  $R$  polje, tada je Frobenijusov endomorfizam injektivan. Zaista, ako je  $\varphi(a) = \varphi(b)$ , tada je  $a^p = b^p$ , pa sledi  $a^p - b^p = (a - b)^p = 0$ . Kako je  $R$  polje, nema delitelje nule, pa je  $a - b = 0$ , odnosno  $a = b$ . Dakle,  $\varphi$  je injektivan.

Za svaki prirodan broj  $n \geq 1$ , preslikavanje  $a \mapsto a^{p^n}$  predstavlja kompoziciju  $n$  Frobenijusovih endomorfizama, pa je i ono homomorfizam prstena. Otuda za proizvoljne elemente  $a_1, \dots, a_m \in R$  važi

$$(a_1 + \dots + a_m)^{p^n} = a_1^{p^n} + \dots + a_m^{p^n}.$$

**Definicija 1.49** Nesvodljiv polinom  $f(X) \in F[X]$  je **separabilan polinom** nad poljem  $F$  ako su svi njegovi koreni u polju razlaganja međusobno različiti, odnosno ako nema višestrukih korena.

**Definicija 1.50** Neka je  $\alpha$  algebarski element nad poljem  $F$ . Kaže se da je element  $\alpha$  **separabilan element** nad  $F$  ako je njegov minimalni polinom nad  $F$  separabilan.

**Definicija 1.51** Algebarsko proširenje  $K$  polja  $F$  je **separabilno proširenje** nad  $F$  ako su svi elementi iz  $K$  separabilni nad  $F$ .

**Lema 1.52** Neka su  $f(X), g(X) \in F[X]$ , a neka je  $\Omega$  proširenje polja  $F$ . Ako je  $r(X)$  najveći zajednički delilac polinoma  $f(X)$  i  $g(X)$  u  $F[X]$ , onda je  $r(X)$  ujedno i najveći zajednički delilac ovih polinoma u  $\Omega[X]$ .

*Dokaz.* Neka su  $f(X), g(X) \in F[X]$  i neka je  $\Omega/F$  proširenje polja. Pretpostavimo da je  $r(X)$  najveći zajednički delilac polinoma  $f(X)$  i  $g(X)$  u  $F[X]$ . Pokazaćemo da je  $r(X)$  ujedno i najveći zajednički delilac ovih polinoma u  $\Omega[X]$ . Primenićemo Euklidov algoritam na polinome  $f(X)$  i  $g(X)$ . Neka je

$$f(X) = a_n X^n + \dots + a_0, \quad g(X) = b_m X^m + \dots + b_0,$$

gde su  $a_n, b_m \in F$  i  $n \geq m$ . Pri deljenju polinoma  $f(X)$  polinomom  $g(X)$ , vodeći član količnika dobija se deljenjem vodećih članova ova dva polinoma:  $\frac{a_n}{b_m} X^{n-m}$ . Kako su  $a_n, b_m \in F$  i kako je  $F$  polje, sledi da je  $\frac{a_n}{b_m} \in F$ . Zato je  $\frac{a_n}{b_m} X^{n-m} \in F[X]$ . Oduzimanjem odgovarajućeg umnoška od  $f(X)$  dobijamo

$$f_1(X) = f(X) - \frac{a_n}{b_m} X^{n-m} g(X).$$

Svi koeficijenti polinoma  $f_1(X)$  pripadaju  $F$ , jer su dobijeni sabiranjem, oduzimanjem i množenjem elemenata iz  $F$ . Pri tome je  $\deg f_1(X) < n$ . Ako je

$$f_1(X) = a'_k X^k + \cdots + a'_0,$$

sledeći član količnika dobija se na isti način:  $\frac{a'_k}{b_m} X^{k-m}$ . Ponovo je  $\frac{a'_k}{b_m} \in F$ , pa i ovaj član pripada  $F[X]$ . Nakon oduzimanja odgovarajućeg umnoška polinoma  $g(X)$ , dobijamo polinom manjeg stepena čiji su koeficijenti i dalje u  $F$ . Ponavljanjem ovog postupka dobijamo polinom  $q(X) \in F[X]$  i ostatak  $r_1(X) \in F[X]$  takve da je

$$f(X) = q(X)g(X) + r_1(X), \quad \deg r_1(X) < \deg g(X).$$

Dakle, u celom postupku deljenja koriste se samo koeficijenti polinoma  $f(X)$  i  $g(X)$  i osnovne računske operacije u polju  $F$ . Zbog toga se pri ovom postupku ne pojavljuju koeficijenti koji pripadaju  $\Omega \setminus F$ . Pošto je  $F \subseteq \Omega$ , imamo  $F[X] \subseteq \Omega[X]$ . Prema tome, svi polinomi koji su dobijeni tokom deljenja u  $F[X]$  pripadaju i  $\Omega[X]$ , pa se isto deljenje može izvršiti i u  $\Omega[X]$  i daje isti količnik  $q(X)$  i isti ostatak  $r_1(X)$ .

Sada nastavljamo Euklidov algoritam deljenjem  $g(X)$  sa  $r_1(X)$ . Na potpuno isti način dobijamo polinom  $q_2(X) \in F[X]$  i ostatak  $r_2(X) \in F[X]$  takve da je

$$g(X) = q_2(X)r_1(X) + r_2(X), \quad \deg r_2(X) < \deg r_1(X).$$

Budući da je  $F[X] \subseteq \Omega[X]$ , ovo deljenje daje iste polinome i u  $\Omega[X]$ . Nastavljajući postupak, dobijamo niz jednakosti

$$\begin{aligned} f(X) &= q_1(X)g(X) + r_1(X), \\ g(X) &= q_2(X)r_1(X) + r_2(X), \\ r_1(X) &= q_3(X)r_2(X) + r_3(X), \\ &\vdots \\ r_{s-2}(X) &= q_s(X)r_{s-1}(X), \end{aligned}$$

pri čemu su svi polinomi  $q_i(X)$  i  $r_i(X)$  elementi  $F[X]$ . Pošto se u svakom koraku koriste samo koeficijenti prethodno dobijenih polinoma i operacije u polju  $F$ , isti niz deljenja i isti niz ostataka dobijamo i kada Euklidov algoritam posmatramo u  $\Omega[X]$ . Poslednji nenulti ostatak Euklidovog algoritma je najveći zajednički delilac polinoma  $f(X)$  i  $g(X)$ . Po pretpostavci, taj ostatak je  $r(X)$ . Stoga je

$$r(X) = \text{NZD}_{F[X]}(f(X), g(X)) = \text{NZD}_{\Omega[X]}(f(X), g(X)).$$

Dakle,  $r(X)$  je najveći zajednički delilac polinoma  $f(X)$  i  $g(X)$  i u  $F[X]$  i u  $\Omega[X]$ .

□

**Teorema 1.53 (Teorema o primitivnom elementu)** *Neka je  $E = F[\alpha_1, \dots, \alpha_r]$  konačno proširenje polja  $F$  i pretpostavimo da su  $\alpha_2, \dots, \alpha_r$  separabilni nad  $F$  (dok  $\alpha_1$  ne mora biti separabilan). Tada postoji element  $\gamma \in E$  takav da je  $E = F[\gamma]$ .*

*Dokaz.* Posmatrajmo prvo slučaj kada je  $F$  konačno. Tada je  $E$  takođe konačno jer je konačno proširenje konačnog polja. Pošto je  $E$  konačno, multiplikativna grupa polja  $E$  je ciklična (na osnovu poznatog tvrđenja da konačna podgrupa multiplikativne grupe polja mora biti ciklična). Neka je  $\beta$  generator multiplikativne grupe polja  $E$  kao ciklične grupe. Tada je  $E = F[\beta]$  i tvrđenje je dokazano u ovom slučaju.

Posmatrajmo sada slučaj kada je  $F$  beskonačno. Dovoljno je dokazati tvrdnju za slučaj  $r = 2$ , jer se tada rezultat može primeniti uzastopno. Naime, imamo

$$F[\alpha_1, \alpha_2, \dots, \alpha_r] = F[\alpha'_1, \alpha_3, \dots, \alpha_r] = F[\alpha''_1, \alpha_4, \dots, \alpha_r] = \dots$$

Neka je zato  $E = F[\alpha, \beta]$ , gde je  $\beta$  separabilan nad  $F$ . Neka su  $f$  i  $g$  minimalni polinomi elemenata  $\alpha$  i  $\beta$  nad  $F$ , redom, i neka je  $L$  polje razlaganja polinoma  $fg$  koje sadrži  $E$ . Označimo korene polinoma  $f$  u  $L$  sa  $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_s$ , a korene polinoma  $g$  sa  $\beta_1 = \beta, \beta_2, \dots, \beta_t$ . Za  $j \neq 1$  važi  $\beta_j \neq \beta$ , pa jednačina

$$\alpha_i + X\beta_j = \alpha + X\beta$$

ima tačno jedno rešenje, i to

$$X = \frac{\alpha_i - \alpha}{\beta - \beta_j}.$$

Pošto je  $F$  beskonačno, možemo izabrati  $c \in F$  koji nije jednak nijednoj od ovih konačno mnogo vrednosti. Za tako izabrani element  $c$  važi

$$\alpha_i + c\beta_j \neq \alpha + c\beta$$

osim ako je  $i = 1 = j$ . Neka je  $\gamma = \alpha + c\beta$ . Tvrđimo da je

$$F[\alpha, \beta] = F[\gamma].$$

Polinomi  $g(X)$  i  $f(\gamma - cX)$  imaju koeficijente u  $F[\gamma]$  i oba imaju  $\beta$  za koren, jer je  $g(\beta) = 0$  i

$$f(\gamma - c\beta) = f(\alpha) = 0.$$

Pokazaćemo da je  $\beta$  njihov jedini zajednički koren. Ako bi  $\beta_j$  bio neki zajednički koren, tada bi postojalo  $i$  takvo da je

$$f(\gamma - c\beta_j) = 0,$$

odakle sledi

$$\gamma - c\beta_j = \alpha_i.$$

Kako je  $\gamma = \alpha + c\beta$ , dobijamo

$$\alpha_i + c\beta_j = \alpha + c\beta.$$

Po izboru elementa  $c$  ova jednakost je moguća samo kada je  $i = 1$  i  $j = 1$ . Dakle,  $\beta$  je jedini zajednički koren polinoma  $g(X)$  i  $f(\gamma - cX)$  u polju  $L$ . Zbog toga je njihov moničan najveći zajednički delilac u  $L[X]$  jednak  $X - \beta$ . Sada prethodnu lemu primenjujemo na polje  $F[\gamma]$  i njegovo proširenje  $L$ . Pošto su  $g(X), f(\gamma - cX) \in F[\gamma][X]$ , prethodna lema daje da njihov moničan najveći zajednički delilac u  $F[\gamma][X]$  ostaje isti pri prelasku u  $L[X]$ . Kako je njihov najveći zajednički delilac u  $L[X]$  jednak  $X - \beta$ , sledi da je

$$\text{NZD}(g(X), f(\gamma - cX)) = X - \beta$$

u  $F[\gamma][X]$ . Prema tome,  $X - \beta \in F[\gamma][X]$ , odakle sledi da je  $\beta \in F[\gamma]$ . Tada je

$$\alpha = \gamma - c\beta \in F[\gamma].$$

Dakle,  $F[\alpha, \beta] \subseteq F[\gamma]$ . Sa druge strane,  $\gamma = \alpha + c\beta \in F[\alpha, \beta]$ , pa je  $F[\gamma] \subseteq F[\alpha, \beta]$ . Prema tome,  $F[\alpha, \beta] = F[\gamma]$ .

□

**Definicija 1.54** *Neka je*

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in F[X].$$

**Izvod** polinoma  $f(X)$  je polinom definisan sa

$$f'(X) = na_n X^{n-1} + (n-1)a_{n-1} X^{n-2} + \cdots + 2a_2 X + a_1.$$

Drugim rečima, ako je

$$f(X) = \sum_{i=0}^n a_i X^i,$$

onda je

$$f'(X) = \sum_{i=1}^n i a_i X^{i-1}.$$

Uobičajena pravila za izvod zbira i proizvoda i dalje važe, ali treba primetiti da je u polju karakteristike  $p$  izvod polinoma  $X^p$  jednak nuli.

**Tvrđenje 1.55** *Neka je  $f(X) \in F[X]$  polinom i neka je  $\alpha$  njegov koren. Tada je  $\alpha$  višestruki koren polinoma  $f(X)$  ako i samo ako je  $\alpha$  zajednički koren polinoma  $f(X)$  i njegovog izvoda  $f'(X)$ , odnosno ako i samo ako važi*

$$f(\alpha) = f'(\alpha) = 0.$$

*Dokaz.* Pretpostavimo najpre da je  $\alpha$  višestruki koren polinoma  $f(X)$ . Tada postoji polinom  $g(X) \in F[X]$  takav da je

$$f(X) = (X - \alpha)^2 g(X).$$

Primenjujući izvod na obe strane jednakosti dobijamo

$$f'(X) = 2(X - \alpha)g(X) + (X - \alpha)^2 g'(X).$$

Uvrštavanjem  $X = \alpha$  sledi  $f'(\alpha) = 0$ , pa je  $\alpha$  koren i polinoma  $f'(X)$ .

Obrnuto, pretpostavimo da je

$$f(\alpha) = f'(\alpha) = 0.$$

Pošto je  $\alpha$  koren polinoma  $f(X)$ , postoji polinom  $g(X) \in F[X]$  takav da je

$$f(X) = (X - \alpha)g(X).$$

Primenom izvoda na jednačinu dobijamo

$$f'(X) = g(X) + (X - \alpha)g'(X).$$

Uvrštavanjem  $X = \alpha$  dobijamo  $f'(\alpha) = g(\alpha)$ . Kako je po pretpostavci  $f'(\alpha) = 0$ , sledi da je  $g(\alpha) = 0$ . Dakle,  $\alpha$  je koren polinoma  $g(X)$ , pa postoji polinom  $h(X) \in F[X]$  takav da je

$$g(X) = (X - \alpha)h(X).$$

Otuda sledi

$$f(X) = (X - \alpha)^2 h(X),$$

što znači da je  $\alpha$  višestruki koren polinoma  $f(X)$ .

□

**Definicija 1.56** Polje  $F$  je **savršeno** ako je svaki nesvodljivi polinom  $f(X) \in F[X]$  separabilan, odnosno ako je svako algebarsko proširenje polja  $F$  separabilno nad  $F$ .

**Tvrđenje 1.57** Polje  $F$  je savršeno ako i samo ako važi jedan od sledećih uslova:

1.  $\text{char}(F) = 0$ ;
2.  $\text{char}(F) = p > 0$  i preslikavanje

$$\varphi : F \longrightarrow F, \quad \varphi(a) = a^p,$$

je surjektivno, tj.  $F = F^p$ .

*Dokaz.* Pretpostavimo najpre da je  $\text{char}(F) = 0$ . Neka je  $f(X) \in F[X]$  nesvodljiv polinom. Kako je karakteristika polja nula, izvod  $f'(X)$  ne može biti jednak nuli. Ako bi  $f(X)$  imao višestruki koren, tada bi  $f(X)$  i  $f'(X)$  imali zajednički nekonstantan delilac. Pošto je  $f(X)$  nesvodljiv, sledilo bi da  $f(X)$  deli  $f'(X)$ , što je nemoguće jer je  $\deg f' < \deg f$ . Dakle, svaki nesvodljiv polinom nad  $F$  je separabilan, pa je svako algebarsko proširenje polja  $F$  separabilno. Prema tome,  $F$  je savršeno.

Pretpostavimo sada da je  $\text{char}(F) = p > 0$  i da je Frobenijusovo preslikavanje

$$\varphi(a) = a^p$$

surjektivno. Neka je  $f(X) \in F[X]$  nesvodljiv polinom. Ako je  $f'(X) \neq 0$ , onda je  $f$  separabilan. Pretpostavimo zato da je  $f'(X) = 0$ . Tada su svi stepeni koji se pojavljuju u polinomu  $f$  deljivi sa  $p$ , pa postoji polinom

$$g(X) = b_0 + b_1 X + \cdots + b_n X^n$$

takav da je

$$f(X) = b_0 + b_1 X^p + \cdots + b_n X^{np} = g(X^p).$$

Kako je Frobenijusovo preslikavanje surjektivno, za svaki koeficijent  $b_i$  postoji  $a_i \in F$  takav da je  $a_i^p = b_i$ . Zato možemo napisati

$$f(X) = a_0^p + a_1^p X^p + \cdots + a_n^p X^{np} = (a_0 + a_1 X + \cdots + a_n X^n)^p.$$

Dakle,  $f(X)$  je  $p$ -ti stepen nekog polinoma iz  $F[X]$ , što je u suprotnosti sa njegovom nesvodljivošću. Prema tome, mora biti  $f'(X) \neq 0$ , pa je svaki nesvodljiv polinom separabilan. Dakle,  $F$  je savršeno.

Obrnuto, pretpostavimo da je  $F$  savršeno i da je  $\text{char}(F) = p > 0$ . Treba pokazati da je Frobenijusovo preslikavanje surjektivno. Neka je  $a \in F$ . Posmatrajmo polinom  $f(X) = X^p - a \in F[X]$ . Neka je  $\alpha$  njegov koren u nekom algebarskom proširenju polja  $F$ . Tada je  $\alpha^p = a$ . Pošto je  $F$  savršeno polje, svaki algebarski element nad  $F$  je separabilan, pa je i  $\alpha$  separabilan nad  $F$ . Zbog toga je njegov minimalni polinom  $p_\alpha(X)$  nad  $F$  separabilan. Kako je  $\alpha$  koren polinoma  $f(X)$ , sledi da  $p_\alpha(X)$  deli  $f(X)$ , odnosno  $p_\alpha(X) \mid X^p - a$ . Izvod polinoma  $f(X)$  je

$$f'(X) = pX^{p-1} = 0,$$

jer je karakteristika polja  $F$  jednaka  $p$ . Dakle, svaki koren polinoma  $f(X) = X^p - a$  je višestruki. Pošto je  $p_\alpha(X)$  nesvodljiv faktor polinoma  $X^p - a$  i istovremeno je separabilan, mora važiti  $\deg p_\alpha(X) = 1$ . Zato je  $p_\alpha(X) = X - \alpha$ , pa sledi da je  $\alpha \in F$ .

Dakle, za svaki  $a \in F$  postoji  $\alpha \in F$  takav da je  $\alpha^p = a$ . To znači da je Frobenijusovo preslikavanje

$$\varphi : F \rightarrow F, \quad \varphi(x) = x^p$$

surjektivno.

□

## Poglavlje 2

# Konstrukcija algebarskog zatvorenja

U nastavku rada koristićemo ideje i rezultate iz [5] i [1], koje ćemo detaljno obrazložiti i razraditi, prilagođavajući ih potrebama i strukturi ovog rada.

**Definicija 2.1** *Polje  $F$  je **algebarski zatvoreno** ako za svako algebarsko proširenje  $K/F$  važi  $F = K$ .*

**Definicija 2.2** *Neka je  $F$  polje. Kažemo da je  $K$  **algebarsko zatvorenje** polja  $F$ , ako je  $K$  algebarsko proširenje polja  $F$  koje je algebarski zatvoreno.*

**Tvrđenje 2.3** *Neka je  $F$  polje. Sledeći uslovi su ekvivalentni:*

1.  $F$  je algebarski zatvoreno polje;
2. svaki polinom  $f(X) \in F[X]$  stepena većeg od 1 ima bar jednu nulu u  $F$ ;
3. svaki nesvodljiv polinom  $f(X) \in F[X]$  je linearan polinom;
4. svaki polinom  $f(X) \in F[X]$  stepena većeg od 1 može se zapisati kao proizvod linearnih faktora.

*Dokaz.* Dokazaćemo da važi niz implikacija

$$(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (1).$$

(1)  $\Rightarrow$  (2).

Pretpostavimo da je  $F$  algebarski zatvoreno polje. Po definiciji,  $F$  je jednako svakom svom algebarskom proširenju. Neka je  $f(X) \in F[X]$  polinom stepena većeg od 1. Neka je  $K$  polje razlaganja polinoma  $f$ . Iz Tvrdjenja 1.46 znamo da ono postoji. Pošto je  $K$  dobijeno dodavanjem korena polinoma  $f$ , kojih ima konačno mnogo, proširenje  $K/F$  je algebarsko. Kako je  $F$  algebarski zatvoreno, sledi da je  $K = F$ . Svi koreni polinoma  $f$  pripadaju polju  $K$ , pa zbog jednakosti  $K = F$  svi koreni pripadaju polju  $F$ . Zbog toga  $f$  ima bar jednu nulu u  $F$ . Dakle, svaki polinom iz  $F[X]$  stepena većeg od 1 ima bar jednu nulu u  $F$ .

(2)  $\Rightarrow$  (3).

Pretpostavimo da svaki polinom iz  $F[X]$  stepena većeg od 1 ima bar jednu nulu u  $F$ . Neka je  $f(X) \in F[X]$  nesvodljiv polinom. Pretpostavimo suprotno da  $f$  nije linearan. Tada je  $\deg f > 1$ . Po pretpostavci,  $f$  ima neku nulu  $\alpha \in F$ . Zato je

$$f(X) = (X - \alpha)g(X)$$

za neki  $g(X) \in F[X]$ . Pošto je  $X - \alpha$  delilac polinoma  $f$ , dobijamo kontradikciju sa činjenicom da je  $f$  nesvodljiv. Prema tome, svaki nesvodljiv polinom mora biti linearan.

(3)  $\Rightarrow$  (4).

Pretpostavimo da je svaki nesvodljiv polinom iz  $F[X]$  linearan. Neka je  $f(X) \in F[X]$  polinom stepena većeg od 1. Svaki polinom se može zapisati kao proizvod nesvodljivih polinoma, pa postoji zapis

$$f(X) = f_1(X)f_2(X) \cdots f_r(X),$$

gde su  $f_1, \dots, f_r$  nesvodljivi polinomi. Po pretpostavci, svaki od polinoma  $f_i$  je linearan, pa važi

$$f_i(X) = a_i(X - \alpha_i),$$

gde je  $\alpha_i \in F$ . Zato je

$$f(X) = a(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_r),$$

gde je  $a \in F$ . Dakle,  $f$  se može zapisati kao proizvod linearnih faktora.

(4)  $\Rightarrow$  (1).

Pretpostavimo da se svaki polinom iz  $F[X]$  stepena većeg od 1 može zapisati kao proizvod linearnih faktora. Neka je  $E/F$  proizvoljno algebarsko proširenje. Pokazaćemo da je  $E = F$ . Neka je  $a \in E$ . Pošto je  $E/F$  algebarsko, element  $a$  je algebarski nad  $F$ , pa postoji njegov minimalni polinom

$$p_a(X) \in F[X].$$

Pretpostavimo da  $a \notin F$ . Tada minimalni polinom  $p_a$  nije linearan, pa je  $\deg p_a > 1$ . Po pretpostavci,  $p_a$  se može zapisati kao proizvod linearnih faktora:

$$p_a(X) = c(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n),$$

gde su  $\alpha_1, \dots, \alpha_n \in F$ . Kako je  $a$  koren polinoma  $p_a$ , sledi da je  $a = \alpha_i$  za neko  $i$ . Ali tada je  $a \in F$ , što je kontradikcija sa pretpostavkom  $a \notin F$ . Dakle, svaki element iz  $E$  pripada polju  $F$ , pa je  $E = F$ . Prema definiciji,  $F$  je algebarski zatvoreno polje.

Time je dokazano da su svi navedeni uslovi ekvivalentni.  $\square$

**Primer 2.4** Polje  $\mathbb{C}$  je algebarski zatvoreno na osnovu fundamentalne teoreme algebre.

Sledeća lema je od posebnog značaja, jer daje dovoljan uslov za algebarsku zatvorenost polja. U njenom dokazu koristićemo svojstva savršenih polja.

**Lema 2.5** Neka je  $L$  algebarsko proširenje polja  $F$ . Ako svaki nekons-tantan polinom iz  $F[X]$  ima koren u  $L$ , tada je  $L$  algebarski zatvoreno.

*Dokaz.* Pretpostavimo najpre da je  $F$  savršeno. Neka je  $f(X) \in F[X]$  moničan i nesvodljiv polinom. Pošto je  $F$  savršeno, polinom  $f(X)$  je separabilan. Neka je  $E$  polje razlaganja polinoma  $f(X)$  nad  $F$ . Tada je  $E/F$  konačno separabilno proširenje, pa prema teoremi o primitivnom elementu (Teorema 1.53) postoji element  $\gamma \in E$  takav da je  $E = F[\gamma]$ . Neka je  $g_\gamma(X) \in F[X]$  minimalni polinom elementa  $\gamma$  nad  $F$ . Po pretpostavci, polinom  $g_\gamma(X)$  ima koren  $\beta \in L$ . Kako su  $\gamma$  i  $\beta$  koreni istog nesvodljivog polinoma  $g_\gamma(X)$ , postoji izomorfizam

$$\Phi : F[\gamma] \longrightarrow F[\beta]$$

takav da je  $\Phi(\gamma) = \beta$  i  $\Phi|_F = \text{id}_F$ . Pošto je  $F[\beta] \subseteq L$ , ovim dobijamo utapanje polja  $E = F[\gamma]$  u  $L$ . Budući da je  $E$  polje razlaganja polinoma

$f(X)$ , postoje  $\alpha_1, \dots, \alpha_n \in E$  takvi da je

$$f(X) = \prod_{i=1}^n (X - \alpha_i).$$

Kako je  $\Phi$  identičko preslikavanje na  $F$ , za svako  $i \in \{1, \dots, n\}$  iz jednakosti  $f(\alpha_i) = 0$  sledi

$$f(\Phi(\alpha_i)) = \Phi(f(\alpha_i)) = \Phi(0) = 0.$$

Pri tome je  $\Phi(\alpha_i) \in L$ . Dakle, svi koreni polinoma  $f(X)$  pripadaju polju  $L$ , pa se  $f(X)$  potpuno razlaže u  $L[X]$ . Time smo pokazali da se svaki nesvodljiv polinom iz  $F[X]$  potpuno razlaže u  $L[X]$ .

Sada ćemo pokazati da je svaki nesvodljiv polinom iz  $L[X]$  linearan. Neka je  $h(X) \in L[X]$  nesvodljiv polinom. Neka je  $\alpha$  koren polinoma  $h(X)$  u nekom algebarskom proširenju  $M$  polja  $L$ . Kako je  $L/F$  algebarsko proširenje, a  $\alpha$  je algebarski nad  $L$ , sledi da je  $\alpha$  algebarski nad  $F$ . Neka je  $g_\alpha(X) \in F[X]$  minimalni polinom elementa  $\alpha$  nad  $F$ . Prema prethodno dokazanom, svaki nesvodljiv polinom iz  $F[X]$  potpuno se razlaže u  $L[X]$ . Kako je  $g_\alpha(X)$  nesvodljiv, on se potpuno razlaže u  $L[X]$ . Pošto je  $\alpha$  koren polinoma  $g_\alpha(X)$ , sledi da je  $\alpha \in L$ . Dakle,  $h(\alpha) = 0$  za neko  $\alpha \in L$ , pa polinom  $X - \alpha$  deli  $h(X)$  u  $L[X]$ . Kako je  $h(X)$  nesvodljiv, sledi da je  $h(X)$  linearan. Prema tome, svaki nesvodljiv polinom iz  $L[X]$  je linearan. Prema tvrdjenju 2.3, zaključujemo da je  $L$  algebarski zatvoreno polje.

Pretpostavimo sada da  $F$  nije savršeno. Tada je  $\text{char}(F) = p > 0$ . Definišimo

$$F' = \{x \in L \mid x^{p^m} \in F \text{ za neko } m \geq 1\}.$$

Pokazaćemo da važe sledeće tvrdnje:

- (a)  $F'$  je polje;
- (b)  $F'$  je savršeno;
- (c) svaki polinom iz  $F'[X]$  ima koren u  $L$ .

Najpre dokazujemo da je  $F'$  polje. Očigledno je  $F' \subseteq L$  i  $F' \neq \emptyset$ , jer je  $1 = 1^p \in F$ . Neka su  $x, y \in F'$ . Tada postoje prirodni brojevi  $m, n \geq 1$  takvi da je  $x^{p^m} \in F$  i  $y^{p^n} \in F$ . Neka je  $k = \max\{m, n\}$ . Tada važi  $x^{p^k} \in F$  i  $y^{p^k} \in F$ . Pošto je karakteristika polja  $L$  jednaka  $p$ , važi

$$(x - y)^{p^k} = x^{p^k} - y^{p^k}.$$

Desna strana ove jednakosti pripada polju  $F$ , pa sledi da i leva strana pripada polju  $F$ . Dakle,

$$(x - y)^{p^k} \in F,$$

odakle dobijamo  $x - y \in F'$ . Zatvorenost za množenje sledi na isti način. Naime,

$$(xy)^{p^k} = x^{p^k} y^{p^k} \in F,$$

pa je  $xy \in F'$ . Ako je  $x \in F'$  i  $x \neq 0$ , postoji  $m \geq 1$  takav da je  $x^{p^m} \in F$ . Kako je  $F$  polje, element  $x^{p^m}$  ima inverz u  $F$ , pa važi

$$(x^{-1})^{p^m} = (x^{p^m})^{-1} \in F.$$

Prema tome,  $x^{-1} \in F'$ . Dakle,  $F'$  je potpolje od  $L$ .

Sada pokazujemo da je  $F'$  savršeno. Neka je  $a \in F'$ . Tada postoji  $m \geq 1$  takav da je  $a^{p^m} = b \in F$ . Posmatrajmo polinom

$$X^{p^{m+1}} - b \in F[X].$$

Po pretpostavci teoreme, ovaj polinom ima koren  $\alpha \in L$ . Zato važi  $\alpha^{p^{m+1}} = b = a^{p^m}$ . Pošto je karakteristika polja  $L$  jednaka  $p$ , dobijamo  $(\alpha^p)^{p^m} = a^{p^m}$ . Frobenijusovo preslikavanje u polju je injektivno, pa sledi  $\alpha^p = a$ . Pošto je  $\alpha^p = a \in F'$ , sledi da je i  $\alpha \in F'$ . Dakle, za svaki element  $a \in F'$  postoji element  $\alpha \in F'$  takav da je  $\alpha^p = a$ . To znači da je Frobenijusovo preslikavanje na  $F'$  surjektivno, pa je prema tvrđenju 1.57  $F'$  savršeno polje.

Sada pokazujemo da svaki polinom iz  $F'[X]$  ima koren u  $L$ . Neka je  $f(X) \in F'[X]$ . Napišimo

$$f(X) = \sum_i a_i X^i,$$

gde je  $a_i \in F'$  za svaki  $i$ . Za svaki koeficijent  $a_i$  postoji prirodan broj  $m_i$  takav da je  $a_i^{p^{m_i}} \in F$ . Neka je

$$m = \max\{m_1, m_2, \dots, m_n\}.$$

Tada za svaki koeficijent važi  $a_i^{p^m} \in F$ , pa polinom

$$g(X) = \sum_i a_i^{p^m} X^i$$

ima koeficijente u  $F$ . Po pretpostavci teoreme, polinom  $g(X)$  ima koren  $\alpha \in L$ . Kako je  $F \subseteq F' \subseteq L$  i  $L/F$  algebarsko proširenje, sledi da

je i  $L/F'$  algebarsko proširenje. Pošto je  $L/F'$  algebarsko proširenje, a pokazali smo da je  $F'$  savršeno polje sledi da je i  $L$  savršeno polje (svaki nesvodljiv polinom u  $L[X]$  deli neki nesvodljiv polinom u  $F'[X]$  koji je separabilan, pa je i svaki nesvodljiv polinom u  $L[X]$  separabilan). Zato postoji  $\beta \in L$  takav da je  $\alpha = \beta^{p^m}$ . Sada imamo

$$(f(\beta))^{p^m} = \left( \sum_i a_i \beta^i \right)^{p^m} = \sum_i a_i^{p^m} \beta^{ip^m} = \sum_i a_i^{p^m} \alpha^i = g(\alpha) = 0.$$

Pošto je  $L$  polje, iz  $p^m$ -tog stepena jednakog nuli sledi da je  $f(\beta) = 0$ . Dakle, svaki polinom iz  $F'[X]$  ima koren u  $L$ . Pošto je  $F'$  savršeno polje i svaki polinom iz  $F'[X]$  ima koren u  $L$ , prema prvom delu dokaza svaki moničan polinom iz  $L[X]$  razlaže se na linearne činioce u  $L[X]$ .

Time je dokazano da je  $L$  algebarski zatvoreno.  $\square$

**Lema 2.6** *Neka je  $K$  proširenje polja  $F$  i neka je*

$$K = F(S),$$

*gde je svaki element skupa  $S$  algebarski nad  $F$ . Tada je  $K$  algebarsko proširenje polja  $F$ .*

*Dokaz.* Neka je  $x \in K$  proizvoljan. Po definiciji polja  $F(S)$ , element  $x$  se može dobiti od elemenata polja  $F$  i konačno mnogo elemenata iz skupa  $S$  primenom konačno mnogo operacija sabiranja, oduzimanja, množenja i deljenja. Dakle, postoje elementi  $\alpha_1, \alpha_2, \dots, \alpha_n \in S$  takvi da  $x \in F(\alpha_1, \alpha_2, \dots, \alpha_n)$ .

Po pretpostavci teoreme svaki  $\alpha_i$  je algebarski nad  $F$ . Posmatrajmo sledeća proširenja

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \dots \subseteq F(\alpha_1, \dots, \alpha_n).$$

Pošto je  $\alpha_1$  algebarski nad  $F$ , proširenje  $F(\alpha_1)/F$  je konačno. Nadalje, pošto je  $\alpha_2$  algebarski nad  $F$ , polinom koji ga anulira ima koeficijente u  $F$ , pa je  $\alpha_2$  koren istog tog polinoma i u većem polju  $F(\alpha_1)$ . Zato je  $\alpha_2$  algebarski nad  $F(\alpha_1)$ , te je proširenje  $F(\alpha_1, \alpha_2)/F(\alpha_1)$  konačno. Induktivno dobijamo da je za svako  $i = 1, \dots, n$

$$F(\alpha_1, \dots, \alpha_i)/F(\alpha_1, \dots, \alpha_{i-1})$$

konačno proširenje. Primenom teoreme o množenju stepena proširenja sledi

$$\prod_{i=1}^n [F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})] < \infty.$$

Dakle,

$$F(\alpha_1, \dots, \alpha_n)/F$$

je konačno proširenje. Kako je svako konačno proširenje algebarsko, zaključujemo da je svaki njegov element algebarski nad  $F$ . Posebno, element  $x$  je algebarski nad  $F$ . Pošto je  $x \in K$  bio proizvoljan, sledi da je svaki element polja  $K$  algebarski nad  $F$ . Prema tome, proširenje  $K/F$  je algebarsko.  $\square$

**Tvrđenje 2.7** *Svako polje ima algebarsko zatvorenje.*

*Dokaz.* Neka je  $F$  polje. Konstruisaćemo algebarsko zatvorenje polja  $F$ , tj. njegovo algebarsko proširenje koje je algebarski zatvoreno. Za njegovu konstrukciju koristićemo prsten polinoma velikog broja promenljivih i odgovarajući količnički prsten po pažljivo odabranom idealu. Na taj način konstruisaćemo proširenje u kome svaki moničan nesvodljiv polinom iz  $F[X]$  ima nulu, što će nas dovesti do algebarskog zatvorenja polja  $F$ .

Posmatrajmo monične nesvodljive polinome  $f \in F[X]$ . Neka su  $X_f$  promenljive, takve da svakom polinomu  $f$  odgovara tačno jedna promenljiva  $X_f$ . Dakle, promenljivih ima onoliko koliko ima nesvodljivih moničnih polinoma i one generišu  $K = F[\dots, X_f, \dots]$ , prsten polinoma nad poljem  $F$ . Elementi ovog prstena su polinomi koji se sastoje iz konačno mnogo promenljivih.

Neka je  $I$  ideal prstena  $K$  generisan polinomima  $f(X_f)$ . Pokazaćemo da je  $I$  pravi ideal. Dovoljno je pokazati da  $1 \notin I$ . Svaki element iz  $I$  može se zapisati u obliku konačne sume  $\sum_{i=1}^n g_i f_i(X_{f_i})$  gde su  $f_1, f_2, \dots, f_n \in F[X]$  monični nesvodljivi polinomi, a  $g_1, g_2, \dots, g_n \in K$ . Pretpostavimo suprotno, da je  $1 \in I$ . Tada postoje monični nesvodljivi polinomi  $f_i \in F[X]$  i elementi  $g_i \in K$  takvi da važi

$$1 = g_1 f_1(X_{f_1}) + g_2 f_2(X_{f_2}) + \dots + g_n f_n(X_{f_n}).$$

Konstruišimo proširenje polja  $F$  koje ćemo označiti sa  $P$ , u kome svaki od polinoma  $f_1, \dots, f_n$  ima nulu  $\alpha_1, \dots, \alpha_n$ . Takvo proširenje postoji i dobijamo ga uzastopnom primenom Kronekerove teoreme na polinome

$f_1, f_2, \dots, f_n$ . Posmatrajmo preslikavanje  $h : K \rightarrow P$  koje je određeno vrednostima  $h(X_{f_i}) = \alpha_i$ , za  $i = 1, \dots, n$ , i  $h(X_f) = 0$  za  $f \notin \{f_1, \dots, f_n\}$ . Drugim rečima, za svaki polinom  $g \in K$ ,  $h(g)$  dobijamo tako što u  $g$  umesto  $X_{f_i}$  uvrstimo  $\alpha_i$ , a umesto svake ostale promenljive  $X_f$  uvrstimo 0. Koeficijenti polinoma su elementi iz  $F$  i oni se slikaju u same sebe. Pošto se pri ovakvom uvrštavanju čuvaju sabiranje i množenje,  $h$  je homomorfizam prstena. Primenjujući homomorfizam  $h$  na gornju jednakost dobićemo:

$$\begin{aligned}
 h(1) &= h(g_1 f_1(X_{f_1}) + g_2 f_2(X_{f_2}) + \dots + g_n f_n(X_{f_n})) \\
 &= h(g_1 f_1(X_{f_1})) + h(g_2 f_2(X_{f_2})) + \dots + h(g_n f_n(X_{f_n})) \\
 &= h(g_1)h(f_1(X_{f_1})) + h(g_2)h(f_2(X_{f_2})) + \dots + h(g_n)h(f_n(X_{f_n})) \\
 &= h(g_1)f_1(h(X_{f_1})) + h(g_2)f_2(h(X_{f_2})) + \dots + h(g_n)f_n(h(X_{f_n})) \\
 &= h(g_1)f_1(\alpha_1) + h(g_2)f_2(\alpha_2) + \dots + h(g_n)f_n(\alpha_n) \\
 &= 0,
 \end{aligned}$$

jer je  $f_i(\alpha_i) = 0$  za svako  $i$ . Sa druge strane, pošto ovaj homomorfizam elemente iz  $F$  slika u same sebe, važi  $h(1) = 1$ . Dobijamo  $1 = 0$ , što je kontradikcija sa činjenicom da u polju važi  $1 \neq 0$ . Prema tome,  $1 \notin I$ , pa je  $I$  pravi ideal.

Posmatrajmo količnički prsten  $K/I$ . U njemu važi  $f(X_f + I) = 0$  za svaki moničan nesvodljiv polinom  $f \in F[X]$ , jer je po konstrukciji  $f(X_f) \in I$ , pa u količniku dobijamo  $f(X_f + I) = 0 + I$ . Dakle, u  $K/I$  svaki moničan nesvodljiv polinom iz  $F[X]$  ima koren (tačnije, element  $X_f + I$  koji ga anulira). Međutim, iz same konstrukcije ne sledi da je  $K/I$  polje, pa ne možemo direktno zaključiti da je ovo algebarsko zatvorenje. Da bismo dobili polje, koristimo Zornovu lemu, koja garantuje da svaki pravi ideal  $I$  u  $K$  leži u nekom maksimalnom idealu  $M$ . Neka je  $M$  maksimalan ideal za koji važi  $I \subseteq M$  i definišimo  $L = K/M$ . Tada je  $L$  polje, jer je prema tvrđenju 1.17 količnik komutativnog prstena po maksimalnom idealu polje.

Postoji prirodan homomorfizam prstena  $F \rightarrow K \rightarrow L$ , pa se  $F$  može identifikovati sa njegovom slikom u  $L$ , odnosno  $L$  je proširenje polja  $F$  (pošto homomorfizmi polja moraju biti injektivni).

Sada posmatramo generatore polja  $L$ . Pošto je  $K$  generisan elementima oblika  $X_f$ , sledi da je i  $L$  generisan elementima oblika  $X_f + M$ , zajedno sa elementima iz  $F$ . Elementi iz  $F$  su trivijalno algebarski nad  $F$ , jer svaki  $a \in F$  zadovoljava linearni polinom  $X - a$ . Za elemente  $X_f + M$ ,

gde je  $f \in F[X]$  moničan i nesvodljiv, važi  $f(X_f + M) = f(X_f) + M$ . Pošto je  $f(X_f) \in I \subseteq M$ , dobijamo  $f(X_f + M) = 0$  u  $L$ , pa je svaki takav element algebarski nad  $F$ . Pošto je  $L$  polje generisano elementima koji su svi algebarski nad  $F$ , iz prethodne leme sledi da je svaki  $x \in L$  algebarski nad  $F$ , pa je  $L/F$  algebarsko proširenje.

Sada pokažimo da je  $L$  algebarski zatvoreno. Neka je  $g \in F[X]$  nekonstantan polinom. Tada se  $g$  može faktorisati na monične nesvodljive faktore  $g = cf_1 \cdots f_n$ , za  $c \in F \setminus \{0\}$ . Pošto svaki  $f_i$  ima koren u  $L$ , postoji element  $\alpha_i \in L$  takav da  $f_i(\alpha_i) = 0$ . Odavde sledi da i  $g$  ima koren u  $L$ . Dakle, svaki nekonstantan polinom iz  $F[X]$  ima nulu u  $L$ , pa je na osnovu leme 2.5  $L$  algebarski zatvoreno polje.

Zaključujemo da je  $L$  algebarsko zatvorenje polja  $F$ .

□

# Zaključak

U ovom radu prikazana je konstrukcija algebarskog zatvorenja proizvoljnog polja. Nakon uvođenja osnovnih pojmova teorije prstena i teorije polja, razmotreni su pojmovi algebarskog i separabilnog proširenja, polja razlaganja i savršenih polja, koji su bili neophodni za razumevanje konstrukcije i dokaza glavnog rezultata.

Centralni deo rada posvećen je dokazu teoreme da svako polje ima algebarsko zatvorenje. Konstrukcija je zasnovana na prstenu polinoma sa velikim brojem promenljivih, pri čemu se svakoj moničnoj nesvodljivoj polinomskoj jednačini pridružuje posebna promenljiva. Formiranjem odgovarajućeg ideala obezbeđuje se da u dobijenom količničkom prstenu svaki od posmatranih polinoma ima koren. Zatim se, primenom Zornove leme, dolazi do maksimalnog ideala, a količnik po tom idealu predstavlja polje koje je algebarsko proširenje polaznog polja. Pokazano je da je tako dobijeno polje algebarski zatvoreno, čime je dokazana egzistencija algebarskog zatvorenja proizvoljnog polja.

Posebna vrednost prikazanog pristupa ogleda se u tome što se konstrukcija može sprovesti bez korišćenja transfinitne indukcije. U odnosu na iterativni pristup, u kojem se koreni polinoma dodaju kroz niz proširenja, ovde se svi monični nesvodljivi polinomi razmatraju istovremeno. Iako je konstrukcija pomoću prstena polinoma tehnički zahtevnija i oslanja se na određene rezultate koji se obrađuju u kasnijim delovima kursa Prsteni, polja i teorija Galoa, ona omogućava da se čitava konstrukcija algebarskog zatvorenja sagleda kroz standardne algebarske objekte. Na taj način uočava se prirodna povezanost između polinoma, ideala, maksimalnih ideala, količničkih prstena i proširenja polja.

# Literatura

- [1] K. Conrad, *Constructing Algebraic Closures*, 2021.
- [2] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed., John Wiley & Sons, 2004.
- [3] M. Z. Grulović, *Predavanja iz Algebre 4*, Departman za matematiku i informatiku, PMF Novi Sad, 2017.
- [4] T. W. Judson, *Abstract Algebra: Theory and Applications*, Orthogonal Publishing L3C, 2020.
- [5] J. S. Milne, *Fields and Galois Theory*, Kea Books, Ann Arbor, MI, 2022.
- [6] S. C. Newman, *A Classical Introduction to Galois Theory*, John Wiley & Sons, Hoboken, NJ, 2012.

## Biografija

Olja Cvetinović rođena je 23. maja 1995. godine u Šapcu. Osnovnu školu „Janko Veselinović” u Šapcu završila je 2009. godine kao nosilac Vukove diplome. Iste godine upisala je Šabačku gimnaziju, koju je završila 2013. godine. Potom je upisala Prirodno-matematički fakultet u Novom Sadu, smer Diplomirani profesor matematike. Osnovne akademske studije završila je u aprilu 2019. godine sa prosečnom ocenom 8,00, a iste godine prešla je na integrisane akademske studije, na studijski program Master profesor matematike. Tokom svog profesionalnog rada stekla je iskustvo u nastavi matematike i informatike. Dve godine radila je kao profesor matematike i informatike u Šabačkoj gimnaziji, dve godine u školi „Foton” u Šapcu, a od septembra 2023. godine zaposlena je u Osnovnoj školi „Nata Jeličić” u Šapcu, gde i danas radi kao nastavnik matematike. Položivši poslednji ispit u oktobru 2024. godine, stekla je uslov za odbranu master rada.

**UNIVERZITET U NOVOM SADU  
PRIRODNO-MATEMATIČKI FAKULTET  
KLJUČNA DOKUMENTACIJSKA  
INFORMACIJA**

Redni broj:

**RBR**

Identifikacioni broj:

**IBR**

Tip dokumentacije: monografska dokumentacija

**TD**

Tip zapisa: tekstualni štampani materijal

**TZ**

Vrsta rada: master rad

**VR**

Autor: Olja Cvetinović

**AU**

Mentor: dr Petar Marković

**MN**

Naslov rada: Konstrukcija algebarskog zatvorenja

**NR**

Jezik publikacije: srpski (latinica)

**JP**

Jezik izvoda: srpski

**JI**

Zemlja publikovanja: Republika Srbija

**ZP**

Uže geografsko područje: Vojvodina

**UGP**

Godina: 2026.

**GO**

Izdavač: autorski reprint

**IZ**

Mesto i adresa: Novi Sad, Prirodno-matematički fakultet, Univerzitet u  
Novom Sadu, Trg Dositeja Obradovića 4

**MA**

Fizički opis rada: 2 poglavlja/39 strana/6 literaturnih citata/0 tabela/0  
slika/0 grafikona/0 priloga

**FO**

Naučna oblast: matematika

**NO**

Naučna disciplina: algebra

**ND**

Predmetna odrednica/Ključne reči: polje, algebarsko proširenje, algebarski zatvoreno polje, algebarsko zatvorenje, polje razlaganja, nesvodljiv polinom, maksimalan ideal

**PO**

UDK

**UDK**

Čuva se: Biblioteka Departmana za matematiku i informatiku, Prirodno-matematički fakultet, Univerzitet u Novom Sadu

**ČU**

Važna napomena:

**VN**

Izvod: U ovom radu prikazan je dokaz poznate teoreme da svako polje ima algebarsko proširenje koje je algebarski zatvoreno. Za razliku od dokaza koji se uobičajeno izučava na studijama, prikazani dokaz ne koristi naprednije metode teorije skupova, kao što je transfinitna indukcija, već se zasniva na Zornovoj lemi. Sa druge strane, u dokazu se koriste rezultati i pojmovi iz teorije polja koji se obrađuju u kasnijim delovima kursa, kao što su savršena polja i teorema o primitivnom elementu. Posebna pažnja posvećena je konstrukciji algebarskog zatvorenja, koja se zasniva na prstenu polinoma sa velikim brojem promenljivih, odgovarajućem idealu i količničkom prstenu.

**IZ**

Datum prihvatanja teme od strane NN veća: 1. septembar 2026.

**DP**

Datum odbrane: 22. septembar 2026.

**DO**

Članovi komisije:

**KO**

Predsednik: dr Boriša Kuzeljević

Član: dr Anna Slivková

Mentor: dr Petar Marković

**UNIVERSITY OF NOVI SAD  
FACULTY OF SCIENCES  
KEY DOCUMENTATION  
INFORMATION**

Accession number:

**RBR**

Identification number:

**IBR**

Type of documentation: monographic publication

**TD**

Type of record: printed textual material

**TZ**

Type of work: master's thesis

**VR**

Author: Olja Cvetinović

**AU**

Supervisor: Dr Petar Marković

**MN**

Title: Construction of an Algebraic closure

**NR**

Language of publication: Serbian (Latin script)

**JP**

Language of abstract: English

**JI**

Country of publication: Republic of Serbia

**ZP**

Narrower geographical area: Vojvodina

**UGP**

Year: 2026.

**GO**

Publisher: author's reprint

**IZ**

Place and address: Novi Sad, Faculty of Sciences, University of Novi Sad,  
Trg Dositeja Obradovića 4

**MA**

Physical description of the thesis: 2 chapters/39 pages/6 bibliographic  
references/0 tables/0 figures/0 graphs/0 appendices

**FO**

Scientific field: mathematics

**NO**

Scientific discipline: algebra

**ND**

Subject headings/Keywords: field, algebraic extension, algebraically closed field, algebraic closure, splitting field, irreducible polynomial, maximal ideal

**PO**

UDC

**UDK**

Kept at: Library of the Department of Mathematics and Informatics, Faculty of Sciences, University of Novi Sad

**ČU**

Important note:

**VN**

Abstract: This thesis presents a proof of the well-known theorem that every field has an algebraic extension that is algebraically closed. Unlike the proof commonly studied in university courses, the proof presented here does not use more advanced methods of set theory, such as transfinite induction, but is instead based on Zorn's lemma. On the other hand, the proof makes use of results and concepts from field theory that are covered in later parts of the course, such as perfect fields and the primitive element theorem. Particular attention is devoted to the construction of an algebraic closure, which is based on a polynomial ring in a large number of variables, the corresponding ideal, and the quotient ring.

**IZ**

Date of acceptance of the thesis topic by the Faculty Council: 1 September 2026.

**DP**

Date of defense: 22 September 2026.

**DO**

Members of the committee:

**KO**

Chair: Dr Boriša Kuzeljević

Member: Dr Anna Slivková

Supervisor: Dr Petar Marković