

# Konstruktibilni brojevi

---

Živković, Paula

Master's thesis / Diplomski rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:217:352976>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-07-22**



Repository / Repozitorij:

[Repository of the Faculty of Science - University of Zagreb](#)



**SVEUČILIŠTE U ZAGREBU**  
**PRIRODOSLOVNO–MATEMATIČKI FAKULTET**  
**MATEMATIČKI ODSJEK**

Paula Živković

**KONSTRUKTIBILNI BROJEVI**

Diplomski rad

Voditelj rada:  
Izv. prof. dr. sc. Zvonko Iljazović

Zagreb, studeni, 2019.

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

1. \_\_\_\_\_, predsjednik
2. \_\_\_\_\_, član
3. \_\_\_\_\_, član

Povjerenstvo je rad ocijenilo ocjenom \_\_\_\_\_.

Potpisi članova povjerenstva:

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_

*Zahvaljujem svojim roditeljima, obitelji, prijateljima i mentoru  
na pomoći i podršci*

# Sadržaj

<b>Sadržaj</b>	<b>iv</b>
<b>Uvod</b>	<b>1</b>
<b>1 Konstruktibilne točke</b>	<b>3</b>
1.1 Pravci i kružnice . . . . .	3
1.2 Određenost točke skupom . . . . .	5
1.3 Konstruktibilnost točke iz skupa . . . . .	10
<b>2 Kvadratni radikali</b>	<b>15</b>
2.1 Grupe, prsteni i polja . . . . .	15
2.2 Prsten $B[x_0]$ . . . . .	21
2.3 Kvadratni radikali . . . . .	29
<b>3 Algebarska svojstva konstruktibilnih brojeva</b>	<b>35</b>
3.1 Jednadžba pravca i kvadratni radikali . . . . .	35
3.2 Konstruktibilni brojevi i kvadratni radikali . . . . .	41
3.3 Polinomi . . . . .	46
3.4 Polinomi i kvadratni radikali . . . . .	52
3.5 Problem duplikacije kocke . . . . .	57
<b>4 Karakterizacija konstruktibilnih brojeva</b>	<b>59</b>
4.1 Točke s konstruktibilnim koordinatama . . . . .	59
4.2 Zbroj, produkt i kvocijent konstruktibilnih brojeva . . . . .	71
4.3 Karakterizacija konstruktibilnih brojeva . . . . .	74
<b>Bibliografija</b>	<b>77</b>

# Uvod

U ovom diplomskom radu bavimo se problemom konstruktibilnosti točaka i brojeva.

U prvom poglavlju proučavamo pravce i kružnice te određenost točaka danim skupom. Nadalje, definiramo kada za neku točku kažemo da se može konstruirati iz danog skupa.

U drugom poglavlju uvodimo pojam kvadratnog radikala i proučavamo svojstva kvadratnih radikala. U tu svrhu promatramo grupe, prstene i polja te proširenja prstena jednim elementom.

U trećem poglavlju dokazujemo da je svaki konstruktibilan broj kvadratni radikal. Nadalje, dajemo kriterij da polinom trećeg stupnja s racionalnim koeficijentima nema rješenje koje je kvadratni radikal. Koristeći navedeni kriterij dajemo negativan odgovor na klasični problem duplikacije kocke.

U posljednjem poglavlju pomoću točaka s konstruktibilnim koordinatama proučavamo zbroj, produkt i kvocijent konstruktibilnih brojeva. Potom dokazujemo da je svaki kvadratni radikal konstruktibilan broj.



# Poglavlje 1

## Konstruktibilne točke

### 1.1 Pravci i kružnice

**Definicija 1.1.1.** Neka je  $p \subseteq \mathbb{R}^2$ . Za  $p$  kažemo da je pravac ako postoje  $T_0 \in \mathbb{R}^2$  i  $v \in \mathbb{R}^2, v \neq (0,0)$  takvi da je  $p = \{T_0 + t \cdot v \mid t \in \mathbb{R}\}$ .

**Lema 1.1.2.** Neka su  $T_0, v \in \mathbb{R}^2, v \neq (0,0)$  te neka je  $p = \{T_0 + t \cdot v \mid t \in \mathbb{R}\}$ . Neka je  $T_1 \in p$ . Tada je  $p = \{T_1 + s \cdot v \mid s \in \mathbb{R}\}$ .

*Dokaz.* Iz  $T_1 \in p$  slijedi da postoji  $t_1 \in \mathbb{R}$  takav da je

$$T_1 = T_0 + t_1 \cdot v. \quad (*)$$

Neka je  $T \in p$ . Tada postoji  $t \in \mathbb{R}$  takav da je  $T = T_0 + t \cdot v$ . Želimo dokazati da postoji  $s \in \mathbb{R}$  takav da je  $T = T_1 + s \cdot v$ . Prema (\*) vrijedi

$$T_0 = T_1 - t_1 \cdot v.$$

Imamo

$$T = T_0 + t \cdot v = (T_1 - t_1 \cdot v) + t \cdot v = T_1 + (t - t_1) \cdot v.$$

Dakle,

$$T = T_1 + (t - t_1) \cdot v,$$

iz čega slijedi da postoji  $s \in \mathbb{R}$  takav da je  $T = T_1 + s \cdot v$ . Dakle,  $T \in \{T_1 + s \cdot v \mid s \in \mathbb{R}\}$ .

Obratno, neka je  $T \in \{T_1 + s \cdot v \mid s \in \mathbb{R}\}$ . Tada postoji  $s \in \mathbb{R}$  takav da je  $T = T_1 + s \cdot v$ . Koristeći (\*) dobivamo da je

$$T = (T_0 + t_1 \cdot v) + s \cdot v = T_0 + (t_1 + s) \cdot v$$



iz čega slijedi da postoji  $t \in \mathbb{R}$  takav da je  $T = T_0 + t \cdot v$ . Prema tome  $T \in p$ . Time je lema dokazana. □

**Lema 1.1.3.** *Neka su  $T_0, v \in \mathbb{R}^2, v \neq (0, 0)$  te neka je  $p = \{T_0 + t \cdot v \mid t \in \mathbb{R}\}$ . Neka je  $\lambda \in \mathbb{R}, \lambda \neq 0$  te neka je  $w = \lambda \cdot v$ . Tada je*

$$p = \{T_0 + s \cdot w \mid s \in \mathbb{R}\}.$$

*Dokaz.* Neka je  $T \in p$ . Tada je  $T = T_0 + t \cdot v$ , za neki  $t \in \mathbb{R}$ . Kako je  $w = \lambda \cdot v$ , slijedi da je  $v = \frac{1}{\lambda} \cdot w$ . Stoga je

$$T = T_0 + t \cdot \left(\frac{1}{\lambda} \cdot w\right) = T_0 + \left(t \cdot \frac{1}{\lambda}\right) \cdot w,$$

iz čega slijedi  $T \in \{T_0 + s \cdot w \mid w \in \mathbb{R}\}$ .

Obratno, neka je  $T \in \{T_0 + s \cdot w \mid s \in \mathbb{R}\}$ . Tada je  $T = T_0 + s \cdot w$ , za neki  $s \in \mathbb{R}$ . Iz  $w = \lambda \cdot v$  slijedi da je

$$T = T_0 + s \cdot (\lambda \cdot v) = T_0 + (s \cdot \lambda) \cdot v.$$

Slijedi da je  $T \in p$ , čime je lema dokazana. □

**Propozicija 1.1.4.** *Neka su  $A, B \in \mathbb{R}^2$  takvi da  $A \neq B$ . Tada postoji jedinstveni pravac  $p$  takav da su  $A, B \in p$ .*

*Dokaz.* Neka je  $v = B - A$ . Očito je  $v \neq (0, 0)$ . Definirajmo  $p = \{A + t \cdot v \mid t \in \mathbb{R}\}$ . Očito je  $p$  pravac. Vrijedi  $A = A + 0 \cdot v$  pa je  $A \in p$ .

Iz

$$B = A + (B - A) = A + 1 \cdot v$$

slijedi  $B \in p$ . Dakle,  $p$  je pravac takav da su  $A, B \in p$ . Neka je  $q$  pravac takav da vrijedi  $A, B \in q$ . Dokažimo da je  $p = q$ .

Budući da je  $q$  pravac, postoje  $T_0, w \in \mathbb{R}^2, w \neq (0, 0)$  takvi da je  $q = \{T_0 + t \cdot w \mid t \in \mathbb{R}\}$ . Iz  $A \in q$  i leme 1.1.2 slijedi

$$q = \{A + t \cdot w \mid t \in \mathbb{R}\}. \quad (\Delta)$$

Kako je  $B \in q$  slijedi da je  $B = A + t \cdot w$ , za neki  $t \in \mathbb{R}$ . Uočimo da je  $t \neq 0$  (u suprotnom bi slijedilo da je  $B = A$ , što je u suprotnosti s pretpostavkom propozicije). Slijedi  $B - A = t \cdot w$  tj.  $v = t \cdot w$ . Vrijedi  $w = \frac{1}{t} \cdot v$ .

Zbog leme 1.1.3 vrijedi  $p = \{A + s \cdot w \mid s \in \mathbb{R}\}$ . Iz ovoga i  $(\Delta)$  slijedi  $p = q$ .

Time je tvrdnja propozicije dokazana. □

**Definicija 1.1.5.** Za  $A, B \in \mathbb{R}^2$ ,  $A \neq B$ , prema propoziciji 1.1.4 postoji jedinstveni pravac  $p$  takav da  $A, B \in p$ . Taj pravac označavamo s  $AB$ .

**Napomena 1.1.6.** Prema dokazu propozicije 1.1.4 slijedi  $AB = \{A + t \cdot (B - A) \mid t \in \mathbb{R}\}$ .

**Napomena 1.1.7.** Neka su  $p$  i  $q$  pravci takvi da je  $p \neq q$  i  $p \cap q \neq \emptyset$ . Tada je  $p \cap q$  jednočlan skup.

*Naime, pretpostavimo da postoje  $A, B \in p \cap q$  takvi da je  $A \neq B$ . Slijedi  $A, B \in p$  i  $A, B \in q$ , što je nemoguće prema propoziciji 1.1.4 jer je  $p \neq q$ . Stoga je  $p \cap q$  jednočlan skup.*

**Definicija 1.1.8.** Za  $A, B \in \mathbb{R}^2$ ,  $A = (a_1, a_2)$ ,  $B = (b_1, b_2)$  definiramo

$$d(A, B) = \sqrt{(b_1 - a_1)^2 + (b_2 - a_2)^2}.$$

Za  $d(A, B)$  kažemo da je udaljenost točaka  $A$  i  $B$ .

**Definicija 1.1.9.** Neka su  $T_0 \in \mathbb{R}^2$  i  $r \in \mathbb{R}$ ,  $r > 0$ . Definiramo skup

$$K(T_0, r) = \{T \in \mathbb{R}^2 \mid d(T_0, T) = r\}.$$

Za  $K(T_0, r)$  kažemo da je kružnica sa središtem u točki  $T_0$  radijusa  $r$ .

## 1.2 Određenost točke skupom

**Definicija 1.2.1.** Neka je  $S \subseteq \mathbb{R}^2$  i neka je  $p$  pravac. Kažemo da je  $p$  pravac određen skupom  $S$  ako postoje  $A, B \in S$ ,  $A \neq B$ , takvi da je  $p = AB$ .

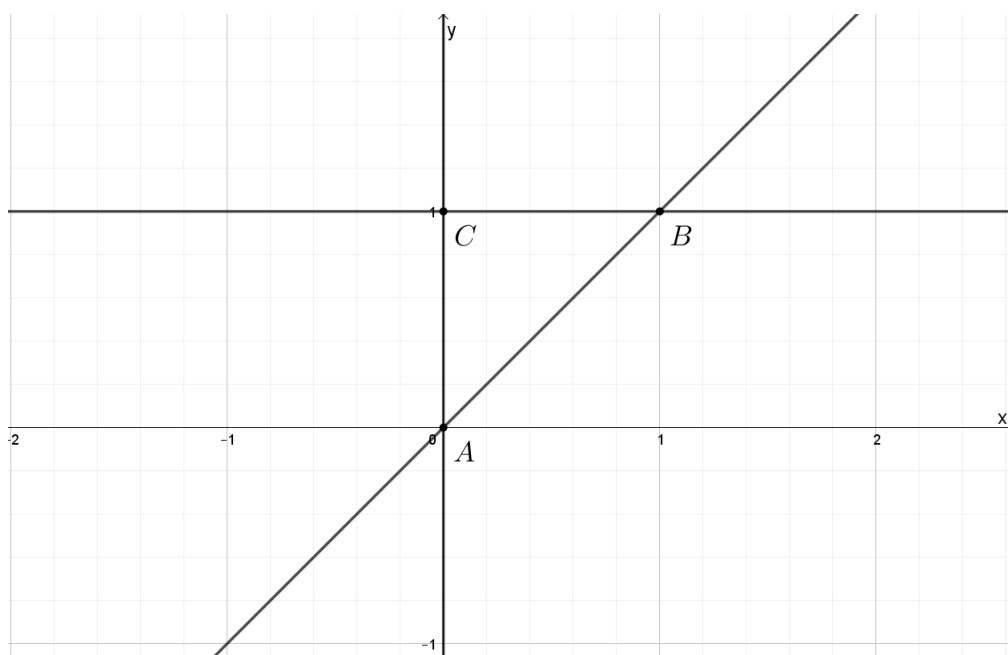
**Primjer 1.2.2.** Neka je  $S = \{A, B, C\} \subseteq \mathbb{R}^2$  gdje su  $A = (0, 0)$ ,  $B = (1, 1)$ ,  $C = (0, 1)$ . Tada su  $AB$ ,  $BC$  i  $AC$  svi pravci određeni skupom  $S$ . Prema napomeni 1.1.6 vrijedi

$$AC = \{A + t \cdot (C - A) \mid t \in \mathbb{R}\} = \{(0, 0) + t \cdot (0, 1) \mid t \in \mathbb{R}\} = \{(0, t) \mid t \in \mathbb{R}\}.$$

Iz ovoga je očito da  $B \notin AC$ . No,  $B \in AB$  pa zaključujemo  $AB \neq AC$ . Također,  $BC \neq AC$ . Vrijedi

$$AB = \{A + t \cdot (B - A) \mid t \in \mathbb{R}\} = \{(0, 0) + t \cdot (1, 1) \mid t \in \mathbb{R}\} = \{(t, t) \mid t \in \mathbb{R}\}$$

pa je očito da  $C \notin AB$  odnosno  $BC \neq AB$ .

Slika 1.1: Pravci određeni skupom  $S$ 

**Definicija 1.2.3.** Neka je  $S \subseteq \mathbb{R}^2$  i neka je  $k$  kružnica. Kažemo da je  $k$  kružnica određena skupom  $S$  ako postoje  $A, B \in S, A \neq B$  takvi da je  $k = K(A, d(A, B))$ .

**Primjer 1.2.4.** Neka je  $S = \{A, B, C\} \subseteq \mathbb{R}^2$ , gdje su  $A = (0, 0), B = (1, 1), C = (0, 1)$ . Tada su

$$K(A, d(A, C)) = K(A, 1),$$

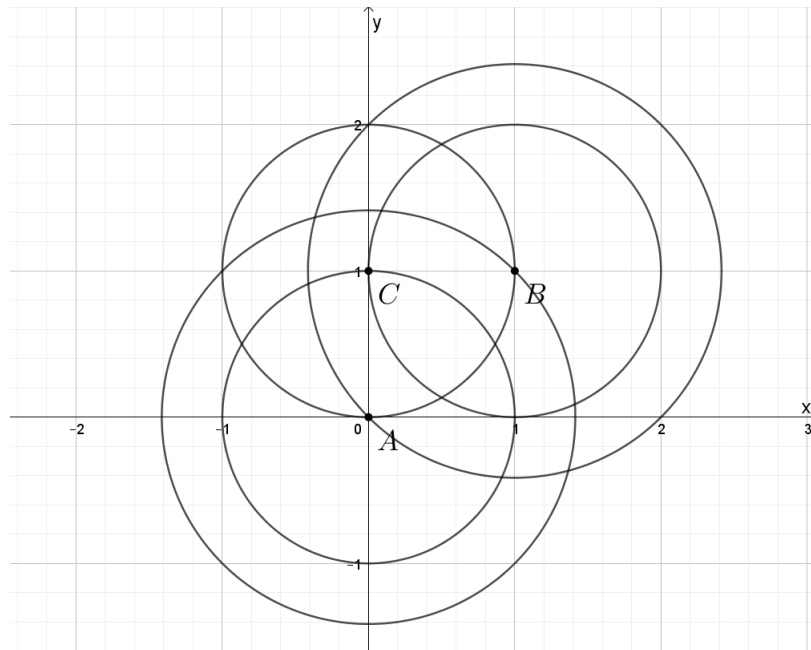
$$K(A, d(A, B)) = K(A, \sqrt{2}),$$

$$K(B, d(B, C)) = K(B, 1),$$

$$K(B, d(B, A)) = K(B, \sqrt{2}),$$

$$K(C, d(C, A)) = K(C, 1) = K(C, d(C, B)),$$

sve kružnice određene skupom  $S$ .

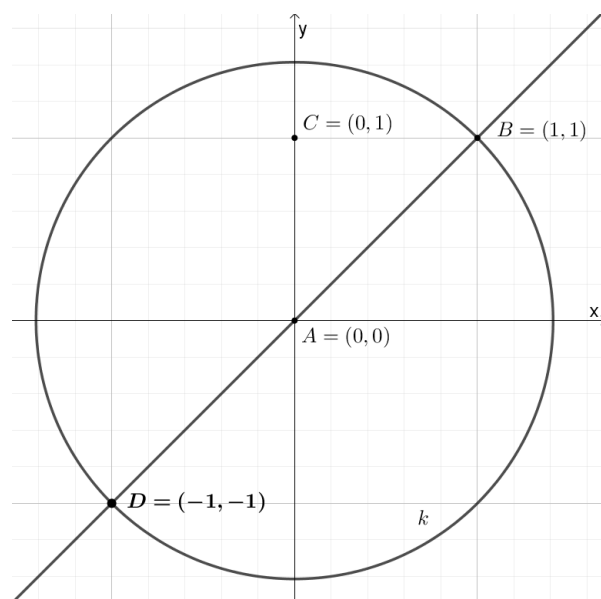
Slika 1.2: Kružnice određene skupom  $S$ 

**Definicija 1.2.5.** Neka je  $S \subseteq \mathbb{R}^2$  te neka je  $T \in \mathbb{R}^2$ . Kažemo da je  $T$  točka određena skupom  $S$  ako vrijedi jedno od sljedećeg:

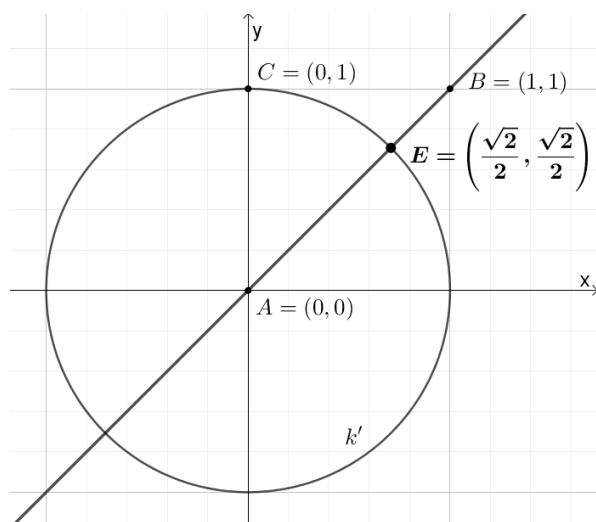
1. Postoje pravci  $p_1$  i  $p_2$  određeni skupom  $S$  takvi da je  $p_1 \neq p_2$  i  $T \in p_1 \cap p_2$ .
2. Postoji pravac  $p$  određen skupom  $S$  te postoji kružnica  $k$  određena skupom  $S$  tako da je  $T \in p \cap k$ .
3. Postoje kružnice  $k_1$  i  $k_2$  određene skupom  $S$  takve da  $k_1 \neq k_2$  i  $T \in k_1 \cap k_2$ .

**Primjer 1.2.6.** Neka je  $S = \{A, B, C\} \subseteq \mathbb{R}^2$ , gdje su  $A = (0, 0)$ ,  $B = (1, 1)$ ,  $C = (0, 1)$ .

1. Imamo  $A \in AB \cap AC$  i  $AB \neq AC$  (prema primjeru 1.2.2). Stoga je  $A$  točka određena skupom  $S$  (prema definiciji 1.2.5). Analogno zaključujemo da su točke  $B$  i  $C$  određene skupom  $S$ .
2. Neka je  $k = K(A, d(A, B))$ . Očito je  $k$  kružnica određena skupom  $S$ . Vrijedi  $d(A, B) = \sqrt{2}$ . Dakle,  $k = K(A, \sqrt{2})$ . Neka je  $D = (-1, -1)$ . Vrijedi  $d(A, D) = \sqrt{2}$  pa je  $D \in k$ . Prema primjeru 1.2.2 vrijedi  $AB = \{(t, t) \mid t \in \mathbb{R}\}$ . Stoga je  $D \in AB$ . Dakle,  $D \in k \cap AB$  pa slijedi da je  $D$  točka određena skupom  $S$ .

Slika 1.3: Točka  $D$  je određena skupom  $S$ 

3. Kružnica  $k' = K(A, d(A, C))$  također je određena skupom  $S$ .  
 Vrijedi da je  $d(A, C) = 1$ . Dakle,  $k' = K(A, 1)$ . Neka je  $E = \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)$ . Vrijedi  $d(A, E) = 1$  pa je  $E \in k'$ . Očito je  $E \in AB$ . Dakle,  $E \in k' \cap AB$  pa slijedi da je  $E$  točka određena skupom  $S$ .

Slika 1.4: Točka  $E$  je određena skupom  $S$

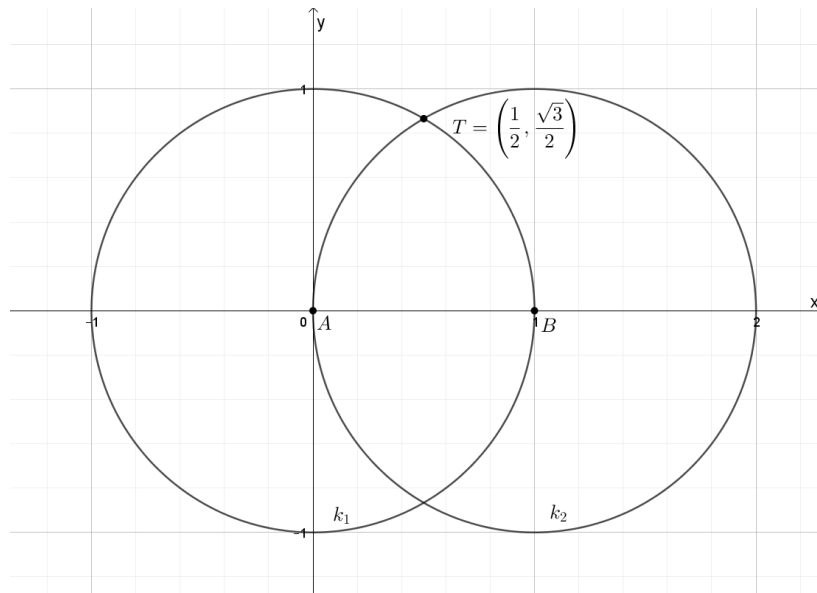
**Primjer 1.2.7.** Neka su  $A = (0, 0)$  i  $B = (1, 0)$  te neka je  $S = \{A, B\}$ .

Neka je  $k_1 = K(A, d(A, B))$  i  $k_2 = K(B, d(A, B))$ . Prema definiciji 1.2.3 te kružnice određene su skupom  $S$ . Vrijedi  $d(A, B) = 1$ . Neka je  $T = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ .

Vrijedi

$$d(A, T) = \sqrt{\frac{1}{4} + \frac{3}{4}} = 1 \quad \text{i} \quad d(B, T) = \sqrt{\frac{1}{4} + \frac{3}{4}} = 1$$

tj.  $T \in K(A, 1)$  i  $T \in K(B, 1)$ . Dakle,  $T \in k_1$  i  $T \in k_2$  pa je  $T \in k_1 \cap k_2$ . Očito je  $k_1 \neq k_2$ . Prema tome,  $T$  je točka određena skupom  $S$ .



Slika 1.5: Točka  $T$  je određena skupom  $S$

**Napomena 1.2.8.** Neka je  $S \subseteq \mathbb{R}^2$  takav da  $S$  ima barem 2 točke. Tada je svaka točka skupa  $S$  određena skupom  $S$ . Naime, neka je  $A \in S$ . Odaberimo neki  $B \in S, B \neq A$ . Prema definiciji 1.2.3 vrijedi da je  $K(B, d(A, B))$  kružnica određena skupom  $S$ , a očito je  $A \in K(B, d(A, B))$ . Nadalje,  $AB$  je pravac određen skupom  $S$  i vrijedi  $A \in AB$ . Dakle,  $A \in K(B, d(A, B)) \cap AB$  pa zaključujemo da je  $A$  točka određena skupom  $S$ .

**Napomena 1.2.9.** Ako je  $S \subseteq \mathbb{R}^2$  jednočlan skup ili  $S = \emptyset$ , onda ne postoji točka određena skupom  $S$ . Naime, za takav skup  $S$  vrijedi da ne postoje pravci i kružnice određene skupom  $S$ .

**Napomena 1.2.10.** Neka su  $T$  i  $S$  podskupovi od  $\mathbb{R}^2$  takvi da je  $T \subseteq S$ . Pretpostavimo da je  $p$  pravac određen skupom  $T$ . Tada postoje  $A, B \in T, A \neq B, p = AB$ . Zbog  $T \subseteq S$  imamo  $A, B \in S$  pa zaključujemo da je pravac  $p$  određen skupom  $S$ . Dakle, svaki pravac određen skupom  $T$  određen je i skupom  $S$ . Pretpostavimo da je  $k$  kružnica određena skupom  $T$ . Tada postoje  $A, B \in T, A \neq B$ , takvi da je  $k = K(A, d(A, B))$ . Kako je  $T \subseteq S$  vrijedi  $A, B \in S$  pa zaključujemo da je kružnica  $k$  određena skupom  $S$ . Dakle, svaka kružnica određena skupom  $T$  određena je i skupom  $S$ . Slijedi da je svaka točka određena skupom  $T$  određena i skupom  $S$ .

### 1.3 Konstruktibilnost točke iz skupa

**Definicija 1.3.1.** Neka je  $S \subseteq \mathbb{R}^2$ . Definiamo skupove  $S^{(n)}, n \in \mathbb{N}_0$  induktivno na sljedeći način.

Neka je  $S^{(0)} = S$ .

Pretpostavimo da smo definirali  $S^{(n)}$  za neki  $n \in \mathbb{N}_0$ .

Definiramo  $S^{(n+1)} = \{A \in \mathbb{R}^2 \mid A \text{ određena skupom } S^{(n)}\}$ .

**Definicija 1.3.2.** Neka je  $S \subseteq \mathbb{R}^2$  te neka je  $A \in \mathbb{R}^2$ . Kažemo da se točka  $A$  može konstruirati iz skupa  $S$  ako postoji  $n \in \mathbb{N}$  takav da je  $A \in S^{(n)}$ .

**Napomena 1.3.3.** Neka je  $S \subseteq \mathbb{R}^2$  i pretpostavimo da  $S$  ima barem dva elementa. Dokažimo indukcijom da za svaki  $n \in \mathbb{N}_0$  vrijedi sljedeće:  $S^{(n)}$  ima barem dva elementa i  $S^{(n)} \subseteq S^{(n+1)}$ .

Za  $n = 0$  tvrdnja vrijedi jer je  $S^{(0)} = S$  pa iz napomene 1.2.8 slijedi da je svaka točka iz  $S^{(0)}$  određena skupom  $S^{(0)}$ , dakle  $S^{(0)} \subseteq S^{(1)}$ .

Pretpostavimo da tvrdnja vrijedi za neki  $n \in \mathbb{N}_0$ . Dakle,  $S^{(n)}$  ima barem dva elementa i vrijedi  $S^{(n)} \subseteq S^{(n+1)}$ . Iz toga slijedi da  $S^{(n+1)}$  ima barem dva elementa pa prema napomeni 1.2.8 slijedi  $S^{(n+1)} \subseteq S^{(n+2)}$ .

Time smo dokazali da tvrdnja vrijedi za svaki  $n \in \mathbb{N}_0$ .

**Primjer 1.3.4.** Neka je  $S = \{A, B\}$ , gdje je  $A = (0, 0), B = (1, 0)$ . Neka je  $P = (\frac{1}{2}, 0)$ . Tvrdimo da se točka  $P$  može konstruirati iz skupa  $S$ .

Neka je  $T_1 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$  i  $T_2 = (\frac{1}{2}, -\frac{\sqrt{3}}{2})$ . U primjeru 1.2.7 smo vidjeli da je  $T_1$  točka određena skupom  $S$ , a na isti način možemo zaključiti da je  $T_2$  točka određena skupom  $S$ . Prema napomeni 1.2.8 točke  $A$  i  $B$  su određene skupom  $S$ . Budući da je  $S^{(1)}$  skup svih točaka određenih skupom  $S^{(0)} = S$ , slijedi da su  $A, B, T_1, T_2 \in S^{(1)}$ . Promotrimo pravce  $AB$  i  $T_1T_2$ . Znamo da je  $AB = \{A + t \cdot (B - A) \mid t \in \mathbb{R}\}$  odnosno

$$AB = \{(t, 0) \mid t \in \mathbb{R}\} \quad (\star)$$

Nadalje,

$$T_1T_2 = \{T_1 + t \cdot (T_2 - T_1) \mid t \in \mathbb{R}\}$$

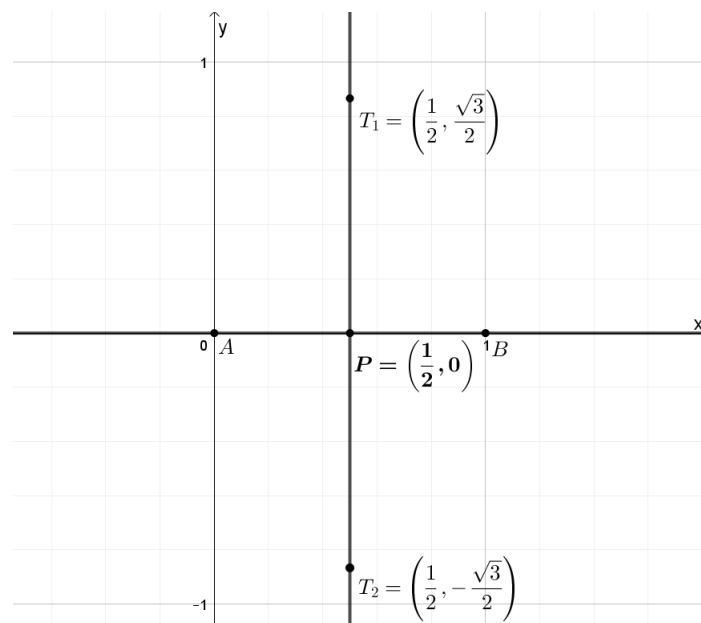
tj.

$$T_1T_2 = \left\{ \left( \frac{1}{2}, \frac{\sqrt{3}}{2} - t \cdot \sqrt{3} \right) \mid t \in \mathbb{R} \right\}. \quad (\star\star)$$

Očito je da  $A \notin T_1T_2$  pa slijedi  $AB \neq T_1T_2$ .

Iz  $(\star)$  slijedi da je  $P \in AB$  (za  $t = \frac{1}{2}$ ), a iz  $(\star\star)$  slijedi da je  $P \in T_1T_2$  (za  $t = \frac{1}{2}$ ).

Dakle,  $P \in AB \cap T_1T_2$ , a pravci  $AB$  i  $T_1T_2$  su određeni skupom  $S^{(1)}$  i međusobno su različiti pa zaključujemo da je  $P$  točka određena skupom  $S^{(1)}$ . Slijedi  $P \in S^{(2)}$ . Time smo dokazali da se točka  $P$  može konstruirati iz skupa  $S$ .



Slika 1.6: Konstrukcija točke  $P$  iz skupa  $S$

**Napomena 1.3.5.** Neka je  $S \subseteq \mathbb{R}^2$  skup koji ima barem dvije točke. Tada se svaka točka  $A \in S$  može konstruirati iz  $S$ . Naime, neka je  $A \in S$ . Znamo da je  $S^{(0)} = S$ , a iz toga slijedi da  $S^{(0)}$  ima barem dvije točke te da je  $A \in S^{(0)}$ . Iz napomene 1.2.8 zaključujemo da je  $A$  točka određena skupom  $S^{(0)}$ . Dakle,  $A \in S^{(1)}$ . Prema tome postoji  $n \in \mathbb{N}$  takav da je  $A \in S^{(n)}$ , što znači da se  $A$  može konstruirati iz skupa  $S$ .



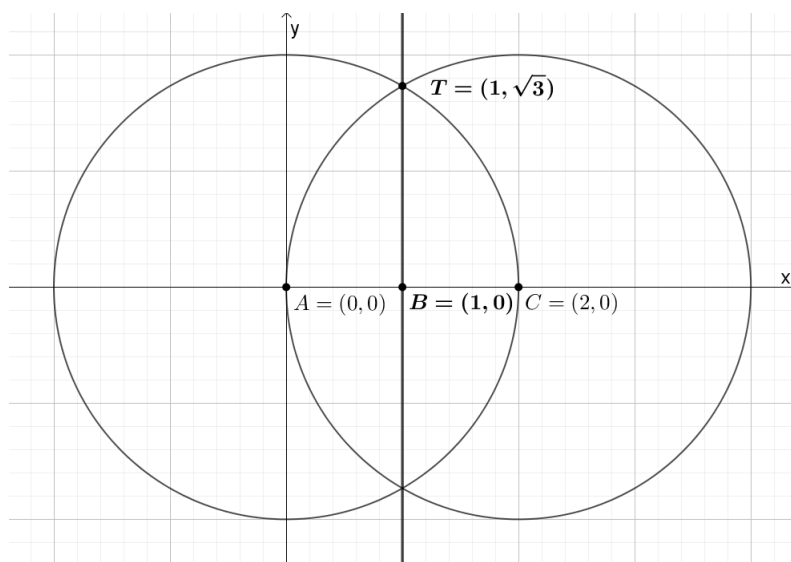
**Napomena 1.3.6.** Neka je  $A \in \mathbb{R}^2$  te neka je  $S = \{A\}$ . Tada ne postoji točka koja se može konstruirati iz skupa  $S$ . Naime, iz  $S^{(0)} = S$  slijedi da je  $S^{(0)}$  jednočlan skup, pa prema napomeni 1.2.9 slijedi da ne postoji točka određena skupom  $S^{(0)}$ . Stoga je  $S^{(1)} = \emptyset$ . Indukcijom, koristeći napomenu 1.2.9, dobivamo da je  $S^{(n)} = \emptyset$ , za svaki  $n \in \mathbb{N}$ . Dakle, ne postoji točka koja se može konstruirati iz skupa  $S$ .

**Definicija 1.3.7.** Neka je  $T \in \mathbb{R}^2$ . Kažemo da je  $T$  konstruktibilna točka ako se  $T$  može konstruirati iz skupa  $\{(0, 0), (1, 0)\}$ .

Iz napomene 1.3.5 slijedi da su točke  $(0, 0)$  i  $(1, 0)$  konstruktibilne. Prema primjeru 1.3.4 točka  $(\frac{1}{2}, 0)$  je konstruktibilna.

**Primjer 1.3.8.** Neka su  $A = (0, 0)$  i  $B = (1, 0)$ . Neka je  $S = \{A, B\}$ . Neka je  $C = (2, 0)$ . Vrijedi  $AB = \{(t, 0) \mid t \in \mathbb{R}\}$  pa je očito  $C \in AB$ . Nadalje, vrijedi  $d(C, B) = 1$  pa je očito  $C \in K(B, 1)$ . Stoga je  $C \in AB \cap K(B, 1)$ . Budući da je  $AB$  pravac određen skupom  $S$  te da je  $K(B, 1)$  kružnica određena skupom  $S$ , slijedi da je  $C$  točka određena skupom  $S$ . Dakle,  $C \in S^{(1)}$ . Uočimo da su  $A, C \in S^{(1)}$  te da je  $d(A, C) = 2$ . Stoga su  $K(A, 2)$  i  $K(C, 2)$  kružnice određene skupom  $S^{(1)}$ .

Neka je  $T = (1, \sqrt{3})$ . Vrijedi  $d(T, A) = 2$  i  $d(T, C) = 2$ , stoga je  $T \in K(A, 2) \cap K(C, 2)$ . Prema tome, točka  $T$  je određena skupom  $S^{(1)}$  tj.  $T \in S^{(2)}$ . Prema napomeni 1.3.3 vrijedi  $B \in S^{(2)}$ . Stoga je  $BT$  pravac određen skupom  $S^{(2)}$ .



Slika 1.7: Pravac  $BT$  je određen skupom  $S^{(2)}$

Vrijedi

$$BT = \{B + t \cdot (T - B) \mid t \in \mathbb{R}\} = \{(1, 0) + t \cdot (0, \sqrt{3}) \mid t \in \mathbb{R}\} = \{(1, t \cdot \sqrt{3}) \mid t \in \mathbb{R}\}.$$

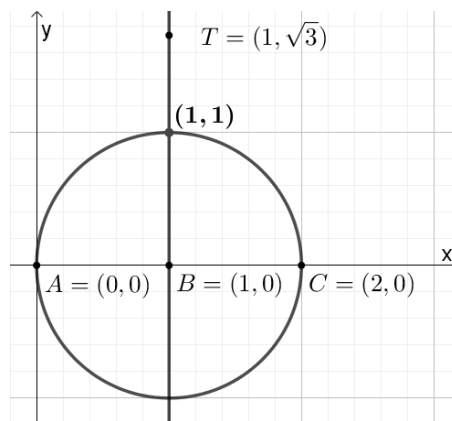
Uočimo da za  $t = \frac{1}{\sqrt{3}}$  vrijedi

$$(1, t \cdot \sqrt{3}) = (1, 1).$$

Dakle,  $(1, 1) \in BT$ . Vrijedi  $d((1, 1), B) = 1$  pa je  $(1, 1) \in K(B, d(A, B))$ . Dakle,

$$(1, 1) \in BT \cap K(B, d(A, B)). \quad (\diamond)$$

Prema napomeni 1.3.3 slijedi da su  $A, B \in S^{(2)}$ . Stoga je kružnica  $K(B, d(A, B))$  određena skupom  $S^{(2)}$ . Iz  $(\diamond)$  slijedi da je točka  $(1, 1)$  određena skupom  $S^{(2)}$ . Prema tome,  $(1, 1) \in S^{(3)}$ . Zaključujemo da se točka  $(1, 1)$  može konstruirati iz skupa  $S$ , što znači da je  $(1, 1)$  konstruktibilna točka.



Slika 1.8: Točka  $(1, 1)$  je konstruktibilna točka

**Definicija 1.3.9.** Neka je  $x \in \mathbb{R}$ . Kažemo da je  $x$  konstruktibilan broj ako postoje konstruktibilna točka  $T \in \mathbb{R}^2$  i  $a \in \mathbb{R}$  takvi da je  $T = (a, x)$  ili  $T = (x, a)$ .



## Poglavlje 2

# Kvadratni radikali

### 2.1 Grupe, prsteni i polja

**Definicija 2.1.1.** *Neka je  $S$  neprazan skup te neka je  $* : S \times S \rightarrow S$ . Tada za  $*$  kažemo da je binarna operacija na skupu  $S$ . U tom slučaju, za  $x, y \in S$  umjesto  $*(x, y)$  obično pišemo  $x * y$ .*

**Definicija 2.1.2.** *Neka je  $*$  binarna operacija na  $S$ . Kažemo da je  $*$  asocijativna binarna operacija na  $S$  ako za sve  $x, y, z \in S$  vrijedi  $(x * y) * z = x * (y * z)$ .*

**Definicija 2.1.3.** *Neka je  $*$  binarna operacija na  $S$  te neka je  $e \in S$ . Kažemo da je  $e$  neutralni element za  $*$  ako za svaki  $x \in S$  vrijedi  $x * e = e * x = x$ .*

**Napomena 2.1.4.** *Neka je  $*$  binarna operacija na  $S$ . Pretpostavimo da su  $e_1, e_2 \in S$  neutralni elementi za  $*$ . Tada je  $e_1 = e_2$ . Naime, budući da je  $e_1$  neutralni element, vrijedi  $e_1 * e_2 = e_2$ , a budući da je  $e_2$  neutralni element, vrijedi  $e_1 * e_2 = e_1$ . Dakle,  $e_1 = e_2$ .*

**Definicija 2.1.5.** *Neka je  $*$  binarna operacija na skupu  $S$ . Za uređeni par  $(S, *)$  kažemo da je monoid ako je  $*$  asocijativna binarna operacija te ako postoji neutralni element za  $*$ .*

**Definicija 2.1.6.** *Neka je  $(S, *)$  monoid te neka je  $e$  neutralni element za  $*$ . Neka je  $x \in S$ . Za  $y \in S$  kažemo da je inverzni element od  $x$  u monoidu  $(S, *)$  ako je  $x * y = y * x = e$ .*

**Napomena 2.1.7.** *Neka je  $(S, *)$  monoid te neka je  $x \in S$ . Pretpostavimo da su  $y_1, y_2 \in S$  inverzni elementi od  $x$ . Tada je  $y_1 = y_2$ . Naime, neka je  $e$  neutralni element za  $*$ . Vrijedi*

$$y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2.$$

*Dakle,  $y_1 = y_2$ .*

**Definicija 2.1.8.** Neka je  $(S, *)$  monoid. Pretpostavimo da za svaki  $x \in S$  postoji inverzni element od  $x$  u  $(S, *)$ . Tada za  $(S, *)$  kažemo da je grupa.

**Definicija 2.1.9.** Neka je  $*$  binarna operacija na  $S$ . Kažemo da je  $*$  komutativna binarna operacija ako za sve  $x, y \in S$  vrijedi  $x * y = y * x$ .

Ako je  $(S, *)$  monoid takav da je  $*$  komutativna binarna operacija, onda za  $(S, *)$  kažemo da je komutativan monoid.

Ako je  $(S, *)$  grupa takva da je  $*$  komutativna binarna operacija, onda za  $(S, *)$  kažemo da je komutativna ili Abelova grupa.

**Napomena 2.1.10.** Neka je  $(S, *)$  grupa, neka je  $e$  neutralni element za  $*$  te neka je  $x \in S$  takav da je  $x * x = x$ . Tada je  $x = e$ .

Neka je  $y$  inverzni element od  $x$ . Slijedi  $y * (x * x) = y * x$  pa je  $(y * x) * x = e$ . Dakle,  $e * x = e$  tj.  $x = e$ .

**Definicija 2.1.11.** Neka je  $P$  skup te neka su  $+$  i  $\cdot$  binarne operacije na  $P$ . Kažemo da je  $(P, +, \cdot)$  prsten ako vrijedi:

1.  $(P, +)$  Abelova grupa
2. operacija  $\cdot$  je asocijativna
3. za sve  $x, y, z \in P$  vrijedi
  - $(x + y) \cdot z = x \cdot z + y \cdot z$
  - $z \cdot (x + y) = z \cdot x + z \cdot y$

**Definicija 2.1.12.** Ako je  $(P, +, \cdot)$  prsten, onda za neutralni element za operaciju  $+$  kažemo da je nula u prstenu  $(P, +, \cdot)$  i označavamo ga s  $0$ .

**Napomena 2.1.13.** Neka je  $(P, +, \cdot)$  prsten. Tada za svaki  $x \in P$  vrijedi  $0 \cdot x = 0$  i  $x \cdot 0 = 0$ . Naime, imamo  $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$ . Dakle,  $0 \cdot x = 0 \cdot x + 0 \cdot x$ . Iz napomene 2.1.10 slijedi  $0 \cdot x = 0$ . Analogno dobivamo da je  $x \cdot 0 = 0$ .

**Napomena 2.1.14.** Neka je  $(P, +, \cdot)$  prsten takav da skup  $P$  ima barem dva elementa. Tada  $(P, \cdot)$  nije grupa.

Pretpostavimo suprotno. Neka je  $e$  neutralni element za operaciju  $\cdot$ . Budući da je  $(P, \cdot)$  grupa, postoji  $x \in P$  takav da je  $0 \cdot x = e$ . Iz prethodne napomene slijedi da je  $e = 0$ . Sada za svaki  $x \in P$  vrijedi  $x = x \cdot e = x \cdot 0 = 0$ . Iz ovoga slijedi da je  $0$  jedini element skupa  $P$ , što je u kontradikciji s tim da  $P$  ima barem 2 elementa.

**Definicija 2.1.15.** Neka je  $(P, +, \cdot)$  prsten. Pretpostavimo da je  $e$  neutralni element za operaciju  $\cdot$ . Tada za  $e$  kažemo da je jedinica u prstenu  $(P, +, \cdot)$ . Za prsten  $(P, +, \cdot)$  takav da postoji neutralni element za operaciju  $\cdot$  kažemo da je prsten s jedinicom. Jedinicu u prstenu  $(P, +, \cdot)$  obično označavamo s 1.

**Definicija 2.1.16.** Neka je  $(P, +, \cdot)$  prsten takav da je operacija  $\cdot$  komutativna. Tada za  $(P, +, \cdot)$  kažemo da je komutativan prsten.

**Definicija 2.1.17.** Neka je  $(P, +, \cdot)$  komutativan prsten s jedinicom takav da  $P$  ima barem dva elementa. Pretpostavimo da svaki  $x \in P$ , takav da je  $x \neq 0$ , ima inverzni element u  $(P, \cdot)$ . Tada za  $(P, +, \cdot)$  kažemo da je polje.

**Napomena 2.1.18.** Neka je  $(P, +, \cdot)$  polje. Tada je  $0 \neq 1$ .

Pretpostavimo suprotno tj.  $0 = 1$ . Neka je  $x \in P$ . Tada je  $x = 1 \cdot x = 0 \cdot x = 0$ . Dakle,  $x = 0$ . Prema tome,  $P = \{0\}$ , što je u kontradikciji s definicijom polja.

**Definicija 2.1.19.** Neka je  $(P, +, \cdot)$  prsten i  $A \subseteq P$ . Kažemo da je  $A$  potprsten od  $(P, +, \cdot)$  ako postoje binarne operacije  $+_A$  i  $\cdot_A$  na  $A$  takve da je  $(A, +_A, \cdot_A)$  prsten te da je  $x +_A y = x + y$  i  $x \cdot_A y = x \cdot y$ , za sve  $x, y \in A$ .

**Napomena 2.1.20.** Ako je  $(P, +, \cdot)$  prsten onda za  $x \in P$  s  $-x$  označavamo inverzni (tj. suprotni) element od  $x$  u  $(P, +)$ . Dakle,  $x + (-x) = 0$  za svaki  $x \in P$ . Nadalje, za  $x, y \in P$  definiramo  $x - y = x + (-y)$ .

**Propozicija 2.1.21.** Neka je  $(P, +, \cdot)$  prsten te neka je  $A$  neprazan podskup od  $P$ . Tada je  $A$  potprsten od  $(P, +, \cdot)$  ako i samo ako za sve  $x, y \in A$  vrijedi  $x - y \in A$  i  $x \cdot y \in A$ .

*Dokaz.* Pretpostavimo da je  $A$  potprsten od  $(P, +, \cdot)$ . Tada postoje binarne operacije  $+_A$  i  $\cdot_A$  na  $A$  takve da je  $(A, +_A, \cdot_A)$  prsten i da je  $x +_A y = x + y$  i  $x \cdot_A y = x \cdot y$ , za sve  $x, y \in A$ .

Neka je  $0_A$  nula u prstenu  $(A, +_A, \cdot_A)$ . Vrijedi  $0_A +_A 0_A = 0_A$  tj.  $0_A + 0_A = 0_A$  pa iz napomene 2.1.10 slijedi  $0_A = 0$ .

Neka je  $x \in A$ . Neka je  $y$  inverzni element od  $x$  u  $(A, +_A)$ . Tada je  $x +_A y = 0_A$  pa je  $x + y = 0$ . Stoga je

$$(-x) + (x + y) = (-x) + 0$$

tj.

$$[(-x) + x] + y = -x.$$

Dobivamo  $0 + y = -x$  odnosno  $y = -x$ . Zaključujemo da je  $-x \in A$ , za svaki  $x \in A$ .

Neka su  $x, y \in A$ . Tada je  $-y \in A$  pa imamo

$$x - y = x + (-y) = x +_A (-y) \in A.$$

Dakle,  $x - y \in A$ .

Nadalje,  $x \cdot y = x \cdot_A y$  pa je očito  $x \cdot y \in A$  za sve  $x, y \in A$ .

Obratno, pretpostavimo da za sve  $x, y \in A$  vrijedi  $x - y \in A$  i  $x \cdot y \in A$ . Odaberimo neki  $x_0 \in A$  (to možemo jer je  $A$  neprazan skup).

Prema pretpostavci vrijedi  $x_0 - x_0 \in A$  tj.  $0 \in A$ .

Nadalje, neka je  $x \in A$ . Imamo  $0, x \in A$  pa je prema pretpostavci  $0 - x \in A$  tj.  $-x \in A$ , za svaki  $x \in A$ .

Neka su  $x, y \in A$ . Pokažimo da je  $x + y \in A$ . Imamo  $x, -y \in A$  pa je  $x - (-y) \in A$  odnosno  $x + y \in A$ .

Nadalje, za sve  $x, y \in A$  prema pretpostavci vrijedi  $x \cdot y \in A$ .

Definirajmo binarne operacije  $+_A$  i  $\cdot_A$  na  $A$  na sljedeći način:

$$x +_A y = x + y,$$

$$x \cdot_A y = x \cdot y.$$

Tvrdimo da je  $(A, +_A, \cdot_A)$  prsten.

Neka su  $x, y, z \in A$ . Koristeći činjenicu da je  $+$  asocijativna binarna operacija na  $P$  dobivamo

$$(x +_A y) +_A z = (x + y) + z = x + (y + z) = x +_A (y +_A z).$$

Dakle,

$$(x +_A y) +_A z = x +_A (y +_A z)$$

tj. operacija  $+_A$  je asocijativna na  $A$ . Analogno dobivamo da je  $+_A$  komutativna binarna operacija.

Budući da je  $0 \in A$  slijedi  $x +_A 0 = x + 0 = x$  za svaki  $x \in A$ . Dakle,  $0$  je neutralni element za  $+_A$ .

Neka je  $x \in A$ . Znamo da je  $-x \in A$ . Imamo  $x +_A (-x) = x + (-x) = 0$ . Prema tome,  $-x$  je inverzni element od  $x$  u  $(A, +_A)$ .

Time smo dokazali da je  $(A, +_A)$  Abelova grupa.

Nadalje, na sličan način dobivamo da je  $\cdot_A$  asocijativna binarna operacija te da za sve  $x, y, z \in A$  vrijedi

$$(x +_A y) \cdot_A z = x \cdot_A z +_A y \cdot_A z,$$

$$z \cdot_A (x +_A y) = z \cdot_A x +_A z \cdot_A y.$$

Time je dokazano da je  $(A, +_A, \cdot_A)$  prsten. Stoga je  $A$  potprsten od  $(P, +, \cdot)$ .

□

**Propozicija 2.1.22.** *Neka je  $(P, +, \cdot)$  prsten te neka je  $\mathcal{A}$  neprazna familija potprstena od  $(P, +, \cdot)$ . Tada je  $\bigcap_{A \in \mathcal{A}} A$  potprsten od  $(P, +, \cdot)$ .*

*Dokaz.* Neka je  $A \in \mathcal{A}$ . Tada je  $A$  potprsten od  $(P, +, \cdot)$ . Stoga je  $A \neq \emptyset$  pa postoji  $x \in A$ . Iz propozicije 2.1.21 slijedi da je  $x - x \in A$  tj.  $0 \in A$ . Dakle, za svaki  $A \in \mathcal{A}$  vrijedi da je  $0 \in A$ . Stoga je  $0 \in \bigcap_{A \in \mathcal{A}} A$  tj.  $\bigcap_{A \in \mathcal{A}} A$  je neprazan skup.

Neka su  $x, y \in \bigcap_{A \in \mathcal{A}} A$ . Neka je  $A \in \mathcal{A}$ . Tada su  $x, y \in A$ . Budući da je  $A$  potprsten od  $(P, +, \cdot)$ , iz propozicije 2.1.21 slijedi da je  $x - y \in A$  i  $x \cdot y \in A$ . Kako je  $x - y \in A$  i  $x \cdot y \in A$ , za svaki  $A \in \mathcal{A}$ , slijedi da je  $x - y \in \bigcap_{A \in \mathcal{A}} A$  i  $x \cdot y \in \bigcap_{A \in \mathcal{A}} A$ . Iz propozicije 2.1.21 slijedi da je  $\bigcap_{A \in \mathcal{A}} A$  potprsten od  $(P, +, \cdot)$ .

□

**Definicija 2.1.23.** *Neka je  $(P, +, \cdot)$  prsten te neka je  $S \subseteq P$ . Definiramo*

$$[S] = \bigcap_{\substack{A \text{ potprsten od } (P, +, \cdot) \\ S \subseteq A}} A.$$

Uočimo da je  $[S]$  potprsten od  $(P, +, \cdot)$ . Naime, to slijedi iz propozicije 2.1.22 i činjenice da je  $[S] = \bigcap_{A \in \mathcal{A}} A$ , gdje je  $\mathcal{A} = \{A \mid A \text{ potprsten od } (P, +, \cdot), S \subseteq A\}$  ( $\mathcal{A} \neq \emptyset$  jer je  $P \in \mathcal{A}$ ). Kažemo da je  $[S]$  potprsten od  $(P, +, \cdot)$  generiran sa  $S$ .

**Napomena 2.1.24.** *Neka je  $(P, +, \cdot)$  prsten te  $S \subseteq P$ .*

1. *Prema definiciji  $[S]$  je presjek svih potprstena od  $(P, +, \cdot)$  koji sadrže  $S$ . Stoga i njihov presjek sadrži  $S$  tj.  $S \subseteq [S]$ .*
2. *Neka je  $A_0$  potprsten od  $(P, +, \cdot)$  takav da je  $S \subseteq A_0$ . Tada je  $[S] \subseteq A_0$ . Naime, neka je  $\mathcal{A} = \{A \mid A \text{ potprsten od } (P, +, \cdot), S \subseteq A\}$ . Tada je  $A_0 \in \mathcal{A}$  pa je  $\bigcap_{A \in \mathcal{A}} A \subseteq A_0$ . Stoga je  $[S] = \bigcap_{A \in \mathcal{A}} A \subseteq A_0$  tj.  $[S] \subseteq A_0$ .*
3. *Vrijedi  $S = [S]$  ako i samo ako je  $S$  potprsten od  $(P, +, \cdot)$ . Naime, ako je  $S = [S]$ , onda je očito  $S$  potprsten od  $(P, +, \cdot)$ . Obratno, pretpostavimo da je  $S$  potprsten od  $(P, +, \cdot)$ . Definirajmo  $A_0 = S$ . Očito je  $S \subseteq A_0$  pa iz (2) slijedi da je  $[S] \subseteq A_0$  tj.  $[S] \subseteq S$ . S druge strane, prema (1) slijedi da je  $S \subseteq [S]$ . Stoga je  $S = [S]$ .*

**Napomena 2.1.25.** *Neka je  $(P, +, \cdot)$  prsten. Za  $n \in \mathbb{N}, n \geq 3$  i  $x_1, \dots, x_n \in P$  definiramo induktivno  $x_1 + \dots + x_n$  na sljedeći način:*

$$x_1 + \dots + x_n + x_{n+1} = (x_1 + \dots + x_n) + x_{n+1}, \quad n \geq 2.$$



Ako su  $x, y \in P$  onda je  $-(x+y) = -x+(-y)$ . Naime, to slijedi iz  $(x+y)+[-x+(-y)] = 0$ . Indukcijom se lako dobiva da za sve  $x_1, \dots, x_n \in P$  vrijedi

$$-(x_1 + \dots + x_n + x_{n+1}) = (-x_1) + \dots + (-x_n).$$

Naime, ako pretpostavimo da ova tvrdnja vrijedi za neki  $n$  ( $n \geq 2$ ), tada imamo

$$\begin{aligned} -(x_1 + \dots + x_n + x_{n+1}) &= -[(x_1 + \dots + x_n) + x_{n+1}] \\ &= -(x_1 + \dots + x_n) + (-x_{n+1}) \\ &= [(-x_1) + \dots + (-x_n)] + (-x_{n+1}) \\ &= (-x_1) + \dots + (-x_n) + (-x_{n+1}) \end{aligned}$$

Indukcijom također dobivamo da za sve  $x_1, \dots, x_n, y_1, \dots, y_n \in P$  vrijedi

$$(x_1 + \dots + x_n) + (y_1 + \dots + y_n) = (x_1 + y_1) + \dots + (x_n + y_n)$$

te da za svaki  $c \in P$  vrijedi

$$c \cdot (x_1 + \dots + x_n) = c \cdot x_1 + \dots + c \cdot x_n.$$

**Propozicija 2.1.26.** Neka je  $(P, +, \cdot)$  prsten. Neka su  $x, y \in P$ . Tada vrijedi:

1.  $-(x \cdot y) = (-x) \cdot y$
2.  $-(x \cdot y) = x \cdot (-y)$
3.  $x \cdot y = (-x) \cdot (-y)$

*Dokaz.*

1. Vrijedi  $(-x) \cdot y + x \cdot y = [(-x) + x] \cdot y = 0 \cdot y = 0$ . Dakle,

$$(-x) \cdot y = -(x \cdot y).$$

2. Dokaz ide analogno kao pod (1).

3. Koristeći (1) i (2) dobivamo

$$(-x) \cdot (-y) = -[x \cdot (-y)] = -[-(x \cdot y)] = x \cdot y.$$

□

## 2.2 Prsten $B[x_0]$

**Definicija 2.2.1.** Neka je  $(P, +, \cdot)$  prsten. Neka je  $B$  potprsten od  $(P, +, \cdot)$  te neka je  $x_0 \in P$ . Definiramo  $B[x_0]$  kao potprsten od  $(P, +, \cdot)$  generiran s  $B \cup \{x_0\}$ . Dakle,  $B[x_0] = [B \cup \{x_0\}]$ .

**Napomena 2.2.2.** Neka je  $(P, +, \cdot)$  prsten te neka je  $x \in P$ . Za  $n \in \mathbb{N}$  definiramo  $x^n$  induktivno na sljedeći način:

$$\begin{aligned}x^1 &= x \\x^{n+1} &= x^n \cdot x\end{aligned}$$

Neka je  $m \in \mathbb{N}$ . Tvrdimo da za svaki  $n \in \mathbb{N}$  vrijedi

$$x^{m+n} = x^m \cdot x^n \quad (\otimes)$$

Dokažimo to indukcijom po  $n$ .

Za  $n = 1$  ( $\otimes$ ) vrijedi po definiciji.

Pretpostavimo da ( $\otimes$ ) vrijedi za neki  $n \in \mathbb{N}$ . Imamo

$$x^{m+(n+1)} = x^{(m+n)+1} = x^{m+n} \cdot x = (x^m \cdot x^n) \cdot x = x^m \cdot (x^n \cdot x) = x^m \cdot x^{n+1}.$$

Dakle,  $x^{m+(n+1)} = x^m \cdot x^{n+1}$ . Prema tome, ( $\otimes$ ) vrijedi za svaki  $n \in \mathbb{N}$ .

**Napomena 2.2.3.** Neka je  $(P, +, \cdot)$  prsten te neka je  $B$  potprsten od  $(P, +, \cdot)$ . Neka su  $x_1, \dots, x_n \in B$ . Tada je  $x_1 + \dots + x_n \in B$ . To slijedi indukcijom po  $n$ . Nadalje, neka su  $x \in B$  i  $n \in \mathbb{N}$ . Tada je  $x^n \in B$ , što također slijedi indukcijom po  $n$ .

**Korolar 2.2.4.** Neka je  $(P, +, \cdot)$  prsten te neka su  $x, y, c \in P$ . Tada vrijedi

$$c \cdot (x - y) = c \cdot x - c \cdot y,$$

$$(x - y) \cdot c = x \cdot c - y \cdot c.$$

*Dokaz.* Koristeći propoziciju 2.1.26 slijedi da je

$$c \cdot (x - y) = c \cdot [x + (-y)] = c \cdot x + c \cdot (-y) = c \cdot x + (-c \cdot y) = c \cdot x - c \cdot y.$$

Dakle,  $c \cdot (x - y) = c \cdot x - c \cdot y$ .

Analogno se dokazuje  $(x - y) \cdot c = x \cdot c - y \cdot c$ . □

**Propozicija 2.2.5.** Neka je  $(P, +, \cdot)$  komutativan prsten te neka je  $B$  potprsten od  $(P, +, \cdot)$  te  $x_0 \in P$ . Definirajmo

$$R = \{b_n x_0^n + \cdots + b_1 x_0 + b_0 \mid b_n, \dots, b_0 \in B\}.$$

Tada je  $R$  potprsten od  $(P, +, \cdot)$ .

*Dokaz.* Neka su  $x, y \in R$ . Tada postoje  $b_m, \dots, b_0, c_n, \dots, c_0 \in B$  takvi da je

$$x = b_m x_0^m + \cdots + b_1 x_0 + b_0,$$

$$y = c_n x_0^n + \cdots + c_1 x_0 + c_0.$$

Bez smanjenja općenitosti neka je  $n \leq m$  (pri tome su  $m, n \in \mathbb{N}_0$ ). Za svaki  $i \in \{n+1, \dots, m\}$  definiramo  $c_i = 0$ . Slijedi  $c_0, \dots, c_m \in B$  i

$$y = c_m x_0^m + \cdots + c_{n+1} x_0^{n+1} + c_n x_0^n + \cdots + c_1 x_0 + c_0.$$

Koristeći napomenu 2.1.25, propoziciju 2.1.26 i korolar 2.2.4 dobivamo

$$\begin{aligned} x - y &= x + (-y) = \\ &= (b_m x_0^m + b_{m-1} x_0^{m-1} + \cdots + b_1 x_0 + b_0) + [(-c_m x_0^m) + (-c_{m-1} x_0^{m-1}) + \cdots + (-c_1 x_0) + (-c_0)] \\ &= (b_m x_0^m - c_m x_0^m) + (b_{m-1} x_0^{m-1} - c_{m-1} x_0^{m-1}) + \cdots + (b_1 x_0 - c_1 x_0) + (b_0 - c_0) \\ &= (b_m - c_m) x_0^m + (b_{m-1} - c_{m-1}) x_0^{m-1} + \cdots + (b_1 - c_1) x_0 + (b_0 - c_0). \end{aligned}$$

Vrijedi  $b_m - c_m, b_{m-1} - c_{m-1}, \dots, b_1 - c_1, b_0 - c_0 \in B$  jer je  $B$  potprsten pa slijedi  $x - y \in R$ . Analogno zaključujemo da je  $x + y \in R$ .

Iz ovoga zaključujemo da za sve  $x_1, \dots, x_n \in R$  vrijedi  $x_1 + \cdots + x_n \in R$ .

Neka su  $b \in B$  i  $i \in \mathbb{N}$ . Tvrđimo da je  $b x_0^i \cdot y \in R$  za svaki  $y \in R$ .

Neka je  $y \in R$ . Tada postoje  $c_m, \dots, c_0 \in B$  takvi da je  $y = c_m x_0^m + \cdots + c_0$ . Vrijedi

$$\begin{aligned} b x_0^i \cdot y &= b x_0^i (c_m x_0^m + c_{m-1} x_0^{m-1} + \cdots + c_1 x_0 + c_0) \\ &= (b x_0^i) (c_m x_0^m) + (b x_0^i) (c_{m-1} x_0^{m-1}) + \cdots + (b x_0^i) (c_1 x_0) + (b x_0^i) c_0 \\ &= (b c_m) x_0^{m+i} + (b c_{m-1}) x_0^{i+m-1} + \cdots + (b c_1) x_0^{i+1} + (b c_0) x_0^i \end{aligned}$$

Dakle,  $b x_0^i \cdot y \in R$  za svaki  $y \in R$ .

Neka su  $x, y \in R$ . Tada postoje  $b_n, \dots, b_0 \in B$  takvi da je  $x = b_n x_0^n + \dots + b_1 x_0 + b_0$ .  
Vrijedi

$$\begin{aligned} x \cdot y &= (b_n x_0^n + b_{n-1} x_0^{n-1} + \dots + b_1 x_0 + b_0) \cdot y \\ &= (b_n x_0^n) \cdot y + (b_{n-1} x_0^{n-1}) \cdot y + \dots + (b_1 x_0) \cdot y + b_0 \cdot y \end{aligned}$$

Za svaki  $i \in \{1, \dots, n\}$  prema dokazanom vrijedi  $(b_i x_0^i) \cdot y \in R$ . Dakle,  $x \cdot y \in R$ .  
Time je tvrdnja propozicije dokazana. □

**Propozicija 2.2.6.** *Neka je  $(P, +, \cdot)$  komutativan prsten s jedinicom. Neka je  $B$  potprsten od  $(P, +, \cdot)$  takav da je  $1 \in B$  te neka je  $x_0 \in P$ . Tada je*

$$B[x_0] = \{b_n x_0^n + \dots + b_1 x_0 + b_0 \mid b_n, \dots, b_0 \in B\}.$$

*Dokaz.* Neka je  $R = \{b_n x_0^n + \dots + b_1 x_0 + b_0 \mid b_n, \dots, b_0 \in B\}$ . Želimo dokazati  $B[x_0] = R$ .

Dokažimo prvo  $B[x_0] \subseteq R$ . Prema propoziciji 2.2.5  $R$  je potprsten od  $(P, +, \cdot)$ . Nadalje,  $B[x_0] = [B \cup \{x_0\}]$ . Stoga je dovoljno dokazati  $B \cup \{x_0\} \subseteq R$  jer će tada prema drugoj točki napomene 2.1.24 slijediti  $[B \cup \{x_0\}] \subseteq R$  tj.  $B[x_0] \subseteq R$ .

Za svaki  $x \in B$  vrijedi  $x \in R$  jer možemo uzeti  $n = 0$  i  $b_0 = x$ . Prema tome,  $B \subseteq R$ .  
Nadalje,  $x_0 = 1 \cdot x_0 + 0$ , pa zbog  $1 \in B$  (također je i  $0 \in B$ , što slijedi iz propozicije 2.1.21) slijedi da je  $x_0 \in R$ , odnosno  $\{x_0\} \subseteq R$ . Dakle,  $B \cup \{x_0\} \subseteq R$ . Time smo dokazali  $B[x_0] \subseteq R$ .

Dokažimo sada  $R \subseteq B[x_0]$ . Neka je  $r \in R$ . Tada postoje  $n \in \mathbb{N}_0$  i  $b_n, \dots, b_0 \in B$  takvi da je  $r = b_n x_0^n + \dots + b_1 x_0 + b_0$ . Znamo da je  $B[x_0]$  potprsten od  $(P, +, \cdot)$ .  
Iz  $B \cup \{x_0\} \subseteq [B \cup \{x_0\}]$  slijedi  $B \cup \{x_0\} \subseteq B[x_0]$ . To znači da su  $b_n, \dots, b_0, x_0 \in B[x_0]$ .  
Iz napomene 2.2.3 slijedi da su  $x_0, x_0^2, \dots, x_0^n \in B[x_0]$ . Slijedi da su  $b_1 x_0, b_2 x_0^2, \dots, b_n x_0^n \in B[x_0]$  pa iz napomene 2.2.3 slijedi  $b_n x_0^n + \dots + b_1 x_0 + b_0 \in B[x_0]$  tj.  $r \in B[x_0]$ . Time smo dokazali  $R \subseteq B[x_0]$ . Dakle,  $R = B[x_0]$ . □

**Definicija 2.2.7.** *Neka je  $(P, +, \cdot)$  polje te neka je  $A \subseteq P$ . Pretpostavimo da postoje binarne operacije  $+_A, \cdot_A$  na  $A$  takve da je  $x +_A y = x + y$  i  $x \cdot_A y = x \cdot y$ , za sve  $x, y \in A$  te takve da je  $(A, +_A, \cdot_A)$  polje. Tada kažemo da je  $A$  potpolje od  $(P, +, \cdot)$ .*

**Napomena 2.2.8.** Ako je  $(P, +, \cdot)$  polje, onda za  $x \in P, x \neq 0$ , s  $x^{-1}$  označavamo inverzni element od  $x$  u monoidu  $(P, \cdot)$ . Dakle,

$$x \cdot x^{-1} = x^{-1} \cdot x = 1.$$

**Propozicija 2.2.9.** Neka je  $(P, +, \cdot)$  polje te  $A \subseteq P$  takav da  $A$  ima barem dva elementa. Onda je:

$$A \text{ potpolje od } (P, +, \cdot) \Leftrightarrow \text{za sve } x, y \in A \text{ vrijedi } x - y \in A, x \cdot y \in A, \\ \text{za svaki } x \in A, x \neq 0 \text{ vrijedi } x^{-1} \in A.$$

*Dokaz.* Pretpostavimo da je  $A$  potpolje od  $(P, +, \cdot)$ . Tada postoje binarne operacije  $+_A, \cdot_A$  na  $A$  takve da  $x +_A y = x + y$  i  $x \cdot_A y = x \cdot y$ , za sve  $x, y \in A$  te takve da je  $(A, +_A, \cdot_A)$  polje. Zaključujemo da je  $A$  potprsten od  $(P, +, \cdot)$  pa iz propozicije 2.1.21 slijedi da za sve  $x, y \in A$  vrijedi  $x - y \in A$  i  $x \cdot y \in A$ .

Neka je  $0_A$  neutralni element za operaciju  $+_A$ . U dokazu propozicije 2.1.21 smo vidjeli da je  $0_A = 0$ .

Neka je  $1_A$  neutralni element za operaciju  $\cdot_A$ . Odaberimo  $x \in A$  takav da  $x \neq 0$  (znamo da takav postoji jer  $A$  ima barem dva elementa). Vrijedi  $x \cdot_A 1_A = x$  tj.

$$x \cdot 1_A = x.$$

Množenjem prethodne jednakosti s  $x^{-1}$  dobivamo

$$x^{-1} \cdot (x \cdot 1_A) = x^{-1} \cdot x$$

pa je

$$(x^{-1} \cdot x) \cdot 1_A = x^{-1} \cdot x.$$

Slijedi  $1 \cdot 1_A = 1$ . Budući da je  $1$  neutralni element za množenje u  $(P, +, \cdot)$ , slijedi  $1 = 1_A$ .

Neka je  $x \in A, x \neq 0$ . Tada je  $x \neq 0_A$ . Budući da je  $(A, +_A, \cdot_A)$  polje, postoji neutralni element  $y$  od  $x$  u monoidu  $(A, \cdot_A)$ . Prema tome,  $x \cdot_A y = 1_A$ , što je ekvivalentno s  $x \cdot y = 1$ . Množenjem prethodne jednakosti s  $x^{-1}$  dobivamo da je  $y = x^{-1}$ . Prema tome,  $x^{-1} \in A$ .

Obratno, pretpostavimo da za sve  $x, y \in A$  vrijedi  $x - y \in A, x \cdot y \in A$  te za svaki  $x \in A, x \neq 0$ , vrijedi  $x^{-1} \in A$ .

Iz propozicije 2.1.21 slijedi da je  $A$  potprsten od  $(P, +, \cdot)$ . Stoga postoje binarne operacije  $+_A$  i  $\cdot_A$  na  $A$  takve da je  $(A, +_A, \cdot_A)$  prsten te da je za sve  $x, y \in A$

$$x \cdot_A y = x \cdot y \quad (\spadesuit)$$

$$x +_A y = x + y$$

Želimo dokazati da je  $(A, +_A, \cdot_A)$  polje. Znamo da je binarna operacija  $\cdot$  komutativna jer je  $(P, +, \cdot)$  polje pa iz  $(\spadesuit)$  slijedi da je  $\cdot_A$  komutativna binarna operacija.

Nadalje, odaberimo  $x \in A, x \neq 0$ . Tada je prema pretpostavci  $x^{-1} \in A$  pa je ponovno prema pretpostavci  $x \cdot x^{-1} \in A$  tj.  $1 \in A$ .

Zaključujemo da je zbog  $(\spadesuit)$  1 neutralni element za  $\cdot_A$ .

Dakle,  $(A, +_A, \cdot_A)$  je komutativan prsten s jedinicom.

Neka je  $0_A$  nula u prstenu  $(A, +_A, \cdot_A)$ . U dokazu propozicije 2.1.21 smo vidjeli da je  $0_A = 0$ .

Neka je  $x \in A, x \neq 0_A$ . Tada je  $x \neq 0$ . Prema pretpostavci vrijedi  $x^{-1} \in A$ . Imamo

$$x \cdot_A x^{-1} = x \cdot x^{-1} = 1.$$

Dakle,  $x \cdot_A x^{-1} = 1$ , a također vrijedi  $x^{-1} \cdot_A x = 1$  (jer je  $\cdot_A$  komutativna binarna operacija).

Dakle,  $x^{-1}$  je inverzni element od  $x$  u monoidu  $(A, \cdot_A)$ .

Time smo dokazali da je  $(A, +_A, \cdot_A)$  polje, odnosno  $A$  je potpolje od  $(P, +, \cdot)$ .  $\square$

**Napomena 2.2.10.** Neka je  $(P, +, \cdot)$  prsten i neka je  $x \in P$ . Tada za sve  $m, n \in \mathbb{N}$  vrijedi

$$(x^m)^n = x^{mn}.$$

Dokažimo to indukcijom po  $n$  (za fiksirani  $m$ ).

Za  $n = 1$  tvrdnja je dokazana.

Pretpostavimo da tvrdnja vrijedi za neki  $n \in \mathbb{N}$  tj.  $(x^m)^n = x^{mn}$ .

Provjerimo za  $n + 1 \in \mathbb{N}$ :

$$(x^m)^{n+1} = (x^m)^n \cdot x^m = x^{mn} \cdot x^m = x^{mn+m} = x^{m(n+1)}.$$

Time je tvrdnja dokazana.

**Lema 2.2.11.** Neka je  $(P, +, \cdot)$  polje. Neka su  $u, v \in P$ .

Tada vrijedi:

- $(u - v)(u + v) = u^2 - v^2$

- Ako je  $u \neq 0$  i  $v \neq 0$ , onda je  $u \cdot v \neq 0$  i  $(u \cdot v)^{-1} = u^{-1} \cdot v^{-1}$ .

*Dokaz.*

1. Koristeći korolar 2.2.4 dobivamo:

$$\begin{aligned}(u - v)(u + v) &= (u - v) \cdot u + (u - v) \cdot v \\ &= (u \cdot u - v \cdot u) + (u \cdot v - v \cdot v) \\ &= u^2 - v^2\end{aligned}$$

2. Pretpostavimo da je  $u \neq 0$  i  $v \neq 0$ . Imamo

$$(u \cdot v) \cdot (u^{-1} \cdot v^{-1}) = (u \cdot v) \cdot (v^{-1} \cdot u^{-1}) = u \cdot u^{-1} = 1.$$

Dakle,

$$(u \cdot v) \cdot (u^{-1} \cdot v^{-1}) = 1 \quad (\blacktriangle)$$

Kada bi vrijedilo  $u \cdot v = 0$ , onda bismo imali  $(u \cdot v) \cdot (u^{-1} \cdot v^{-1}) = 0$  pa bi iz  $(\blacktriangle)$  slijedilo  $1 = 0$ , što je nemoguće prema napomeni 2.1.18. Dakle,  $u \cdot v \neq 0$ .

Kada jednakost  $(\blacktriangle)$  pomnožimo s  $(u \cdot v)^{-1}$  dobivamo

$$(u \cdot v)^{-1} \cdot [(u \cdot v) \cdot (u^{-1} \cdot v^{-1})] = (u \cdot v)^{-1}$$

pa je  $u^{-1} \cdot v^{-1} = (u \cdot v)^{-1}$ .

Time je lema dokazana. □

**Propozicija 2.2.12.** *Neka je  $(P, +, \cdot)$  polje te neka je  $B$  potpolje od  $(P, +, \cdot)$ . Neka je  $x_0 \in P$  takav da je  $x_0^2 \in B$ . Tada je  $B[x_0]$  potpolje od  $(P, +, \cdot)$  i vrijedi  $B[x_0] = \{a + b \cdot x_0 \mid a, b \in \mathbb{R}\}$ .*

*Dokaz.* Znamo da je  $B[x_0]$  potprsten od  $(P, +, \cdot)$ . Prema propoziciji 2.1.21 za sve  $x, y \in B[x_0]$  vrijedi  $x - y \in B[x_0]$  i  $x \cdot y \in B[x_0]$ . Ostaje pokazati da za svaki  $x \in B[x_0]$ ,  $x \neq 0$  vrijedi  $x^{-1} \in B[x_0]$ .

Očito je  $(P, +, \cdot)$  komutativan prsten s jedinicom. Nadalje, odaberimo neki  $z \in B$ . Prema propoziciji 2.2.9 vrijedi  $z^{-1} \in B$ , pa prema istoj propoziciji vrijedi  $z \cdot z^{-1} \in B$  tj.  $1 \in B$ .

Prema propoziciji 2.2.6 vrijedi  $B[x_0] = \{b_n x_0^n + \dots + b_1 x_0 + b_0 \mid b_n, \dots, b_0 \in B\}$ . Tvrdimo da za svaki  $n \in \mathbb{N}_0$  i sve  $b_n, \dots, b_0 \in B$  postoje  $a, b \in B$  takvi da je

$$b_n x_0^n + \dots + b_1 x_0 + b_0 = a + b \cdot x_0.$$

Dokažimo to indukcijom po  $n$ .

Za  $n = 0, n = 1$  tvrdnja je očita.

Pretpostavimo da tvrdnja vrijedi za neki  $n \in \mathbb{N}$ .

Neka su  $b_{n+1}, \dots, b_0 \in B$ . Prema induktivnoj pretpostavci postoje  $a, b \in B$  takvi da je

$$b_n x_0^n + \dots + b_1 x_0 + b_0 = a + b \cdot x_0.$$

Vrijedi

$$b_{n+1} x_0^{n+1} + b_n x_0^n + \dots + b_1 x_0 + b_0 = b_{n+1} x_0^{n+1} + (b_n x_0^n + \dots + b_1 x_0 + b_0) = b_{n+1} x_0^{n+1} + (a + b \cdot x_0).$$

Promotrimo dva moguća slučaja:

*1. slučaj:  $n + 1$  je paran.*

Tada je  $n + 1 = 2k, k \in \mathbb{N}$ .

Imamo

$$b_{n+1} x_0^{n+1} = b_{n+1} x_0^{2k} = b_{n+1} (x_0^2)^k,$$

pa iz pretpostavke propozicije i napomene 2.2.3 slijedi  $b_{n+1} x_0^{n+1} \in B$ .

Stoga je

$$b_{n+1} x_0^{n+1} + a + b \cdot x_0 = a' + b \cdot x_0,$$

gdje je  $a' \in B$ .

*2. slučaj:  $n + 1$  je neparan.*

Tada je  $n + 1 = 2k + 1, k \in \mathbb{N}$ .

Imamo

$$b_{n+1} x_0^{n+1} = b_{n+1} x_0^{2k+1} = b_{n+1} x_0^{2k} \cdot x_0.$$

Prema prethodnom slučaju zaključujemo da je  $b_{n+1} x_0^{2k} \in B$  tj.

$$b_{n+1} x_0^{2k} \cdot x_0 = b' \cdot x_0,$$

gdje je  $b' \in B$ . Dakle,

$$b_{n+1} x_0^{n+1} + a + b \cdot x_0 = a + (b + b') \cdot x_0.$$

U oba slučaja smo dobili da postoje  $c, d \in B$  takvi da je



$$b_{n+1}x_0^{n+1} + b_nx_0^n + \cdots + b_0 = c + d \cdot x_0.$$

Time je tvrdnja dokazana.

Uočimo da iz prethodno dokazane tvrdnje slijedi  $B[x_0] = \{a + b \cdot x_0 \mid a, b \in B\}$ .

Neka je  $x \in B[x_0]$ ,  $x \neq 0$ . Tada postoje  $a, b \in B$  takvi da je  $x = a + b \cdot x_0$ . Tvrdimo da je  $x^{-1} \in B[x_0]$ .

1. slučaj:  $a = b \cdot x_0$ .

Tada je očito  $b \cdot x_0 \in B$  pa je  $a + b \cdot x_0 \in B$  tj.  $x \in B$ .

Budući da je  $B$  potpolje od  $(P, +, \cdot)$ , vrijedi  $x^{-1} \in B$  pa je očito  $x^{-1} \in B[x_0]$ .

2. slučaj:  $a \neq b \cdot x_0$ .

Tada je  $a - b \cdot x_0 \neq 0$ . Koristeći prethodnu lemu dobivamo sljedeće:

$$\begin{aligned} x^{-1} &= (a + b \cdot x_0)^{-1} = (a + b \cdot x_0)^{-1} \cdot 1 = (a + b \cdot x_0)^{-1} \cdot [(a - b \cdot x_0)^{-1} \cdot (a - b \cdot x_0)] = \\ &= [(a + b \cdot x_0)^{-1} \cdot (a - b \cdot x_0)^{-1}] \cdot (a - b \cdot x_0) \\ &= [(a + b \cdot x_0) \cdot (a - b \cdot x_0)]^{-1} \cdot (a - b \cdot x_0) \\ &= [a^2 - (b \cdot x_0)^2]^{-1} \cdot (a - b \cdot x_0) \\ &= (a^2 - b^2 \cdot x_0^2)^{-1} \cdot (a - b \cdot x_0). \end{aligned}$$

Dakle,  $x^{-1} = (a^2 - b^2 \cdot x_0^2)^{-1} \cdot (a - b \cdot x_0)$ .

Iz pretpostavke znamo da je  $x_0^2 \in B$  pa je  $a^2 - b^2 \cdot x_0^2 \in B$  te je  $(a^2 - b^2 \cdot x_0^2)^{-1} \in B$ .

Dakle,  $(a^2 - b^2 \cdot x_0^2)^{-1} \in B[x_0]$ , a očito je  $a - b \cdot x_0 \in B[x_0]$ . Zaključujemo da je

$$(a^2 - b^2 \cdot x_0^2)^{-1} \cdot (a - b \cdot x_0) \in B[x_0]$$

tj.  $x^{-1} \in B[x_0]$ .

Time smo dokazali da je  $B[x_0]$  potpolje od  $(P, +, \cdot)$ .

□

## 2.3 Kvadratni radikali

**Napomena 2.3.1.** Neka su  $+$  i  $\cdot$  standardne operacije na  $\mathbb{R}$ . Znamo da je  $(\mathbb{R}, +, \cdot)$  polje te da je  $\mathbb{Q}$  potpolje od  $(\mathbb{R}, +, \cdot)$ .

**Definicija 2.3.2.** Za  $n \in \mathbb{N}$  i  $x_0, \dots, x_n \in \mathbb{R}$  definiramo induktivno  $\mathbb{Q}[x_0, \dots, x_n]$  na sljedeći način.

Za  $x_0, x_1 \in \mathbb{R}$  neka je

$$\mathbb{Q}[x_0, x_1] = (\mathbb{Q}[x_0])[x_1].$$

Pretpostavimo da je  $n \in \mathbb{N}$  te da smo za sve  $x_0, \dots, x_n \in \mathbb{R}$  definirali  $\mathbb{Q}[x_0, \dots, x_n]$ .

Za  $x_0, \dots, x_{n+1} \in \mathbb{R}$  definiramo

$$\mathbb{Q}[x_0, \dots, x_{n+1}] = (\mathbb{Q}[x_0, \dots, x_n])[x_{n+1}].$$

**Definicija 2.3.3.** Neka je  $n \in \mathbb{N}_0$  te neka su  $x_0, \dots, x_n \in \mathbb{R}$  takvi da je  $x_0^2 \in \mathbb{Q}$  te  $x_{i+1}^2 \in \mathbb{Q}[x_0, \dots, x_i]$ , za svaki  $i \in \{0, \dots, n-1\}$ . Tada za konačan niz  $x_0, \dots, x_n$  kažemo da je **korijenski niz**.

**Propozicija 2.3.4.** Ako je  $x_0, \dots, x_n$  korijenski niz, tada je  $\mathbb{Q}[x_0, \dots, x_n]$  potpolje od  $(\mathbb{R}, +, \cdot)$ .

*Dokaz.* Dokažimo tvrdnju indukcijom po  $n$ .

Ako je  $x_0 \in \mathbb{R}$  takav da je  $x_0^2 \in \mathbb{Q}$ , onda je  $\mathbb{Q}[x_0]$  potpolje od  $(\mathbb{R}, +, \cdot)$  prema propoziciji 2.2.12. Dakle, tvrdnja vrijedi za  $n = 0$ .

Pretpostavimo da tvrdnja vrijedi za neki  $n \in \mathbb{N}_0$ .

Neka je  $x_0, \dots, x_{n+1}$  korijenski niz. Uočimo da je  $x_0, \dots, x_n$  korijenski niz pa iz pretpostavke indukcije slijedi da je  $\mathbb{Q}[x_0, \dots, x_n]$  potpolje od  $(\mathbb{R}, +, \cdot)$ .

Nadalje, prema definiciji korijenskog niza vrijedi  $x_{n+1}^2 \in \mathbb{Q}[x_0, \dots, x_n]$ . Stoga iz propozicije 2.2.12 slijedi da je  $(\mathbb{Q}[x_0, \dots, x_n])[x_{n+1}]$  potpolje od  $(\mathbb{R}, +, \cdot)$ .

Iz  $\mathbb{Q}[x_0, \dots, x_{n+1}] = (\mathbb{Q}[x_0, \dots, x_n])[x_{n+1}]$  zaključujemo da je  $\mathbb{Q}[x_0, \dots, x_{n+1}]$  potpolje od  $(\mathbb{R}, +, \cdot)$ .

Time je tvrdnja propozicije dokazana. □

**Definicija 2.3.5.** Neka je  $z \in \mathbb{R}$ . Kažemo da je  $z$  **kvadratni radikal** ako postoji korijenski niz  $x_0, \dots, x_n$  takav da je  $z \in \mathbb{Q}[x_0, \dots, x_n]$ .

**Napomena 2.3.6.** Svaki racionalni broj je kvadratni radikal. Naime, po definiciji je  $\mathbb{Q}[1] = [\mathbb{Q} \cup \{1\}]$  pa je  $\mathbb{Q}[1] = [\mathbb{Q}]$ , no  $[\mathbb{Q}] = \mathbb{Q}$  prema napomeni 2.1.24. Dakle,  $\mathbb{Q}[1] = \mathbb{Q}$ . Očito je konačan niz  $x_0 = 1$  korijenski niz, pa zaključujemo da je svaki racionalan broj kvadratni radikal.

**Napomena 2.3.7.** Neka su  $S, T \subseteq \mathbb{R}$  takvi da je  $S \subseteq T$ . Tada je  $[S] \subseteq [T]$ .

Naime, iz  $T \subseteq [T]$  slijedi  $S \subseteq [T]$ . Iz napomene 2.1.24 i činjenice da je  $[T]$  potprsten od  $(\mathbb{R}, +, \cdot)$ , slijedi  $[S] \subseteq [T]$ .

**Lema 2.3.8.** Za sve  $n \in \mathbb{N}_0$  i  $x_0, \dots, x_n \in \mathbb{R}$  vrijedi

$$\mathbb{Q} \subseteq \mathbb{Q}[x_0, \dots, x_n],$$

$$x_0, \dots, x_n \in \mathbb{Q}[x_0, \dots, x_n].$$

*Dokaz.* Dokažimo ovu tvrdnju indukcijom po  $n$ .

Pretpostavimo da je  $x_0 \in \mathbb{R}$ . Vrijedi  $\mathbb{Q}[x_0] = [\mathbb{Q} \cup \{x_0\}]$  pa iz

$$\mathbb{Q} \subseteq \mathbb{Q} \cup \{x_0\} \subseteq [\mathbb{Q} \cup \{x_0\}],$$

$$x_0 \in \mathbb{Q} \cup \{x_0\} \subseteq [\mathbb{Q} \cup \{x_0\}]$$

slijedi da je  $\mathbb{Q} \subseteq \mathbb{Q}[x_0]$  i  $x_0 \in \mathbb{Q}[x_0]$ . Dakle, tvrdnja vrijedi za  $n = 0$ .

Pretpostavimo da tvrdnja vrijedi za neki  $n \in \mathbb{N}_0$ .

Neka su  $x_0, \dots, x_{n+1} \in \mathbb{R}$ . Koristeći induktivnu pretpostavku dobivamo:

$$\begin{aligned} \mathbb{Q} \subseteq \mathbb{Q}[x_0, \dots, x_n] \subseteq \mathbb{Q}[x_0, \dots, x_n] \cup \{x_{n+1}\} &\subseteq [\mathbb{Q}[x_0, \dots, x_n] \cup \{x_{n+1}\}] = (\mathbb{Q}[x_0, \dots, x_n])[x_{n+1}] \\ &= \mathbb{Q}[x_0, \dots, x_{n+1}]. \end{aligned}$$

Dakle,  $\mathbb{Q} \subseteq \mathbb{Q}[x_0, \dots, x_{n+1}]$ .

Uočimo da smo dokazali da je  $\mathbb{Q}[x_0, \dots, x_n] \subseteq \mathbb{Q}[x_0, \dots, x_{n+1}]$ .

Prema induktivnoj pretpostavci vrijedi  $x_0, \dots, x_n \in \mathbb{Q}[x_0, \dots, x_n]$ . Stoga je  $x_0, \dots, x_n \in \mathbb{Q}[x_0, \dots, x_{n+1}]$ . Nadalje, također smo pokazali da je  $\mathbb{Q}[x_0, \dots, x_n] \cup \{x_{n+1}\} \subseteq \mathbb{Q}[x_0, \dots, x_{n+1}]$ .

Iz toga očito slijedi da je  $x_{n+1} \in \mathbb{Q}[x_0, \dots, x_{n+1}]$ . Prema tome,  $x_0, \dots, x_{n+1} \in \mathbb{Q}[x_0, \dots, x_{n+1}]$ .

Time smo dokazali da tvrdnja vrijedi za  $n + 1$  pa je lema dokazana.  $\square$

**Propozicija 2.3.9.** Za sve  $n \in \mathbb{N}_0$  i  $x_0, \dots, x_n \in \mathbb{R}$  vrijedi

$$\mathbb{Q}[x_0, \dots, x_n] = [\mathbb{Q} \cup \{x_0, \dots, x_n\}].$$

*Dokaz.* Dokažimo tvrdnju indukcijom po  $n$ .

Za  $n = 0$  tvrdnja slijedi iz definicije 2.2.1.

Pretpostavimo da tvrdnja vrijedi za neki  $n \in \mathbb{N}_0$ .

Neka su  $x_0, \dots, x_{n+1} \in \mathbb{R}$ . Tvrdimo da je

$$\mathbb{Q}[x_0, \dots, x_{n+1}] = [\mathbb{Q} \cup \{x_0, \dots, x_{n+1}\}]. \quad (\star)$$

Koristeći induktivnu pretpostavku i napomenu 2.3.7 dobivamo

$$\mathbb{Q}[x_0, \dots, x_n] = [\mathbb{Q} \cup \{x_0, \dots, x_n\}] \subseteq [\mathbb{Q} \cup \{x_0, \dots, x_{n+1}\}].$$

Dakle,

$$\mathbb{Q}[x_0, \dots, x_n] \subseteq [\mathbb{Q} \cup \{x_0, \dots, x_{n+1}\}]. \quad (\diamond)$$

Nadalje, vrijedi  $x_{n+1} \in \mathbb{Q} \cup \{x_0, \dots, x_{n+1}\} \subseteq [\mathbb{Q} \cup \{x_0, \dots, x_{n+1}\}]$ .

Dakle,

$$x_{n+1} \in [\mathbb{Q} \cup \{x_0, \dots, x_{n+1}\}]. \quad (\diamond\diamond)$$

Iz  $(\diamond)$  i  $(\diamond\diamond)$  slijedi

$$\mathbb{Q}[x_0, \dots, x_n] \cup \{x_{n+1}\} \subseteq [\mathbb{Q} \cup \{x_0, \dots, x_{n+1}\}].$$

Prema napomeni 2.1.24 slijedi

$$[\mathbb{Q}[x_0, \dots, x_n] \cup \{x_{n+1}\}] \subseteq [\mathbb{Q} \cup \{x_0, \dots, x_{n+1}\}],$$

tj.

$$(\mathbb{Q}[x_0, \dots, x_n])[x_{n+1}] \subseteq [\mathbb{Q} \cup \{x_0, \dots, x_{n+1}\}].$$

Dakle,

$$\mathbb{Q}[x_0, \dots, x_{n+1}] \subseteq [\mathbb{Q} \cup \{x_0, \dots, x_{n+1}\}]. \quad (\star\star)$$

S druge strane, prema lemi 2.3.8 vrijedi

$$\mathbb{Q} \cup \{x_0, \dots, x_{n+1}\} \subseteq \mathbb{Q}[x_0, \dots, x_{n+1}].$$

Prema napomeni 2.1.24 vrijedi

$$[\mathbb{Q} \cup \{x_0, \dots, x_{n+1}\}] \subseteq \mathbb{Q}[x_0, \dots, x_{n+1}]. \quad (\star\star\star)$$

Iz  $(\star\star)$  i  $(\star\star\star)$  slijedi  $(\star)$ .

Time je tvrdnja propozicije dokazana.

□

**Propozicija 2.3.10.** *Skup svih kvadratnih radikala je potpolje od  $(\mathbb{R}, +, \cdot)$ .*

*Dokaz.* Neka su  $a$  i  $b$  kvadratni radikali. Tada postoje korijenski nizovi  $x_0, \dots, x_n$  i  $y_0, \dots, y_m$  takvi da je  $a \in \mathbb{Q}[x_0, \dots, x_n]$  i  $b \in \mathbb{Q}[y_0, \dots, y_m]$ .

Tvrdimo da je  $x_0, \dots, x_n, y_0, \dots, y_m$  korijenski niz.

Očito je  $x_0^2 \in \mathbb{Q}$  odnosno  $x_{i+1}^2 \in \mathbb{Q}[x_0, \dots, x_i]$  za svaki  $i \in \{0, \dots, n-1\}$ .

Znamo da je  $y_0^2 \in \mathbb{Q}$  pa iz leme 2.3.8 slijedi da je  $y_0^2 \in \mathbb{Q}[x_0, \dots, x_n]$ .

Neka je  $i \in \{0, \dots, m-1\}$ . Koristeći propoziciju 2.3.9 i napomenu 2.3.7 dobivamo

$$\begin{aligned} y_{i+1}^2 \in \mathbb{Q}[y_0, \dots, y_i] &= [\mathbb{Q} \cup \{y_0, \dots, y_i\}] \subseteq [\mathbb{Q} \cup \{x_0, \dots, x_n, y_0, \dots, y_i\}] \\ &= \mathbb{Q}[x_0, \dots, x_n, y_0, \dots, y_i]. \end{aligned}$$

Dakle,  $y_{i+1}^2 \in \mathbb{Q}[x_0, \dots, x_n, y_0, \dots, y_i]$ . Prema tome,  $x_0, \dots, x_n, y_0, \dots, y_m$  je korijenski niz.

Iz propozicije 2.3.9 i napomene 2.3.7 slijedi

$$\begin{aligned} \mathbb{Q}[x_0, \dots, x_n] &= [\mathbb{Q} \cup \{x_0, \dots, x_n\}] \subseteq [\mathbb{Q} \cup \{x_0, \dots, x_n, y_0, \dots, y_m\}] \\ &= \mathbb{Q}[x_0, \dots, x_n, y_0, \dots, y_m]. \end{aligned}$$

Dakle,  $\mathbb{Q}[x_0, \dots, x_n] \subseteq \mathbb{Q}[x_0, \dots, x_n, y_0, \dots, y_m]$ .

Analogno dobivamo  $\mathbb{Q}[y_0, \dots, y_m] \subseteq \mathbb{Q}[x_0, \dots, x_n, y_0, \dots, y_m]$ .

Iz prethodnih dviju inkluzija slijedi  $a, b \in \mathbb{Q}[x_0, \dots, x_n, y_0, \dots, y_m]$ .

Budući da je  $\mathbb{Q}[x_0, \dots, x_n, y_0, \dots, y_m]$  potprsten od  $(\mathbb{R}, +, \cdot)$ ,  $a-b \in \mathbb{Q}[x_0, \dots, x_n, y_0, \dots, y_m]$  i  $a \cdot b \in \mathbb{Q}[x_0, \dots, x_n, y_0, \dots, y_m]$ . Stoga su  $a-b$  i  $a \cdot b$  kvadratni radikali.

Pretpostavimo da je  $a$  kvadratni radikal te da je  $a \neq 0$ . Tada postoji korijenski niz  $x_0, \dots, x_n$  takav da je  $a \in \mathbb{Q}[x_0, \dots, x_n]$ . Prema propoziciji 2.3.4  $\mathbb{Q}[x_0, \dots, x_n]$  je potpolje od  $(\mathbb{R}, +, \cdot)$ . Iz propozicije 2.2.9 slijedi da je  $a^{-1} \in \mathbb{Q}[x_0, \dots, x_n]$ . Stoga je  $a^{-1}$  kvadratni radikal.

Prema napomeni 2.3.6 skup  $\mathbb{Q}$  je skup kvadratnih radikala. Stoga skup svih kvadratnih radikala ima barem dva elementa.

Iz propozicije 2.2.9 slijedi tvrdnja propozicije. □

**Propozicija 2.3.11.** *Neka je  $a$  kvadratni radikal,  $a \geq 0$ . Tada je  $\sqrt{a}$  kvadratni radikal.*

*Dokaz.* Budući da je  $a$  kvadratni radikal, postoji korijenski niz  $x_0, \dots, x_n$  takav da je

$$a \in \mathbb{Q}[x_0, \dots, x_n].$$

Vrijedi  $x_0^2 \in \mathbb{Q}$ ,  $x_{i+1}^2 \in \mathbb{Q}[x_0, \dots, x_i]$ , za svaki  $i \in \{0, \dots, n-1\}$  i  $(\sqrt{a})^2 \in \mathbb{Q}[x_0, \dots, x_n]$  jer je  $(\sqrt{a})^2 = a$ . Prema tome,  $x_0, \dots, x_n, \sqrt{a}$  je korijenski niz.

Prema lemi 2.3.8 vrijedi  $\sqrt{a} \in \mathbb{Q}[x_0, \dots, x_n, \sqrt{a}]$ , iz čega zaključujemo da je  $\sqrt{a}$  kvadratni radikal.  $\square$



## Poglavlje 3

# Algebarska svojstva konstruktibilnih brojeva

### 3.1 Jednadžba pravca i kvadratni radikali

**Propozicija 3.1.1.** *Neka je  $p$  pravac. Tada postoje  $a, b, c \in \mathbb{R}$ ,  $a \neq 0$  ili  $b \neq 0$ , takvi da za sve  $x, y \in \mathbb{R}$  vrijedi*

*$(x, y)$  je element pravca  $p$  ako i samo ako vrijedi  $ax + by + c = 0$ .*

*Dokaz.* Postoje  $T, v \in \mathbb{R}^2$ ,  $v \neq (0, 0)$  takvi da je  $p = \{T + \lambda \cdot v \mid \lambda \in \mathbb{R}\}$ . Imamo  $T = (t_1, t_2)$  i  $v = (v_1, v_2)$ , gdje su  $t_1, t_2, v_1, v_2 \in \mathbb{R}$ . Slijedi  $p = \{(t_1, t_2) + \lambda \cdot (v_1, v_2) \mid \lambda \in \mathbb{R}\}$ .

Dakle,

$$p = \{(t_1 + \lambda \cdot v_1, t_2 + \lambda \cdot v_2) \mid \lambda \in \mathbb{R}\}. \quad (\boxplus)$$

*1. slučaj:*  $v_1 \neq 0$  i  $v_2 \neq 0$ .

Neka su  $x, y \in \mathbb{R}$ . Pretpostavimo da je  $(x, y) \in p$ . Tada prema  $(\boxplus)$  postoji  $\lambda \in \mathbb{R}$  takav da je

$$(x, y) = (t_1 + \lambda \cdot v_1, t_2 + \lambda \cdot v_2)$$

tj.

$$x = t_1 + \lambda \cdot v_1,$$

$$y = t_2 + \lambda \cdot v_2.$$

Slijedi

$$\lambda = \frac{x - t_1}{v_1} \quad \text{i} \quad \lambda = \frac{y - t_2}{v_2},$$



pa je

$$\frac{x - t_1}{v_1} = \frac{y - t_2}{v_2}. \quad (1)$$

Stoga je

$$v_2x - v_2t_1 = v_1y - v_1t_2 \quad (2)$$

iz čega slijedi

$$v_2x - v_1y - v_2t_1 + v_1t_2 = 0. \quad (3)$$

Dakle, ako je  $(x, y) \in p$ , onda vrijedi (3).

Obratno, pretpostavimo da vrijedi (3). Tada vrijedi (2), pa i (1). Definirajmo  $\lambda \in \mathbb{R}$  s  $\lambda = \frac{x-t_1}{v_1}$ . Iz (1) slijedi

$$\lambda = \frac{x - t_1}{v_1} \quad \text{i} \quad \lambda = \frac{y - t_2}{v_2}$$

pa je

$$\begin{aligned} x &= t_1 + \lambda \cdot v_1, \\ y &= t_2 + \lambda \cdot v_2. \end{aligned}$$

Dakle,  $(x, y) = (t_1 + \lambda \cdot v_1, t_2 + \lambda \cdot v_2)$ . Iz (⊕) slijedi da je  $(x, y) \in p$ .

Dakle, dokazali smo sljedeće:

$(x, y) \in p$  ako i samo vrijedi (3). Ako stavimo

$$\begin{aligned} a &= v_2, \\ b &= -v_1, \\ c &= -v_2t_1 + v_1t_2, \end{aligned}$$

onda imamo da je  $(x, y) \in p$  ako i samo ako vrijedi  $ax + by + c = 0$ .

2. slučaj:  $v_1 = 0$ .

Tada je  $v_2 \neq 0$  jer je  $v \neq (0, 0)$ .

Neka su  $x, y \in \mathbb{R}$ . Pretpostavimo da je  $(x, y) \in p$ . Tada prema (⊕) postoji  $\lambda \in \mathbb{R}$  takav da je

$$(x, y) = (t_1 + \lambda \cdot v_1, t_2 + \lambda \cdot v_2)$$

tj.

$$\begin{aligned}x &= t_1, \\y &= t_2 + \lambda \cdot v_2.\end{aligned}$$

Dakle, ako je  $(x, y) \in p$  onda je  $x = t_1$ .

Obratno, pretpostavimo da su  $x, y \in \mathbb{R}$  takvi da je  $x = t_1$ . Definirajmo  $\lambda \in \mathbb{R}$  s  $\lambda = \frac{y-t_2}{v_2}$ . Tada je  $y = t_2 + \lambda \cdot v_2$  pa je

$$\begin{aligned}(x, y) &= (t_1, t_2 + \lambda \cdot v_2) \text{ tj.} \\(x, y) &= (t_1 + \lambda \cdot v_1, t_2 + \lambda \cdot v_2).\end{aligned}$$

Iz (⊕) slijedi da je  $(x, y) \in p$ .

Prema tome,  $(x, y) \in p$  ako i samo ako je  $x = t_1$ .

Definirajmo

$$\begin{aligned}a &= 1, \\b &= 0, \\c &= -t_1.\end{aligned}$$

Tada je  $x = t_1$  ako i samo ako je  $ax + by + c = 0$ .

Prema tome,  $(x, y) \in p$  ako i samo ako  $ax + by + c = 0$ .

3. slučaj:  $v_2 = 0$ .

Tada je  $v_1 \neq 0$  jer je  $v \neq (0, 0)$ .

Neka su  $x, y \in \mathbb{R}$ . Pretpostavimo da je  $(x, y) \in p$ . Tada prema (⊕) postoji  $\lambda \in \mathbb{R}$  takav da je

$$(x, y) = (t_1 + \lambda \cdot v_1, t_2 + \lambda \cdot v_2)$$

tj.

$$\begin{aligned}x &= t_1 + \lambda \cdot v_1, \\y &= t_2.\end{aligned}$$

Dakle, ako je  $(x, y) \in p$  onda je  $y = t_2$ .

Obratno, pretpostavimo da su  $x, y \in \mathbb{R}$  takvi da je  $y = t_2$ . Definirajmo  $\lambda \in \mathbb{R}$  s  $\lambda = \frac{x-t_1}{v_1}$ . Tada je  $x = t_1 + \lambda \cdot v_1$  pa je

$$\begin{aligned}(x, y) &= (t_1 + \lambda \cdot v_1, t_2) \text{ tj.} \\(x, y) &= (t_1 + \lambda \cdot v_1, t_2 + \lambda \cdot v_2).\end{aligned}$$

Iz (⊞) slijedi da je  $(x, y) \in p$ .

Prema tome,  $(x, y) \in p$  ako i samo ako je  $y = t_2$ .

Definirajmo

$$\begin{aligned} a &= 0, \\ b &= 1, \\ c &= -t_2. \end{aligned}$$

Tada je  $(x, y) \in p$  ako i samo ako  $ax + by + c = 0$ .

Time je propozicija dokazana. □

**Napomena 3.1.2.** Neka su  $A, B \in \mathbb{R}^2$ ,  $A \neq B$ , takvi da su  $A = (x_1, y_1)$ ,  $B = (x_2, y_2)$ , gdje su  $x_1, y_1, x_2, y_2$  kvadratni radikali. Tada postoje kvadratni radikali  $a, b, c$  takvi da je  $ax + by + c = 0$  jednačba pravca  $AB$  tj. takvi da je  $a \neq 0$  ili  $b \neq 0$  te za svaki  $(x, y) \in \mathbb{R}^2$  vrijedi  $ax + by + c = 0$ .

Prema napomeni 1.1.6 vrijedi

$$AB = \{A + \lambda \cdot (B - A) \mid \lambda \in \mathbb{R}\}.$$

Označimo  $T = A$  i  $v = B - A$ .

Imamo  $T = (t_1, t_2)$ ,  $v = (v_1, v_2)$  iz čega slijedi da su

$$\begin{aligned} t_1 &= x_1, \quad t_2 = y_1, \\ v_1 &= x_2 - x_1, \quad v_2 = y_2 - y_1. \end{aligned}$$

Očito su  $t_1, t_2$  kvadratni radikali, a iz propozicije 2.3.10 slijedi da su i  $v_1, v_2$  kvadratni radikali.

Znamo da je  $AB = \{A + \lambda \cdot v \mid \lambda \in \mathbb{R}\}$ . Iz dokaza propozicije 3.1.1 slijedi da postoje  $a, b, c \in \mathbb{R}$  takvi da je  $ax + by + c = 0$  jednačba pravca  $AB$ , pri čemu se  $a, b, c$  mogu izraziti kao zbroj i produkt brojeva  $t_1, t_2, v_1, v_2$ .

Iz propozicije 2.3.10 slijedi da su  $a, b, c$  kvadratni radikali.

**Propozicija 3.1.3.** Neka su  $p_1, p_2$  pravci takvi da je  $p_1 \neq p_2$  i  $p_1 \cap p_2 \neq \emptyset$ . Neka je  $a_1x + b_1y + c_1 = 0$  jednačba pravca  $p_1$ , a  $a_2x + b_2y + c_2 = 0$  jednačba pravca  $p_2$ . Tada je  $a_1 \neq 0$  ili  $a_2 \neq 0$  te je  $b_1a_2 - a_1b_2 \neq 0$ .

*Dokaz.* Odaberimo  $T \in p_1 \cap p_2$ . Imamo  $T = (x_0, y_0)$ .

Uočimo da ne postoji  $T' \neq T$  takav da je  $T' \in p_1 \cap p_2$ . U suprotnom bi  $p_1, p_2$  bili različiti pravci koji bi sadržavali točke  $T$  i  $T'$ , što je nemoguće prema propoziciji 1.1.4.

Pretpostavimo da su  $a_1 = 0$  i  $a_2 = 0$ .

Tada su  $b_1 \neq 0$  i  $b_2 \neq 0$  te je

$$b_1y + c_1 = 0 \text{ jednadžba pravca } p_1,$$

$$b_2y + c_2 = 0 \text{ jednadžba pravca } p_2.$$

Dakle,

$$y = -\frac{c_1}{b_1} \text{ je jednadžba pravca } p_1,$$

$$y = -\frac{c_2}{b_2} \text{ je jednadžba pravca } p_2.$$

Iz činjenice da je  $T \in p_1$  i  $T \in p_2$  slijedi

$$y_0 = -\frac{c_1}{b_1} \text{ i } y_0 = -\frac{c_2}{b_2}$$

pa je

$$-\frac{c_1}{b_1} = -\frac{c_2}{b_2}.$$

Slijedi da je  $p_1 = p_2$ , što je u kontradikciji s pretpostavkom propozicije.

Prema tome,  $a_1 \neq 0$  ili  $a_2 \neq 0$ .

Pretpostavimo da je  $a_1 = 0$ .

Tada je  $b_1 \neq 0$  i  $a_2 \neq 0$  pa je  $b_1a_2 - a_1b_2 = b_1a_2 \neq 0$ .

Analogno dobivamo da je  $b_1a_2 - a_1b_2 = -a_1b_2 \neq 0$  ako je  $a_2 = 0$ .

Pretpostavimo da je  $a_1 \neq 0$  i  $a_2 \neq 0$ .

Iz  $T \in p_1$  i  $T \in p_2$  slijedi

$$a_1x_0 + b_1y_0 + c_1 = 0,$$

$$a_2x_0 + b_2y_0 + c_2 = 0.$$

Množenjem prve jednakosti s  $a_1$ , a druge jednakosti s  $a_2$  te oduzimanjem dobivamo

$$(b_1a_2 - a_1b_2)y_0 + c_1a_2 - a_1c_2 = 0. \quad (\oplus)$$

Pretpostavimo da je

$$b_1a_2 - a_1b_2 = 0. \quad (\oplus\oplus)$$

Iz  $(\oplus)$  slijedi da je

$$c_1a_2 - a_1c_2 = 0. \quad (\oplus\oplus\oplus)$$

Odaberimo  $y_1 \in \mathbb{R}$  takav da je  $y_1 \neq y_0$ .

Iz  $(\oplus\oplus)$  i  $(\oplus\oplus\oplus)$  slijedi da je

$$(b_1a_2 - a_1b_2)y_1 + c_1a_2 - a_1c_2 = 0.$$

Množenjem prethodne jednakosti s  $-1$  i sređivanjem dobivamo

$$-b_1a_2y_1 + a_1b_2y_1 - c_1a_2 + a_1c_2 = 0. \quad (\diamond)$$

Definirajmo  $x_1 = \frac{-(b_1y_1 + c_1)}{a_1}$ .

Tada vrijedi

$$a_1x_1 + b_1y_1 + c_1 = 0 \quad (\diamond\diamond)$$

Stoga je  $(x_1, y_1) \in p_1$ . Tvrdimo da je  $(x_1, y_1) \in p_2$ .

Množenjem jednakosti  $(\diamond\diamond)$  s  $a_2$  dobivamo

$$a_1a_2x_1 + b_1a_2y_1 + c_1a_2 = 0. \quad (\diamond\diamond\diamond)$$

Zbrajanjem  $(\diamond)$  i  $(\diamond\diamond\diamond)$  dobivamo

$$a_1a_2x_1 + a_1b_2y_1 + a_1c_2 = 0.$$

Dijeljenjem prethodne jednakosti s  $a_1$  dobivamo

$$a_2x_1 + b_2y_1 + c_2 = 0.$$

Dakle,  $(x_1, y_1) \in p_2$ .

Prema tome,  $(x_1, y_1) \in p_1 \cap p_2$ , a očito je  $(x_1, y_1) \neq T$  (jer je  $y_1 \neq y_0$ ), no kao što smo vidjeli, to je nemoguće.

Zaključak:  $b_1a_2 - a_1b_2 \neq 0$ . □

## 3.2 Konstruktibilni brojevi i kvadratni radikali

**Lema 3.2.1.** *Neka su  $a, b, c$  kvadratni radikali takvi da je  $a \neq 0$ . Neka je  $x \in \mathbb{R}$  takav da je  $ax^2 + bx + c = 0$ . Tada je  $x$  kvadratni radikal.*

*Dokaz.* Budući da je  $x$  rješenje kvadratne jednadžbe, mora vrijediti

$$x = \frac{-b + \sqrt{b^2 - 4ac}}{2a}$$

ili

$$x = \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

U oba slučaja, zbog propozicija 2.3.10 i 2.3.11, vrijedi da je  $x$  kvadratni radikal. □

**Teorem 3.2.2.** *Svaki konstruktibilan broj je kvadratni radikal.*

*Dokaz.* Dovoljno je dokazati sljedeće:

ako je  $T$  konstruktibilna točka, onda su koordinate točke  $T$  kvadratni radikali.

Neka je  $S = \{(0, 0), (1, 0)\}$ . Ako je  $T$  konstruktibilna točka, onda se  $T$  može konstruirati iz skupa  $S$ , dakle postoji  $n \in \mathbb{N}$  takav da je  $T \in S^{(n)}$ .

Stoga je dovoljno dokazati sljedeće:

za svaki  $n \in \mathbb{N}_0$  i za svaki  $T \in S^{(n)}$  koordinate točke  $T$  su kvadratni radikali.

Dokažimo ovu tvrdnju indukcijom po  $n$ .

Za  $n = 0$  tvrdnja je jasna jer su brojevi 0 i 1 kvadratni radikali (prema napomeni 2.3.6).

Pretpostavimo da je  $n \in \mathbb{N}_0$  te da su koordinate svake točke  $T \in S^{(n)}$  kvadratni radikali.

Neka je  $T \in S^{(n+1)}$ . Tvrdimo da su koordinate točke  $T$  kvadratni radikali. Iz  $T \in S^{(n+1)}$  slijedi da je  $T$  točka određena skupom  $S^{(n)}$ .

Imamo tri slučaja:

1. postoje pravci  $p_1, p_2$  određeni skupom  $S^{(n)}$  takvi da je  $p_1 \neq p_2$  te  $T \in p_1 \cap p_2$ ,
2. postoje pravac  $p$  i kružnica  $k$  određeni skupom  $S^{(n)}$  takvi da je  $T \in p \cap k$ ,
3. postoje kružnice  $k_1, k_2$  određene skupom  $S^{(n)}$  takve da je  $k_1 \neq k_2$  i  $T \in k_1 \cap k_2$ .

Promotrimo prvi slučaj.

Imamo  $p_1 = AB$ , gdje su  $A, B \in S^{(n)}$ ,  $A \neq B$ .

Prema induktivnoj pretpostavci koordinate točaka  $A$  i  $B$  su kvadratni radikali. Iz napomene 3.1.2 slijedi da postoje kvadratni radikali  $a_1, b_1, c_1$  takvi da je  $a_1x + b_1y + c_1 = 0$  jednačba pravca  $p_1$ .

Analogno postoje kvadratni radikali  $a_2, b_2, c_2$  takvi da je  $a_2x + b_2y + c_2 = 0$  jednačba pravca  $p_2$ .

Imamo  $T = (x_0, y_0)$ , gdje su  $x_0, y_0 \in \mathbb{R}$ .

S obzirom da je  $T \in p_1 \cap p_2$  slijedi da vrijedi

$$a_1x_0 + b_1y_0 + c_1 = 0,$$

$$a_2x_0 + b_2y_0 + c_2 = 0.$$

Množenjem prve jednakosti s  $a_2$ , a druge s  $a_1$ , te oduzimanjem druge od prve dobivamo

$$b_1a_2y_0 - a_1b_2y_0 + c_1a_2 - a_1c_2 = 0,$$

što je ekvivalentno s

$$(b_1a_2 - a_1b_2)y_0 + c_1a_2 - a_1c_2 = 0.$$

Prema propoziciji 3.1.3 znamo da je  $b_1a_2 - a_1b_2 \neq 0$ .

Slijedi

$$y_0 = (c_1a_2 - a_1c_2)(b_1a_2 - a_1b_2)^{-1}.$$

Prema propoziciji 2.3.10 slijedi da je  $y_0$  kvadratni radikal.

Iz propozicije 3.1.3 slijedi da je  $a_1 \neq 0$  ili  $a_2 \neq 0$ . Ako je  $a_1 \neq 0$ , onda iz  $a_1x_0 + b_1y_0 + c_1 = 0$  slijedi da je

$$x_0 = (-b_1y_0 - c_1) \cdot a_1^{-1},$$

što povlači da je  $x_0$  kvadratni radikal.

Ako je  $a_2 \neq 0$ , onda iz  $a_2x_0 + b_2y_0 + c_2 = 0$  slijedi da je

$$x_0 = (-b_2y_0 - c_2) \cdot a_2^{-1},$$

što znači da je  $x_0$  kvadratni radikal.

Dakle, koordinate točke  $T$  su kvadratni radikali.

Promotrimo sada drugi slučaj.

Analogno kao u prethodnom slučaju zaključujemo da postoje kvadratni radikali  $a, b, c$  takvi da je  $ax + by + c = 0$  jednadžba pravca  $p$ .

Budući da je  $k$  kružnica određena sa  $S^{(n)}$ , postoje  $R, T_1 \in S^{(n)}$  takvi da je  $k = K(R, d(R, T_1))$ . Prema induktivnoj pretpostavci postoje kvadratni radikali  $u, v, u_1, v_1$  takvi da je

$$R = (u, v), T_1 = (u_1, v_1).$$

Označimo  $r = d(R, T_1)$ . Vrijedi  $r = \sqrt{(u_1 - u)^2 + (v_1 - v)^2}$ . Iz propozicija 2.3.10 i 2.3.11 slijedi da je  $r$  kvadratni radikal.

Imamo  $T = (x_0, y_0)$  gdje su  $x_0, y_0 \in \mathbb{R}$ .

Iz  $k = K(R, r)$  i  $T \in k$  slijedi da je  $d(T, R) = r$  tj.

$$\sqrt{(u - x_0)^2 + (v - y_0)^2} = r.$$

Dakle,

$$(u - x_0)^2 + (v - y_0)^2 = r^2. \quad (\star\star)$$

S druge strane, iz  $T \in p$  slijedi

$$ax_0 + by_0 + c = 0. \quad (\star)$$

Znamo da je  $a \neq 0$  ili  $b \neq 0$ .

Pretpostavimo da je  $a \neq 0$ . Tada iz  $(\star)$  slijedi da je

$$x_0 = \frac{-by_0 - c}{a}. \quad (\Delta)$$

Uvrštavanjem prethodne jednakosti u  $(\star\star)$  dobivamo

$$\left[ u - \left( \frac{-by_0 - c}{a} \right) \right]^2 + (v - y_0)^2 = r^2,$$

što je ekvivalentno

$$\left[ \frac{b}{a}y_0 + \left( u + \frac{c}{a} \right) \right]^2 + (v - y_0)^2 = r^2.$$

Slijedi

$$\left( \frac{b}{a} \right)^2 y_0^2 + 2 \frac{b}{a} \left( u + \frac{c}{a} \right) y_0 + \left( u + \frac{c}{a} \right)^2 + v^2 - 2vy_0 + y_0^2 = r^2$$



tj.

$$\left[\left(\frac{b}{a}\right)^2 + 1\right]y_0^2 + \left[2\frac{b}{a}\left(u + \frac{c}{a}\right) - 2v\right]y_0 + \left(u + \frac{c}{a}\right)^2 + v^2 - r^2 = 0.$$

Označimo

$$A = \left(\frac{b}{a}\right)^2 + 1,$$

$$B = 2\frac{b}{a}\left(u + \frac{c}{a}\right) - 2v,$$

$$C = \left(u + \frac{c}{a}\right)^2 + v^2 - r^2.$$

Prema propoziciji 2.3.10 slijedi da su  $A, B, C$  kvadratni radikali. Očito je  $A \neq 0$  pa iz leme 3.2.1 slijedi da je  $y_0$  kvadratni radikal. Iz  $(\Delta)$  slijedi da je  $x_0$  kvadratni radikal.

Zaključujemo da su koordinate točke  $T$  kvadratni radikali. Do ovog zaključka dolazimo na isti način i u slučaju  $b \neq 0$ .

Promotrimo sada treći slučaj.

Kao u prethodnom slučaju zaključujemo da postoje kvadratni radikali  $u_1, v_1, u_2, v_2, r_1, r_2$  takvi da je  $r_1 > 0, r_2 > 0$  i

$$k_1 = K((u_1, v_1), r_1),$$

$$k_2 = K((u_2, v_2), r_2).$$

Tvrdimo da je

$$(u_1, v_1) \neq (u_2, v_2) \quad (\triangleleft)$$

Pretpostavimo suprotno tj.  $(u_1, v_1) = (u_2, v_2)$ .

Iz  $T \in k_1$  slijedi da je

$$d(T, (u_1, v_1)) = r_1,$$

a iz  $T \in k_2$  da je

$$d(T, (u_2, v_2)) = r_2.$$

Stoga je  $r_1 = r_2$  pa je  $k_1 = k_2$ , što je nemoguće jer je  $k_1 \neq k_2$ .  
Prema tome je  $(u_1, v_1) \neq (u_2, v_2)$ .

Imamo  $T = (x_0, y_0)$ , gdje su  $x_0, y_0 \in \mathbb{R}$ .

Iz  $T \in k_1$  slijedi da je  $d(T, (u_1, v_1)) = r_1$ , pa je

$$\sqrt{(u_1 - x_0)^2 + (v_1 - y_0)^2} = r_1,$$

tj.

$$(u_1 - x_0)^2 + (v_1 - y_0)^2 = r_1^2. \quad (1)$$

Iz  $T \in k_2$  analogno slijedi

$$(u_2 - x_0)^2 + (v_2 - y_0)^2 = r_2^2. \quad (2)$$

Kvadriranjem (1) i (2) dobivamo

$$u_1^2 - 2u_1x_0 + x_0^2 + v_1^2 - 2v_1y_0 + y_0^2 = r_1^2,$$

$$u_2^2 - 2u_2x_0 + x_0^2 + v_2^2 - 2v_2y_0 + y_0^2 = r_2^2.$$

Oduzimanjem ovih dviju jednakosti dobivamo

$$(2u_2 - 2u_1)x_0 + u_1^2 - u_2^2 + (2v_2 - 2v_1)y_0 + v_1^2 - v_2^2 = r_1^2 - r_2^2.$$

Označimo

$$a = 2u_2 - 2u_1,$$

$$b = 2v_2 - 2v_1,$$

$$c = u_1^2 - u_2^2 + v_1^2 - v_2^2 - (r_1^2 - r_2^2).$$

Tada je

$$ax_0 + by_0 + c = 0 \quad (3)$$

Uočimo da su  $a, b, c$  kvadratni radikali.

Iz ( $\Leftarrow$ ) slijedi da je  $u_1 \neq u_2$  ili  $v_1 \neq v_2$  pa je  $a \neq 0$  ili  $b \neq 0$ .

Sada iz (3) i (1), na isti način kao i u prethodnom slučaju, dobivamo da su  $x_0$  i  $y_0$  kvadratni radikali. Dakle, koordinate točke  $T$  su kvadratni radikali.

Zaključak: koordinate svake točke iz  $S^{(n+1)}$  su kvadratni radikali.

Time je tvrdnja teorema dokazana. □

### 3.3 Polinomi

**Definicija 3.3.1.** Za funkciju  $f : \mathbb{R} \rightarrow \mathbb{R}$  kažemo da je polinom ako postoje  $n \in \mathbb{N}_0$  i  $a_0, \dots, a_n \in \mathbb{R}$  takvi da je  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ , za svaki  $x \in \mathbb{R}$ .

**Teorem 3.3.2.** Neka su  $n \in \mathbb{N}$  i  $a_0, \dots, a_n \in \mathbb{R}$ . Neka je  $f : \mathbb{R} \rightarrow \mathbb{R}$  funkcija definirana s  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ , za svaki  $x \in \mathbb{R}$ . Pretpostavimo da je  $f(x) = 0$  za svaki  $x \in \mathbb{R}$ . Tada je

$$a_n = a_{n-1} = \dots = a_1 = a_0 = 0. \quad (\blacktriangleleft)$$

*Dokaz.* Za  $x = 0$  dobivamo

$$0 = f(0) = a_n 0^n + \dots + a_1 0 + a_0,$$

iz čega slijedi  $a_0 = 0$ .

Pretpostavimo sada da ( $\blacktriangleleft$ ) ne vrijedi tj. da postoji  $i \in \{1, \dots, n\}$  takav da je  $a_i \neq 0$ . Neka je  $p = \min\{i \in \{1, \dots, n\} \mid a_i \neq 0\}$ . Tada je  $a_p \neq 0$  i  $a_0 = \dots = a_{p-1} = 0$ . Stoga je

$$f(x) = a_n x^n + \dots + a_p x^p, \text{ za svaki } x \in \mathbb{R}. \quad (\nabla)$$

Uočimo da je  $p < n$ . Naime, u suprotnom bi za svaki  $x \in \mathbb{R}$  vrijedilo  $f(x) = a_p x^p$  pa bismo posebno za  $x = 1$  dobili  $0 = f(1) = a_p$ , što je u kontradikciji s  $a_p \neq 0$ .

Neka je  $x \in \mathbb{R}$ ,  $x \neq 0$ . Koristeći ( $\nabla$ ) dobivamo

$$\begin{aligned} 0 = f(x) &= a_n x^n + \dots + a_p x^p \\ &= x^p (a_n x^{n-p} + \dots + a_p). \end{aligned}$$

Dakle,  $x^p (a_n x^{n-p} + \dots + a_p) = 0$ , pa zbog  $x^p \neq 0$  slijedi da je

$$a_n x^{n-p} + \dots + a_p = 0.$$

Dakle,  $a_n x^{n-p} + \dots + a_{p+1} x + a_p = 0$ , za svaki  $x \in \mathbb{R}$ ,  $x \neq 0$ . Iz prethodne jednakosti slijedi

$$(a_n x^{n-p-1} + \dots + a_{p+2} x + a_{p+1}) x = -a_p, \text{ za svaki } x \in \mathbb{R}, x \neq 0. \quad (\nabla\nabla)$$

Uočimo da iz prethodne jednakosti i  $a_p \neq 0$  slijedi da ne mogu svi brojevi  $a_n, \dots, a_{p+1}$  biti jednaki 0.

Definirajmo  $M = |a_n| + \dots + |a_{p+1}|$ . Uočimo da je  $M > 0$ .  
Odaberimo  $x \in \mathbb{R}$  takav da je

$$0 < x < \min \left\{ \frac{|a_p|}{2M}, 1 \right\}.$$

Iz  $x < \frac{|a_p|}{2M}$  slijedi  $M \cdot x < \frac{|a_p|}{2}$ .

Koristeći ovo,  $x < 1$  i  $|x| = x$  (jer je  $x > 0$ ) dobivamo

$$\begin{aligned} \left| (a_n x^{n-p-1} + \dots + a_{p+2} x + a_{p+1}) x \right| &= |a_n x^{n-p-1} + \dots + a_{p+2} x + a_{p+1}| \cdot |x| \\ &\leq (|a_n x^{n-p-1}| + \dots + |a_{p+2} x| + |a_{p+1}|) \cdot |x| \\ &= (|a_n| \cdot |x|^{n-p-1} + \dots + |a_{p+2}| \cdot |x| + |a_{p+1}|) \cdot |x| \\ &\leq (|a_n| + \dots + |a_{p+2}| + |a_{p+1}|) \cdot |x| \\ &= M \cdot x < \frac{|a_p|}{2}. \end{aligned}$$

Dakle,

$$\left| (a_n x^{n-p-1} + \dots + a_{p+2} x + a_{p+1}) x \right| < \frac{|a_p|}{2}.$$

No, iz  $(\nabla\nabla)$  slijedi

$$\left| (a_n x^{n-p-1} + \dots + a_{p+2} x + a_{p+1}) x \right| = |a_p|,$$

što je u kontradikciji s prethodnom nejednakošću.

Time je tvrdnja teorema dokazana. □

**Korolar 3.3.3.** Neka su  $m, n \in \mathbb{N}_0$  te neka su  $a_0, \dots, a_m, b_0, \dots, b_n \in \mathbb{R}$  takvi da je  $a_m \neq 0$  i  $b_n \neq 0$ . Pretpostavimo da za svaki  $x \in \mathbb{R}$  vrijedi

$$a_m x^m + \dots + a_1 x + a_0 = b_n x^n + \dots + b_1 x + b_0. \quad (\because)$$

Tada je  $m = n$  i  $a_i = b_i$ , za svaki  $i \in \{0, \dots, m\}$ .

*Dokaz.* Pretpostavimo da je  $m > n$ .

Iz  $(\because)$  slijedi

$$a_m x^m + \dots + a_{n+1} x^{n+1} + (a_n - b_n) x^n + \dots + (a_1 - b_1) x + (a_0 - b_0) = 0, \text{ za svaki } x \in \mathbb{R}.$$

Iz teorema 3.3.2 slijedi da je  $a_m = 0$ , što je u kontradikciji s pretpostavkom korolara. Na isti način vidimo da pretpostavka da je  $m < n$  također vodi do kontradikcije. Dakle,  $m = n$ .

Sada iz (.) slijedi

$$(a_m - b_m)x^m + \cdots + (a_1 - b_1)x + (a_0 - b_0) = 0.$$

Iz teorema 3.3.2 slijedi

$$a_m - b_m = \cdots = a_1 - b_1 = a_0 - b_0 = 0.$$

Stoga je  $a_m = b_m, \dots, a_1 = b_1, a_0 = b_0$ . □

**Definicija 3.3.4.** *Neka je  $f : \mathbb{R} \rightarrow \mathbb{R}$  funkcija definirana s  $f(x) = 0$ , za svaki  $x \in \mathbb{R}$ . Takvu funkciju nazivamo nulpolinom.*

Uočimo da je nulpolinom zaista polinom zato što možemo uzeti bilo koji  $n \in \mathbb{N}_0$  i  $a_0 = \cdots = a_n = 0$ .

Uočimo da iz korolara 3.3.3 slijedi da za svaki polinom  $f$ , različit od nulpolinoma, postoje jedinstveni  $n \in \mathbb{N}_0$  i  $a_0, \dots, a_n \in \mathbb{R}$  takvi da je

$$a_n \neq 0 \text{ i } f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \text{ za svaki } x \in \mathbb{R}.$$

Naime, ako je  $f$  različit od nulpolinoma, onda po definiciji polinoma postoje  $k \in \mathbb{N}_0$  i  $a_0, \dots, a_k \in \mathbb{R}$  takvi da je  $f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$ , za svaki  $x \in \mathbb{R}$ .

Neka je  $n = \max\{i \in \{0, \dots, k\} \mid a_i \neq 0\}$  (uočimo da je ova definicija dobra jer sigurno postoji  $i \in \{0, \dots, k\}$  takav da je  $a_i \neq 0$ , što slijedi iz činjenice da  $f$  nije nulpolinom).

Tada je

$$a_n \neq 0 \text{ i } a_{n+1} = \cdots = a_k = 0.$$

Za svaki  $x \in \mathbb{R}$  vrijedi

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_{n+1} x^{n+1} + a_n x^n + \cdots + a_1 x + a_0.$$

Uočimo da ustvari vrijedi  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ , za svaki  $x \in \mathbb{R}$ .

Time smo pokazali da postoje  $n \in \mathbb{N}_0$  i  $a_0, \dots, a_n \in \mathbb{R}$ ,  $a_n \neq 0$ , takvi da je  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ , a jedinstvenost slijedi iz korolara 3.3.3.

Za  $n$  kažemo da je stupanj polinoma  $f$ . Za  $a_0, \dots, a_n$  kažemo da su koeficijenti polinoma  $f$ . Za  $a_0$  kažemo da je slobodni koeficijent, a za  $a_n$  da je vodeći koeficijent polinoma  $f$ . Uočimo da smo ove pojmove definirali za polinom  $f$  koji je različit od nulpolinoma.

**Napomena 3.3.5.** Uočimo da smo dokazali sljedeće:

ako je  $f$  polinom stupnja  $n$  te  $k \in \mathbb{N}_0$  i  $a_0, \dots, a_k \in \mathbb{R}$  takvi da je  $f(x) = a_k x^k + \dots + a_1 x + a_0$ , za svaki  $x \in \mathbb{R}$ , onda je  $n \leq k$ .

**Teorem 3.3.6.** Neka je  $f$  polinom stupnja  $n$ ,  $n \in \mathbb{N}$ . Neka je  $\alpha \in \mathbb{R}$ . Tada postoje polinom  $g$  stupnja  $n - 1$  i  $r \in \mathbb{R}$  takvi da je

$$f(x) = (x - \alpha) \cdot g(x) + r, \quad \text{za svaki } x \in \mathbb{R}.$$

*Dokaz.* Dokažimo ovu tvrdnju indukcijom po  $n$ .

Za  $n = 1$  postoje  $a_0, a_1 \in \mathbb{R}$ ,  $a_1 \neq 0$  takvi da je

$$f(x) = a_1 x + a_0.$$

Za svaki  $x \in \mathbb{R}$  vrijedi

$$f(x) = a_1 x - a_1 \alpha + a_1 \alpha + a_0 = a_1(x - \alpha) + r,$$

gdje je  $r = a_1 \alpha + a_0$ .

Definirajmo funkciju  $g : \mathbb{R} \rightarrow \mathbb{R}$  s  $g(x) = a_1$ , za svaki  $x \in \mathbb{R}$ . Očito je  $g$  polinom stupnja 0. Vrijedi

$$f(x) = (x - \alpha) \cdot g(x) + r, \quad \text{za svaki } x \in \mathbb{R}.$$

Dakle, tvrdnja teorema vrijedi ako je stupanj polinoma  $f$  jednak 1.

Pretpostavimo sada da je  $n \in \mathbb{N}$  te da tvrdnja teorema vrijedi ako je  $f$  stupnja  $n$  ili stupnja manjeg od  $n$ .

Pretpostavimo da je  $f$  polinom stupnja  $n + 1$ . Tada postoje  $a_0, \dots, a_{n+1} \in \mathbb{R}$ ,  $a_{n+1} \neq 0$ , takvi da je

$$f(x) = a_{n+1} x^{n+1} + a_n x^n + \dots + a_1 x + a_0, \quad \text{za svaki } x \in \mathbb{R}.$$

Neka je  $x \in \mathbb{R}$ . Imamo

$$\begin{aligned} f(x) &= a_{n+1} x^{n+1} - a_{n+1} \alpha x^n + a_{n+1} \alpha x^n + a_n x^n + \dots + a_1 x + a_0 \\ &= a_{n+1} x^n (x - \alpha) + (a_{n+1} \alpha + a_n) x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0. \end{aligned}$$

Definirajmo  $h : \mathbb{R} \rightarrow \mathbb{R}$  s

$$h(x) = (a_{n+1}\alpha + a_n)x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

Uočimo da je  $h$  polinom. Za svaki  $x \in \mathbb{R}$  vrijedi

$$f(x) = a_{n+1}x^n(x - \alpha) + h(x). \quad (\heartsuit)$$

Definirajmo  $g : \mathbb{R} \rightarrow \mathbb{R}$  s  $g(x) = a_{n+1}x^n$ , za svaki  $x \in \mathbb{R}$ .

Imamo tri slučaja.

*1. slučaj:  $h$  je nulpolinom.*

Definirajmo  $r = 0$ . Očito je  $g$  polinom stupnja  $n$ . Iz  $(\heartsuit)$  slijedi da je

$$f(x) = (x - \alpha) \cdot g(x) + r, \quad \text{za svaki } x \in \mathbb{R}.$$

*2. slučaj:  $h$  je polinom stupnja 0.*

Tada postoji  $r \in \mathbb{R}$ ,  $r \neq 0$  takav da je  $h(x) = r$ , za svaki  $x \in \mathbb{R}$ . Iz  $(\heartsuit)$  slijedi da je

$$f(x) = (x - \alpha) \cdot g(x) + r, \quad \text{za svaki } x \in \mathbb{R}.$$

*3. slučaj:  $h$  je polinom stupnja većeg od 0.*

Iz napomene 3.3.5 slijedi da je stupanj polinoma  $h$  manji ili jednak  $n$ . Iz induktivne pretpostavke slijedi da postoje  $r \in \mathbb{R}$  i  $h'$  polinom stupnja manjeg ili jednakog  $n - 1$  takvi da je

$$h(x) = (x - \alpha) \cdot h'(x) + r, \quad \text{za svaki } x \in \mathbb{R}.$$

Neka je  $x \in \mathbb{R}$ . Iz  $(\heartsuit)$  slijedi

$$\begin{aligned} f(x) &= a_{n+1}x^n(x - \alpha) + (x - \alpha) \cdot h'(x) + r, \\ &= (x - \alpha) [a_{n+1}x^n + h'(x)] + r. \end{aligned}$$

Definirajmo  $k : \mathbb{R} \rightarrow \mathbb{R}$  s

$$k(x) = a_{n+1}x^n + h'(x).$$

Uočimo da je  $k$  polinom stupnja  $n$  (jer je  $a_{n+1} \neq 0$ ).

Dakle,

$$f(x) = (x - \alpha) \cdot k(x) + r, \quad \text{za svaki } x \in \mathbb{R}.$$

Time je tvrdnja teorema dokazana. □

**Definicija 3.3.7.** *Neka je  $f$  polinom te neka je  $x \in \mathbb{R}$  takav da je  $f(x) = 0$ . Tada kažemo da je  $x$  nultočka polinoma  $f$ .*

**Korolar 3.3.8.** Neka je  $f$  polinom stupnja  $n, n \geq 1$ . Pretpostavimo da je  $x_0$  nultočka od  $f$ . Tada postoji polinom  $g$  stupnja  $n - 1$  takav da je  $f(x) = (x - x_0) \cdot g(x)$ , za svaki  $x \in \mathbb{R}$ .

*Dokaz.* Prema teoremu 3.3.6 postoje polinom  $g$  stupnja  $n - 1$  i  $r \in \mathbb{R}$  takvi da je  $f(x) = (x - x_0) \cdot g(x) + r$ , za svaki  $x \in \mathbb{R}$ .

Uočimo da za  $x = x_0$  dobivamo  $f(x_0) = r$  tj.  $0 = r$  (jer je  $x_0$  nultočka polinoma  $f$ ). Slijedi da je  $f(x) = (x - x_0) \cdot g(x)$ , za svaki  $x \in \mathbb{R}$ .  $\square$

**Propozicija 3.3.9.** Neka su  $a, b, c \in \mathbb{R}$  te neka je  $f : \mathbb{R} \rightarrow \mathbb{R}$  funkcija definirana s

$$f(x) = x^3 + ax^2 + bx + c, \text{ za svaki } x \in \mathbb{R}.$$

Pretpostavimo da su  $x_1, x_2$  nultočke od  $f$ ,  $x_1 \neq x_2$ . Tada je  $-(x_1 + x_2) - a$  također nultočka od  $f$ .

*Dokaz.* Prema korolaru 3.3.8 postoji polinom  $g$  stupnja 2 takav da je  $f(x) = (x - x_1) \cdot g(x)$ , za svaki  $x \in \mathbb{R}$ .

Za  $x = x_2$  dobivamo  $f(x_2) = (x_2 - x_1) \cdot g(x_2)$ .

Vrijedi  $f(x_2) = 0$  i  $x_2 - x_1 \neq 0$  pa je  $g(x_2) = 0$ , tj.  $x_2$  je nultočka polinoma  $g$ .

Prema korolaru 3.3.8 postoji polinom  $h$  stupnja 1 takav da je  $g(x) = (x - x_2) \cdot h(x)$ , za svaki  $x \in \mathbb{R}$ . Slijedi

$$f(x) = (x - x_1)(x - x_2) \cdot h(x), \text{ za svaki } x \in \mathbb{R}. \quad (\boxplus)$$

Budući da je  $h$  polinom stupnja 1, postoje koeficijenti  $u, v \in \mathbb{R}$  takvi da je  $u \neq 0$  i

$$h(x) = ux + v, \text{ za svaki } x \in \mathbb{R}.$$

Neka je  $x \in \mathbb{R}$ . Slijedi

$$\begin{aligned} f(x) &= (x - x_1)(x - x_2) \cdot h(x) \\ &= (x - x_1)(x - x_2)(ux + v) \\ &= [x^2 - (x_1 + x_2)x + x_1x_2](ux + v) \\ &= ux^3 - u(x_1 + x_2)x^2 + x_1x_2ux + vx^2 - v(x_1 + x_2)x + x_1x_2v. \end{aligned}$$

Dakle,

$$f(x) = ux^3 + [v - u(x_1 + x_2)]x^2 + [x_1x_2u - v(x_1 + x_2)]x + x_1x_2v.$$



Iz definicije funkcije  $f$  za svaki  $x \in \mathbb{R}$  slijedi

$$x^3 + ax^2 + bx + c = ux^3 + [v - u(x_1 + x_2)]x^2 + [x_1x_2u - v(x_1 + x_2)]x + x_1x_2v.$$

Prema korolaru 3.3.3 vrijedi

$$\begin{aligned} u &= 1, \\ v - u(x_1 + x_2) &= a. \end{aligned}$$

Slijedi da je  $v - (x_1 + x_2) = a$  tj.  $v = (x_1 + x_2) + a$ .

Nadalje, zbog  $u = 1$  vrijedi

$$h(x) = x + v, \text{ za svaki } x \in \mathbb{R},$$

pa je posebno

$$h(-v) = 0.$$

Uočimo da iz  $(\ominus)$  slijedi da je  $-v$  nultočka od  $f$ . No,  $-v = -(x_1 + x_2) - a$ .

Dakle,  $-(x_1 + x_2) - a$  je nultočka od  $f$ . □

### 3.4 Polinomi i kvadratni radikali

**Napomena 3.4.1.** Neka je  $\alpha$  kvadratni radikal. Tada postoje  $n \in \mathbb{N}_0$  i korijenski niz  $x_0, \dots, x_n$  takvi da je  $\alpha \in \mathbb{Q}[x_0, \dots, x_n]$ .

No,  $x_0, \dots, x_n$  nije jedini korijenski niz s tim svojstvom. Naime, ako uzmemo bilo koji  $q \in \mathbb{Q}$ , onda je  $x_0, \dots, x_n, q$  također korijenski niz (jer je  $q^2 \in \mathbb{Q} \subseteq \mathbb{Q}[x_0, \dots, x_n]$  prema lemi 2.3.8) te vrijedi  $\alpha \in \mathbb{Q}[x_0, \dots, x_n, q]$  jer je prema propoziciji 2.3.9

$$\mathbb{Q}[x_0, \dots, x_n, q] = [\mathbb{Q} \cup \{x_0, \dots, x_n, q\}] = [\mathbb{Q} \cup \{x_0, \dots, x_n\}] = \mathbb{Q}[x_0, \dots, x_n].$$

**Definicija 3.4.2.** Neka je  $\alpha$  kvadratni radikal te neka je

$$S = \{n \in \mathbb{N}_0 \mid \text{postoji korijenski niz } x_0, \dots, x_n \text{ takav da je } \alpha \in \mathbb{Q}[x_0, \dots, x_n]\}.$$

Očito je  $S \subseteq \mathbb{N}_0$ , a vrijedi da je  $S \neq \emptyset$  jer je  $\alpha$  kvadratni radikal.

Neka je  $k = \min S$ . Tada za  $k$  kažemo da je **stupanj kvadratnog radikala**  $\alpha$ .

**Napomena 3.4.3.** Neka je  $(P, +, \cdot)$  prsten te neka je  $R$  potprsten od  $(P, +, \cdot)$ . Neka je  $x_0 \in R$ . Tada je  $R[x_0] = R$ . Naime, vrijedi

$$R[x_0] = [R \cup \{x_0\}] = [R] = R.$$

**Teorem 3.4.4.** Neka su  $a_0, a_1, a_2, a_3 \in \mathbb{Q}$ ,  $a_3 \neq 0$ . Neka je  $f : \mathbb{R} \rightarrow \mathbb{R}$  funkcija definirana s  $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ , za svaki  $x \in \mathbb{R}$ . Tada vrijedi:

ako  $f$  ima nultočku koja je kvadratni radikal, onda  $f$  ima nultočku koja je racionalan broj.

*Dokaz.* Pretpostavimo da postoji kvadratni radikal koji je nultočka od  $f$ .  
Pretpostavimo da  $f$  nema nultočku koja je racionalan broj.

Neka je  $A$  skup svih  $n \in \mathbb{N}_0$  takvi da postoji kvadratni radikal  $x$  takav da je  $n$  stupanj kvadratnog radikala  $x$  i  $x$  je nultočka od  $f$ . Skup  $A$  je neprazan prema pretpostavci s početka dokaza. Očito je  $A \subseteq \mathbb{N}_0$ .

Neka je  $m = \min A$ . Zbog  $m \in A$  postoji kvadratni radikal  $x$  takav da je  $m$  stupanj kvadratnog radikala  $x$  i  $x$  je nultočka od  $f$ .

Iz činjenice da je  $m$  stupanj kvadratnog radikala  $x$  slijedi da postoji korijenski niz  $x_0, \dots, x_m$  takav da je

$$x \in \mathbb{Q}[x_0, \dots, x_m] \quad (*)$$

Imamo dvije mogućnosti:  $m = 0$  i  $m > 0$ .

Pretpostavimo da je  $m = 0$

Tada je  $x \in \mathbb{Q}[x_0]$ . Vrijedi  $x_0^2 \in \mathbb{Q}$ . Iz propozicije 2.2.12 slijedi da postoje  $a, b \in \mathbb{Q}$  takvi da je  $x = a + bx_0$ .

S obzirom da je  $x$  nultočka od  $f$ , slijedi

$$f(a + bx_0) = 0$$

odnosno

$$a_3(a + bx_0)^3 + a_2(a + bx_0)^2 + a_1(a + bx_0) + a_0 = 0.$$

Kvadriranjem i kubiranjem dobivamo

$$a_3(a^3 + 3a^2bx_0 + 3ab^2x_0^2 + b^3x_0^3) + a_2(a^2 + 2abx_0 + b^2x_0^2) + a_1(a + bx_0) + a_0 = 0.$$

Sređivanjem prethodnog izraza dobivamo

$$a_3a^3 + a_33ab^2x_0^2 + a_2a^2 + a_2b^2x_0^2 + a_1a + a_0 + (a_33a^2b + a_3b^3x_0^2 + a_22ab + a_1b)x_0 = 0.$$

Označimo

$$C = a_3a^3 + a_33ab^2x_0^2 + a_2a^2 + a_2b^2x_0^2 + a_1a + a_0$$

$$D = a_33a^2b + a_3b^3x_0^2 + a_22ab + a_1b.$$

Dakle,

$$C + Dx_0 = 0.$$

Uočimo da su  $C, D \in \mathbb{Q}$ . Vrijedi  $x_0 \notin \mathbb{Q}$  (u suprotnom bi prema napomeni 3.4.3 vrijedilo  $\mathbb{Q}[x_0] = \mathbb{Q}$ , pa bi iz  $x \in \mathbb{Q}[x_0]$  slijedilo  $x \in \mathbb{Q}$ , što je nemoguće jer  $f$  nema racionalnu nultočku). Posebno,  $x_0 \neq 0$ .

Kada bi vrijedilo  $D \neq 0$ , onda bi iz

$$C + Dx_0 = 0$$

slijedilo da je

$$x_0 = -\frac{C}{D},$$

tj. imali bismo da je  $x_0 \in \mathbb{Q}$ , a to je nemoguće.

Dakle,  $D = 0$ , pa iz  $C + Dx_0 = 0$  slijedi da je i  $C = 0$ .

Tvrdimo da je  $a - bx_0$  također nultočka od  $f$ . Vrijedi

$$\begin{aligned} f(a - bx_0) &= a_3(a - bx_0)^3 + a_2(a - bx_0)^2 + a_1(a - bx_0) + a_0 \\ &= a_3(a^3 - 3a^2bx_0 + 3ab^2x_0^2 - b^3x_0^3) + a_2(a^2 - 2abx_0 + b^2x_0^2) + a_1a - a_1bx_0 + a_0 \\ &= a_3a^3 + a_33ab^2x_0^2 + a_2a^2 + a_2b^2x_0^2 + a_1a + a_0 - (a_33a^2b + a_3b^3x_0^2 + a_22ab + a_1b)x_0 \\ &= C - Dx_0 \\ &= 0 - 0 \cdot x_0 = 0 \end{aligned}$$

Dakle,  $f(a - bx_0) = 0$  tj.  $a - bx_0$  je nultočka od  $f$

Pretpostavimo da je  $a + bx_0 = a - bx_0$ .

Tada je  $2bx_0 = 0$ , a iz  $x_0 \neq 0$  slijedi  $b = 0$ . Iz  $x = a + bx_0$  slijedi  $x = a$ , tj.  $x \in \mathbb{Q}$ , što je nemoguće.

Dakle,  $a + bx_0 \neq a - bx_0$ .

Definirajmo funkciju  $g : \mathbb{R} \rightarrow \mathbb{R}$  s

$$g(x) = x^3 + \frac{a_2}{a_3}x^2 + \frac{a_1}{a_3}x + \frac{a_0}{a_3}, \text{ za svaki } x \in \mathbb{R}.$$

Iz činjenice da je  $a_3 \cdot g(x) = f(x)$ , za svaki  $x \in \mathbb{R}$ , slijedi da je svaka nultočka od  $f$  ujedno i nultočka od  $g$ , i obratno.

Znamo da su  $a + bx_0$  i  $a - bx_0$  dvije različite nultočke od  $f$ , pa su i dvije različite nultočke od  $g$ . Iz propozicije 3.3.9 slijedi da je i

$$-[(a + bx_0) + (a - bx_0)] - \frac{a_2}{a_3}$$

također nultočka od  $g$ .

Dakle,  $-2a - \frac{a_2}{a_3}$  je nultočka od  $g$ , pa i od  $f$ . No, to je nemoguće jer je  $-2a - \frac{a_2}{a_3} \in \mathbb{Q}$ .

Zaključak:  $m \neq 0$  tj.  $m > 0$ .

Budući da je  $x_0, \dots, x_m$  korijenski niz,  $x_0, \dots, x_{m-1}$  je također korijenski niz. Iz propozicije 2.3.4 slijedi da je  $\mathbb{Q}[x_0, \dots, x_{m-1}]$  potpolje od  $(\mathbb{R}, +, \cdot)$ . Po definiciji vrijedi

$$\mathbb{Q}[x_0, \dots, x_m] = (\mathbb{Q}[x_0, \dots, x_{m-1}])[x_m]$$

pa iz (\*) slijedi  $x \in (\mathbb{Q}[x_0, \dots, x_{m-1}])[x_m]$ .

Iz činjenice da je  $x_m^2 \in \mathbb{Q}[x_0, \dots, x_{m-1}]$  i propozicije 2.2.12, slijedi da postoje  $a, b \in \mathbb{Q}[x_0, \dots, x_{m-1}]$  takvi da je

$$x = a + bx_m.$$

Budući da je  $x$  nultočka od  $f$  vrijedi  $f(a + bx_m) = 0$  pa je

$$a_3(a + bx_m)^3 + a_2(a + bx_m)^2 + a_1(a + bx_m) + a_0 = 0.$$

Kubiranjem, kvadriranjem i sređivanjem izraza, kao u prethodnom dijelu dokaza, dobivamo

$$C + Dx_m = 0,$$

gdje su

$$C = a_3a^3 + a_33ab^2x_m^2 + a_2a^2 + a_2b^2x_m^2 + a_1a + a_0$$

$$D = a_33a^2b + a_3b^3x_m^2 + a_22ab + a_1b.$$

S obzirom da je  $x_m^2 \in \mathbb{Q}[x_0, \dots, x_{m-1}]$ , da je  $\mathbb{Q}[x_0, \dots, x_{m-1}]$  potpolje od  $(\mathbb{R}, +, \cdot)$  te da je prema lemi 2.3.8  $\mathbb{Q} \subseteq \mathbb{Q}[x_0, \dots, x_{m-1}]$ , slijedi da su  $C, D \in \mathbb{Q}[x_0, \dots, x_{m-1}]$ .

Pretpostavimo da je  $D \neq 0$ . Tada je

$$x_m = -\frac{C}{D}$$

pa slijedi da je  $x_m \in \mathbb{Q}[x_0, \dots, x_{m-1}]$ . Sada iz  $x = a + bx_m$  slijedi da je  $x \in \mathbb{Q}[x_0, \dots, x_{m-1}]$ . To je u kontradikciji sa činjenicom da je  $m$  stupanj kvadratnog radikala  $x$ .

Dakle,  $D = 0$  pa iz  $C + Dx_m = 0$  slijedi da je i  $C = 0$ .

Kao i u prethodnom dijelu dokaza dobivamo da je

$$f(a - bx_m) = C - Dx_m.$$

Stoga je  $f(a - bx_m) = 0$ , tj.  $a - bx_m$  je nultočka od  $f$ .

Tvrdimo da je  $a + bx_m \neq a - bx_m$ .

Pretpostavimo suprotno. Tada iz  $a + bx_m = a - bx_m$  slijedi

$$2bx_m = 0 \text{ tj. } bx_m = 0.$$

Imamo  $x = a + bx_m = a$ , pa je  $x \in \mathbb{Q}[x_0, \dots, x_{m-1}]$ , kontradikcija!

Prema tome,  $a + bx_m$  i  $a - bx_m$  su dvije različite nultočke od  $f$ , pa i od  $g$ , gdje je  $g : \mathbb{R} \rightarrow \mathbb{R}$  funkcija definirana s

$$g(x) = x^3 + \frac{a_2}{a_3}x^2 + \frac{a_1}{a_3}x + \frac{a_0}{a_3}, \text{ za svaki } x \in \mathbb{R}.$$

Iz propozicije 3.3.9 slijedi da je

$$-[(a + bx_m) + (a - bx_m)] - \frac{a_2}{a_3}$$

nultočka od  $g$ . Dakle,  $-2a - \frac{a_2}{a_3}$  je nultočka od  $g$ , pa i od  $f$ .

Označimo

$$y = -2a - \frac{a_2}{a_3}.$$

Imamo da je  $y$  nultočka od  $f$  i  $y \in \mathbb{Q}[x_0, \dots, x_{m-1}]$ . Očito je  $y$  kvadratni radikal. Neka je  $k$  stupanj kvadratnog radikala  $y$ . Iz definicije 3.4.2 slijedi da je  $k \leq m - 1$ . Iz definicije skupa  $A$  slijedi da je  $k \in A$ . No, budući da je  $m = \min A$ , mora vrijediti  $m \leq k$ . Ovo je u kontradikciji s  $k \leq m - 1$ .

Time smo dokazali da  $f$  ima racionalnu nultočku. □

### 3.5 Problem duplikacije kocke

Promotrimo sada jednu preciznu formulaciju, izraženu terminologijom ovog rada, klasičnog problema duplikacije kocke.

Pitanje je sljedeće: *Je li moguće za sve  $A, B \in \mathbb{R}^2$ , iz skupa  $\{A, B\}$ , konstruirati točke  $C$  i  $D$  takve da je kocka, kojoj je dužina  $\overline{CD}$  brid, dvostruko većeg volumena od kocke s bridom  $\overline{AB}$ ?*

Pretpostavimo da je odgovor na prethodno pitanje potvrđan.

Neka su  $A = (0, 0)$  i  $B = (1, 0)$ . Tada postoje točke  $C, D \in \mathbb{R}^2$  koje se mogu konstruirati iz skupa  $\{A, B\}$  te takve da kocka s bridom  $\overline{CD}$  ima dvostruko veći volumen od kocke s bridom  $\overline{AB}$ . Slijedi

$$(d(C, D))^3 = 2(d(A, B))^3.$$

No,  $d(A, B) = 1$  pa je

$$d(C, D) = \sqrt[3]{2}.$$

Uočimo da su prema definiciji,  $C$  i  $D$  konstruktibilne točke.

Neka su  $c_1, c_2, d_1, d_2 \in \mathbb{R}$  takvi da je

$$C = (c_1, c_2), \quad D = (d_1, d_2).$$

Prema definiciji 1.3.9 slijedi da su  $c_1, c_2, d_1, d_2$  konstruktibilni brojevi.

Nadalje, prema teoremu 3.2.2 slijedi da su  $c_1, c_2, d_1, d_2$  kvadratni radikali.

Znamo da je

$$d(C, D) = \sqrt{(d_1 - c_1)^2 + (d_2 - c_2)^2}.$$

Iz propozicija 2.3.10 i 2.3.11 slijedi da je  $d(C, D)$  kvadratni radikal.

Dakle,  $\sqrt[3]{2}$  je kvadratni radikal.

Neka je  $f : \mathbb{R} \rightarrow \mathbb{R}$  polinom oblika

$$f(x) = x^3 - 2.$$

Očito je  $\sqrt[3]{2}$  nultočka od  $f$ . Iz teorema 3.4.4 slijedi da postoji  $x_0 \in \mathbb{Q}$  takav da je  $x_0$  nultočka od  $f$ .

Neka su  $p \in \mathbb{Z}, q \in \mathbb{N}$  relativno prosti brojevi takvi da je

$$x_0 = \frac{p}{q}.$$

Iz  $f(x) = 0$  slijedi

$$\frac{p^3}{q^3} - 2 = 0,$$

što je ekvivalentno s

$$\frac{p^3}{q^3} = 2$$

tj.

$$p^3 = 2q^3. \quad (\in)$$

Iz ovoga vidimo da je  $p^3$  paran broj, odnosno da je  $p$  paran broj. Slijedi da je  $p = 2k$ , za neki  $k \in \mathbb{Z}$ .

Uvrštavanjem prethodne jednakosti u  $(\in)$  slijedi da je

$$(2k)^3 = 2q^3$$

tj.

$$8k^3 = 2q^3.$$

Prema tome,  $4k^3 = q^3$ .

Sada slijedi da je  $q^3$  paran broj pa je i  $q$  paran broj. Ovo je nemoguće jer su  $p$  i  $q$  relativno prosti.

Time smo dokazali da nije moguće za sve  $A, B \in \mathbb{R}^2$  iz skupa  $\{A, B\}$  konstruirati točke  $C, D$  takve da kocka s bridom  $\overline{CD}$  ima dvostruko veći volumen od kocke s bridom  $\overline{AB}$ . Drugim riječima, duplikacija kocke nije moguća.

## Poglavlje 4

# Karakterizacija konstruktibilnih brojeva

### 4.1 Točke s konstruktibilnim koordinatama

**Napomena 4.1.1.** Neka je  $S \subseteq \mathbb{R}^2$  skup koji ima barem dva elementa. Tada za sve  $m, n \in \mathbb{N}$ , takve da je  $n \leq m$ , vrijedi  $S^{(n)} \subseteq S^{(m)}$ .

Dokažimo to.

Neka je  $n \in \mathbb{N}$ . Dovoljno je dokazati da za svaki  $k \in \mathbb{N}$  vrijedi

$$S^{(n)} \subseteq S^{(n+k)}. \quad (\because)$$

Dokažimo zadnju tvrdnju indukcijom po  $k$ .

Za  $k = 1$  tvrdnja slijedi iz napomene 1.3.3.

Pretpostavimo da za neki  $k \in \mathbb{N}$  vrijedi

$$S^{(n)} \subseteq S^{(n+k)}.$$

Prema napomeni 1.3.3 slijedi

$$S^{(n+k)} \subseteq S^{(n+k+1)}.$$

Stoga je  $S^{(n)} \subseteq S^{(n+k+1)}$ .

Time smo dokazali da  $(\because)$  vrijedi za svaki  $k \in \mathbb{N}$ .

**Propozicija 4.1.2.** Neka su  $A, B, C, D$  konstruktibilne točke,  $A \neq B$ ,  $C \neq D$ .

1. Pretpostavimo da je  $AB \neq CD$  te da je  $T \in AB \cap CD$ . Tada je  $T$  konstruktibilna točka.



2. *Pretpostavimo da je  $T \in K(A, d(A, B)) \cap CD$   
Tada je  $T$  konstruktibilna točka.*
3. *Pretpostavimo da su kružnice  $K(A, d(A, B))$  i  $K(C, d(C, D))$  različite te da je točka  $T$   
u njihovom presjeku.  
Tada je  $T$  konstruktibilna točka.*

*Dokaz.* Neka je  $S = \{(0, 0), (1, 0)\}$ . Budući da je  $A$  konstruktibilna točka vrijedi da se  $A$  može konstruirati iz skupa  $S$  odnosno da postoji  $n_1 \in \mathbb{N}$  takav da je  $A \in S^{(n_1)}$ . Iz istog razloga postoje  $n_2, n_3, n_4 \in \mathbb{N}$  takvi da vrijedi  $B \in S^{(n_2)}, C \in S^{(n_3)}, D \in S^{(n_4)}$ .

Neka je  $n = \max\{n_1, n_2, n_3, n_4\}$ .

Očito je  $n_1 \leq n, n_2 \leq n, n_3 \leq n, n_4 \leq n$  pa iz napomene 4.1.1 slijedi da su

$$S^{(n_1)} \subseteq S^{(n)}, S^{(n_2)} \subseteq S^{(n)}, S^{(n_3)} \subseteq S^{(n)}, S^{(n_4)} \subseteq S^{(n)}.$$

Stoga su  $A, B, C, D \in S^{(n)}$ .

Slijedi da su pravci  $AB$  i  $CD$  određeni skupom  $S^{(n)}$  te da su kružnice  $K(A, d(A, B))$  i  $K(C, d(C, D))$  također određene skupom  $S^{(n)}$ .

1. Očito je  $T$  točka određena skupom  $S^{(n)}$ . Dakle,  $T \in S^{(n+1)}$ . Slijedi po definiciji da je  $T$  konstruktibilna točka.
2. Također zaključujemo da je  $T$  određena skupom  $S^{(n)}$  tj.  $T \in S^{(n+1)}$ . Dakle,  $T$  je konstruktibilna točka.
3. Analogno kao u prethodnim slučajevima se pokaže da je  $T$  konstruktibilna točka.

□

**Lema 4.1.3.** *Neka je  $x$  konstruktibilan broj. Tada su točke  $(x, 0), (0, x), (-x, 0)$  i  $(0, -x)$  konstruktibilne.*

*Dokaz.* Budući da je  $x$  konstruktibilan broj, postoji  $y \in \mathbb{R}$  takav da je  $(x, y)$  konstruktibilna točka ili je  $(y, x)$  konstruktibilna točka.

*1. slučaj:  $(x, y)$  je konstruktibilna točka.*

Dokažimo da je  $(x, 0)$  konstruktibilna točka. To je jasno ako je  $y = 0$ .

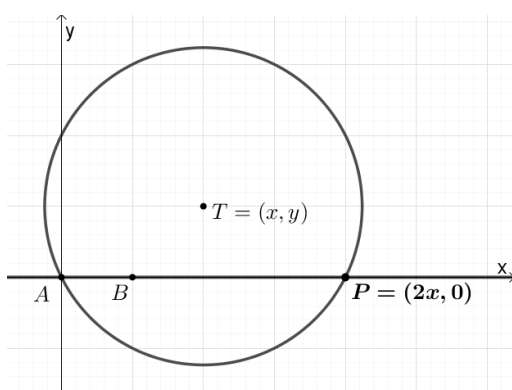
Za  $x = 0$  je točka  $(x, 0)$  također konstruktibilna (konstruktibilnost točke  $(0, 0)$  slijedi direktno iz definicije 1.3.7).

Pretpostavimo da su  $x \neq 0$  i  $y \neq 0$ . Označimo  $T = (x, y)$ ,  $A = (0, 0)$  i  $B = (1, 0)$ . Točke  $T, A$  i  $B$  su konstruktibilne te je  $T \neq A$  i  $A \neq B$ .

Neka je  $P = (2x, 0)$ . Prema napomeni 1.1.6 vrijedi  $AB = \{(t, 0) \mid t \in \mathbb{R}\}$ . Stoga je  $P \in AB$ . Nadalje, imamo

$$d(P, T) = \sqrt{x^2 + y^2} = d(A, T).$$

Stoga je  $P \in K(T, d(A, T))$ . Dakle,  $P \in AB \cap K(T, d(A, T))$ , pa iz drugog dijela propozicije 4.1.2 slijedi da je  $P$  konstruktibilna točka.



Slika 4.1: Točka  $P$  je konstruktibilna točka

Neka je  $T' = (x, -y)$ . Vrijedi

$$d(T', A) = \sqrt{x^2 + y^2} = d(A, T),$$

$$d(T', P) = \sqrt{x^2 + y^2} = d(P, T),$$

iz čega zaključujemo da je

$$T' \in K(A, d(A, T)) \cap K(P, d(P, T)). \quad (\triangleleft)$$

Kružnice  $K(A, d(A, T))$  i  $K(P, d(P, T))$  su različite jer za točku  $F = (0, \sqrt{x^2 + y^2})$  vrijedi

$$F \in K(A, d(A, T))$$

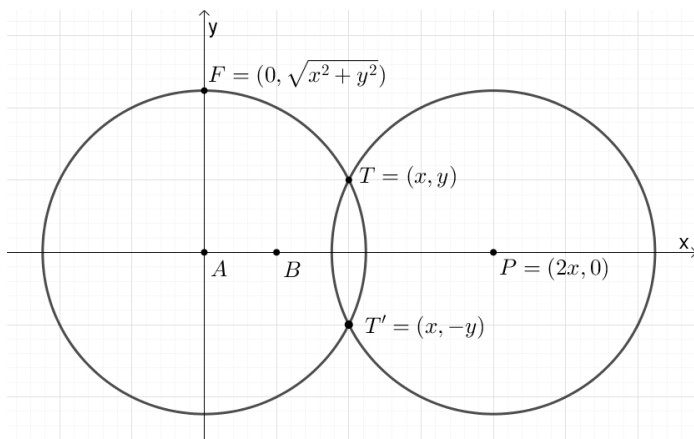
$$\text{jer je } d(F, A) = \sqrt{(0-0)^2 + (0-\sqrt{x^2+y^2})^2} = \sqrt{x^2+y^2}$$

te

$$F \notin K(P, d(P, T))$$

jer je  $d(F, P) = \sqrt{(2x - 0)^2 + (0 - \sqrt{x^2 + y^2})^2} = \sqrt{(2x)^2 + x^2 + y^2} > \sqrt{x^2 + y^2} = d(P, T)$ .

Iz ( $\leq$ ) i propozicije 4.1.2 slijedi da je  $T'$  konstruktibilna točka. Uočimo da je  $T' \neq T$  (jer je  $y \neq 0$ ).



Slika 4.2: Točka  $T'$  je konstruktibilna točka

Prema napomeni 1.1.6 vrijedi

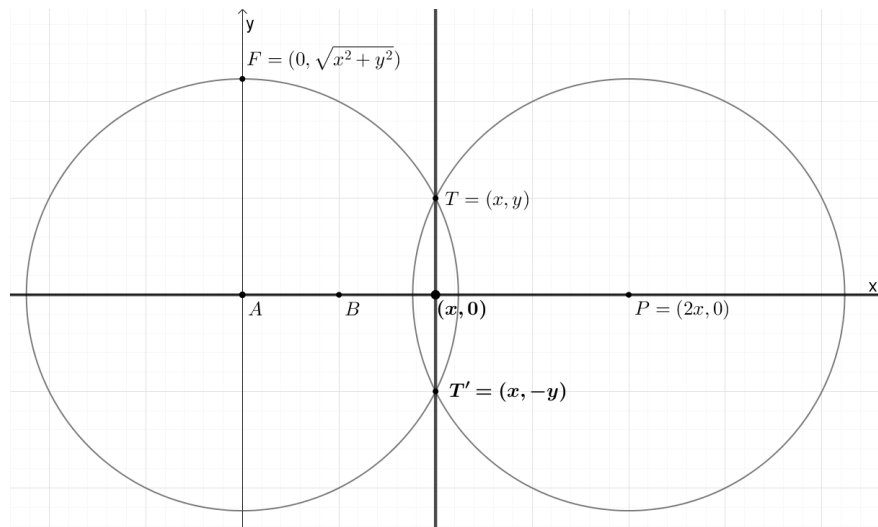
$$\begin{aligned} T'T &= \{T' + t \cdot (T - T') \mid t \in \mathbb{R}\} \\ &= \{(x, -y) + t \cdot (0, 2y) \mid t \in \mathbb{R}\} \\ &= \{(x, -y + t \cdot 2y) \mid t \in \mathbb{R}\}. \end{aligned}$$

Uočimo da je za  $t = \frac{1}{2}$

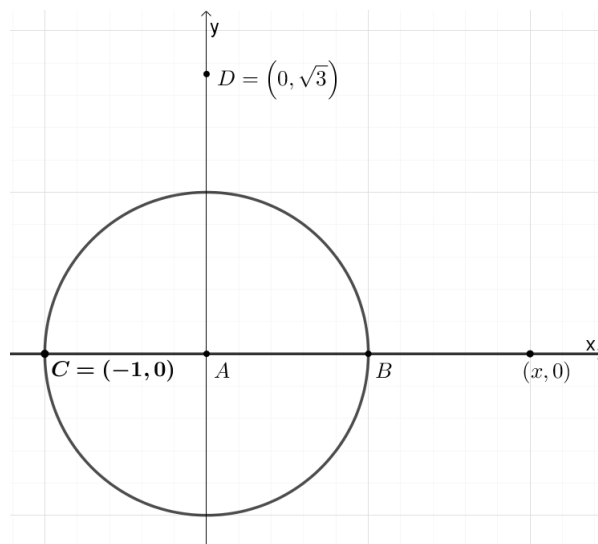
$$(x, -y + t \cdot 2y) = (x, 0).$$

Dakle,  $(x, 0) \in T'T$ . Očito je  $(x, 0) \in AB$ . Stoga je  $(x, 0) \in T'T \cap AB$ .

Pravci  $AB$  i  $T'T$  su različiti (jer  $A \in AB$  i  $A \notin T'T$ .) Iz propozicije 4.1.2 slijedi da je  $(x, 0)$  konstruktibilna točka.

Slika 4.3: Točka  $(x, 0)$  je konstruktibilna točka

Neka su  $C = (-1, 0)$  i  $D = (0, \sqrt{3})$ . Vrijedi  $C \in AB \cap K(A, d(A, B))$ , što znači da je  $C$  konstruktibilna točka (prema propoziciji 4.1.2).

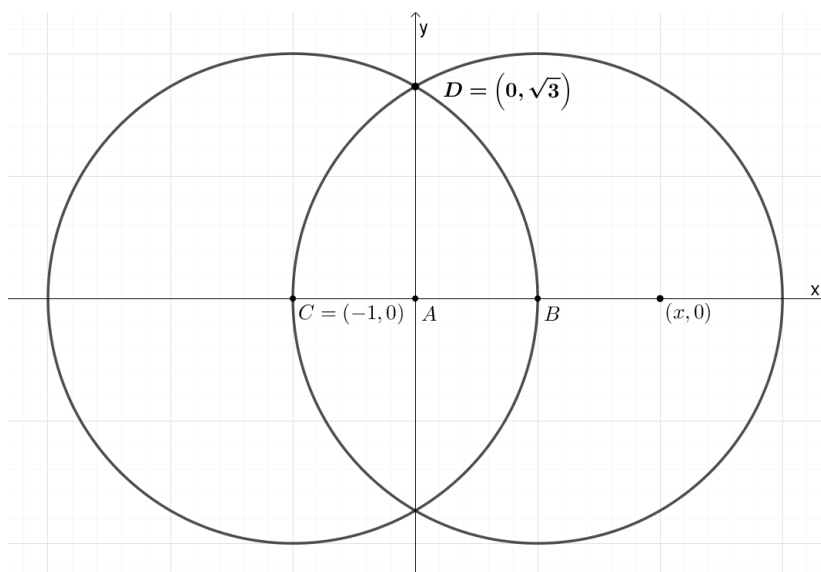
Slika 4.4: Točka  $C$  je konstruktibilna točka

Imamo

$$d(C, D) = 2 = d(B, C).$$

Stoga je  $D \in K(C, d(B, C))$ . Isto tako vrijedi  $D \in K(B, d(B, C))$ .

Očito je da su kružnice  $K(C, d(B, C))$  i  $K(B, d(B, C))$  različite. Iz činjenice da se točka  $D$  nalazi u presjeku tih dviju kružnica, slijedi da je  $D$  konstruktibilna točka (prema propoziciji 4.1.2).



Slika 4.5: Točka  $D$  je konstruktibilna točka

Prema napomeni 1.1.6 vrijedi

$$\begin{aligned} AD &= \{A + \lambda \cdot (D - A) \mid \lambda \in \mathbb{R}\} \\ &= \{\lambda(0, \sqrt{3}) \mid \lambda \in \mathbb{R}\} \\ &= \{(0, \lambda \sqrt{3}) \mid \lambda \in \mathbb{R}\}. \end{aligned}$$

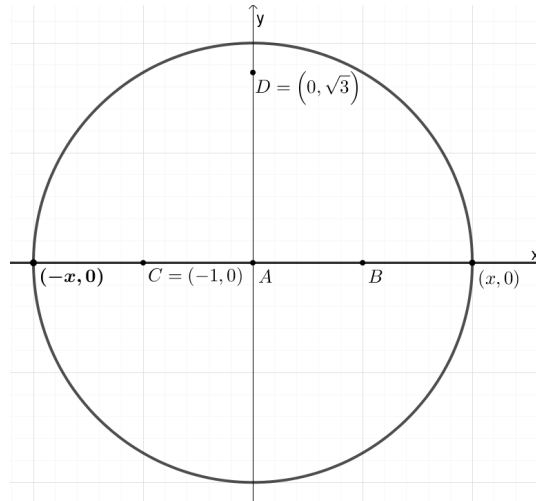
Svaki realan broj  $t$  se može napisati u obliku  $t = \lambda \sqrt{3}$  (uzmemo  $\lambda = \frac{t}{\sqrt{3}}$ ).

Stoga je

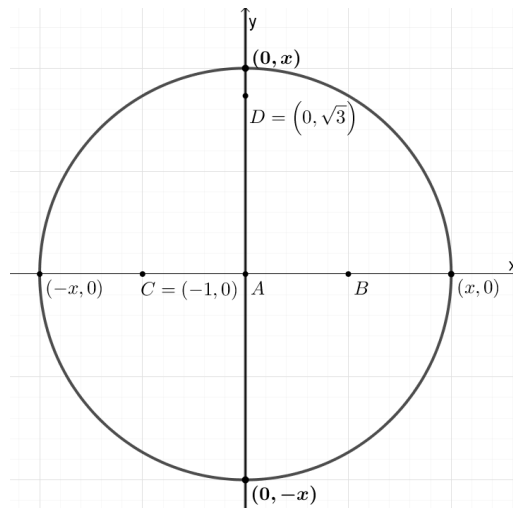
$$\{(0, \lambda \sqrt{3}) \mid \lambda \in \mathbb{R}\} = \{(0, t) \mid t \in \mathbb{R}\}.$$

Dakle,  $AD = \{(0, t) \mid t \in \mathbb{R}\}$ .

Promotrimo  $AB \cap K(A, d(A, (x, 0)))$ .  
 Uočimo da je  $(-x, 0) \in AB \cap K(A, d(A, (x, 0)))$ . Iz činjenice da su točke  $A, B, (x, 0)$  konstruktibilne, zaključujemo da je točka  $(-x, 0)$  konstruktibilna (prema propoziciji 4.1.2).

Slika 4.6: Točka  $(-x, 0)$  je konstruktibilna točka

Nadalje,  $(0, x) \in AD$  pa iz  $(0, x) \in AD \cap K(A, d(A, (x, 0)))$  slijedi da je  $(0, x)$  konstruktibilna točka (prema propoziciji 4.1.2).  
 Analogno zaključujemo da je  $(0, -x)$  konstruktibilna točka.

Slika 4.7: Točke  $(0, x)$  i  $(0, -x)$  su konstruktibilne točke

2. slučaj:  $(y, x)$  je konstruktibilna točka.

Dokažimo da je  $(0, x)$  konstruktibilna točka. To je jasno ako je  $x = 0$  ili  $y = 0$ . Stoga možemo pretpostaviti da je  $x \neq 0$  i  $y \neq 0$ .

Neka su  $A, B$  i  $D$  točke kao u prvom slučaju te neka je  $M = (y, x)$ . Neka je  $R = (0, 2x)$ . Očito je  $R \in AD \cap K(M, d(A, M))$ . Iz propozicije 4.1.2 slijedi da je  $R$  konstruktibilna točka.

Označimo  $M' = (-y, x)$ . Vrijedi  $M' \in K(A, d(A, M)) \cap K(R, d(R, M))$ , a ove su kružnice različite jer je

$$\begin{aligned} (\sqrt{x^2 + y^2}, 0) &\in K(A, d(A, M)), \text{ a} \\ (\sqrt{x^2 + y^2}, 0) &\notin K(R, d(R, M)). \end{aligned}$$

Iz propozicije 4.1.2 slijedi da je  $M'$  konstruktibilna točka.

Vrijedi

$$\begin{aligned} M'M &= \{M' + t \cdot (M - M') \mid t \in \mathbb{R}\} \\ &= \{(-y, x) + t \cdot (2y, 0) \mid t \in \mathbb{R}\}. \end{aligned}$$

Za  $t = \frac{1}{2}$  imamo

$$(-y, x) + t \cdot (2y, 0) = (0, x).$$

Stoga je  $(0, x) \in M'M$ . Očito je  $(0, x) \in AD$ , a pravci  $AD$  i  $M'M$  su različiti (jer je  $M \in M'M$ , a  $M \notin AD$ ). Dakle,  $(0, x) \in M'M \cap AD$  pa prema propoziciji 4.1.2 slijedi da je  $(0, x)$  konstruktibilna točka.

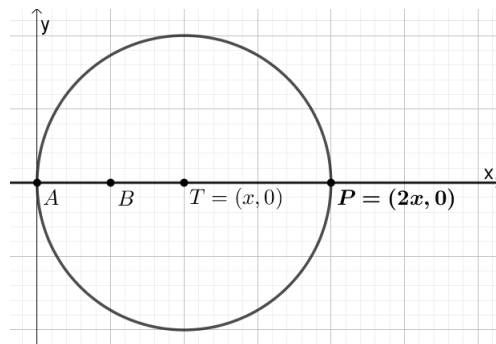
Sada analogno, kao u prethodnom slučaju, dobivamo da su  $(0, -x)$ ,  $(x, 0)$  i  $(-x, 0)$  konstruktibilne točke.  $\square$

**Propozicija 4.1.4.** *Neka su  $x$  i  $y$  konstruktibilni brojevi. Tada je  $(x, y)$  konstruktibilna točka.*

*Dokaz.* Prema lemi 4.1.3 su točke  $(x, 0)$  i  $(0, y)$  konstruktibilne. Stoga, da bismo dokazali da je  $(x, y)$  konstruktibilna točka, možemo pretpostaviti da je  $x \neq 0$  i  $y \neq 0$ .

Uvedimo oznake:

$$A = (0, 0), B = (1, 0), T = (x, 0), P = (2x, 0).$$

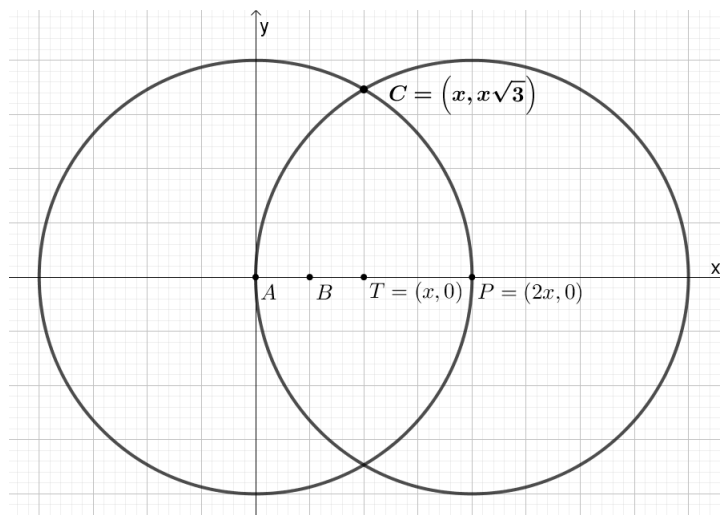
Slika 4.8: Točka  $P$  je konstruktibilna točka

Vrijedi  $P \in AB \cap K(T, d(T, A))$  pa iz propozicije 4.1.2 slijedi da je  $P$  konstruktibilna točka.

Promotrimo točku  $C = (x, x\sqrt{3})$ . Uočimo da je

$$C \in K(P, d(P, A)) \cap K(A, d(A, P))$$

(navedene kružnice su različite jer je  $A \in K(P, d(P, A))$ , a  $A \notin K(A, d(A, P))$ ). Dakle,  $C$  je konstruktibilna točka.

Slika 4.9: Točka  $C$  je konstruktibilna točka

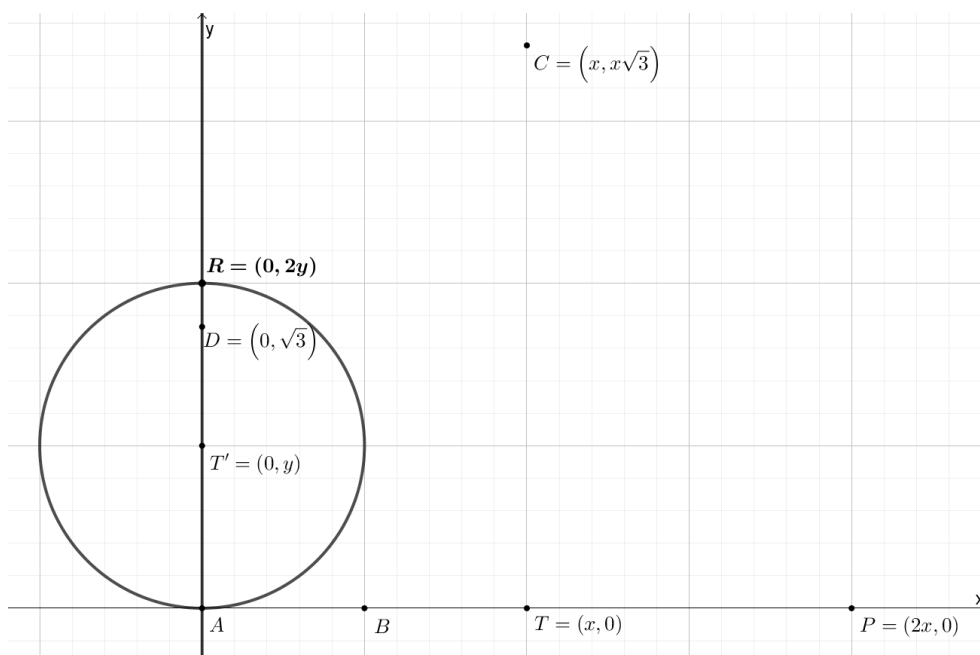


Neka je  $D = (0, \sqrt{3})$ .

U dokazu prethodne leme smo vidjeli da je  $D$  konstruktibilna točka te da je

$$AD = \{(0, t) \mid t \in \mathbb{R}\}.$$

Za točke  $T' = (0, y)$  i  $R = (0, 2y)$  vrijedi  $R \in AD \cap K(T', d(T', A))$ . Stoga je  $R$  konstruktibilna točka.



Slika 4.10: Točka  $R$  je konstruktibilna točka

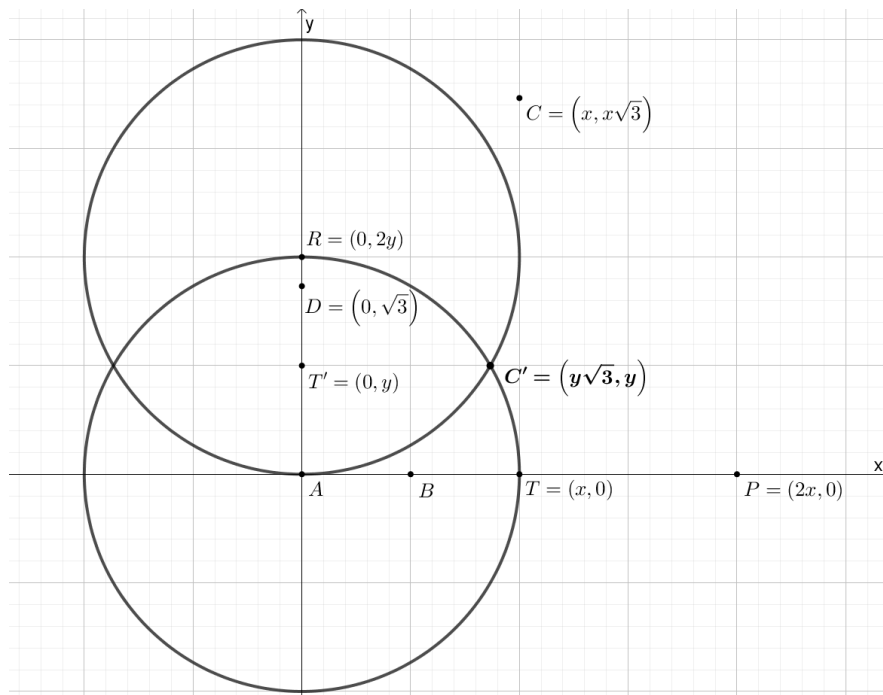
Promotrimo točku  $C' = (y\sqrt{3}, y)$ .

Vrijedi

$$C' \in K(A, d(A, R)) \cap K(R, d(R, A))$$

(navedene kružnice su različite jer je  $R \in K(A, d(A, R))$ , a  $R \notin K(R, d(A, R))$ ).

Stoga je  $C'$  konstruktibilna točka.

Slika 4.11: Točka  $C'$  je konstruktibilna točka

Promotrimo pravce  $TC$  i  $T'C'$ .

$$\begin{aligned}
 TC &= \{T + \lambda(C - T) \mid \lambda \in \mathbb{R}\} \\
 &= \{(x, 0) + \lambda(0, x\sqrt{3}) \mid \lambda \in \mathbb{R}\} \\
 &= \{(x, \lambda x\sqrt{3}) \mid \lambda \in \mathbb{R}\}.
 \end{aligned}$$

Za  $\lambda = \frac{y}{x\sqrt{3}}$  dobivamo

$$(x, \lambda x\sqrt{3}) = (x, y).$$

Dakle,  $(x, y) \in TC$ .

$$\begin{aligned}
 T'C' &= \{T' + \mu(C' - T') \mid \mu \in \mathbb{R}\} \\
 &= \{(0, y) + \mu(y\sqrt{3}, 0) \mid \mu \in \mathbb{R}\} \\
 &= \{(\mu y\sqrt{3}, y) \mid \mu \in \mathbb{R}\}.
 \end{aligned}$$

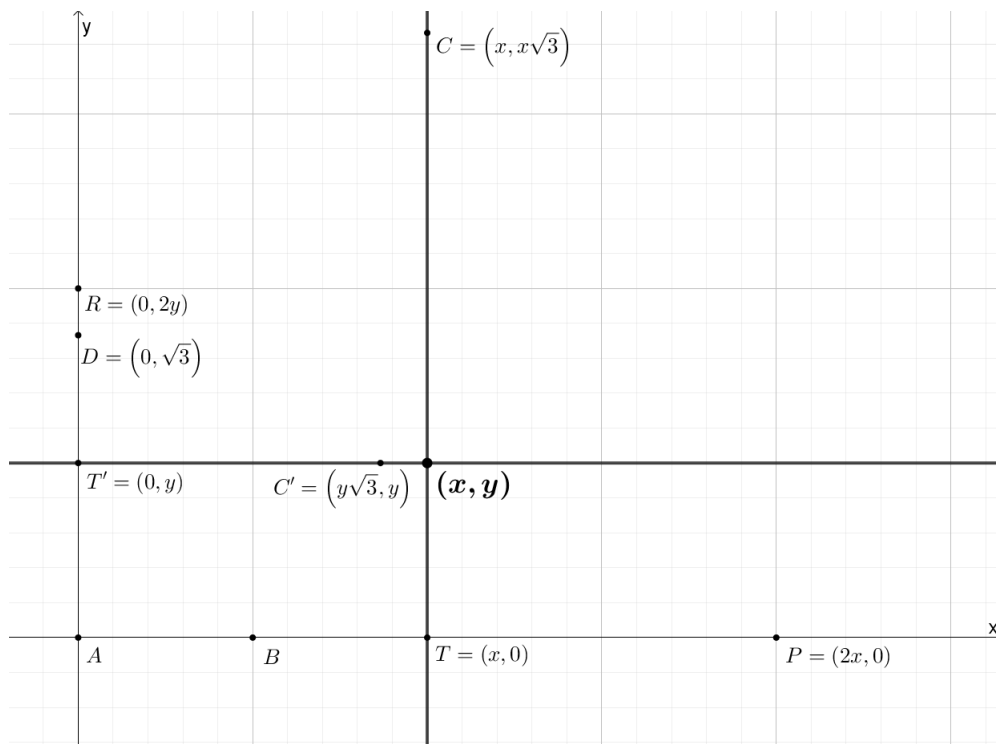
Za  $\mu = \frac{x}{y\sqrt{3}}$  dobivamo

$$(\mu y\sqrt{3}, y) = (x, y).$$

Dakle,  $(x, y) \in T'C'$ .

Uočimo da su pravci  $TC$  i  $T'C'$  različiti (jer  $T' \notin TC$ , a  $T' \in T'C'$ ).

Vrijedi  $(x, y) \in TC \cap T'C'$  pa prema propoziciji 4.1.2 slijedi da je  $(x, y)$  konstruktibilna točka.



Slika 4.12: Točka  $(x, y)$  je konstruktibilna točka

Time je propozicija dokazana.

□

## 4.2 Zbroj, produkt i kvocijent konstruktibilnih brojeva

**Propozicija 4.2.1.** *Neka su  $x$  i  $y$  konstruktibilni brojevi. Tada je:*

1.  $-x$  konstruktibilan broj,
2.  $x + y$  konstruktibilan broj.

*Dokaz.*

1. Prema lemi 4.1.3 točka  $(-x, 0)$  je konstruktibilna. Prema tome,  $-x$  je konstruktibilan broj.
2. Neka su  $A = (0, 0)$ ,  $B = (1, 0)$ ,  $C = (x, 0)$  i  $D = (x, y)$ . Možemo pretpostaviti da je  $y \neq 0$ .

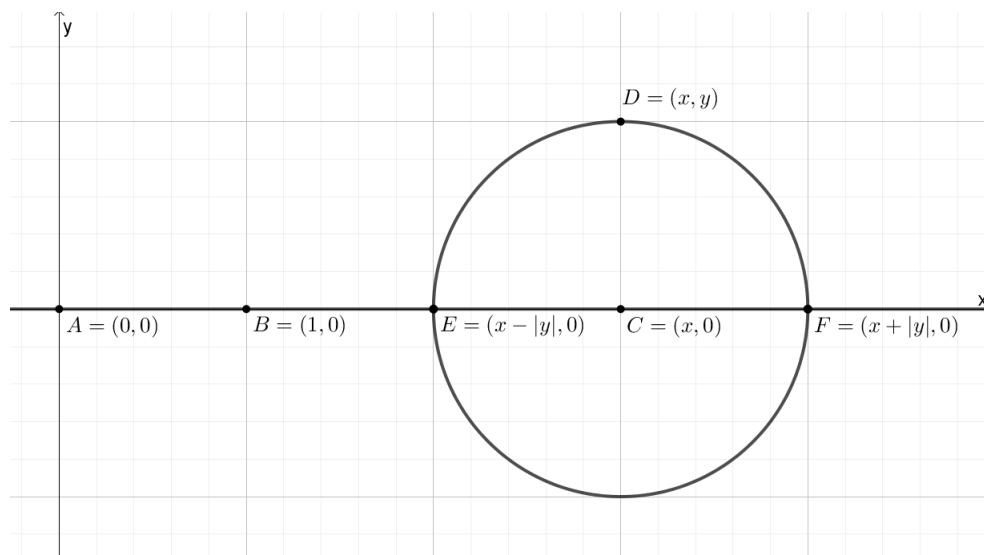
Prema lemi 4.1.3 i propoziciji 4.1.4 slijedi da su točke  $C$  i  $D$  konstruktibilne.

Nadalje, za točke  $E = (x - |y|, 0)$  i  $F = (x + |y|, 0)$  vrijedi

$$E, F \in AB \cap K(C, d(C, D)).$$

Prema propoziciji 4.1.2 slijedi da su  $E$  i  $F$  konstruktibilne točke.

Slijedi da su brojevi  $x - |y|$  i  $x + |y|$  konstruktibilni. Jedan od ta dva broja je jednak broju  $x + y$  pa je time druga tvrdnja propozicije dokazana.



Slika 4.13: Točke  $E$  i  $F$  su konstruktibilne točke

□

**Propozicija 4.2.2.** *Neka su  $x$  i  $y$  konstruktibilni brojevi.*

1. *Broj  $x \cdot y$  je konstruktibilan.*
2. *Pretpostavimo da je  $y \neq 0$ . Tada je  $\frac{x}{y}$  konstruktibilan broj.*

*Dokaz.*

1. Možemo pretpostaviti da su  $x \neq 0$  i  $y \neq 0$ .

Neka su  $A = (0, 0)$ ,  $C = (x, 1)$ ,  $D = (0, y)$  i  $E = (1, y)$ . Prema propoziciji 4.1.4 točke  $C$ ,  $D$  i  $E$  su konstruktibilne.

Vrijedi

$$\begin{aligned} AC &= \{\lambda C \mid \lambda \in \mathbb{R}\} \\ &= \{(\lambda x, \lambda) \mid \lambda \in \mathbb{R}\} \end{aligned}$$

i

$$\begin{aligned} DE &= \{D + \mu(1, 0) \mid \mu \in \mathbb{R}\} \\ &= \{(\mu, y) \mid \mu \in \mathbb{R}\}. \end{aligned}$$

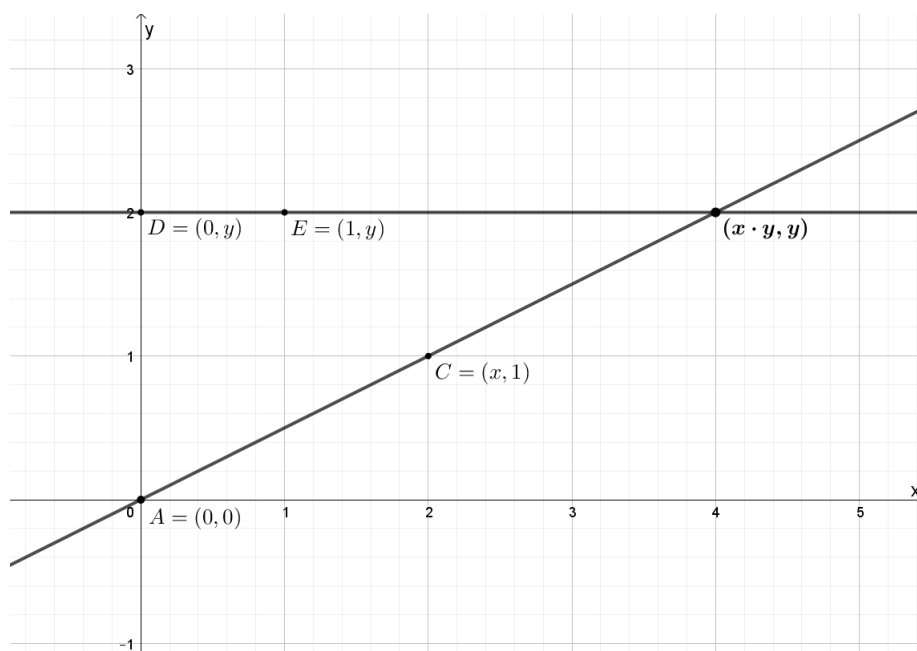
Uočimo da su pravci  $AC$  i  $DE$  različiti (jer je  $A \in AC$ , a  $A \notin DE$ ).

Pogledajmo što se nalazi u presjeku pravaca  $AC$  i  $DE$ . Tražimo  $\lambda, \mu \in \mathbb{R}$  za koje vrijedi

$$(\lambda x, \lambda) = (\mu, y).$$

Za  $\lambda = y$  i  $\mu = x \cdot y$  navedena jednakost vrijedi.

Zaključujemo da se točka  $(x \cdot y, y)$  nalazi u presjeku pravaca  $AC$  i  $DE$ . Dakle,  $(x \cdot y, y)$  je konstruktibilna točka tj.  $x \cdot y$  je konstruktibilan broj.

Slika 4.14: Točka  $(x \cdot y, y)$  je konstruktibilna točka

2. Možemo pretpostaviti da je  $x \neq 0$ .  
Neka su  $A = (0, 0)$ ,  $C = (y, 1)$ ,  $D = (x, 0)$  i  $E = (x, 1)$ .

Vrijedi

$$\begin{aligned} AC &= \{\lambda(y, 1) \mid \lambda \in \mathbb{R}\} \\ &= \{(\lambda y, \lambda) \mid \lambda \in \mathbb{R}\} \end{aligned}$$

i

$$\begin{aligned} DE &= \{D + \mu(0, 1) \mid \mu \in \mathbb{R}\} \\ &= \{(x, \mu) \mid \mu \in \mathbb{R}\}. \end{aligned}$$

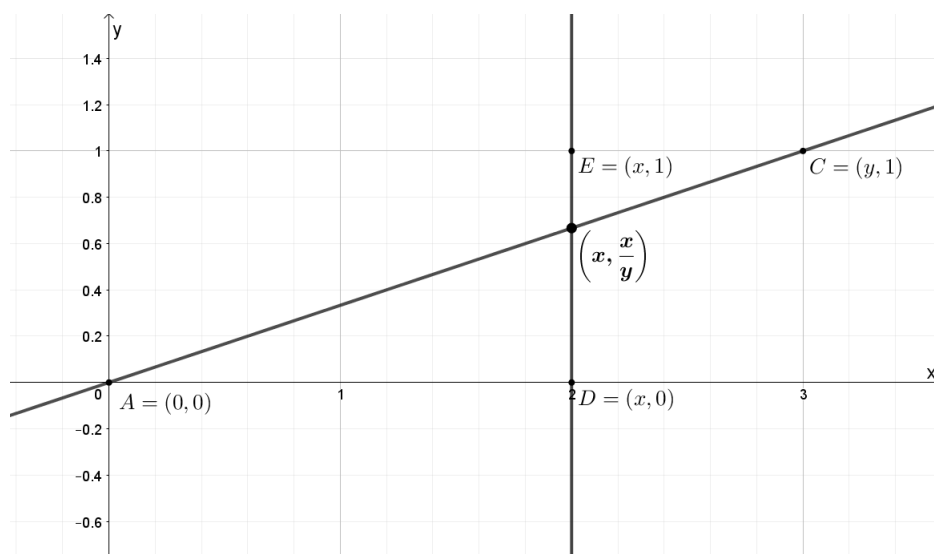
Pravci  $AC$  i  $DE$  su različiti jer je  $A \in AC$  i  $A \notin DE$ .

Uočimo da se točka  $(x, \frac{x}{y})$  nalazi u presjeku pravaca  $AC$  i  $DE$  (za  $\lambda = \mu = \frac{x}{y}$ ).

Prema propoziciji 4.1.4 točke  $C$ ,  $D$  i  $E$  su konstruktibilne pa slijedi da je točka  $(x, \frac{x}{y})$  konstruktibilna.

Dakle,  $\frac{x}{y}$  je konstruktibilan broj.

□



Slika 4.15: Točka  $(x, \frac{x}{y})$  je konstruktibilna točka

### 4.3 Karakterizacija konstruktibilnih brojeva

**Propozicija 4.3.1.** *Neka je  $x$  konstruktibilan broj,  $x \geq 0$ . Tada je  $\sqrt{x}$  konstruktibilan broj.*

*Dokaz.* Možemo pretpostaviti da je  $x > 0$ .

Neka su  $A = (0, 0)$ ,  $B = (0, 1)$ ,  $C = (x - 1, 0)$ ,  $D = (2x, 0)$  i  $E = (0, 2\sqrt{x})$ .

Prema propozicijama 4.2.1 i 4.2.2 brojevi  $x - 1$  i  $2x$  su konstruktibilni pa su prema propoziciji 4.1.4 točke  $C$  i  $D$  konstruktibilne.

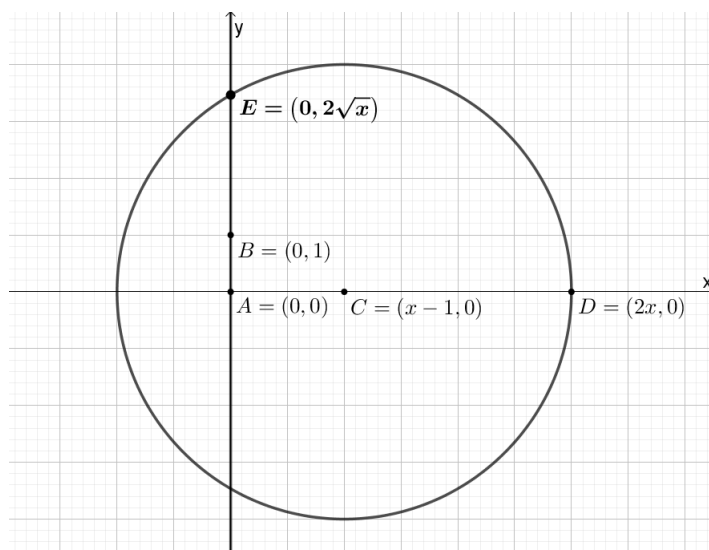
Nadalje,  $A$  i  $B$  su konstruktibilne, a vrijedi  $AB = \{(0, t) \mid t \in \mathbb{R}\}$ .

Imamo

$$\begin{aligned}
 d(C, E) &= \sqrt{(x-1)^2 + (2\sqrt{x})^2} \\
 &= \sqrt{x^2 - 2x + 1 + 4x} \\
 &= \sqrt{x^2 + 2x + 1} \\
 &= \sqrt{(x+1)^2} \\
 &= x + 1.
 \end{aligned}$$

Također,  $d(C, D) = x + 1$ . Stoga je

$$E \in AB \cap K(C, d(C, D)).$$



Slika 4.16: Točka  $E$  je konstruktibilna točka

Zaključujemo da je  $E$  konstruktibilna točka. Stoga je  $2\sqrt{x}$  konstruktibilan broj.

Iz drugog dijela propozicije 4.2.2 slijedi da je  $\frac{2\sqrt{x}}{2}$  konstruktibilan broj.

Dakle,  $\sqrt{x}$  je konstruktibilan broj.

□

**Propozicija 4.3.2.** *Svaki racionalan broj je konstruktibilan.*

*Dokaz.* Znamo da je 1 konstruktibilan broj pa iz drugog dijela propozicije 4.2.1 lako indukcijom dobivamo da je svaki prirodan broj konstruktibilan.

Iz  $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-n \mid n \in \mathbb{N}\}$  i prvog dijela propozicije 4.2.1 slijedi da je svaki cijeli broj konstruktibilan.

Svaki racionalan broj  $q$  se može napisati u obliku  $q = \frac{m}{n}$ ,  $m \in \mathbb{Z}$ ,  $n \in \mathbb{N}$ , pa iz drugog dijela propozicije 4.2.2 slijedi da je svaki racionalan broj konstruktibilan. □

**Propozicija 4.3.3.** *Ako je  $x_0, \dots, x_n$  korijenski niz, onda je svaki element od  $\mathbb{Q}[x_0, \dots, x_n]$  konstruktibilan broj.*



*Dokaz.* Dokažimo ovo indukcijom po  $n$ .

Za  $n = 0$  imamo  $x_0^2 \in \mathbb{Q}$  i

$$\mathbb{Q}[x_0] = \{a + b \cdot x_0 \mid a, b \in \mathbb{Q}\} \quad (\nabla)$$

(prema propoziciji 2.2.12).

Označimo  $x_0^2 = r$ . Prema propoziciji 4.3.2 slijedi da je  $r$  konstruktibilan broj.

Budući da je

$$x_0 = \sqrt{r} \text{ ili } x_0 = -\sqrt{r},$$

iz propozicija 4.3.1 i 4.2.1 slijedi da je  $x_0$  konstruktibilan broj.

Iz  $(\nabla)$  i propozicija 4.2.2, 4.2.1 i 4.3.2 slijedi da je svaki element od  $\mathbb{Q}[x_0]$  konstruktibilan broj.

Pretpostavimo da je  $n \in \mathbb{N}_0$  te da tvrdnja vrijedi za svaki korijenski niz  $x_0, \dots, x_n$ .

Neka je  $x_0, \dots, x_{n+1}$  korijenski niz.

Imamo  $\mathbb{Q}[x_0, \dots, x_{n+1}] = (\mathbb{Q}[x_0, \dots, x_n])[x_{n+1}]$ . Vrijedi  $x_{n+1}^2 \in \mathbb{Q}[x_0, \dots, x_n]$  te prema propoziciji 2.2.12 vrijedi

$$\mathbb{Q}[x_0, \dots, x_{n+1}] = \{a + b \cdot x_{n+1} \mid a, b \in \mathbb{Q}[x_0, \dots, x_n]\}.$$

Prema induktivnoj pretpostavci svaki element od  $\mathbb{Q}[x_0, \dots, x_n]$  je konstruktibilan broj.

Na isti način kao i prije dolazimo do zaključka da je  $x_{n+1}$  konstruktibilan broj, odnosno da je svaki element od  $\mathbb{Q}[x_0, \dots, x_{n+1}]$  konstruktibilan broj.

Time je tvrdnja propozicije dokazana. □

**Korolar 4.3.4.** *Svaki kvadratni radikal je konstruktibilan broj.*

*Dokaz.* Tvrdnja slijedi iz prethodne propozicije i definicije kvadratnog radikala. □

**Korolar 4.3.5.** *Realan broj je konstruktibilan ako i samo ako je kvadratni radikal.*

*Dokaz.* Tvrdnja slijedi iz prethodnog korolara i teorema 3.2.2. □

# Bibliografija

- [1] H. S. M. Coxeter, *Introduction to Geometry*, J. Wiley, New York, 1969.
- [2] B. Pavković, D. Veljan, *Elementarna matematika 1*, Tehnička knjiga, Zagreb, 1992.



# Sažetak

U ovom diplomskom radu smo proučavali konstruktibilnost brojeva i točaka. Glavni cilj bio je pokazati kada je realni broj konstruktibilan. Rad smo podijelili na četiri poglavlja u kojima smo pomoću poznatih pojmova poput pravca, kružnice, grupe, prstena, polja, polinoma, ali i nekih *novih* pojmova, objasnili što znači da se točka može konstruirati iz danog skupa, što je konstruktibilna točka te naposljetku, što je konstruktibilan broj. Kroz prikazanu terminologiju i teoriju dokazali smo koji uvjet realni broj treba ispuniti da bi bio konstruktibilan.



# Summary

In this thesis we were studying the constructibility of numbers and points. The main goal was to show when a real number is constructible. We divided the paper into four chapters in which we explained, using known concepts such as a line, a circle, a group, a ring, a field, a polynomial, and some *new* ones, what does it mean that a point can be constructed from a given set, what is a constructible point, and finally, what is a constructible number. Through the terminology and theory presented, we have proved which condition a real number must fulfill in order to be constructible.



# Životopis

Rođena sam 21. travnja 1994. godine u Zagrebu. Pohađala sam Osnovnu školu Tina Ujevića u Zagrebu. Nakon završetka osnovne škole upisala sam Drugu gimnaziju, također u Zagrebu. Maturirala sam 2013. godine te iste godine započela svoje fakultetsko obrazovanje upisom na preddiplomski sveučilišni studij Matematika; smjer: nastavnički, na Prirodoslovno-matematičkom fakultetu Sveučilišta u Zagrebu. Na istom fakultetu sam 2017. godine upisala diplomski studij Matematika; smjer: nastavnički.