Kvadratna polja

Turić, Marija

Master's thesis / Diplomski rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, School of Applied Mathematics and Informatics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet primijenjene matematike i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:952579

Sveučilište Josipa Jurja Strossmayera u Osijeku

Fakultet primijenjene matematike i informatike

Sveučilišni diplomski studij matematike
modul: financijska matematika i statistika

Kvadratna polja

Diplomski rad

Mentor:

izv. prof. dr. sc. Mirela Jukić Bokun

Student:

Marija Turić

Osijek, 2023.

Sadržaj

1 | Uvod

Algebra je područje matematike koje se bavi algebarskim strukturama. Algebarska struktura je skup na kojem je definirana barem jedna operacija i zadovoljena su određena svojstva. Jedna od osnovnih algebarskih struktura su polja kod kojih se definiraju operacije zbrajanja i množenja.

Može se postaviti pitanje je li jednadžbu

$$y^2 = x^3 - 2$$

moguće riješiti u cijelim brojevima korištenjem faktorizacije

$$x^3 = (y + \sqrt{-2})(y - \sqrt{-2}).$$

Navedena motivacija nas vodi do proučavanja svojstava polja algebarskih brojeva i njihovih prstena cijelih brojeva. Najjednostavniji među njima, osim polja $\mathbb{Q}$ i pripadnog prstena $\mathbb{Z}$, su kvadratna polja što je ujedno i tema ovog diplomskog rada.

Prije istraživanja kvadratnih polja, u drugom poglavlju definirat ćemo osnovne algebarske strukture te navesti neke pojmove i tvrdnje iz teorije algebarskih brojeva. Treće poglavlje posvećeno je kvadratnim poljima i njihovim prstenima cijelih brojeva. Nadalje, definirat ćemo invertibilni element te iskazati i dokazati tvrdnje vezane za invertibilne elemente u realnim i imaginarnim kvadratnim poljima. U završnom četvrtom poglavlju ćemo se baviti s jedinstvenošću faktorizacije u kvadratnim poljima.

2 | Osnovni pojmovi

U ovom poglavlju definirat ćemo osnovne algebarske strukture. Nadalje, uvest ćemo neke pojmove te iskazati i dokazati neke tvrdnje iz teorije algebarskih brojeva koje su nužne za razumijevanje ovog rada. Više o osnovnim algebarskim strukturama te pojmovima i tvrdnjama iz teorije algebarskih brojeva se može naći u [2, 3, 5, 6].

Definicija 1. *Neka je R neprazan skup na kojem su zadane dvije binarne operacije, zbrajanje $(a,\ b) \mapsto a + b$ i množenje $(a,\ b) \mapsto a \cdot b$, za $(a,\ b \in R)$. Kažemo da je uređena trojka $(R,\ +,\ \cdot)$ prsten ako vrijedi:*

(1) $(R,\ +)$ je Abelova grupa s neutralnim elementom 0,

(2) $(R,\ \cdot)$ je polugrupa,

(3) množenje je i slijeva i zdesna distributivno u odnosu na zbrajanje, odnosno za sve $a,\ b,\ c \in R$ vrijedi $a \cdot (b + c) = ab + ac$, $(a + b) \cdot c = ac + bc$.

Ako vrijedi komutativnost množenja, onda kažemo da je R komutativan prsten. Kažemo da je R prsten s jedinicom ili unitalan prsten ako je R u odnosu na množenje monoid. Primjeri komutativnog prstena s jedinicom su skupovi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Definicija 2. *Neka je R prsten s jedinicom. Kažemo da je $a \in R$ invertibilan element ako postoji $b \in R$ takav da je $ab = ba = 1$. Takav element b nazivamo inverz od a i označavamo s a^{-1}.*

Skup svih invertibilnih elemenata u R označavamo s $R^\star$. U prstenu $\mathbb{Z}$ su 1 i -1 jedini invertibilni elementi.

Definicija 3. *Neka je R komutativan netrivijalan prsten s jedinicom. Ako je $R^\star = R \setminus \{0\}$ kažemo da je prsten R polje.*

Primjeri polja su $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Definicija 4. *Neka su F i K polja te $F \subseteq K$. Tada kažemo da je K proširenje polja F.*

Primjerice, $\mathbb{R}$ je proširenje polja $\mathbb{Q}$, a $\mathbb{C}$ je proširenje polja $\mathbb{Q}$ i $\mathbb{R}$. Ako je K proširenje polja F, tada K možemo promatrati i kao vektorski prostor nad poljem F. Ako je taj vektorski prostor konačnodimenzionalan kažemo da je K konačno proširenje polja F. Tada dimenziju od K nazivamo stupanj proširenja te označavamo s $[K : F]$.

Neka je R prsten. Općenito, polinom u jednoj varijabli nad R je izraz oblika

$$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

gdje su $a_0,\ a_1,\ a_2, \ldots,\ a_n \in R$. Prsten polinoma u jednoj varijabli nad R označavamo s $R[x]$.

Definicija 5. *Neka je K proširenje polja F. Za element $\delta \in K$ kažemo da je algebarski nad F ako postoji nekonstantni polinom $Q \in F[x]$ takav da je $Q(\delta) = 0$.*

Ukoliko δ nije algebarski kažemo da je transcendentan nad F. Mi ćemo u nastavku promatrati algebarske brojeve nad poljem $\mathbb{Q}$.

Primjer 1. *Broj $\sqrt{2}$ je algebarski. Naime, $\mathbb{Q} \subseteq \mathbb{R}$ i $\sqrt{2} \in \mathbb{R}$. Kako je $P(x) = x^2 - 2 \in \mathbb{Q}[x]$ i $P(\sqrt{2}) = 0$ zaključujemo da je $\sqrt{2}$ algebarski broj.*

Primjer 2 (vidjeti [2])**.** *Transcendentni brojevi su $e, \pi \in \mathbb{R}$.*

Teorem 1 (vidjeti [5, Teorem 12.1.])**.** *Za svaki algebarski broj δ postoji jedinstveni polinom*

$$A(x) = a_n x^n + \cdots + a_1 x + a_0$$

sa sljedećim svojstvima:

(1) $A(x) \in \mathbb{Z}[x]$,

(2) $a_n > 0$ *i* $a_0,\ a_1, \ldots,\ a_n$ *su relativno prosti,*

(3) $A(\delta) = 0$,

(4) ako je $B(x) \in \mathbb{Q}[x]$ *takav da je* $B(\delta) = 0$, *onda* $A(x) \mid B(x)$ *u* $\mathbb{Q}[x]$,

(5) $A(x)$ *je ireducibilan nad* $\mathbb{Q}$.

Definicija 6. *Polinom $A(x)$ opisan u Teoremu 1 je cjelobrojni minimalni polinom algebarskog broja δ. Minimalni polinom od δ je polinom $Q(x) = \frac{1}{a_n} A(x)$ takav da je $Q(\delta) = 0$.*

Kažemo da je δ algebarski broj stupnja n ako je δ algebarski i stupanj pripadnog mu minimalnog polinoma je n. Na primjer, $\sqrt{3}$ je algebarski broj stupnja 2 jer je $\sqrt{3}$ korijen polinoma $Q(x) = x^2 - 3$.

Teorem 2 (vidjeti [5, Teorem 12.2.])**.** *Skup svih algebarskih brojeva čini polje.*

Polje algebarskih brojeva je proširenje polja racionalnih brojeva $\mathbb{Q}$.

Definicija 7. *Algebarski broj δ čiji minimalni polinom ima cjelobrojne koeficijente naziva se algebarski cijeli broj.*

U nastavku ćemo iskazati i dokazati da je zbroj i produkt dva algebarska cijela broja također algebarski cijeli broj.

Teorem 3 (vidjeti [3, Theorem 1]). *Ako su α, β algebarski cijeli brojevi, onda su $\alpha+\beta$ i $\alpha\cdot\beta$ algebarski cijeli brojevi.*

Za dokaz prethodnog teorema potrebna nam je sljedeća lema.

Lema 1 (vidjeti [3, Lemma 1]). *Broj α je algebarski cijeli broj ako i samo ako je α svojstvena vrijednost kvadratne matrice s cjelobrojnim elementima.*

Dokaz. Neka je A kvadratna matrica s cjelobrojnim elementima. Karakteristični polinom od A je

$$k_A(\lambda) = \det(\lambda I - A),$$

pri čemu primijetimo kako je $k_A(\lambda)$ minimalni polinom s cjelobrojnim koeficijentima. Kako je α svojstvena vrijednost matrice A, onda je

$$k_A(\alpha) = 0$$

pa je α algebarski cijeli broj.
Obratno, pretpostavimo da je α algebarski cijeli broj. Tada postoje cijeli brojevi a_i takvi da je

$$\alpha^n = -a_1\alpha^{n-1} - \cdots - a_{n-1}\alpha - a_n.$$

Nadalje, definiramo vektor

$$x = (1\ \alpha\ \ldots\ \alpha^{n-1})^T$$

pa je

$$\alpha x = \begin{bmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^{n-1} \\ \alpha^n \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ -a_n & -a_{n-1} & -a_{n-2} & -a_{n-3} & \ldots & -a_1 \end{bmatrix} \begin{bmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-2} \\ \alpha^{n-1} \end{bmatrix} = Ax,$$

gdje je A kvadratna matrica s cjelobrojnim elementima. Iz prethodnog slijedi da je α svojstvena vrijednost matrice A sa svojstvenim vektorom x i time je dokazana lema. □

Dokaz Teorema 3. Neka su α, β algebarski cijeli brojevi. Ideja dokaza je pronaći ne−nul vektor x i dvije kvadratne matrice A i B s cjelobrojnim elementima takve da je $Ax = \alpha x$ i $Bx = \beta x$. To će implicirati da su $\alpha+\beta$ i $\alpha\cdot\beta$ redom svojstvene vrijednosti matrica $A+B$ i $A\cdot B$. Pretpostavimo sada da je

$$\begin{aligned} \alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n &= 0, \\ \beta^m + b_1\beta^{m-1} + \cdots + b_{m-1}\beta + b_m &= 0, \end{aligned}$$

gdje su $a_i,\ b_j \in \mathbb{Z}$, $i \in \{1,\ \ldots,\ n\}$, $j \in \{1,\ \ldots,\ m\}$. Nadalje, neka je x vektor s mn redaka, odnosno

$$x = (1\ \alpha\ \alpha^2\ \ldots\ \alpha^{n-1}\ \beta\ \alpha\beta\ \alpha^2\beta\ \ldots\ \alpha^{n-1}\beta\ \ldots\ \beta^{m-1}\ \alpha\beta^{m-1}\ \alpha^2\beta^{m-1}\ \ldots\ \alpha^{n-1}\beta^{m-1})^T.$$

Promotrimo vektor αx te uočavamo da je

$$\alpha^n \beta^j = -a_1 \alpha^{n-1} \beta^j - \cdots - a_{n-1} \alpha \beta^j - a_n \beta^j,\ 0 \leq j < m.$$

Kako je svaki $\alpha^i \beta^j$ linearna kombinacija elemenata iz x postoji kvadratna matrica A s cjelobrojnim koeficijentima takva da je $Ax = \alpha x$. Analogno se pokaže da postoji kvadratna matrica B s cjelobrojnim koeficijentima takva da je $Bx = \beta x$. Slijedi

$$\begin{aligned} (A+B)x &= Ax + Bx = \alpha x + \beta x = (\alpha + \beta)x, \\ (A \cdot B)x &= A(Bx) = A(\beta x) = \beta(Ax) = \beta(\alpha x) = (\alpha\beta)x \end{aligned}$$

pa su $\alpha + \beta$ i $\alpha \cdot \beta$ redom svojstvene vrijednosti matrica $A + B$ i $A \cdot B$. Dakle, prema prethodnoj lemi slijedi da su $\alpha + \beta$ i $\alpha \cdot \beta$ algebarski cijeli brojevi. □

Skup svih algebarskih cijelih brojeva čini prsten.

Propozicija 1 (vidjeti [5, Propozicija 12.3.]). *Jedini algebarski cijeli brojevi u skupu racionalnih brojeva su cijeli brojevi.*

Dokaz. Svaki cijeli broj p je algebarski cijeli broj jer je p korijen polinoma $g(x) = x - p$. Ako je $\frac{p}{q}$ algebarski cijeli broj, gdje je $q \in \mathbb{N}$, p i q relativno prosti, onda imamo

$$\left(\frac{p}{q}\right)^n + a_1 \left(\frac{p}{q}\right)^{n-1} + \cdots + a_n = 0, \tag{2.1}$$

gdje su $a_1, \ldots, a_n \in \mathbb{Z}$. Množenjem jednakosti (2.1) s q^n dobivamo

$$p^n + a_1 q p^{n-1} + \cdots + a_n q^n = 0.$$

Iz prethodne jednakosti slijedi $q \mid p^n$. Kako su p i q relativno prosti, onda je $q = \pm 1$ pa zaključujemo da je $\frac{p}{q}$ cijeli broj.

□

3 | Kvadratno polje

Osnovni pojmovi i tvrdnje koje su korištene u ovom poglavlju bazirani su na [1, 2, 3, 4, 5].

Definicija 8. *Neka je m racionalan broj koji nije potpun kvadrat. Kvadratno polje $\mathbb{Q}(\sqrt{m})$ je skup svih brojeva oblika $x + y\sqrt{m}$, gdje su $x,\ y \in \mathbb{Q}$ uz uobičajene operacije zbrajanja i množenja, tj.*

$$\begin{aligned}(x_1 + y_1\sqrt{m}) + (x_2 + y_2\sqrt{m}) &= (x_1 + x_2) + (y_1 + y_2)\sqrt{m},\\ (x_1 + y_1\sqrt{m}) \cdot (x_2 + y_2\sqrt{m}) &= (x_1x_2 + y_1y_2m) + (x_1y_2 + x_2y_1)\sqrt{m}.\end{aligned}$$

Uvjerimo se da je $\mathbb{Q}(\sqrt{m})$ polje. Najprije, pokažimo da je $(\mathbb{Q}(\sqrt{m}),\ +)$ Abelova grupa:

(1) asocijativnost: $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$, za sve $\alpha,\ \beta,\ \gamma \in \mathbb{Q}(\sqrt{m})$

$$\begin{aligned}(\alpha + \beta) + \gamma &= (a + b\sqrt{m} + e + f\sqrt{m}) + g + h\sqrt{m}\\ &= (a + e) + g + ((b + f) + h)\sqrt{m}\\ &= a + (e + g) + (b + (f + h))\sqrt{m}\\ &= a + b\sqrt{m} + (e + f\sqrt{m} + g + h\sqrt{m}) = \alpha + (\beta + \gamma),\end{aligned}$$

(2) postoji $0 \in \mathbb{Q}(\sqrt{m})$ takav da je $\alpha + 0 = 0 + \alpha = \alpha$, za svaki $\alpha \in \mathbb{Q}(\sqrt{m})$

$$\begin{aligned}\alpha + 0 &= a + b\sqrt{m} + 0 + 0 \cdot \sqrt{m} = (a + 0) + (b + 0)\sqrt{m} = \alpha,\\ 0 + \alpha &= 0 + 0 \cdot \sqrt{m} + a + b\sqrt{m} = (0 + a) + (0 + b)\sqrt{m} = \alpha,\end{aligned}$$

(3) za svaki $\alpha \in \mathbb{Q}(\sqrt{m})$ postoji $-\alpha \in \mathbb{Q}(\sqrt{m})$ takav da je $\alpha + (-\alpha) = -\alpha + \alpha = 0$

$$\begin{aligned}\alpha + (-\alpha) &= a + b\sqrt{m} - a - b\sqrt{m} = (a - a) + (b - b)\sqrt{m} = 0,\\ -\alpha + \alpha &= -a - b\sqrt{m} + a + b\sqrt{m} = (-a + a) + (-b + b)\sqrt{m} = 0,\end{aligned}$$

(4) komutativnost: $\alpha + \beta = \beta + \alpha$, za sve $\alpha,\ \beta \in \mathbb{Q}(\sqrt{m})$

$$\begin{aligned}\alpha + \beta &= a + b\sqrt{m} + e + f\sqrt{m} = (a + e) + (b + f)\sqrt{m}\\ &= (e + a) + (f + b)\sqrt{m} = e + f\sqrt{m} + a + b\sqrt{m} = \beta + \alpha.\end{aligned}$$

Dakle, $(\mathbb{Q}(\sqrt{m}),\ +)$ je Abelova grupa. Nadalje, pokažimo da je $(\mathbb{Q}(\sqrt{m}) \setminus \{0\},\ \cdot)$ Abelova grupa:

(1) asocijativnost: $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$, za sve $\alpha,\ \beta,\ \gamma \in \mathbb{Q}(\sqrt{m})$

$$\begin{aligned}(\alpha \cdot \beta) \cdot \gamma &= ((a+b\sqrt{m}) \cdot (e+f\sqrt{m})) \cdot (g+h\sqrt{m}) \\ &= (ae+bfm) \cdot g + (ae+bfm) \cdot h\sqrt{m} \\ &+ (af+be) \cdot g\sqrt{m} + (af+be) \cdot hm \\ &= (a+b\sqrt{m}) \cdot fg\sqrt{m} + (a+b\sqrt{m}) \cdot eg \\ &+ (a+b\sqrt{m}) \cdot eh\sqrt{m} + (a+b\sqrt{m}) \cdot fhm \\ &= (a+b\sqrt{m}) \cdot ((e+f\sqrt{m}) \cdot (g+h\sqrt{m})) = \alpha \cdot (\beta \cdot \gamma),\end{aligned}$$

(2) postoji $1 \in \mathbb{Q}(\sqrt{m})$ takav da je $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$, za svaki $\alpha \in \mathbb{Q}(\sqrt{m})$

$$\begin{aligned}\alpha \cdot 1 &= (a+b\sqrt{m}) \cdot (1+0 \cdot \sqrt{m}) = 1 \cdot a + 1 \cdot b\sqrt{m} + 0 + 0 = \alpha, \\ 1 \cdot \alpha &= (1+0 \cdot \sqrt{m}) \cdot (a+b\sqrt{m}) = a \cdot 1 + 0 + b\sqrt{m} + 0 = \alpha,\end{aligned}$$

(3) za svaki $\alpha \in \mathbb{Q}(\sqrt{m}) \setminus \{0\}$ postoji $\alpha^{-1} \in \mathbb{Q}(\sqrt{m})$ takav da je $\alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = 1$

$$\begin{aligned}\alpha \cdot \alpha^{-1} &= (a+b\sqrt{m}) \cdot \frac{a-b\sqrt{m}}{a^2-mb^2} = 1, \\ \alpha^{-1} \cdot \alpha &= \frac{a-b\sqrt{m}}{a^2-mb^2} \cdot (a+b\sqrt{m}) = 1,\end{aligned}$$

(4) komutativnost: $\alpha \cdot \beta = \beta \cdot \alpha$, za sve $\alpha,\ \beta \in \mathbb{Q}(\sqrt{m})$

$$\begin{aligned}\alpha \cdot \beta &= (a+b\sqrt{m}) \cdot (e+f\sqrt{m}) = ae + af\sqrt{m} + b\sqrt{m}e + bfm \\ &= ea + f\sqrt{m}a + eb\sqrt{m} + fbm = (e+f\sqrt{m}) \cdot a + (e+f\sqrt{m}) \cdot b\sqrt{m} \\ &= \beta \cdot \alpha.\end{aligned}$$

Dakle, $(\mathbb{Q}(\sqrt{m}) \setminus \{0\}, \cdot)$ je Abelova grupa. Preostaje nam pokazati distributivnost slijeva i zdesna u odnosu na zbrajanje. Pokazat ćemo da vrijedi distributivnost slijeva, analogno se pokaže za distributivnost zdesna. Slijedi

$$\begin{aligned}\alpha \cdot (\beta+\gamma) &= (a+b\sqrt{m}) \cdot (e+g+(f+h)\sqrt{m}) \\ &= a \cdot (e+g) + a \cdot (f+h)\sqrt{m} + b\sqrt{m} \cdot (e+g) + b\sqrt{m} \cdot (f+h)\sqrt{m} \\ &= (a+b\sqrt{m})e + (a+b\sqrt{m})f\sqrt{m} + (a+b\sqrt{m})g + (a+b\sqrt{m})h\sqrt{m} \\ &= \alpha \cdot \beta + \alpha \cdot \gamma.\end{aligned}$$

Specijalno, za $m = -1$, polje $\mathbb{Q}(i)$ se zove polje Gaussovih brojeva i njegove elemente označavat ćemo s $x + yi$. U nastavku ćemo karakterizirati jednakost dva kvadratna polja.

Propozicija 2 (vidjeti [3, Proposition 2]). *Neka su $\mathbb{Q}(\sqrt{m})$ i $\mathbb{Q}(\sqrt{n})$ kvadratna polja. Tada je $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$ ako i samo ako je $\frac{m}{n}$ kvadrat racionalnog broja.*

Dokaz. Ako je $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$, onda je $\sqrt{m} \in \mathbb{Q}(\sqrt{n})$ i možemo pisati

$$\sqrt{m} = x + y\sqrt{n},$$

gdje su $x,\ y \in \mathbb{Q}$. Kvadriranjem prethodne jednakosti dobivamo

$$m = x^2 + 2xy\sqrt{n} + y^2 n.$$

Slijedi

$$\begin{aligned} m &= x^2 + y^2 n, \\ 2xy &= 0 \end{aligned}$$

pa je ili $x = 0$ ili $y = 0$. Za $y = 0$ dobivamo

$$m = x^2,$$

što je kontradikcija s pretpostavkom da m nije potpun kvadrat. Preostaje slučaj $x = 0$ za koji se dobiva

$$\frac{m}{n} = y^2,$$

što je i trebalo dokazati.
Obratno, ako je $\frac{m}{n} = y^2$, gdje je $y \in \mathbb{Q}$, onda je $m = y^2 n$. Iz ove jednakosti slijedi

$$\begin{aligned} \sqrt{m} &= y\sqrt{n}, \\ \sqrt{n} &= \frac{1}{y}\sqrt{m}. \end{aligned}$$

Dakle,

$$\begin{aligned} u + v\sqrt{m} &= u + vy\sqrt{n}, \\ s + t\sqrt{n} &= s + \frac{t}{y}\sqrt{m}. \end{aligned}$$

Iz prethodnih jednakosti slijedi $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\sqrt{n})$ i $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\sqrt{m})$ i time je jednakost dva kvadratna polja dokazana. □

Propozicija 3 (vidjeti [3, Proposition 3])**.** *Ako je F kvadratno polje, onda je $F = \mathbb{Q}(\sqrt{m})$, gdje je m jedinstveno određen kvadratno slobodan cijeli broj različit od 1.*

Dokaz. Ako je $F = \mathbb{Q}\left(\sqrt{\frac{x}{y}}\right)$, gdje su $x,\ y \in \mathbb{Z}$, onda je

$$F = \mathbb{Q}\left(\sqrt{y^2\left(\frac{x}{y}\right)}\right) = \mathbb{Q}(\sqrt{xy}).$$

Neka je $F = \mathbb{Q}(\sqrt{n})$, gdje je n cijeli broj. Ako n nije kvadratno slobodan, onda postoji cijeli broj $z \neq 1$ takav da $z^2 \mid n$. Tada je $F = \mathbb{Q}\left(\sqrt{\frac{n}{z^2}}\right)$ i možemo nastaviti dijeliti broj n s kvadratom prirodnog broja dok ne dođemo do kvadratnog

slobodnog broja m takav da je $F = \mathbb{Q}(\sqrt{m})$. Preostaje nam još pokazati jedinstvenost. Pretpostavimo da je

$$\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n}),$$

pri čemu su m i n kvadratno slobodni. Prema prethodnoj propoziciji znamo da je

$$\frac{m}{n} = y^2,\ y \in \mathbb{Q}$$

pa zaključujemo da m i n moraju biti istog predznaka. Označimo s

$$y = \frac{s}{t},$$

gdje su $s,\ t$ cijeli brojevi. Dobivamo

$$mt^2 = ns^2.$$

Ako postoji q prost broj koji dijeli m, onda se q pojavljuje s parnim eksponentom u faktorizaciji na proste faktore broja mt^2 i broja ns^2. Ali to također znači da $q \mid n$. Analognim zaključivanjem dobivamo da svaki prost broj koji dijeli n također dijeli m. Kako su m i n kvadratno slobodni te imaju isti prosti faktor i istog su predznaka, onda zaključujemo da su jednaki. □

Napomena 1. *U nastavku gdje god pišemo m podrazumijevamo da je m kvadratno slobodan cijeli broj različit od 1.*

3.1 Skalarne funkcije

Kako bismo mogli definirati dvije važne skalarne funkcije na $\mathbb{Q}(\sqrt{m})$, najprije moramo uvesti pojam konjugirani element.

Definicija 9. *Neka je $\gamma = u + v\sqrt{m} \in \mathbb{Q}(\sqrt{m})$. Kažemo da je $\overline{\gamma} = u - v\sqrt{m}$ konjugirani element od γ.*

Sljedeća propozicija govori o svojstvima konjugiranog elementa.

Propozicija 4 (vidjeti [4])**.** *Neka su $\gamma,\ \delta \in \mathbb{Q}(\sqrt{m})$. Tada vrijedi:*

(1) $\overline{\gamma + \delta} = \overline{\gamma} + \overline{\delta}$,

(2) $\overline{\gamma \cdot \delta} = \overline{\gamma} \cdot \overline{\delta}$,

(3) $\overline{\overline{\gamma}} = \gamma$,

(4) $\overline{\gamma} = \gamma \Leftrightarrow \gamma \in \mathbb{Q}$.

Dokaz. Neka su $\gamma = u + v\sqrt{m},\ \delta = s + t\sqrt{m} \in \mathbb{Q}(\sqrt{m})$.
(1)

$$\begin{aligned} \overline{\gamma + \delta} &= \overline{((u+s) + (v+t)\sqrt{m})} \\ &= (u+s) - (v+t)\sqrt{m} \\ &= u - v\sqrt{m} + s - t\sqrt{m} = \overline{\gamma} + \overline{\delta}. \end{aligned}$$

(2)

$$\begin{aligned}\overline{\gamma\cdot\delta} &= \overline{((us+vtm)+(ut+vs)\sqrt{m})}\\ &= (us+vtm)-(ut+vs)\sqrt{m}\\ &= u(s-t\sqrt{m})-v\sqrt{m}(s-t\sqrt{m})=\overline{\gamma}\cdot\overline{\delta}.\end{aligned}$$

(3)

$$\overline{\overline{\gamma}}=\overline{(u-v\sqrt{m})}=\gamma.$$

(4) Ako je $\overline{\gamma}=\gamma$, onda slijedi $\gamma=u\in\mathbb{Q}$.
Obratno, ako je $\gamma\in\mathbb{Q}$, onda je $\gamma=\overline{\gamma}$. □

Pokažimo još da su $\gamma+\overline{\gamma}$ i $\gamma\overline{\gamma}$ racionalni za $\gamma\in\mathbb{Q}(\sqrt{m})$. Neka je $\gamma=u+v\sqrt{m}\in\mathbb{Q}(\sqrt{m})$. Slijedi

$$\begin{aligned}\gamma+\overline{\gamma} &= u+v\sqrt{m}+(u-v\sqrt{m})=2u\in\mathbb{Q},\\ \gamma\cdot\overline{\gamma} &= (u+v\sqrt{m})\cdot(u-v\sqrt{m})=u^2-uv\sqrt{m}+uv\sqrt{m}-mv^2=u^2-mv^2\in\mathbb{Q}.\end{aligned}$$

U nastavku ćemo definirati dvije skalarne funkcije te iskazati i dokazati njihova svojstva.

Definicija 10. *Preslikavanje* $N:\mathbb{Q}(\sqrt{m})\to\mathbb{Q}$ *zadano s*

$$N(\delta)=\delta\overline{\delta}$$

nazivamo normom u $\mathbb{Q}(\sqrt{m})$.

Teorem 4 (vidjeti [5, Teorem 12.5.])**.** *Za* $\gamma,\ \delta\in\mathbb{Q}(\sqrt{m})$ *vrijedi:*

(1) $N(\gamma\delta)=N(\gamma)N(\delta)$ *(multiplikativnost norme),*

(2) $N(\gamma)=0\Leftrightarrow\gamma=0$.

Dokaz. (1) Neka su $\gamma,\ \delta\in\mathbb{Q}(\sqrt{m})$. Iz definicije norme i multiplikativnosti konjugiranog elementa dobivamo

$$\begin{aligned}N(\gamma\delta) &= \gamma\delta\cdot\overline{\gamma\delta}=\gamma\cdot\delta\cdot\overline{\gamma}\cdot\overline{\delta}\\ &= (\gamma\cdot\overline{\gamma})\cdot(\delta\cdot\overline{\delta})=N(\gamma)\cdot N(\delta).\end{aligned}$$

(2) Ako je $\gamma=0$, onda je $N(\gamma)=\gamma\overline{\gamma}=0$.
Obratno, ako je $N(\gamma)=0$, onda je $\gamma\overline{\gamma}=0$ pa je $\gamma=0$ ili $\overline{\gamma}=0$. Kako $\overline{\gamma}=0$ povlači da je $\gamma=0$, dokazali smo tvrdnju. □

Definicija 11. *Preslikavanje* $Tr:\mathbb{Q}(\sqrt{m})\to\mathbb{Q}$ *zadano s*

$$Tr(\delta)=\delta+\overline{\delta}$$

nazivamo tragom u $\mathbb{Q}(\sqrt{m})$.

Propozicija 5 (vidjeti [4, Theorem 2.2.])**.** *Za* $\gamma,\ \delta\in\mathbb{Q}(\sqrt{m})$ *vrijedi* $Tr(\gamma+\delta)=Tr(\gamma)+Tr(\delta)$.

Dokaz. Iz definicije traga i svojstva konjugiranog elementa dobivamo

$$\begin{aligned} Tr(\gamma+\delta) &= \gamma+\delta+\overline{\gamma+\delta} = \gamma+\delta+\overline{\gamma}+\overline{\delta} \\ &= \gamma+\overline{\gamma}+\delta+\overline{\delta} = Tr(\gamma)+Tr(\delta). \end{aligned}$$

□

Propozicija 6 (vidjeti [3, Proposition 4]). *Ako je γ algebarski cijeli broj u $\mathbb{Q}(\sqrt{m})$, onda su $N(\gamma)$, $Tr(\gamma)$ cijeli brojevi.*

Dokaz. Neka je γ algebarski cijeli broj. Tada postoje cijeli brojevi c_i takvi da je

$$\gamma^n + c_1\gamma^{n-1} + \cdots + c_{n-1}\gamma + c_n = 0.$$

Konjugiranjem prethodne jednakosti dobivamo

$$\overline{\gamma}^n + c_1\overline{\gamma}^{n-1} + \cdots + c_{n-1}\overline{\gamma} + c_n = 0$$

pa je također i $\overline{\gamma}$ algebarski cijeli broj. Pokazali smo u Teoremu 3 da je zbroj i produkt algebarskih cijelih brojeva ponovno algebarski cijeli broj pa slijedi da su $Tr(\gamma) = \gamma + \overline{\gamma}$ i $N(\gamma) = \gamma \cdot \overline{\gamma}$ algebarski cijeli brojevi. Prema Propoziciji 1 norma i trag su cijeli brojevi. □

Sada možemo odrediti kakvog su oblika algebarski cijeli brojevi u kvadratnom polju $\mathbb{Q}(\sqrt{m})$, o čemu govori sljedeći teorem.

Teorem 5 (vidjeti [5, Teorem 12.4.]). *Ako je $m \equiv 1 \pmod 4$, onda su algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{m})$ svi brojevi oblika*

$$q + r\frac{1+\sqrt{m}}{2},$$

gdje su q, $r \in \mathbb{Z}$. Ako je $m \equiv 2$ ili $3 \pmod 4$, onda su algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{m})$ svi brojevi oblika

$$s + t\sqrt{m},$$

gdje su s, $t \in \mathbb{Z}$.

Dokaz. Neka je $\gamma = s + t\sqrt{m}$ algebarski cijeli broj u $\mathbb{Q}(\sqrt{m})$ te neka je

$$\begin{aligned} a &= 2t, \\ b &= Tr(\gamma) = 2s, \\ c &= N(\gamma) = s^2 - mt^2. \end{aligned}$$

Prema Propoziciji 6 slijedi da su b i c cijeli brojevi. Vrijedi

$$ma^2 = b^2 - 4c \tag{3.1}$$

te kako je desna strana ove jednakosti cijeli broj i m kvadratno slobodan cijeli broj, slijedi da je i a cijeli broj.
Neka je $m \equiv 2$ ili $3 \pmod 4$. Iz (3.1) slijedi $b^2 \equiv a^2 m \pmod 4$. Kako kvadrat

cijelog broja kod dijeljenja s 4 daje ostatak 0 ili 1, vrijedi $b^2 \equiv 0$ ili $1 \pmod 4$. Nadalje, vrijedi i jedna od sljedeće tri mogućnosti $a^2m \equiv 0 \pmod 4$ ili $a^2m \equiv 2 \pmod 4$ ili $a^2m \equiv 3 \pmod 4$. Za b neparan broj, kongruencija $b^2 \equiv a^2m \pmod 4$ nije zadovoljena pa je b paran broj i vrijedi $b^2 \equiv 0 \pmod 4$. Kada bi a bio neparan, onda bi bilo da je $a^2m \equiv 2$ ili $3 \pmod 4$. Dakle, a mora isto biti paran broj. Slijedi da su s i t cijeli brojevi.
Neka je $m \equiv 1 \pmod 4$. Ako je a paran, onda je $a^2m \equiv 0 \pmod 4$, a u suprotnom je $a^2m \equiv 1 \pmod 4$. Sada iz $b^2 \equiv a^2m \pmod 4$ slijedi da su a i b iste parnosti. Zbog toga je $s - t = \frac{1}{2}(b - a)$ cijeli broj. Označimo s

$$\begin{aligned} q &:= s - t, \\ r &:= 2t. \end{aligned}$$

Zaključili smo da je q cijeli broj, a kako je $r = a$ onda je i on cijeli broj. Osim toga, dobivamo $s + t\sqrt{m} = q + r\frac{1+\sqrt{m}}{2}$.

□

Označimo s

$$\lambda := \begin{cases} \sqrt{m}, & \text{ako je } m \equiv 2 \text{ ili } 3 \pmod 4 \\ \frac{1+\sqrt{m}}{2}, & \text{ako je } m \equiv 1 \pmod 4. \end{cases}$$

Tada je λ algebarski cijeli broj u $\mathbb{Q}(\sqrt{m})$ i skup svih algebarskih cijelih brojeva u $\mathbb{Q}(\sqrt{m})$ je oblika $\mathbb{Z}[\lambda] = \{a + b\lambda : a, b \in \mathbb{Z}\}$.

Napomena 2. *Uočimo da su algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{m})$ su svi brojevi oblika $s + t\sqrt{m}$, $s, t \in \mathbb{Z}$ i ako je $m \equiv 1 \pmod 4$ su još i brojevi oblika $\frac{s+t\sqrt{m}}{2}$, s, t neparni.*

Sljedeća tablica prikazuje algebarske cijele brojeve za pojedina kvadratna polja.

$\mathbb{Q}(\sqrt{m})$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(i)$	$\mathbb{Q}(\sqrt{3})$	$\mathbb{Q}(\sqrt{13})$
$\mathbb{Z}[\lambda]$	$\mathbb{Z}[(1+\sqrt{-3})/2]$	$\mathbb{Z}[i]$	$\mathbb{Z}[\sqrt{3}]$	$\mathbb{Z}[(1+\sqrt{13})/2]$

Tablica 3.1: Algebarski cijeli brojevi u kvadratnim poljima

Propozicija 7 (vidjeti [3, Proposition 5][3]). *Neka su $\gamma, \delta \in \mathbb{Z}[\lambda]$. Tada je $\gamma + \delta$, $\gamma - \delta$, $\gamma \cdot \delta \in \mathbb{Z}[\lambda]$.*

Dokaz. Prisjetimo se da je $\gamma \in \mathbb{Z}[\lambda]$ ako i samo ako je γ algebarski cijeli broj i $\gamma \in \mathbb{Q}(\sqrt{m})$. Prema Teoremu 3 skup algebarskih cijelih brojeva je zatvoren s obzirom na zbrajanje, oduzimanje i množenje te je također i kvadratno polje $\mathbb{Q}(\sqrt{m})$ zatvoreno s istim tim operacijama. Slijedi $\gamma \pm \delta$, $\gamma \cdot \delta \in \mathbb{Z}[\lambda]$. □

Stoga je $\mathbb{Z}[\lambda]$ je prsten cijelih brojeva u kvadratnom polju $\mathbb{Q}(\sqrt{m})$.

Teorem 6 (vidjeti [4, Theorem 3.6.]). *Za svako kvadratno polje $\mathbb{Q}(\sqrt{m})$ vrijedi $\mathbb{Z}[\lambda] \cap \mathbb{Q} = \mathbb{Z}$ i svaki element kvadratnog polja $\mathbb{Q}(\sqrt{m})$ se može zapisati kao omjer elemenata iz njegovog prstena cijelih brojeva.*

Dokaz. Svaki element prstena $\mathbb{Z}[\lambda]$ je oblika $a + b\lambda$, gdje su $a,\ b \in \mathbb{Z}$. Kako $\lambda \notin \mathbb{Q}$ te ako je $a + b\lambda \in \mathbb{Q}$, onda je $b = 0$ i dobivamo da je $a + b\lambda = a \in \mathbb{Z}$.
Pokažimo sada da se svaki element kvadratnog polja $\mathbb{Q}(\sqrt{m})$ može zapisati kao omjer dva elementa iz $\mathbb{Z}[\lambda]$. Neka je

$$\alpha = x + y\sqrt{m},$$

gdje su $x,\ y \in \mathbb{Q}$ i zapišimo x i y kao razlomak sa zajedničkim nazivnikom, odnosno

$$\begin{aligned} x &= \frac{a}{c}, \\ y &= \frac{b}{c}, \end{aligned}$$

za neki c cijeli broj. Tada je

$$x + y\sqrt{m} = \frac{a + b\sqrt{m}}{c}.$$

Budući da je $\{a + b\sqrt{m} : a,\ b \in \mathbb{Z}\} \subset \mathbb{Z}[\lambda]$, time smo gotovi. □

3.2 Invertibilni elementi

Definicija 12. *Invertibilni element ili jedinica u $\mathbb{Q}(\sqrt{m})$ je algebarski cijeli broj α takav da je $\frac{1}{\alpha}$ algebarski cijeli broj.*

U nastavku ćemo iskazati i dokazati karakterizaciju invertibilnog elementa.

Teorem 7 (vidjeti [5, Teorem 12.5.])**.** *Neka je β algebarski cijeli broj u $\mathbb{Q}(\sqrt{m})$. Tada je β invertibilni element ako i samo ako je $N(\beta) = \pm 1$.*

Dokaz. Pretpostavimo je β invertibilni element. Iz multiplikativnosti norme dobivamo

$$N(\beta)N\left(\frac{1}{\beta}\right) = N(1) = 1. \tag{3.2}$$

Primjenom Propozicije 6 slijedi da su $N(\beta)$ i $N(\frac{1}{\beta})$ cijeli brojevi te iz (3.2) slijedi da je $N(\beta) = \pm 1$.
Pretpostavimo sada da je

$$N(\beta) = \pm 1$$

pa je

$$\beta\overline{\beta} = \pm 1.$$

Iz prethodne jednakosti slijedi

$$\frac{1}{\beta} = \pm\overline{\beta}.$$

Kako je β algebarski cijeli broj u $\mathbb{Q}(\sqrt{m})$ onda njegov minimlani polinom nad $\mathbb{Q}$ ima cjelobrojne koeficijente, a to je također i minimalni polinom od $\overline{\beta}$. Dakle, $\overline{\beta}$ je algebarski cijeli broj u $\mathbb{Q}(\sqrt{m})$. Nadalje, ako je $\overline{\beta}$ korijen polinoma

$$x^2 + bx + c = 0,$$

gdje su $b,\ c \in \mathbb{Z}$, onda je $-\overline{\beta}$ korijen polinoma

$$x^2 - bx + c = 0,$$

koji je također ireducibilan nad $\mathbb{Q}$. Zaključujemo da je i $-\overline{\beta}$ algebarski cijeli broj u $\mathbb{Q}(\sqrt{m})$ pa je i $\frac{1}{\beta}$ algebarski cijeli broj. Dakle, β je invertibilni element. □

Uočimo da je produkt dva invertibilna elementa također invertibilan element. Naime, kako su α i β invertibilni elementi iz multipikativnosti norme dobivamo da je

$$N(\alpha\beta) = N(\alpha)N(\beta) = \pm 1.$$

Primjenom prethodnog teorema slijedi da je $\alpha\beta$ invertibilni element.

Kažemo da je kvadratno polje $\mathbb{Q}(\sqrt{m})$ realno ako je $m > 0$, a imaginarno ako je $m < 0$. U imaginarnim kvadratnim poljima postoji konačno mnogo invertibilnih elemenata, o čemu govori sljedeći teorem.

Teorem 8 (vidjeti [5, Teorem 12.6.]). *Invertibilni elementi u imaginarnom kvadratnom polju $\mathbb{Q}(\sqrt{m})$ su ± 1 i to su jedini invertibilni elementi osim u slučajevima $m = -1$ i $m = -3$. Invertibilni elementi u $\mathbb{Q}(i)$ su $\pm 1,\ \pm i$, a u $\mathbb{Q}(\sqrt{-3})$ su $\pm 1,\ \frac{1\pm\sqrt{-3}}{2},\ \frac{-1\pm\sqrt{-3}}{2}$.*

Dokaz. Prema Teoremu 7 moramo pronaći sve algebarske cijele brojeve γ takve da je $N(\gamma) = \pm 1$. Ako je $m \equiv 2$ ili $3 \pmod 4$, onda je

$$\gamma = a + b\sqrt{m},$$

gdje su $a,\ b \in \mathbb{Z}$. Dakle, moramo riješiti jednadžbu

$$a^2 - mb^2 = \pm 1$$

u skupu cijelih brojeva. Kako je m negativan, onda jednadžba

$$a^2 - mb^2 = -1$$

nema rješenja.
Ako je $m \leq -2$, onda je

$$1 = a^2 - mb^2 \geq 2b^2$$

pa je jedino rješenje $b = 0$ te $a = \pm 1$ iz čega dobivamo da je $\gamma = \pm 1$.
Ako je $m = -1$, onda imamo jednadžbu

$$a^2 + b^2 = 1$$

čija su cjelobrojna rješenja $a = \pm 1,\ b = 0$ i $a = 0,\ b = \pm 1$. Iz prethodnog slijedi $\gamma = \pm 1,\ \pm i$.
Ukoliko je $m \equiv 1 \pmod 4$, onda je

$$\gamma = a + b\frac{1+\sqrt{m}}{2},$$

gdje su $a,\ b \in \mathbb{Z}$. Jednadžba koju moramo sada riješiti je oblika

$$\left(a+\frac{b}{2}\right)^2 - \frac{m}{4}b^2 = \pm 1.$$

Ponovno, zbog $m < 0$ jednadžba

$$\left(a+\frac{b}{2}\right)^2 - \frac{m}{4}b^2 = -1$$

nema rješenja.
Ako je $m \leq -7$, onda je

$$1 = \left(a+\frac{b}{2}\right)^2 - \frac{m}{4}b^2 \geq \frac{7}{4}b^2$$

pa je jedino rješenje $b = 0$ te $a = \pm 1$ iz čega dobivamo $\gamma = \pm 1$.
Od ostalih negativnih $m-$ova, jedino $m = -3$ zadovoljava kongruenciju koju ovdje promatramo. Za $m = -3$ imamo sljedeću jednadžbu

$$\left(a+\frac{b}{2}\right)^2 + \frac{3}{4}b^2 = 1, \tag{3.3}$$

odnosno

$$a^2 + ab + b^2 = 1.$$

Iz (3.3) slijedi da je $|b| \leq 1$ te dobivamo tri slučaja:

(1) Ako je $b = -1$, onda je $a = 0$ ili $a = 1$ pa je $\gamma = \frac{-1-\sqrt{-3}}{2}$ ili $\gamma = \frac{1-\sqrt{-3}}{2}$,

(2) Ako je $b = 0$, onda je $a = \pm 1$ pa je $\gamma = \pm 1$,

(3) Ako je $b = 1$, onda je $a = -1$ ili $a = 0$ pa je $\gamma = \frac{1+\sqrt{-3}}{2}$ ili $\gamma = \frac{-1+\sqrt{-3}}{2}$.

□

Sljedeći teorem nam govori da u realnim kvadratnim poljima nemamo konačno mnogo invertibilnih elemenata. Prije samog iskaza teorema, prisjetit ćemo se poznate jednadžbe iz teorije brojeva koja će nam biti potrebna za dokaz tog teorema.

Definicija 13. *Diofantska jednadžba oblika*

$$x^2 - my^2 = 1, \tag{3.4}$$

gdje je m kvadratno slobodan prirodan broj, naziva se Pellova jednadžba.

Definicija 14. *Jednadžbe oblika*

$$x^2 - my^2 = n,$$

gdje je m kvadratno slobodan prirodan broj i n cijeli broj različit od 0*, nazivaju se pellovske jednadžbe.*

Pellova jednadžba ima beskonačno mnogo rješenja. Više o rješenjima gore navedenih jednadžbi može se naći u [5].

Teorem 9 (vidjeti [5, Teorem 12.7.]). *U svakom realnom kvadratnom polju postoji beskonačno mnogo invertibilnih elemenata.*

Dokaz. Brojevi $\gamma = x + y\sqrt{m}$, $x, y \in \mathbb{Z}$ su algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{m})$ s normom

$$N(\gamma) = x^2 - my^2.$$

Ako je ta norma jednaka 1, odnosno

$$x^2 - my^2 = 1 \tag{3.5}$$

onda je γ invertibilni element. Jednadžba (3.5) je Pellova jednadžba i ona za kvadratno slobodan broj $m > 1$ ima beskonačno mnogo rješenja. □

Dakle, problem pronalaženja invertibilnih elemenata u realnim kvadratnim poljima povezan je s rješavanjem Pellove i pellovskih jednadžbi. Preciznije:

- ako je $m \equiv 2$ ili $3 \pmod 4$, onda je $x + y\sqrt{m}$ invertibilni element u $\mathbb{Q}(\sqrt{m})$ ako i samo ako vrijedi $x^2 - my^2 = \pm 1$,
- ako je $m \equiv 1 \pmod 4$, onda je $\frac{x+y\sqrt{m}}{2}$ invertibilni element u $\mathbb{Q}(\sqrt{m})$ ako i samo ako vrijedi $x^2 - my^2 = \pm 4$.

Teorem 10 (vidjeti [5, Korolar 12.8.]). *Grupa invertibilnih elemenata u realnom kvadratnom polju $\mathbb{Q}(\sqrt{m})$ ima dva generatora: -1 i ξ_m, gdje je*

$$\xi_m = u + v\sqrt{m}$$

ili

$$\xi_m = \frac{u + v\sqrt{m}}{2},$$

dok je $u + v\sqrt{m}$ fundamentalno rješenje jedne od jednadžbi $x^2 - my^2 = \pm 1, \pm 4$. Dakle, svaki se invertibilni element može napisati u obliku $\pm\xi_m^n$, $n \in \mathbb{Z}$. Fundamentalna jedinica kvadratnog polja $\mathbb{Q}(\sqrt{m})$ je generator ξ_m. Ako je $x_1 + y_1\sqrt{m}$ fundamentalno rješenje Pellove jednadžbe, onda je $x_1 + y_1\sqrt{m} = (u + v\sqrt{m})^v$, gdje je $v \in \{1, 2, 3, 6\}$.

Pitamo se kako naći fundamentalno rješenje. Traženje takvog rješenja usko je povezano s konvergentama u razvoju broja $\sqrt{m}$ u verižni razlomak. Više o tome se može pronaći u [5]. U nastavku navodimo primjere pronalaženja invertibilnih elemenata u realnim kvadratnim poljima.

Primjer 3. *Odredimo sve invertibilne elemente u kvadratnom polju $\mathbb{Q}(\sqrt{3})$.*
Primijetimo da je $m \equiv 3 \pmod 4$ pa je $x + y\sqrt{3}$ invertibilni element u $\mathbb{Q}(\sqrt{3})$ ako i samo ako vrijedi

$$x^2 - 3y^2 = \pm 1.$$

Trebamo naći fundamentalna rješenja pripadnih jednadžbi. Razvijanjem $\sqrt{3}$ *u verižni razlomak dobivamo paran period. Kako je period paran broj, onda jednadžba*

$$x^2 - 3y^2 = -1$$

nema cjelobrojnih rješenja. Fundamentalno rješenje jednadžbe

$$x^2 - 3y^2 = 1$$

je oblika $2 + \sqrt{3}$*. Dakle, invertibilni elementi u* $\mathbb{Q}(\sqrt{3})$ *su* ± 1*,* $\pm(2+\sqrt{3})^n$*,* $n \in \mathbb{Z}$*.*

Primjer 4. *Odredimo sve invertibilne elemente u* $\mathbb{Q}(\sqrt{5})$*.*
Uočimo da je $m \equiv 1 \pmod 4$ *pa je* $\frac{x+y\sqrt{5}}{2}$ *invertibilni element u* $\mathbb{Q}(\sqrt{5})$ *ako i samo ako vrijedi*

$$x^2 - 5y^2 = \pm 4.$$

Fundamentalno rješenje jednadžbe

$$x^2 - 5y^2 = -4$$

je $1 + \sqrt{5}$*, dok je* $3 + \sqrt{5}$ *fundamentalno rješenje jednadžbe*

$$x^2 - 5y^2 = 4.$$

Invertibilni elementi u $\mathbb{Q}(\sqrt{5})$ *su* ± 1*,* $\pm\left(\frac{3+\sqrt{5}}{2}\right)^n$*,* $n \in \mathbb{Z}$*,* $\pm\left(\frac{1+\sqrt{5}}{2}\right)^n$*,* $n \in \mathbb{Z}$*.*

4 | Djeljivost i faktorizacija

Osnovni pojmovi i tvrdnje koje su korištene u ovom poglavlju su bazirane na [4, 5].

4.1 Djeljivost

Definicija 15. *Neka su α, β algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{m})$, $\beta \neq 0$. Ako postoji algebarski cijeli broj $\delta \in \mathbb{Q}(\sqrt{m})$ takav da vrijedi*

$$\alpha = \beta\delta,$$

onda kažemo da β dijeli α i pišemo $\beta \mid \alpha$.

U ovom slučaju α zovemo djeljenik, a β djelitelj. Rezultat pri dijeljenju nazivamo količnik.

Primjer 5. *Kako je*

$$6 + 14\sqrt{-3} = (2 - 4\sqrt{-3})(-3 + \sqrt{-3})$$

zaključujemo da $(2 - 4\sqrt{-3}) \mid (6 + 14\sqrt{-3})$.

Sljedeći teorem nam daje karakterizaciju djeljivosti algebarskog cijelog broja u $\mathbb{Q}(\sqrt{m})$ s cijelim brojem.

Teorem 11 (vidjeti [4, Theorem 3.5.])**.** *Neka je $a \in \mathbb{Z}$ i $\delta = b + c\sqrt{m}$ algebarski cijeli broj u $\mathbb{Q}(\sqrt{m})$. Tada $a \mid \delta$ u $\mathbb{Q}(\sqrt{m})$ ako i samo ako $a \mid b$ i $a \mid c$ u $\mathbb{Z}$.*

Dokaz. Neka je $\delta = b + c\sqrt{m}$ djeljiv s a. Po definiciji djeljivosti postoji $\beta = b' + c'\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ takav da je

$$\delta = a \cdot \beta = a \cdot (b' + c'\sqrt{m}).$$

Tada je

$$b + c\sqrt{m} = a \cdot b' + a \cdot c'\sqrt{m}.$$

Izjednačavanjem dobivamo

$$\begin{aligned} b &= a \cdot b', \\ c &= a \cdot c' \end{aligned}$$

pa zaključujemo da $a \mid b$ i $a \mid c$ u $\mathbb{Z}$.
Obratno, ako $a \mid b$ i $a \mid c$ u $\mathbb{Z}$, onda po definiciji djeljivosti postoje b', $c' \in \mathbb{Z}$ takvi da je

$$\begin{aligned} b &= a \cdot b', \\ c &= a \cdot c'. \end{aligned}$$

Tada je

$$\delta = b + c\sqrt{m} = a \cdot b' + a \cdot c'\sqrt{m} = a \cdot (b' + c'\sqrt{m})$$

pa zaključujemo da $a \mid \delta$ u $\mathbb{Q}(\sqrt{m})$. □

U nastavku će nam biti važan obrat po kontrapoziciji sljedećeg teorema.

Teorem 12 (vidjeti [5]). *Neka su α, β algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{m})$. Ako $\beta \mid \alpha$ u $\mathbb{Q}(\sqrt{m})$, onda $N(\beta) \mid N(\alpha)$ u $\mathbb{Z}$.*

Dokaz. Neka su α, $\beta \in \mathbb{Q}(\sqrt{m})$ te neka $\beta \mid \alpha$. Po definiciji djeljivosti postoji $\delta \in \mathbb{Q}(\sqrt{m})$ takav da je

$$\alpha = \beta\delta.$$

Tada je

$$N(\alpha) = N(\beta\delta) = N(\beta)N(\delta),$$

iz čega zaključujemo da $N(\beta) \mid N(\alpha)$ u $\mathbb{Z}$ ($\beta \neq 0$ povlači $N(\beta) \neq 0$). □

Primjer 6. *Neka je*

$$\begin{aligned} \alpha &= 2 + 3\sqrt{-6} \\ \beta &= 2 - \sqrt{-6}, \end{aligned}$$

tada je $N(\alpha) = 58$ i $N(\beta) = 10$. Kako $N(\beta) \nmid N(\alpha)$ u $\mathbb{Z}$, onda $\beta \nmid \alpha$ u $\mathbb{Q}(\sqrt{-6})$.

Napomena 3. *Obrat Teorema 12 ne vrijedi.*

Primjer 7. *Ako je*

$$\begin{aligned} \alpha &= 6 - 9i \\ \beta &= 2 + 3i, \end{aligned}$$

tada je $N(\alpha) = 117$ i $N(\beta) = 13$. Vidimo da $N(\beta) \mid N(\alpha)$, ali

$$\frac{6-9i}{2+3i} = \frac{6-9i}{2+3i} \cdot \frac{2-3i}{2-3i} = \frac{-15}{13} - \frac{36}{13}i \notin \mathbb{Z}[i].$$

Ako je $\frac{\alpha}{\beta}$ invertibilni element, onda kažemo da su α i β asocirani (pridruženi) brojevi. U nastavku ćemo navesti primjer asociranih brojeva.

Primjer 8. *Neka je $\alpha = -2 + 3i$, $\beta = 3 + 2i$, tada su α i β asocirani u $\mathbb{Z}[i]$. Također, brojevi asocirani broju α su i:*

$$\begin{aligned} \gamma &= -3 - 2i, \\ \delta &= -2 + 3i, \\ \zeta &= 2 - 3i. \end{aligned}$$

4.2 Ireducibilnost

Definicija 16. *Kažemo da je algebarski cijeli broj $\delta \in \mathbb{Q}(\sqrt{m})$ koji nije 0 ni invertibilni element u $\mathbb{Q}(\sqrt{m})$ ireducibilan ako je djeljiv samo s invertibilnim elementima i sebi pridruženim brojevima.*

Primjer 9. *Provjerimo je li 2 ireducibilan u $\mathbb{Q}(\sqrt{-6})$.*
Primijetimo da je $-6 \equiv 2 \pmod 4$ pa su algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{-6})$ brojevi oblika

$$a + b\sqrt{-6},$$

gdje su $a, b \in \mathbb{Z}$. Ako algebarski cijeli broj u $\mathbb{Q}(\sqrt{-6})$ nije 0 ni invertibilni element onda je

$$N(a + b\sqrt{-6}) = a^2 + 6b^2 \geq 4.$$

Pretpostavimo sada da je

$$2 = \alpha\beta,$$

gdje su $\alpha, \beta \in \mathbb{Q}(\sqrt{-6})$. Iz multiplikativnosti norme dobivamo

$$N(\alpha)N(\beta) = 4,$$

a kako je najmanja norma 4 slijedi $N(\alpha) = \pm 1$ ili $N(\beta) = \pm 1$. Prema Teoremu 7, jedan od brojeva α ili β je invertibilini element, a onda je drugi od njih pridružen broju 2.
Dakle, 2 je ireducibilan u $\mathbb{Q}(\sqrt{-6})$.

Definicija 17. *Za algebarski cijeli broj $\tau \in \mathbb{Q}(\sqrt{m})$ koji nije 0 ni invertibilni element u $\mathbb{Q}(\sqrt{m})$ kažemo da je prost ako τ ima svojstvo da ako $\tau \mid \alpha\beta$, gdje su α, β algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{m})$, onda $\tau \mid \alpha$ ili $\tau \mid \beta$.*

Svaki prost broj je ireducibilan. Naime, ako je $\tau = \alpha\beta$ prost u $\mathbb{Q}(\sqrt{m})$, onda je jedan od brojeva $\frac{\alpha}{\tau}$ ili $\frac{\beta}{\tau}$ algebarski cijeli broj. No, kako α i β dijele τ slijedi da je jedan od njih invertibilni element, a drugi je pridružen broju τ. Općenito ireducibilni element ne mora biti prost što pokazuje sljedeći primjer.

Primjer 10 (vidjeti [5])**.** *Broj 2 je ireducibilan, ali nije prost u $\mathbb{Q}(\sqrt{-5})$.*
Uočimo da je $-5 \equiv 3 \pmod 4$ pa su algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{-5})$ svi brojevi oblika

$$a + b\sqrt{-5},$$

gdje su $a, b \in \mathbb{Z}$. Ako algebarski cijeli broj u $\mathbb{Q}(\sqrt{-5})$ nije 0 ni invertibilni element, onda je

$$N(a + b\sqrt{-5}) = a^2 + 5b^2 \geq 4.$$

Pretpostavimo sada da je

$$2 = \alpha\beta,$$

gdje su $\alpha, \beta \in \mathbb{Q}(\sqrt{-5})$. Primijenom multiplikativnosti norme dobivamo

$$N(\alpha)N(\beta) = 4,$$

a kako je najmanja norma 4, *slijedi* $N(\alpha) = \pm 1$ *ili* $N(\beta) = \pm 1$ *pa je jedan od brojeva* α *ili* β *invertibilni element. Dakle,* 2 *je ireducibilan. Međutim,* 2 *nije prost u* $\mathbb{Q}(\sqrt{-5})$ *jer*

$$2 \mid (1+\sqrt{-5})(1-\sqrt{-5}) = 6,$$

ali $2 \nmid (1+\sqrt{-5})$ *ni* $2 \nmid (1-\sqrt{-5})$ *jer* $N(2) = 4 \nmid 6 = N(1 \pm \sqrt{-5})$.

Teorem 13 (vidjeti [4, Theorem 3.10.])**.** *Neka je* δ *algebarski cijeli broj u* $\mathbb{Q}(\sqrt{m})$. *Ako je* $N(\delta) = \pm p$, *gdje je* p *prost prirodan broj, onda je* δ *ireducibilan.*

Dokaz. Pretpostavimo da je

$$\delta = \alpha\beta,$$

gdje su α, β algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{m})$. Multiplikativnost norme povlači

$$N(\delta) = N(\alpha)N(\beta) = \pm p.$$

Kako su prema Propoziciji 6 $N(\alpha)$ i $N(\beta)$ cijeli brojevi, onda jedan od njih mora biti jednak ± 1. Prema Teoremu 7 taj je broj invertibilni element te zbog $\delta = \alpha\beta$, onda drugi od njih mora biti pridružen δ. □

Primjer 11. *Provjerimo je li* $3 + 2\sqrt{5}$ *ireducibilan u* $\mathbb{Q}(\sqrt{5})$.
Kako je

$$N(3 + 2\sqrt{5}) = -11,$$

a 11 *je prost broj, prema prethodnom teoremu slijedi da je* $3 + 2\sqrt{5}$ *ireducibilan u* $\mathbb{Q}(\sqrt{5})$.

Napomena 4. *Kriterij u Teoremu 13 je dovoljan, ali ne i nužan uvjet ireducibilnosti.*

Primjer 12. *Broj* 3 *je ireducibilan u* $\mathbb{Q}(\sqrt{-13})$ *iako mu norma nije prost broj.*
Najprije, primijetimo da je $-13 \equiv 3 \pmod 4$ *pa su algebarski cijeli brojevi u* $\mathbb{Q}(\sqrt{-13})$ *svi brojevi oblika*

$$a + b\sqrt{-13},$$

gdje su a, $b \in \mathbb{Z}$. *Ako algebarski cijeli broj u* $\mathbb{Q}(\sqrt{-13})$ *nije* 0 *ni invertibilni element, onda je*

$$N(a + b\sqrt{-13}) = a^2 + 13b^2 \geq 4.$$

Pretpostavimo sada da je

$$3 = \beta\gamma,$$

gdje su β, $\gamma \in \mathbb{Q}(\sqrt{-13})$. *Zbog multiplikativnosti norme dobivamo*

$$N(\beta)N(\gamma) = 9$$

te kako je najmanja norma 4, *slijedi* $N(\beta) = \pm 1$ *ili* $N(\gamma) = \pm 1$ *pa je jedan od brojeva* β *ili* γ *invertibilni element. Međutim,* $N(3) = 9$ *što nije prost broj.*
Dakle, 3 *je ireducibilan u* $\mathbb{Q}(\sqrt{-13})$ *iako mu norma nije prost broj.*

Teorem 14. *Svaki algebarski cijeli broj* δ *u* $\mathbb{Q}(\sqrt{m})$, *koji nije* 0 *ni invertibilni element, može se prikazati kao produkt ireducibilnih brojeva u* $\mathbb{Q}(\sqrt{m})$.

Dokaz. Ako je δ ireducibilan broj, onda smo gotovi. Ako δ nije ireducibilan broj, onda se on može rastaviti na umnožak $\alpha\beta$, gdje su α i β algebarski cijeli brojevi koji nisu invertibilni elementi. Nastavljajući ovaj postupak, faktoriziramo α i β, ako nisu ireducibilni. Ovaj postupak faktorizacije mora završiti jer bi inače dobili da δ ima oblik $\alpha_1\alpha_2\cdots\alpha_n$, gdje je n po volji velik, a niti jedan α_j nije invertibilni element. To bi povlačilo da je

$$|N(\delta)| = \prod_{j=1}^{n} |N(\alpha_j)| \geq 2^n, \tag{4.1}$$

jer je $|N(\alpha_j)|$ prirodan broj veći od 1. No, iz (4.1) vidimo da ako nastavimo opisani postupak, dobivamo da $|N(\delta)|$ teži u beskonačno, što ne smije biti. □

Prethodnim teoremom pokazali smo da faktorizacija na ireducibilne faktore u $\mathbb{Q}(\sqrt{m})$ uvijek postoji, ali ona ne mora biti jedinstvena.

Primjer 13 (vidjeti [5, Primjer 12.1.]). *Promotrimo broj* 55 *i njegove tri faktorizacije u* $\mathbb{Q}(\sqrt{-6})$*:*

$$55 = 5 \cdot 11 = (1 + 3\sqrt{-6})(1 - 3\sqrt{-6}) = (7 + \sqrt{-6})(7 - \sqrt{-6}).$$

Uvjerimo se da su brojevi 5, 11, $(1 \pm 3\sqrt{-6})$, $(7 \pm \sqrt{-6})$ *ireducibilni u* $\mathbb{Q}(\sqrt{-6})$*.*
Kao što smo spomenuli u Primjeru 9, algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{m})$ *su svi brojevi oblika* $a + b\sqrt{-6}$*, gdje su* $a, b \in \mathbb{Z}$*. Ako algebarski cijeli broj u* $\mathbb{Q}(\sqrt{-6})$ *nije* 0 *ni invertibilni element, onda je*

$$\begin{aligned} N(a + b\sqrt{-6}) &= a^2 + 6b^2 \geq 4, \\ N(a + b\sqrt{-6}) &\neq 5, \\ N(a + b\sqrt{-6}) &\neq 11. \end{aligned}$$

Pretpostavimo sada da je

$$5 = \alpha\beta,$$

gdje su $\alpha, \beta \in \mathbb{Q}(\sqrt{-6})$*. Multiplikativnost norme povlači*

$$N(\alpha) \cdot N(\beta) = 25$$

te zbog naših prethodnih zaključaka slijedi $N(\alpha) = \pm 1$ *ili* $N(\beta) = \pm 1$*. Dakle,* 5 *je ireducibilan u* $\mathbb{Q}(\sqrt{-6})$*. Analogno se pokaže da je* 11 *ireducibilan u* $\mathbb{Q}(\sqrt{-6})$*.*
Nadalje, ako je

$$1 \pm 3\sqrt{-6} = \alpha\beta,$$

gdje su $\alpha, \beta \in \mathbb{Q}(\sqrt{-6})$ *onda iz multiplikativnosti norme doivamo*

$$N(\alpha) \cdot N(\beta) = 55.$$

Iz prethodne jednakosti i prijašnjih zaključaka slijedi $N(\alpha) = \pm 1$ *ili* $N(\beta) = \pm 1$*. Dakle,* $1 \pm 3\sqrt{-6}$ *je ireducibilan. Analogno se pokaže ireducibilnost broja* $7 \pm \sqrt{-6}$*.*
Dakle, broj 55 *nema jedinstvenu faktorizaciju na ireducibilne faktore u* $\mathbb{Q}(\sqrt{-6})$*.*

4.3 Jedinstvenost faktorizacije

Pitamo se za koje vrijednosti od m, $\mathbb{Q}(\sqrt{m})$ ima svojstvo jedinstvene faktorizacije. Vidjet ćemo da je to u vezi s Euklidovim algoritmom.

Definicija 18. *Ako se svaki algebarski cijeli broj u $\mathbb{Q}(\sqrt{m})$, koji nije 0 ni invertibilni element može na jedinstven način zapisati kao produkt ireducibilnih faktora, do na poredak faktora i zamjenu faktora pridruženim brojevima, onda kažemo da kvadratno polje $\mathbb{Q}(\sqrt{m})$ ima svojstvo jedinstvene faktorizacije.*

Definicija 19. *Kvadratno polje je euklidsko ako se za algebarske cijele brojeve u $\mathbb{Q}(\sqrt{m})$ može provesti Euklidov algoritam, odnosno ako za algebarske cijele brojeve α, $\beta \in \mathbb{Q}(\sqrt{m})$, $\beta \neq 0$ postoje algebarski cijeli brojevi γ, $\delta \in \mathbb{Q}(\sqrt{m})$ takvi da je*

$$\alpha = \beta\gamma + \delta,\ |N(\delta)| < |N(\beta)|.$$

Teorem 15 (vidjeti [5, Teorem 12.11.])**.** *Ako je kvadratno polje euklidsko, onda ono ima svojstvo jedinstvene faktorizacije.*

Dokaz. Najprije, pokažimo da ako su α i β algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{m})$ kojima su jedini zajednički djelitelji invertibilni elementi, onda postoje algebarski cijeli brojevi μ_0, $\eta_0 \in \mathbb{Q}(\sqrt{m})$ takvi da je

$$\alpha\mu_0 + \beta\eta_0 = 1.$$

Neka je I skup svih brojeva oblika

$$\alpha\mu + \beta\eta,$$

gdje su μ, η algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{m})$. Ako je $\kappa \in I$ različit od 0, onda je $|N(\kappa)|$ pozitivan cijeli broj pa možemo odabrati element

$$\xi = \alpha\mu_1 + \beta\eta_1$$

skupa I takav da $|N(\xi)|$ poprima najmanju pozitivnu vrijednost među $|N(\kappa)|$. Kako je kvadratno polje $\mathbb{Q}(\sqrt{m})$ euklidsko, onda postoje algebarski cijeli brojevi γ, $\delta \in \mathbb{Q}(\sqrt{m})$ takvi da je

$$\alpha = \xi\gamma + \delta,\ |N(\delta)| < |N(\xi)|.$$

Tada je

$$\delta = \alpha - \gamma(\alpha\mu_1 + \beta\eta_1) = \alpha(1 - \gamma\mu_1) + \beta(-\gamma\eta_1) \in I.$$

Iz definicije od ξ slijedi da je $N(\delta) = 0$, odnosno $\delta = 0$. Dakle, $\alpha = \xi\gamma$ i $\xi \mid \alpha$. Analogno se pokaže da $\xi \mid \beta$ pa je ξ invertibilan element. Također je i ξ^{-1} invertibilan element pa imamo

$$1 = \xi^{-1}\xi = \xi^{-1}(\alpha\mu_1 + \beta\eta_1) = \alpha\xi^{-1}\mu_1 + \beta\xi^{-1}\eta_1 = \alpha\mu_0 + \beta\eta_0.$$

Nadalje, dokažimo da ako je τ ireducibilan u $\mathbb{Q}(\sqrt{m})$, onda je i on prost, odnosno ako $\tau \mid \gamma\delta$, onda $\tau \mid \gamma$ ili $\tau \mid \delta$. Naime, ako $\tau \nmid \gamma$, onda su invertibilni elementi

jedini zajednički djelitelji od τ i γ pa postoje algebarski cijeli brojevi μ_0 i η_0 takvi da je

$$\tau\mu_0 + \gamma\eta_0 = 1.$$

Množenjem prethodne jednakosti s δ dobivamo

$$\delta = \tau\delta\mu_0 + \gamma\delta\eta_0,$$

pa slijedi da $\tau \mid \delta$. Odavde indukcijom slijedi da ako $\tau \mid (\gamma_1 \cdots \gamma_n)$, onda τ dijeli neki γ_j.
Pretpostavimo da postoje dvije faktorizacije na ireducibilne faktore algebarskog cijelog broja δ, odnosno

$$\delta = \sigma_1\sigma_2 \cdots \sigma_m = \tau_1\tau_2 \cdots \tau_n. \tag{4.2}$$

Ako je $m = 1$, onda je δ ireducibilan i mora biti da je $n = 1$ i $\delta = \tau_1$. Pretpostavimo da je $m > 1$. Kako je σ_1 prost, onda $\sigma_1 \mid \tau_1\tau_2 \cdots \tau_n$ povlači da σ_1 dijeli neki τ_j. Zamjenom uloga τ_1 i τ_j dobivamo da $\sigma_1 \mid \tau_1$. Kako je τ_1 ireducibilan, onda je σ_1 njemu asociran broj, tj.

$$\tau_1 = \xi\sigma_1,$$

gdje je ξ invertibilan element. Uvrštavanjem prethodne jednakosti u (4.2) i dijeljenjem s σ_1 dobivamo

$$\sigma_2\sigma_3 \cdots \sigma_m = \xi\tau_2\tau_3 \cdots \tau_n.$$

Ponavljajući postupak dobivamo jedinstvenost faktorizacije na ireducibilne faktore. □

Chatland i Davenport (1950.) su pokazali da postoji točno 21 euklidsko polje $\mathbb{Q}(\sqrt{m})$ i to za sljedeće vrijednosti:

$$m = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Primjer 14 (vidjeti [5, Primjer 12.2.]). *Dokažimo da su kvadratna polja $\mathbb{Q}(\sqrt{m})$ za $m = -3,\ -2,\ -1,\ 2,\ 5$ euklidska.*
Neka su $\gamma,\ \delta$ algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{m})$ i $\delta \neq 0$. Tada je

$$\frac{\gamma}{\delta} = x + y\sqrt{m},$$

gdje su x i y racionalni brojevi. Odaberimo $u,\ v \in \mathbb{Z}$ koji su najbliži x i y te neka je

$$\begin{aligned} r &= x - u, \\ s &= y - v. \end{aligned}$$

Tada je

$$\begin{aligned} 0 \leq\ & |r| \leq \frac{1}{2}, \\ 0 \leq\ & |s| \leq \frac{1}{2}. \end{aligned}$$

Označimo

$$\begin{aligned} u + v\sqrt{m} &= \beta, \\ \gamma - \delta\beta &= \alpha, \end{aligned}$$

gdje su α *i* β *algebarski cijeli brojevi u* $\mathbb{Q}(\sqrt{m})$*. Slijedi*

$$\begin{aligned} N(\alpha) &= N(\gamma - \delta\beta) = N\left(\delta \cdot \left(\frac{\gamma}{\delta} - \beta\right)\right) = N(\delta) \cdot N\left(\frac{\gamma}{\delta} - \beta\right) \\ &= N(\delta) \cdot N(r + s\sqrt{m}) = N(\delta) \cdot (r^2 - ms^2) \end{aligned}$$

pa je

$$|N(\alpha)| = |N(\delta)| \cdot |r^2 - ms^2|. \tag{4.3}$$

Ako je $|m| \leq 2$ *dobivamo*

$$|r^2 - ms^2| \leq r^2 + 2s^2 \leq \frac{3}{4} < 1.$$

Iz (4.3) *slijedi* $|N(\alpha)| < |N(\delta)|$*, odnosno za* $m = -2,\ -1,\ 2$ *polje* $\mathbb{Q}(\sqrt{m})$ *je euklidsko. Za* $m = -3,\ 5$ *postupamo na malo drugačiji način. Neka su* x *i* y *definirani kao prije. Odaberimo* $v \in \mathbb{Z}$ *najbliži broju* $2y$ *te označimo*

$$s = y - \frac{1}{2}v$$

pa je

$$0 \leq |s| \leq \frac{1}{4}.$$

Nadalje, odaberimo $u \in \mathbb{Z}$ *najbliži broju* $x - \frac{1}{2}v$ *te označimo*

$$r = x - u - \frac{1}{2}v$$

pa je

$$0 \leq |r| \leq \frac{1}{2}.$$

Označimo

$$\begin{aligned} u + v \cdot \frac{1 + \sqrt{m}}{2} &= \beta, \\ \gamma - \delta\beta &= \alpha. \end{aligned}$$

Kao i ranije dobivamo

$$N(\alpha) = N(\delta) \cdot (r^2 - ms^2).$$

Kako je $|m| \leq 5$*, slijedi*

$$|r^2 - ms^2| \leq r^2 + 5s^2 \leq \frac{9}{16} < 1.$$

Dakle, $|N(\alpha)| < |N(\delta)|$ *pa za* $m = -3,\ 5$ *polje* $\mathbb{Q}(\sqrt{m})$ *je euklidsko.*

No, euklidska polja nisu jedina polja s jedinstvenom faktorizacijom. Heegner(1952.),
Baker(1966.) i Stark(1967.) su pokazali da ako je m negativan, onda za

$$m = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

kvadratno polje $\mathbb{Q}(\sqrt{m})$ ima svojstvo jedinstvene faktorizacije. Hipoteza je da za pozitivan m takvih polja ima beskonačno mnogo.

Primjer 15. *Dokažimo da su jedine cjelobrojne točke na krivulji*

$$y^2 = x^3 - 2$$

točke $(3,\ 5)$ *i* $(3,\ -5)$.
Najprije uočimo sljedeće: ako bi x bio paran, onda bi

$$y^2 = x^3 - 2 \equiv 2 \pmod 4$$

što je nemoguće. Dakle, x mora biti neparan pa je i y također neparan. Promatrajmo rastav

$$x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}). \tag{4.4}$$

Prema prethodnom primjeru kvadratno polje $\mathbb{Q}(\sqrt{-2})$ je euklidsko pa onda prema Teoremu 15 ima svojstvo jedinstvene faktorizacije. Pokazat ćemo da su jedini zajednički djelitelji od $y + \sqrt{-2}$ i $y - \sqrt{-2}$ invertibilni elementi i iskoristiti jedinstvenost faktorizacije. Neka $\gamma \mid (y + \sqrt{-2})$ i $\gamma \mid (y - \sqrt{-2})$. Tada $\gamma \mid 2\sqrt{-2}$ pa $N(\gamma) \mid N(2\sqrt{-2}) = 8$. Kako je y neparan iz $N(\gamma) \mid N(y + \sqrt{-2}) = y^2 + 2$ slijedi da $N(\gamma)$ ne može biti paran pa je $N(\gamma) = 1$. Zbog jedinstvenosti faktorizacije iz (4.4) slijedi da postoje $\alpha,\ \beta,\ \epsilon \in \mathbb{Z}[\sqrt{-2}]$ takvi da je

$$\begin{aligned} y + \sqrt{-2} &= \alpha^3, \\ y - \sqrt{-2} &= \epsilon\beta^3, \\ N(\epsilon) &= 1. \end{aligned}$$

Ako je $\alpha = a + b\sqrt{-2}$, onda je

$$\begin{aligned} y + \sqrt{-2} &= (a + b\sqrt{-2})^3 \\ &= (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}. \end{aligned}$$

Odavde slijedi

$$\begin{aligned} a^3 - 6ab^2 &= y, \\ 3a^2b - 2b^3 &= 1. \end{aligned}$$

Iz posljednje jednažbe slijedi $b \mid 1$ pa je $b = \pm 1$. Za $b = 1$ slijedi $a = \pm 1$, dok je $b = -1$ nemoguće. Za $a = 1$ se dobije $y = -5$, a za $a = -1$ je $y = 5$. Time je početna jednadžba rješena.

U prethodnom primjeru dano je rješenje motivacijskog primjera iz Uvoda.

Primjer 16. *Promotrimo dvije faktorizacije broja* 13 *u* $\mathbb{Q}(\sqrt{-3})$*:*

$$13 = \frac{7+\sqrt{-3}}{2} \cdot \frac{7-\sqrt{-3}}{2} = (1+2\sqrt{-3})(1-2\sqrt{-3}).$$

Možemo se zapitati zašto te dvije faktorizacije nisu u suprotnosti s činjenicom da polje $\mathbb{Q}(\sqrt{-3})$ *ima svojstvo jedinstvene faktorizacije. Pripadne faktorizacije u* $\mathbb{Q}(\sqrt{-3})$ *su jednake do na množenje invertibilnim elementima. Naime, vrijedi sljedeće*

$$\frac{7+\sqrt{-3}}{2} \cdot \frac{1+\sqrt{-3}}{2} = 1+2\sqrt{-3}.$$

Teorem 16 (vidjeti [5, Teorem 12.12.])**.** *Ako* $\mathbb{Q}(\sqrt{m})$ *ima svojstvo jedinstvene faktorizacije, onda svakom ireducibilnom broju* $\tau \in \mathbb{Q}(\sqrt{m})$ *odgovara točno jedan prirodni prosti broj* a *takav da* $\tau \mid a$*.*

Dokaz. Kako ireducibilan broj τ dijeli cijeli broj $N(\tau)$ $(N(\tau) = \tau\bar{\tau})$, postoje prirodni brojevi koji su djeljivi s τ. Neka je a najmanji takav broj te pokažimo da je on prost.
Pretpostavimo suprotno, odnosno neka je

$$a = p \cdot q,\ 1 < p,\ q < a.$$

Zbog svojstva jedinstvene faktorizacije slijedi $\tau \mid p$ ili $\tau \mid q$, što je kontradikacija s $1 < p,\ q < a$.
Preostaje nam još pokazati jedinstvenost. Pretpostavimo suprotno, odnosno da τ dijeli još neki prirodni prost broj $b \neq a$. Tada su a i b relativno prosti pa postoje $x,\ y \in \mathbb{Z}$ takvi da je

$$ax + by = 1.$$

Iz prethodne jednakosti slijedi da $\tau \mid 1$ što je kontradikcija.
Dakle, prirodan prost broj a je jedinstven. □

Može se pokazati da vrijedi i sljedeći teorem.

Teorem 17 (vidjeti [5, Teorem 12.13.])**.** *Prosti brojevi u* $\mathbb{Q}(i)$ *su prosti prirodni brojevi oblika*

$$q = 4l + 3,$$

faktori τ *i* τ' *iz faktorizacije* $q = \tau\tau'$ *prostih prirodnih brojeva oblika*

$$q = 4l + 1,$$

broj $(1+i)$ *te brojevi koji su pridruženi navedenim brojevima.*

Literatura

[1] T. Andreescu, D. Andrica, I. Cucurezeanu, *An Introduction to Diophantine Equations*, Springer Science + Business Media, LLC, 2010.

[2] A. Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, Cambridge, 1984.

[3] *Notes on Algebraic Numbers*, dostupno na `\https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=d6c065e71c1f53516e5a0e330c8ddffbb7dac737`

[4] *Factoring in quadratic fields*, dostupno na `\https://kconrad.math.uconn.edu/blurbs/gradnumthy/quadraticgrad.pdf`

[5] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[6] H. Kraljević, *Algebra*, Odjel za matematiku, Sveučilište J. J. Strossmayera u Osijeku, skripta, 2007.

Sažetak

U ovom radu smo definirali osnovne algebarske strukture te pojmove algebarskog broja, algebarskog cijelog broja i naveli važne tvrdnje vezane uz njih. Definirali smo kvadratno polje i dvije važne skalarne funkcije na njima te naveli i dokazali njihova svojstva. Uveli smo pojam invertibilnog elementa te naveli tvrdnje i primjere vezane uz njih u imaginarnim i realnim kvadratnim poljima. Upoznali smo se s pojmom ireducibilnog elementa i naveli primjere i tvrdnje vezano uz njega. Na kraju smo se bavili s jedinstvenošću faktorizacije.

Ključne riječi

algebarski cijeli brojevi, kvadratno polje, invertibilni elementi, ireducibilnost, jedinstvenost faktorizacije

Quadratic Fields

Summary

In this work, we have defined the basic algebraic structures and the notion of algebraic number, algebraic integer and stated important claims related to them. We have defined a quadratic field and two important scalar functions on them and stated and proved their properties. We introduced the concept of an invertible element and stated claims and examples related to them in imaginary and real quadratic fields. We were acquainted with the concept of an irreducible element and given examples and statements related to it. Finally, we dealt with the unique factorization.

Keywords

algebraic integers, quadratic fields, invertible elements, irreducibility, unique factorization

Životopis

Rođena sam 1. listopada 1999. godine u Požegi. Pohađala sam Osnovnu školu "fra Kaje Adžića" u Pleternici. Po završetku osnovne škole 2014. godine upisujem Prirodoslovno-matematičku gimnaziju u Požegi koju završavam 2018. godine. Iste godine upisujem preddiplomski studij Matematika na Odjelu za matematiku odnosno današnjem Fakultetu primijenjene matematike i informatike na Sveučilištu J.J. Strossmayera u Osijeku. Preddiplomski studij završavam 2021. godine s temom završnog rada "Simetrične matrice" pod mentorstvom doc. dr. sc. Suzane Miodragović. Na istom fakultetu upisujem diplomski studij matematike, smjer Financijska matematika i statistika.