Realna kvadratna proširenja

Sindičić, Lovro

Realna kvadratna proširenja

Sindičić, Lovro

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Lovro Sindičić

REALNA KVADRATNA PROŠIRENJA

Diplomski rad

Voditelj rada:
prof. dr. sc. Boris Širola

Zagreb, prosinac 2020.

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 se prije svega svojim roditeljima i ostalim članovima obitelji koji su mi uvijek bili podrška.

Zahvaljujem mentoru prof. dr. sc. Borisu Široli na pruženoj prilici za pisanje diplomskog rada, na zanimljivoj temi, razumijevanju i podršci pri pisanju ovog diplomskog rada te na posvećenom vremenu i savjetima koji su bili od neizmjerne pomoći.

Zahvaljujem se svim profesorima i asistentima koji su prošli kroz moje školovanje i od kojih sam jako puno naučio.

Posebno velika zahvala mojim dragim kolegama s diplomskog studija koji su mi također bili velika podrška u mom studiranju od kojih sam također mnogo naučio i na koje sam se uvijek mogao osloniti.

Dn 3, 89

Sadržaj

Uvod

Sama riječ algebra pripada u orijentalizme, odnosno riječi arapskog porijekla. Prva dva slova označavaju određen član u arapskome jeziku kao što to imamo primjer u riječima alkohol ili alkemija koje su također arapskog porijekla. Ostatak riječi potječe od riječi gabr koja označava namještavanje slomljenih kostiju. Upravo tako i sama algebra povezuje na prvi pogled ne spojive dijelove matematike i onda tako spojeni čine jednu veliku moćnu cjelinu. Algebra je jedna od osnovnih grana matematike koja se bavi proučavanjem algebarskih struktura i operacija. Strukturu imaju skupovi na kojima je definirana barem jedna operacija. Stoga je algebarska struktura skup na kojem je definirana barem jedna operacija. Neke od osnovnih algebarskih struktura su: grupe, prsteni, ideali i polja. Na njima su definirane algebarske operacije, kao što su naprimjer kompozicija, zbrajanje i množenje.

Glavni cilj ovog diplomskog rada je istražiti kvadratna proširenja polja racionalnih brojeva, i to prvenstveno tzv. realna kvadratna proširenja. Rad se sastoji od četiri poglavlja. Počinjemo s kratkim i uvodnim poglavljem u kojem ćemo navesti određene definicije koje ćemo primjenjivati u proučavanju teme ovog rada. Tako navodimo definicije prstena, ideala, integralne domene i polja te nekoliko primjera prstena i polja. Drugo poglavlje posvećeno je proučavanju općenitih kvadratnih proširenja $\mathbb{F}|\mathbb{K}$, kako bismo u trećem poglavlju mogli uvesti pojam realnog kvadratnog proširenja, što i je glavna tema ovog diplomskog rada. Pokazano je da je svako takvo proširenje određeno nekim kvadratnim ireducibilnim polinomom $f \in \mathbb{K}[X]$ (Teorem 2.0.9). Koristeći tu činjenicu, u specijalnom slučaju kada imamo Galoisovo polje $\mathbb{K} = \mathbb{F}_p$ od p elemenata, direktno pokazujemo kako se može konstruirati kvadratno proširenje $\mathbb{F} = \mathbb{F}_{p^2}$. U Primjeru 2.0.13 provodimo konkretne konstrukcije takvih kvadratnih proširenja za neke proste brojeve p. U trećem poglavlju bavimo se algebarskim brojevima. Posebno u odjeljku 3.1 uvodimo pojam algebarskog broja nad danim poljem $\mathbb{F}$, a onda za svako proširenje polja $\mathbb{K}|\mathbb{F}$ definiramo skup $\mathcal{A}(\mathbb{K}|\mathbb{F})$, svih elemenata $\alpha \in \mathbb{K}$ koji su algebarski nad $\mathbb{F}$. Nizom pomoćnih tvrdnji dokazujemo da taj skup $\mathcal{A}(\mathbb{K}|\mathbb{F})$ ima strukturu polja (Teorem 3.1.5). Preciznije rečeno, to je potpolje od $\mathbb{K}$ koje se zove *algebarsko zatvorenje* od $\mathbb{F}$ u $\mathbb{K}$. Uz algebarske brojeve u odjeljku 3.2 definiramo posebnu vrstu algebarskih brojeva, tzv. *algebarskih cijelih brojeva*. Tu naša razmatranje restringiramo na slučaj kada je promatrano polje potpolje polja kompleksnih brojeva $\mathbb{C}$. Posebno dokazu-

jemo važan rezultat da skup svih algebarskih cijelih brojeva u $\mathbb{C}$ ima strukturu prstena, tojest to je potprsten od $\mathbb{C}$. U nastavku ovoga odjeljka bavimo se kvadratnim proširenjima polja racionalnih brojeva $\mathbb{Q}$. Svako je takvo proširenje K oblika $K = \mathbb{Q}(\sqrt{d})$, za neki kvadratno slobodan cijeli broj $d \in \mathbb{Z}\setminus\{0, 1\}$ (Propozicija 3.2.10). Za takva kvadratna proširenja $K = \mathbb{Q}(\sqrt{d})$ definiramo funkcije *trag* $T : K \to \mathbb{Q}$ i *norma* $N : K \to \mathbb{Q}$, a zatim određujemo prstene cijelih brojeva R_d u K (Teorem 3.2.15).

Završno četvrto poglavlje je centralni dio ovog diplomskog rada. U njemu detaljno proučavamo strukturu prstena algebarskih cijelih brojeva na realnim kvadratnim proširenjima $K = \mathbb{Q}(\sqrt{d})$. Posebno nas u odjeljku 4.1 zanima razumijeti grupu U_d, invertibilnih elemenata u prstenu K (Propozicija 4.1.6). Naglasimo kako je sadržaj toga odjeljka usko vezan uz probleme rješavanja Pellovih i pelovskih jednadžbi. U odjeljku 4.2 želimo tek malo bolje razumijeti otvoren problem jedinstvene faktorizacije u prstenima R_d. Odjeljak 4.3 je rezerviran za proučavanje ideala u prstenima cijelih R_d. Tu posebno dokazujemo da se svaki ideal $I \trianglelefteq R_d$ može prikazati kao produkt prostih ideala, i to na jedinstven način ako nam poredak faktora nije bitan (Teorem 4.3.14). U pododjeljku 4.3.1 definiramo relaciju ekvivalencije $\sim$ na skupu ideala u R_d. Ako za svaki ideal $I \trianglelefteq R_d$ s $[I]$ označimo pripadnu klasu tog ideala po $\sim$, onda definiramo operaciju množenja $[I]\,[J] = [IJ]$, za bilo koje ideale $I, J \trianglelefteq R_d$. Dokazujemo Teorem 4.3.21 koji govori da je uz to množenje skup svih klasa ideala $Cl(R_d)$ abelova grupa; tzv. *grupa klasa ideala* od R_d. Rad završavamo važnim rezultatom da je ta grupa konačna (Korolar 4.3.24).

Za kraj naglasimo kako je jedan od glavnih ciljeva ovog diplomskog rada bio, kroz detaljno proučavanje važne klase realnih kvadratnih proširenja, napraviti mali uvod u algebarsku teoriju brojeva, bogatu i važnu matematičku disciplinu.

Poglavlje 1

Osnovni pojmovi

U ovom uvodnom poglavlju podsjetit ćemo se na neke standardne pojmove rezultate osnovnih algebarskih struktura. Pored grupa, prsteni su sljedeće osnovne algebarske strukture koje se pojavljuju u analizi, teoriji brojeva kao i u mnogim drugim granama matematike.

1.1 Prsteni

Definicija 1.1.1. *Neprazan skup R na kojem su definirane binarne operacije zbrajanja $+ : R \times R \to R$ i množenja $\cdot : R \times R \to R$ zove se **prsten** ukoliko vrijedi sljedeće:*

1. $(R, +)$ *je komutativna grupa;*

2. $(R, \cdot)$ *je polugrupa;*

3. *za svake $x, y, z \in R$ vrijede distributivnosti:*

$$x \cdot (y + z) = x \cdot y + x \cdot z, \quad (x + y) \cdot z = x \cdot z + y \cdot z.$$

Ako u R postoji element $1 = 1_R$ takav da je

$$1 \cdot x = x \cdot 1 = x, \ \forall x \in R$$

tada se taj element 1 zove **jedinica** u prstenu, a R **prsten s jedinicom**.
Ako za sve $x, y \in R$ imamo da je $x \cdot y = y \cdot x$, onda kažemo da je R **komutativan** prsten. U suprotnom, R je **nekomutativan**.

Napomena 1.1.2. *U daljnjem tekstu ćemo ispuštati točku koja označava množenje dva elementa u prstenu. Dakle, za $x, y \in R$ pisat ćemo xy umjesto $x \cdot y$.*

U ovom radu ćemo se isključivo bavimo komutativnim prstenima i to tzv. *poljima algebarskih brojeva*, i njihovim pripadajućim *prstenima cijelih brojeva*. Ali podsjetimo se ovdje i nekih drugih važnih primjera komutativnih prstena.
Neka je R komutativan prsten s jedinicom.
Formalna suma

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad a_i \in R,\ a_n \neq 0 \tag{1.1}$$

naziva se polinom u varijabli x. Skup svih polinoma oblika (1.1) označavamo s $R[x]$. Definiramo stupanj polinoma s $\deg(f(x)) = n$, ako je a_n vodeći koeficijent polinoma $f(x)$, dok stupanj nul-polinoma 0 definiramo s $\deg(0) = -1$.
Zbroj polinoma $f(x) = \sum_{k=0}^{n} a_kx^k$ i $g(x) = \sum_{k=0}^{m} b_kx^k$, $n \geq m$, definirajmo s

$$f(x) + g(x) = \sum_{k=0}^{n}(a_k + b_k)x^k$$

gdje smo uzeli da je $b_{m+1} = b_{m+2} = \cdots = b_n = 0$
Umnožak polinoma definiran je s

$$f(x)g(x) = \sum_{k=0}^{n+m}\left(\sum_{i+j=k} a_ib_j\right)x^k$$

Lagano se provjeri da ove dvije operacije zadovoljavaju aksiome prstena.
Stoga $R[X]$ je komutativan prsten s jedinicom.

Radi daljnje potrebe podsjetimo se još jedne definicije.

Definicija 1.1.3. *Element $\lambda \neq 0$ nekog prstena R takav da je $\lambda x = 0$ za neki $0 \neq x \in R$ zove se **djelitelj nule**.*
*Kažemo da je prsten R **integralna domena** ako on nema djelitelja nule.*

1.2 Ideali

Podsjetimo kako i u ovom odjeljku pretpostavljamo da je svaki prsten koji promatramo komutativan i s jedinicom. Kad god imamo neki prsten, zanimljivo je u njemu razumjeti jednu specijalnu vrstu potprstena; to su tzv. ideali. Podsjetimo se i na njihovu definiciju.

Definicija 1.2.1. *Neka je R prsten. Neprazan podskup $I \subseteq R$ je **ideal** u R ako su ispunjena sljedeća dva uvjeta:*

1. *I je potprsten od R;*

2. *Za sve $r \in R$ i $x \in I$ je $rx \in I$*

Činjenicu da je I ideal u prstenu R označavamo s

$$I \trianglelefteq R.$$

Podsjetimo se još nekih važnih pojmova koje uvodimo u nizu od nekoliko definicija.

Definicija 1.2.2. *Neka je R prsten i $I \trianglelefteq R$ neki ideal. Skup $S \subseteq R$ je **skup generatora** od I ako je*

$$I = \langle S \rangle = \bigcap_{\substack{J \trianglelefteq R \\ S \subseteq J}} J;$$

tj. I je najmanji ideal u R koji sadrži skup S.

Definicija 1.2.3. *Za elemente x i y prstena R, gdje je $y \neq 0$, kažemo da y **dijeli** x, te pišemo $y \mid x$, ako postoji neki $r \in R$ takav da je $x = ry$.*

Podsjetimo se kako je element ω u prstenu R **invertibilan** ukoliko postoji neki element $x \in R$ takav da je $\omega x = 1$. Posebno definiramo

$$R^* = \text{skup invertibilnih elemenata u } R.$$

Lagano se vidi da R^* ima strukturu multiplikativne grupe.

Ponekad će nam biti zgodno koristiti i oznaku

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

Definicija 1.2.4. *Za elemente $a, b \in R$ kažemo da su **asocirani**, i koristimo oznaku $a \sim b$ ako*

$$\exists u \in R^* \;\; a = ub$$

Element $c \in R$ je **ireducibilan** ako su ispunjena sljedeća dva uvjeta:

1. $0 \neq c \notin R^*$
2. Ako je $c = ab$, onda je ili $a \in R^*$ ili $b \in R^*$.

Skup svih ireducibilnih elemenata u R označavat ćemo s $\operatorname{Irr} R$.

Definicija 1.2.5. *Element $p \in R$ je **prost** ako su ispunjeni sljedeći uvjeti:*

1. *$0 \neq p \notin R^*$;*
2. *Ako $p \mid ab$, onda ili $p \mid a$ ili $p \mid b$.*

Definicija 1.2.6. *Prsten R je **tijelo**, ili prsten s dijeljenjem, ako je svaki ne-nul element u R invertibilan; tj,, ukoliko je*

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

1.3 Polja

Definicija 1.3.1. *Komutativan prsten s jedinicom u kojem je svaki nenul element invertibilan zove se* ***polje****.*

Sada definiramo jednu važnu invarijantu za polja. Zapravo, dat ćemo malo generalniju definiciju, za komutativne prstene.

Definicija 1.3.2. *Neka je R komutativan prsten, s nulom $0 = 0_R$. Pretpostavimo da postoji prirodan broj n takav da je $na = 0$ za svaki element $a \in R$. Najmanji takav prirodan broj zove se* ***karakteristika prstena*** *R, i označava s $char(R)$. (U tom slučaju kažemo da je R prsten* pozitivne karakteristike*.) Ukoliko takav n ne postoji, onda kažemo da je R prsten* karakteristike nula*, i pišemo $char(R) = 0$.*

Očito je prsten cijelih brojeva karakteristike nula; tojest, $\mathrm{char}(\mathbb{Z}) = 0$. Isto tako i polja racionalnih brojeva $\mathbb{Q}$, realnih brojeva $\mathbb{R}$ i kompleksnih brojeva $\mathbb{C}$ su također karakteristike nula. Kao dobro poznate primjere prstena pozitivne karakteristike imamo *prstene ostataka modulo n*, kada je $n \in \mathbb{N}$, $n > 1$. To su prsteni $\mathbb{Z}/n\mathbb{Z}$, kvocijenti prstena $\mathbb{Z}$ po idealima $n\mathbb{Z}$, koje ćemo mi kraće označavati s $\mathbb{Z}_n$. Primijetimo da je karakteristika $\mathrm{char}(\mathbb{Z}_n) = n$. Doista, ako je $\overline{k} \in \mathbb{Z}_n$, onda je

$$n\overline{k} = \underbrace{\overline{k} + \overline{k} + \cdots + \overline{k}}_{n \text{ puta}} = \overline{nk} = \overline{n}\overline{k} = \overline{0} = 0$$

jer je $\overline{n} = \overline{0}$. Pokažimo da je n najmanji prirodni broj sa svojstvom $n\overline{k} = \overline{0}$ za svaki $\overline{k} \in \mathbb{Z}_n$. Pretpostavimo da postoji $1 \leq m < n$ takav da je $m\overline{k} = \overline{0}$ za svaki $\overline{k} \in \mathbb{Z}_n$. Tada za $k = 1$ dobivamo

$$m\overline{1} = \underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{n \text{ puta}} = \overline{m} = \overline{0},$$

što implicira $m = pn$ za neki $p \geq 1$. Time dobivamo kontradikciju jer je $m < n$.
Dakle vrijedi, $m = n$.

Jer će nam to u nekom trenu biti potrebno, podsjetimo se da su posebno prsteni $\mathbb{Z}_p$ polja, kada je $p \in \mathbb{N}$ prost broj.

Sada ćemo se podsjetiti na još neke pojmove, i na pripadajuću notaciju, jer ćemo to u daljnjem stalno koristiti.

Definicija 1.3.3. *Ako su $\mathbb{K}$ i $\mathbb{F}$ polja takva da je $\mathbb{K} \subseteq \mathbb{F}$, onda kažemo da je $\mathbb{K}$* ***potpolje*** *od $\mathbb{F}$, ili da je $\mathbb{F}$ proširenje od $\mathbb{K}$. Oznaka za to će biti*

$$\mathbb{F} \mid \mathbb{K};$$

analogno, za polja $\mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \ldots \mathbb{K}_n$, pišemo

$$\mathbb{K}_n \,|\, \mathbb{K}_{n-1} \,|\, \ldots \,|\, \mathbb{K}_1.$$

*Ako posebno imamo $\mathbb{F} \,|\, \mathbb{M} \,|\, \mathbb{K}$, onda kažemo da je $\mathbb{M}$ **međupolje** koje sadrži $\mathbb{K}$ i sadržano je u $\mathbb{F}$; ili kraće, da je $\mathbb{M}$ međupolje za $\mathbb{F} \,|\, \mathbb{K}$.*

Definicija 1.3.4. *Neka je $\mathbb{F} \,|\, \mathbb{K}$ i $S \subseteq \mathbb{F}$ neki podskup. Definirajmo polje $\mathbb{K}(S)$ kao najmanje potpolje od $\mathbb{F}$ koje sadrži i polje $\mathbb{K}$ i skup S, tj.*

$$\mathbb{K}(S) = \bigcap_{\substack{\mathbb{F} \,|\, \mathbb{E} \,|\, \mathbb{K} \\ \mathbb{K} \cup S \subseteq \mathbb{E}}} \mathbb{E};$$

*polje $\mathbb{K}(S)$ zovemo **proširenje** od $\mathbb{K}$ u $\mathbb{F}$ **generirano** sa S. Posebno, ako je skup $S = \{a\}$ jednočlan, pišemo $\mathbb{K}(a)$ umjesto $\mathbb{K}(\{a\})$. Analogno, za skup $S = \{a_1, a_2, \ldots, a_n\}$ pišemo $\mathbb{K}(a_1, a_2, \ldots, a_n)$.*

Primjer 1.3.5.

$$\mathbb{F} = \mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} \,|\, a, b \in \mathbb{Q}\}$$

Pokažimo da je $\mathbb{F}$ stvarno proširenje skupa $\mathbb{Q}$ generirano s $\sqrt{n}$.

Svako polje koje sadrži $\mathbb{Q}$ i $\sqrt{n}$ mora sadržavati skup $\mathbb{F}$. Tvrdnja slijedi iz zatvorenosti polja na množenje i zbrajanje. Još samo trebamo dokazati da $\mathbb{F}$ ima strukturu polja. Skup je očito grupa s obzirom na zbrajanje i zatvoren je za množenje. Jedino što treba provjeriti da svaki nenul element $a + b\sqrt{n} \in \mathbb{F}$ ima inverz u $\mathbb{F}$.

$$(a + b\sqrt{n})^{-1} = \frac{1}{a + b\sqrt{n}} = \frac{1}{a + b\sqrt{n}} \, \frac{a - b\sqrt{n}}{a - b\sqrt{n}} = \frac{a}{a^2 - nb^2} - \frac{b}{a^2 - nb^2}\sqrt{n};$$

tj., $(a + b\sqrt{n})^{-1} = x + y\sqrt{n}$, gdje su $x := \frac{a}{a^2 - nb^2}$ i $y := \frac{b}{a^2 - nb^2}$ oba iz polja $\mathbb{Q}$. Zaključujemo onda da $\mathbb{F}$ stvarno ima strukturu polja i to je stvarno proširenje skupa skupa $\mathbb{Q}$ generirano s $\sqrt{n}$.

Neka su $\mathbb{K} \subseteq \mathbb{F}$ neka polja; tj., imamo proširenje polja $\mathbb{F} \,|\, \mathbb{K}$. Tada je posebno $(\mathbb{F}, +)$ komutativna (aditivna) grupa, a preslikavanje $\mathbb{K} \times \mathbb{F} \to \mathbb{F}$, $(k, x) \mapsto kx$, je skalarno množenje. Lako se provjeri da je onda $\mathbb{F}$ vektorski prostor nad $\mathbb{K}$ i posebno onda ima smisla govoriti o dimenziji od $\mathbb{F}$, nad $\mathbb{K}$.

Ako imamo proširenje polja $\mathbb{F}/\mathbb{K}$, onda možemo gledati $\mathbb{F}$ kao vektorski prostor nad $\mathbb{K}$. Označimo

$$[\mathbb{F} : \mathbb{K}] := dim_{\mathbb{K}}\mathbb{F}$$

U specijalnom slučaju kada je $[\mathbb{F} : \mathbb{K}] = 2$ kažemo da je to **kvadratno proširenje**, a ako je $[\mathbb{F} : \mathbb{K}] = 3$ imamo **kubno proširenje**, itd. Kako je glavni predmet proučavanja u ovom radu tek jedna specijalna, ali važna klasa kvadratnih proširenja, navedimo i sljedeću definiciju koja uvodi generalniju klasu proširenja polja. Ta je klasa proširenja polja od centralnog interesa u okviru *Algebarske teorije brojeva*.

Definicija 1.3.6. *Svako međupolje $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{C}$, takvo da je proširenje $\mathbb{F} | \mathbb{Q}$ konačno, zove se* ***polje algebarskih brojeva****.*

Uvodimo još jednu fundamentalnu klasu proširenja polja, koja je u središtu proučavanja u okviru Teorije polja.

Definicija 1.3.7. *Kažemo da je $\alpha \in \mathbb{F}$* ***algebarski nad*** *$\mathbb{K}$, ako postoji polinom $0 \neq F \in \mathbb{K}[X]$ takav da je*

$$F(\alpha) = 0$$

inače, kažemo da je α ***transcendentan nad*** *$\mathbb{K}$.*

Proučavanje polja algebarskih brojeva započelo je i 19. stoljeću. Motivacija je došla iz rješavanja raznih diofantskih jednadžbi, a ponajprije poznatog *Velikog Fermatovog problema*.
To je središnja tema u grani matematike koja se naziva algebarska teorija brojeva.

Definicija 1.3.8. *Kažemo da je proširenje $\mathbb{F}/\mathbb{K}$* ***algebarsko*** *(nad $\mathbb{K}$), ako je svaki $\alpha \in \mathbb{F}$ algebarski, nad $\mathbb{K}$.*

Na kraju ovog kratkog preglednog dijela o poljima navedimo i dokažimo rezultat, koji povezuje konačna proširenja polja s algebarskim proširenjima.

Propozicija 1.3.9. *Ako je proširenje polja $\mathbb{F} | \mathbb{K}$ konačno, onda je ono i algebarsko proširenje.*

Dokaz. Neka je $a \in \mathbb{F}$ proizvoljan i neka je $[\mathbb{F} : \mathbb{K}] = n,\ n \in \mathbb{N}$
Trebamo pokazati da za $a \in \mathbb{F}$ postoji $f(x) \in \mathbb{K}[x]$ takav da vrijedi $f(a) = 0$. Budući da je $\mathbb{F}$ polje vrijedi $1, a, a^2, \ldots, a^n \in \mathbb{F}$. Također $1, a, a^2, \ldots, a^n$ je skup od $n + 1$ vektora koji se nalaze u n dimenzionalnom vektorskom prostoru, i onda su oni međusobno linearno zavisni nad $\mathbb{K}$. Odnosno postoje neki $k_0, k_1, \ldots, k_m \in \mathbb{K}$, pri čemu je $m \leq n$ i $k_m \neq 0$, takvi da vrijedi

$$k_0 + k_1 a + \cdots + k_n a^n = 0$$

Dakle, α je broj koji je algebarski nad $\mathbb{K}$. Kako je α bio proizvoljan imamo propoziciju dokazanu. □

Obrat gornje tvrdnje ne vrijedi.
Ako bi za primjer uzeli proširenje polja $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \ldots, \sqrt{n}, \ldots)$. Jasno je da je svaki element algebarski, jer $\sqrt{n}$ zadovoljava jednadžbu $x^2 - n = 0$. Tako da je ovo proširenje algebarsko, ali nije konačno.
Sada ćemo još opisati jednu također važnu konstrukciju tzv. *polja kvocijenata*, koju ćemo u daljnjem radu trebati. Za to, najprije se podsjetimo kako smo od cijelih brojeva $\mathbb{Z}$ došli do skupa racionalnih brojeva $\mathbb{Q}$. Neka je sada R bilo koja komutativna integralna domena s jedinicom $1_A = 1$ i nulom $0_A = 0$, onda definiramo skup razlomaka $\frac{x}{y}$, koje označavamo i s x/y,

$$Q(A) := \left\{ \frac{x}{y} \mid x, y \in A, y \neq 0 \right\}.$$

Na tom skupu formalnih razlomaka definiramo sljedeće.

Definicija 1.3.10. *Za dva formalna razlomka x_1/y_1 i x_2/y_2 kažemo da su **jednaki**, i koristimo standardnu oznaku $x_1/y_1 = x_2 = y_2$, ako i samo ako je $x_1y_2 = x_2y_1$.*

$$\frac{x_1}{y_1} = \frac{x_2}{y_2} \iff x_1y_2 = x_2y_1. \tag{1.2}$$

*Na skupu formalnih razlomaka $Q(A)$ definiramo operaciju **zbrajanja** tako da za x_1/y_1 i x_2/y_2 definiramo njihov **zbroj***

$$\frac{x_1}{y_1} + \frac{x_2}{y_2} := \frac{x_1y_2 + x_2y_1}{y_1y_2}. \tag{1.3}$$

*Isto tako definiramo operaciju **množenja** formalnih razlomaka tako da za x_1/y_1 i x_2/y_2 definiramo njihov **produkt**, ili **umnožak**, s*

$$\frac{x_1}{y_1} \cdot \frac{x_2}{y_2} := \frac{x_1x_2}{y_1y_2}. \tag{1.4}$$

Teorem 1.3.11. *Operacije zbrajanja i množenja na skupu formalnih razlomaka $Q(R)$ su dobro definirane, i uz te operacije $(Q(R), +, \cdot)$ ima strukturu polja koje se zove **polje kvocijenata** od R. Nadalje, preslikavanje $r \to r/1$, iz R u $Q(R)$, je mononomorfizam prstena s jednicom i pomoću njega identificiramo R s njegovom slikom, te tako smatramo da je $R \leq Q(R)$ potprsten.*

Primjer 1.3.12.

1. Kako smo već primijetili, za $R = \mathbb{Z}$ dobivamo polje racionalnih brojeva $Q(\mathbb{Z}) = \mathbb{Q}$.
2. Ako je $R = \mathbb{R}[x]$ prsten realnih polinoma u jednoj varijabli, onda dobivamo polje racionalnih funkcija

$$Q(\mathbb{R}[x]) = \left\{ \frac{f(x)}{g(x)} \mid f, g \in \mathbb{R}[x] \text{ i } g \neq 0 \right\}.$$

Poglavlje 2

Kvadratna proširenja

Prije smo definirali pojam konačnih proširenja polja, i posebno kvadratnih proširenja. Kao dobro poznat primjer kvadratnog proširenja polja imamo $\mathbb{C} \mid \mathbb{R}$. Sada ćemo proučiti kvadratna proširenja polja u malo generalnijem kontekstu.

Pretpostavimo da je $\mathbb{F} \mid \mathbb{K}$ proizvoljno kvadratno proširenje. Ako s 1 označimo jedinicu u poljima $\mathbb{K}$ i $\mathbb{F}$, onda naprimjer za bilo koji element $w \in \mathbb{F} \setminus \mathbb{K}$ imamo da je $\{1, w\}$ baza od $\mathbb{F}$ kao $\mathbb{K}$-vektorskog prostora. Tada je posebno

$$\mathbb{F} = \{a + bw \mid a, b \in \mathbb{K}\}.$$

Isto tako dobro je primijetiti i sljedeće. Budući da je $w \in \mathbb{F}$, onda je i $w^2 \in \mathbb{F}$ pa zato postoje neki $a_0, b_0 \in \mathbb{K}$ takvi da je

$$w^2 = a_0 + b_0 w \quad \Leftrightarrow \quad w^2 - b_0 w - a_0 = 0.$$

Drugim riječima, w je nultočka polinoma $f(X) \in \mathbb{K}[X]$ definiranog s

$$f(X) = X^2 - b_0 X - a_0.$$

Tako smo od kvadratnog proširenja $\mathbb{F} \mid \mathbb{K}$ došli do gornjeg kvadratnog polinoma $f(X)$, koji to proširenje kako ćemo kasnije vidjeti zapravo i određuje.

Možemo krenuti od proizvoljnog kvadratnog polinoma iz $\mathbb{K}[X]$ pa doći do nekog kvadratnog proširenja polja $\mathbb{K}$. Da bismo precizno objasnili o čemu se radi, trebamo se podsjetiti na još neke važne pojmove iz Teorije polja. Kao motivaciju za to sjetimo se da ako uzmemo proizvoljan ne-konstantan polinom $f(X) \in \mathbb{R}[X]$, moguće je da on nema nultočaka u $\mathbb{R}$. Naprimjer polinom $f(X) = X^2 + 1$ je takav, ali svaki će takav polinom $f(X)$ imati barem jednu nultočku u polju kompleksnih brojeva $\mathbb{C}$. Zapravo vrijedi i općenitije, o čemu govori sljedeći dobro poznat teorem koji mi ovdje nećemo dokazivati.

Teorem 2.0.1. (Osnovni teorem algebre)

Neka je $f(X) = c_0 + c_1X + \cdots + c_nX^n$ *polinom u prstenu* $\mathbb{C}[X]$*, stupnja* $n = \deg f(X) \geq 1$*. Tada postoji barem jedna nultočka* $z_0 \in \mathbb{C}$ *toga polinoma. Štoviše, postoji točno* n *vrijednosti* $z_1, \ldots, z_n \in \mathbb{C}$*, koje nisu nužno međusobno različite, takve da je*

$$f(X) = c_n(X - z_1) \cdots (X - z_n).$$

Drugačije rečeno, $\mathcal{N}(f) := \{z_1, \ldots, z_n\}$ *je skup* svih *nultočaka polinoma* $f(X)$*.*

Činjenicu da svaki nekonstantan polinom s kompleksnim koeficijentima ima barem jednu nultočku u polju kompleksnih brojeva kraće opisujemo frazom da je polje $\mathbb{C}$ algebarski zatvoreno.

Iako je proširenje polja $\mathbb{C} \mid \mathbb{R}$ po mnogo čemu vrlo specifično, ono je tek jedan specijalan slučaj općenitog fenomena. Spomenimo prvo jednu važnu definiciju.

Definicija 2.0.2. *Kažemo da je polje* $\mathbb{K}$ ***algebarski zatvoreno****, ako svaki ne-konstantan polinom iz* $\mathbb{K}[X]$ *ima bar jednu nultočku u* $\mathbb{K}$*.*

Kao jednostavnu posljedicu te definicije imamo ovaj korolar, koji je direktna generalizacija navedenog u Osnovnom teoremu algebre.

Korolar 2.0.3. *Pretpostavimo da je polje* $\mathbb{K}$ *algebarski zatvoreno, i da je polinom* $f(X) \in \mathbb{K}[X]$ *stupnja* $n = \deg f(X) \geq 1$*. Tada postoji* n *vrijednosti* $x_1, \ldots, x_n \in \mathbb{K}$ *takvih da je*

$$f(X) = \alpha(X - x_1) \cdots (X - x_n),$$

pri čemu je $\alpha \in \mathbb{K}$ *vodeći koeficijent polinoma* $f(X)$*.*

Dokaz. Dokaz provodimo jakom indukcijom po n, stupnju polinoma $f(X)$. Ako je $n = 1$, onda polinom oblika $f(X) = \alpha X + \beta$, za neke $\alpha, \beta \in \mathbb{K}$ možemo zapisati kao $f(X) = \alpha\left(X + \frac{\beta}{\alpha}\right)$ i zaključujemo da za takve polinome korolar vrijedi.
Sada pretpostavimo da je korolar dokazan za sve polinome čiji je stupanj manji od n, i neka nam je dan polinom $f(X)$ čiji je stupanj jednak n.

Kako je polje $\mathbb{K}$ algebarski zatvoreno, postoji neka njegova nultočka $x_1 \in \mathbb{K}$ tj., imamo da je $f(x_1) = 0$. Sada podijelimo, po *Teoremu o dijeljenju s ostatkom* za polinome polinom $f(X)$ polinomom $X - x_1$. Tada postoje neki polinomi $q(X), r(X) \in \mathbb{K}[X]$ takvi da je

$$f(X) = (X - x_1)q(X) + r(X), \tag{2.1}$$

pri čemu je polinom $r(X)$ ili nul-polinom, ili je različit od nul-polinoma i stupnja je $\deg r(X) < \deg(X - x_1) = 1$. Ali kad bi bilo ovo drugo moralo bi biti da je $r(X) = C$, polinom konstante

$0 \neq C \in \mathbb{K}$. Uvrštavanjem $X = x_1$ u (2.1), dobili bismo da je $0 = f(x_1) = r(x_1) = C$, što je kontradikcija. Zaključujemo da je $r(X)$ nul-polinom, i onda je

$$f(X) = (X - x_1)q(X).$$

Ali sada je jasno da je polinom $q(X)$ stupnja $n-1$, te da je njegov vodeći koeficijent jednak α, pa onda na njega možemo primijeniti pretpostavku indukcije. To znači da postoje neki $x_2, \ldots, x_n \in \mathbb{K}$ takvi da je

$$q(X) = \alpha(X - x_2) \cdots (X - x_n).$$

Tako korolar evidentno slijedi. □

Sljedeći osnovni teorem je vrlo netrivijalan rezultat, koji također navodimo bez dokaza jer bi nas odvelo daleko od teme ovog rada.

Teorem 2.0.4. *Neka je $\mathbb{K}$ proizvoljno polje.*

(i) Postoji algebarsko proširenje $\mathbb{F}/\mathbb{K}$ takvo da je $\mathbb{F}$ algebarski zatvoreno polje.

(ii) Ako su $\mathbb{F}_1$ i $\mathbb{F}_2$ dva algebarska proširenja od $\mathbb{K}$, i oba su algebarski zatvorena, onda postoji izomorfizam polja $\sigma : \mathbb{F}_1 \to \mathbb{F}_2$ nad $\mathbb{K}$; tj., $\sigma_{|\mathbb{K}} = 1_{\mathbb{K}}$, restrikcija od σ na $\mathbb{K}$ je identiteta na $\mathbb{K}$.

Prva tvrdnja gornjeg teorema daje egzistenciju polja $\mathbb{F}$, koje ima navedena svojstva, dok tvrdnja (ii) pokazuje da je takvo polje $\mathbb{F}$ zapravo do na izomorfizam polja jedinstveno. Kao posljedicu svega imamo da je sljedeća definicija sasvim korektna.

Definicija 2.0.5. *Polje $\mathbb{F}$ iz tvrdnje (i) prethodnog teorema zove se* ***algebarski zatvarač*** *polja $\mathbb{K}$, i standardno označava s $\overline{\mathbb{K}}$; tj.,*

$$\overline{\mathbb{K}} := \textit{algebarski zatvarač od } \mathbb{K}.$$

Pokažimo sada da proizvoljni kvadratni polinom određuje kvadratno proširenje . U tu svrhu pretpostavimo da je $f(X) \in \mathbb{K}[X]$ neki kvadratni polinom oblika

$$f(X) = X^2 + \alpha X + \beta,$$

gdje su koeficijenti $\alpha, \beta \in \mathbb{K}$. Odmah vidimo da time što smo uzeli da je polinom $f(X)$ normiran nismo ništa izgubili na općenitosti. Promotrimo onda algebarski zatvarač $\overline{\mathbb{K}}$, polja $\mathbb{K}$. Kažimo još jednom da konstrukcija polja $\overline{\mathbb{K}}$ nije jedinstvena, ali svake dvije konstrukcije daju međusobno izomorfna polja. Sada je jasno da postoje neki $w_1, w_2 \in \overline{\mathbb{K}}$ takvi da je

$$f(X) = (X - w_1)(X - w_2).$$

Naravno, nas posebno zanima situacija kada recimo $w_1 \in \overline{\mathbb{K}} \setminus \mathbb{K}$.
Definiramo skup

$$\mathbb{F} := \{a + bw_1 \mid a, b \in \mathbb{K}\},$$

za koji imamo sljedeću opservaciju.

Propozicija 2.0.6. *Pretpostavimo da je $w_1 \in \overline{\mathbb{K}} \setminus \mathbb{K}$. Onda je skup $\mathbb{F}$ potpolje od $\overline{\mathbb{K}}$ koje je kvadratno proširenje od $\mathbb{K}$. Nadalje, i nultočka w_2 polinoma $f(X)$ nalazi se u $\mathbb{F} \setminus \mathbb{K}$.*

Dokaz. Budući je w_1 nultočka polinoma $f(X)$, imamo da je

$$w_1^2 + \alpha w_1 + \beta = 0 \quad \Leftrightarrow \quad w_1^2 = -\alpha w_1 - \beta.$$

Neka su sada $y_i = a_i + b_i w_1 \in \mathbb{F}$, za $i = 1, 2$. Očito je $y_1 - y_2 \in \mathbb{F}$, što pokazuje da je $(\mathbb{F}, +)$ aditivna podgrupa od $(\overline{\mathbb{K}}, +)$. Nadalje, korištenjem gornje ekvivalencije, imamo

$$\begin{aligned} y_1 y_2 &= a_1 a_2 + (a_1 b_2 + a_2 b_1) w_1 + b_1 b_2 w_1^2 \\ &= (a_1 a_2 - b_1 b_2 \beta) + (a_1 b_2 + a_2 b_1 - b_1 b_2 \alpha) w_1. \end{aligned}$$

Kako su oba izraza u zagradama, iz posljednje jednakosti, očito elementi iz polja $\mathbb{K}$, zaključujemo da je $y_1 y_2 \in \mathbb{F}$. Po definiciji potprstena, vidimo da je $\mathbb{F}$ potprsten polja $\overline{\mathbb{K}}$.

Sada želimo pokazati da je $\mathbb{F}$ doista i polje tj., da svaki nenul element iz toga prstena jest invertibilan. Da bi to pokazali prvo primijetimo kako je evidentno neki element $a + bw_1 \in \mathbb{F}$ jednak 0 ako i samo ako je $a = b = 0$. Onda uzmimo neki $a + bw_1 \neq 0$, pri čemu je sasvim jasno da možemo pretpostaviti da je $b \neq 0$. Tvrdimo da postoji neki $x + yw_1$ takav da je

$$(a + bw_1)(x + yw_1) = 1.$$

Sasvim isti račun kao kad smo gore množili y_1 i y_2 nam daje sustav od dvije jednadžbe u nepoznanicama x i y:

$$\begin{cases} ax - by\beta = 1 \\ bx + (a - b\alpha)y = 0 \end{cases}$$

Primjenom Cramerovog pravila, za rješavanje sustava jednadžbi, gledajmo determinantu sustava

$$D := \begin{vmatrix} a & -b\beta \\ b & a - b\alpha \end{vmatrix} = a^2 - \alpha ab + \beta b^2.$$

Ako pokažemo da je $D \neq 0$, onda je jasno da gornji sustav ima jedinstveno rješenje u x i y; i gotovi smo. Da bi to dokazali pretpostavimo suprotno, i onda jednakost $D = 0$ podijelimo s b^2. Sjetimo se da smo gore pretpostavili da je $b \neq 0$ tako da smijemo provesti dijeljenje. Dobivamo:

$$(a/b)^2 - \alpha(a/b) + \beta = 0 \quad \Rightarrow \quad (-a/b)^2 + \alpha(-a/b) + \beta = 0.$$

No to bi značilo da je element $\omega := -a/b$, koji je evidentno iz $\mathbb{K}$, nultočka našeg polinoma $f(X)$. Znači, dobili bismo da je $\omega = w_1$ ili $\omega = w_2$. No prva jednakost je nemoguća jer smo pretpostavili da $w_1 \notin \mathbb{K}$, ali isto tako po Vieteovoj formuli $w_1 + w_2 = -\alpha$, koristeći činjenicu da je $\alpha \in \mathbb{K}$ vidimo da imamo $w_1 \notin \mathbb{K}$ ako i samo ako $w_2 \notin \mathbb{K}$. Drugim riječima, imamo da je $w_2 \in \mathbb{F} \setminus \mathbb{K}$, kako smo i tvrdili. Time je dokaz propozicije gotov. □

Navedimo još jednu definiciju koju ćemo koristiti u nastavku.

Definicija 2.0.7. *Neka je $\mathbb{K}$ proizvoljno polje. Kažemo da je polinom $f(X) \in \mathbb{K}[X]$* ***ireducibilan polinom****, nad $\mathbb{K}$, ukoliko je on ireducibilan kao element prstena $\mathbb{K}[X]$. Precizno rečeno, $f(X)$ je ireducibilan ako je on stupnja* $\deg f(X) \geq 1$ *i takav je da ne postoje neki polinomi $g(X), h(X) \in \mathbb{K}[X]$, oba stupnja barem jedan, a takvi da je $f(X) = g(X)h(X)$.*

Sada imamo ovu jednostavnu lemu, čiji dokaz ispuštamo.

Lema 2.0.8. *Neka je $\mathbb{K}$ polje. Kvadratni polinom $f(X) \in \mathbb{K}[X]$ je ireducibilan nad $\mathbb{K}$ ako i samo ako on nema nultočaka u $\mathbb{K}$.*

Kao rezime dosadašnjih razmatranja imamo sljedeći teorem, koji u potpunosti opisuje dobivanje svih kvadratnih proširenja nekog fiksiranog polja. Njegov je dokaz zapravo dan preko gornje Propozicije 2.0.6 i ostale dane argumentacije. Samo spomenimo kako taj teorem ima i generalniju formu, za proizvoljna konačna proširenja polja, ali je dokaz bitno kompliciraniji i između ostalog on nam neće trebati u ovom radu.

Teorem 2.0.9. *Neka je $\mathbb{K}$ proizvoljno polje, i neka je $\overline{\mathbb{K}}$ algebarski zatvarač od $\mathbb{K}$. Ako je $\mathbb{F}$ međupolje $\mathbb{K} \subseteq \mathbb{F} \subseteq \overline{\mathbb{K}}$ takvo da je proširenje $\mathbb{F}|\mathbb{K}$ štoviše kvadratno, onda postoji ireducibilan kvadratni polinom $f(X) \in \mathbb{K}[X]$ takav da je $F = \{a + bw \,|\, a, b \in \mathbb{K}\}$, pri čemu je $w \in \overline{\mathbb{K}}$ bilo koja od dvije nultočki polinoma $f(X)$.*

Obratno, ako je $f(X) \in \mathbb{K}[X]$ kvadratni ireducibilan polinom, i ako je $w \in \overline{\mathbb{K}}$ neka njegova nultočka, onda je skup $F = \{a + bw \,|\, a, b \in \mathbb{K}\}$ potpolje od $\overline{\mathbb{K}}$ koje je kvadratno proširenje polja $\mathbb{K}$.

Kao zanimljivu posljedicu prethodnog teorema pokazat ćemo kako se mogu dobiti konkretne realizacije polja koja imaju p^2 elemenata, za neke proste brojeve p, ali prije toga dajemo nekoliko pripremnih napomena i komentara.

Kao važnu klasu polja imamo konačna polja, koja se još zovu i **Galoisova polja** koja su dobila ime u čast francuskom matematičaru *E. Galoisu*. Osnovni dobro poznati primjeri takvih polja su kvocijenti

$$\mathbb{F}_p = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\},$$

kada je p prost broj. Može se pokazati, što mi ovdje nećemo napraviti u punoj općenitosti, kako vrijedi sljedeći teorem.

Teorem 2.0.10. *Neka su prost broj $p \in \mathbb{N}$ i $f \in \mathbb{N}$ proizvoljni, pa definirajmo $q = p^f$. Tada postoji, i do na izomorfizam je jedinstveno, konačno polje $\mathbb{F}_q$ od q elemenata.*

No, kako smo rekli, ono što želimo napraviti je konstrukcija polja od p^2 elemenata, za neke konkretne p-ove. Tako ćemo dobiti kvadratna proširenja $\mathbb{F}_{p^2}$ polja $\mathbb{F}_p$. Jasno, realizacija tih polja koristit će gore dokazan teorem 2.0.9. U tu svrhu gledajmo prsten polinoma $A = \mathbb{F}_p[X]$, i primijetimo kako su svi linearni polinomi

$$X, \quad X + \overline{1}, \quad X + \overline{2}, \ldots, \quad X + \overline{p-1}$$

ireducibilni. Sada, ono što nas zanima je naći neki kvadratni polinom koji će biti ireducibilan. U prvi mah možda nije odmah jasno da takav uopće postoji, pa zato dokažimo sljedeću elementarnu lemu koja nam daje malo generalniju informaciju negoli nama u ovom trenutku jest potrebno. Kako je lema kombinatorne naravi, podsjetimo se što su *kombinacije s ponavljanjem*. Dakle, recimo da imamo skup $L_n = \{1, 2, \ldots, n\}$, od prvih n prirodnih brojeva. I zanima nas koliko možemo naći uređenih m-torki $(x_1, \ldots, x_m)$, gdje je

$$1 \leq x_1 \leq x_2 \leq \cdots \leq x_m \leq n.$$

Dobro je poznato da je takvih m-torki $\binom{n+m-1}{m}$.

Lema 2.0.11. *Neka je $p \in \mathbb{N}$ prost broj. U prstenu polinoma $\mathbb{F}_p[X]$ je barem $\binom{p}{2}$ kvadratnih normiranih ireducibilnih polinoma.*

Dokaz. Svaki kvadratni normiran polinom iz $\mathbb{F}_p[X]$ je oblika $X^2+\alpha X+\beta$, za neke $\alpha, \beta \in \mathbb{F}_p$. Znači, takvih je polinoma p^2. S druge strane, neki takav polinom će biti reducibilan ako i samo ako se može napisati kao produkt dva linearna polinoma tj., kao produkt $(X+\overline{k})(X+\overline{\ell})$, za neke $\overline{k}, \overline{\ell} \in \mathbb{F}_p$. To su produkti $X^2, X(X + \overline{1}), \ldots, X(X + \overline{p-1}), \ldots$ Takvih je produkata onoliko koliko ima i kombinacija s ponavljanjem od po 2 elementa u p-članom skupu; tj., ima ih $\binom{p+1}{2}$. Sada treba primijetiti kako su svi ti polinomi međusobno različiti. Naime, pretpostavimo da imamo dva različita dvočlana skupa $\{\overline{k}, \overline{l}\}$ i $\{\overline{s}, \overline{t}\}$ takva da je

$$(X + \overline{k})(X + \overline{l}) := \Phi(X) =: (X + \overline{s})(X + \overline{t})$$

To bi značilo da je polinom $\Phi(X)$ stupnja 2, i ima barem tri međusobno različite nultočke, što je nemoguće. Zaključujemo da imamo točno

$$p^2 - \binom{p+1}{2} = \binom{p}{2}$$

normiranih kvadratnih ireducibilnih polinoma. □

Napomena 2.0.12. *Iako nama u radu to neće trebati, dobro je primijetiti kako se gornja lema može generalizirati. Naime, sličnim kombinatornim metodama prebrojavanja može se vidjeti da vrijedi sljedeće:*
Ako je $p \in \mathbb{N}$ prost broj, onda u prstenu polinoma $\mathbb{F}_p[X]$ ima točno $2\binom{p+1}{3}$ kubnih normiranih ireducibilnih polinoma. Jasno, mogli bismo dalje računati broj normiranih ireducibilnih polinoma četvrtog stupnja u prstenu $\mathbb{F}_p[X]$, itd.

Pogledajmo sada neke konkretne primjere: kvadratnih normiranih ireducibilnih polinoma nad konačnim poljima $\mathbb{F}_p$, a onda i pripadajućih konstrukcija kvadratnih proširenja tih polja $\mathbb{F}_p$.

Primjer 2.0.13. *(1) Uzmimo $p = 2$. Po gornjoj lemi znamo da je u $\mathbb{F}_2[X]$ točno $\binom{2}{2} = 1$ kvadratni normiran ireducibilan polinom. Lako se provjeri da je to polinom*

$$f(X) = X^2 + X + \overline{1}.$$

Sada pomoću polinoma f realizirajmo polje $\mathbb{F}_4 = \mathbb{F}_{2^2}$. Prema Teoremu 2.0.9 možemo uzeti simbol w koji odgovara nultočki polinoma f u algebarskom zatvaraču $\overline{\mathbb{F}_2}$ i onda staviti

$$\mathbb{F}_4 = \{a + bw \mid a, b \in \mathbb{F}_2\} = \{\overline{0}, \overline{1}, w, \overline{1} + w\},$$

pri čemu je $w^2 + w + \overline{1} = 0 \Leftrightarrow w^2 = \overline{1} + w$. Zbrajanje je evidentno. A za množenje imamo da je $\overline{0}\, a = \overline{0}$ i $\overline{1}\, a = a$, za svaki $a \in \mathbb{F}_4$, te je posebno

$$w^2 = w\, w = \overline{1} + w, \quad w(\overline{1} + w) = \overline{1}, \quad (\overline{1} + w)(\overline{1} + w) = w.$$

(2) Uzmimo $p = 3$. Ovdje lema govori da imamo točno $\binom{3}{2} = 3$ kvadratna normirana ireducibilna polinoma. Lako se provjeri da su to polinomi:

$$X^2 + \overline{1}, \quad X^2 + X + \overline{2}, \quad X^2 + \overline{2}X + \overline{2}.$$

Sada izaberimo naprimjer prvi od gornja tri polinoma; tj., stavimo

$$f(X) = X^2 + \overline{1}.$$

Sada realizirajmo kvadratno proširenje $\mathbb{F}_9 \,|\, \mathbb{F}_3$, gdje ponovo uzmimo simbol w, i onda stavimo

$$\begin{aligned}\mathbb{F}_9 &= \{a + bw \mid a, b \in \mathbb{F}_2\} \\ &= \{\overline{0}, \overline{1}, \overline{2}, w, \overline{1} + w, \overline{2} + w, \overline{2}w, \overline{1} + \overline{2}w, \overline{2} + \overline{2}w\}.\end{aligned}$$

Sada je $w^2 + \overline{1} = \overline{0} \Leftrightarrow w^2 = \overline{2}$, i zato je množenje u $\mathbb{F}_9$ dano kao

$$(a_1 + b_1 w)(a_2 + b_2 w) = a_1 a_2 + \overline{2} b_1 b_2 + (a_1 b_2 + a_2 b_1) w.$$

Naprimjer; $(\overline{1}+w)^2 = \overline{2}w$, $(\overline{1}+w)(\overline{2}+\overline{2}w) = w$, *itd.*

(3) Uzmimo $p = 5$. *Sada znamo da u* $\mathbb{F}_5[X]$ *imamo barem* $\binom{5}{2} = 10$ *kvadratnih normiranih ireducibilnih polinoma. To su polinomi*

$$X^2+\overline{2}, \quad X^2+\overline{3}, \quad X^2+X+\overline{1}, \quad X^2+X+\overline{2}, \ \ldots\ , X^2+\overline{4}X+\overline{1}, \quad X^2+\overline{4}X+\overline{2}.$$

Kao i u prethodnom primjeru, gledajmo za f *prvi od navedenih polinoma; tj., stavimo*

$$f(X) = X^2+\overline{2}.$$

Sada realiziramo kvadratno proširenje $\mathbb{F}_{5^2}\,|\,\mathbb{F}_5$, *gdje ponovo uzmimo simbol* w, *i onda stavimo*

$$\mathbb{F}_{5^2} = \{a+bw \,|\, a,b \in \mathbb{F}_5\}.$$

Sada je $w^2+\overline{2} = \overline{0} \ \Leftrightarrow\ w^2 = \overline{3}$, *i zato je množenje u* $\mathbb{F}_{5^2}$ *dano kao*

$$(a_1+b_1w)(a_2+b_2w) = a_1a_2 + \overline{3}b_1b_2 + (a_1b_2+a_2b_1)w.$$

(4) Uzmimo još $p = 17$. *Po gornjoj lemi znamo da u* $\mathbb{F}_{17}[X]$ *od ukupno* $17^2 = 289$ *kvadratnih normiranih polinoma, njih je* $\binom{17}{2} = 136$ *ireducibilno. Sad, bilo bi nešto posla da se pronađe sve ireducibilne polinome, no to nas neće u trenutku zanimati. Nego ono što će nas zanimati je naći jedan takav konkretan polinom. I onda probajmo potražiti taj polinom u obliku*

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

Uz malo posla, korištenjem elementarne teorije brojeva koja govori o tzv. kvadratnim ostatcima, moglo bi se pokazati da ćemo za svaki prost p *moći naći neki ireducibilan polinom gornjeg oblika. Naime, želimo vidjeti je li postoji neki* $\alpha \in \mathbb{F}_{17}$ *takav da polinom* $f(X)$ nema *niti jednu nultočku u polju* $\mathbb{F}_{17}$. *Da to vidimo računamo redom kvadrate elemenata iz* $\mathbb{F}_{17}$. *Lako se računa da su kvadrati* $\overline{k}^2$, *kada je* $k \in \{0,1,\ldots,16\}$ *u skupu*

$$\{\overline{0},\overline{1},\overline{4},\overline{9},\overline{16},\overline{8},\overline{2},\overline{15},\overline{13}\}.$$

I onda kao posljedicu imamo da je svaki

$$\alpha \in \{\overline{3},\overline{5},\overline{6},\overline{7},\overline{10},\overline{11},\overline{12},\overline{14}\}$$

dobar. Ako uzmemo sada naprimjer

$$f(X) = X^2+\overline{3},$$

imamo realizaciju kvadratnog proširenja $\mathbb{F}_{17^2} \mid \mathbb{F}_{17}$*, gdje stavimo*

$$\mathbb{F}_{17^2} = \{a + bw \mid a, b \in \mathbb{F}_{17}\};$$

pri čemu je množenje dano s

$$(a_1 + b_1 w)(a_2 + b_2 w) = a_1 a_2 + \overline{14} b_1 b_2 + (a_1 b_2 + a_2 b_1) w.$$

Ovo poglavlje završavamo jednom napomenom koja sugerira kako su gornja razmatranja tek specijalan slučaj sasvim općenite konstrukcije proširenja polja.

Napomena 2.0.14. *Moglo bi se pokazati da je skup realnih brojeva*

$$\mathbb{Q}\left(\sqrt[3]{2}\right) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$$

potpolje od $\mathbb{R}$*, te da je* $\mathbb{Q}\left(\sqrt[3]{2}\right) \mid \mathbb{Q}$ *kubno proširenje. Tu primijetimo da je polinom* $f(X) = X^3 - 2$ *ireducibilan u prstenu polinoma* $\mathbb{Q}[X]$ *prema Eisensteinovom kriteriju za* $p = 2$*.*

Sasvim analogno, što je i bilo spomenuto, mogli bismo gledati ponovo prsten polinoma $\mathbb{F}_p[X]$*, i onda u njemu pronaći neki kubni normiran ireducibilan polinom. Pokazuje se da barem jedan takav uvijek postoji, iako ga možda uvijek neće biti sasvim jednostavno pronaći. Onda bismo za neki takav polinom*

$$f(X) = X^3 + \alpha X^2 + \beta X + \gamma,$$

gdje su $\alpha, \beta, \gamma \in \mathbb{F}_p$*, mogli uzeti* $w \in \overline{\mathbb{F}_p}$ *takav da je*

$$w^3 + \alpha w^2 + \beta w + \gamma = \overline{0}.$$

Ako definiramo skup

$$\mathbb{K} = \{a + bw + cw^2 \mid a, b, c \in \mathbb{F}_p\},$$

može se pokazati da je zapravo $\mathbb{K} \cong \mathbb{F}_{p^3}$*, do na izomorfizam jedinstveno konačno polje od* p^3 *elemenata. Jasno, pritom je množenje u tom skupu u potpunosti određeno polinomom* f*.*

Poglavlje 3

Algebarski brojevi

U prvom odjeljku bavimo se algebarskim brojevima gdje ćemo iskazati neke osnovne rezultate koji će nas dovesti do tvrdnje da skup algebarskih brojeva nad poljem $\mathbb{F}$ ima strukturu polja, a u drugom odjeljku definiramo pojam algebarskog cijelog broja zajedno s realnim kvadratnim proširenjem što je tema ovog diplomskog rada.

3.1 Algebarski brojevi

Najprije se podsjetimo sljedećeg dobro poznatog rezultata, čiji dokaz ispuštamo.

Lema 3.1.1. *Ako je $\mathbb{F}$ polje, onda je prsten polinoma u jednoj varijabli $\mathbb{F}[x]$ domena glavnih ideala, odnosno svaki ideal $I \trianglelefteq \mathbb{F}[x]$ je glavni.*

Sada dokazujemo ovu propoziciju.

Propozicija 3.1.2. *Neka su dana polja $\mathbb{F} \subseteq \mathbb{E}$ i neka je $\alpha \in \mathbb{E}$ element koji je korijen nekog nenul polinoma iz $\mathbb{F}[x]$. Tada postoji jedinstven ireducibilan i normiran polinom $p(x) \in \mathbb{F}[x]$ takav da je $p(\alpha) = 0$ i da je stupanj*

$$\deg(p) \leq \deg(f),$$

*za svaki polinom $f(x) \in \mathbb{F}[x]$ za koji vrijedi $f(\alpha) = 0$. Polinom $p(x)$ zove se **minimalan polinom** od α.*

Dokaz. Definirajmo skup

$$I = \{f(x) \in \mathbb{F}[x] \mid f(\alpha) = 0\};$$

tj., I je skup svih polinoma $f \in \mathbb{F}[x]$ kojima je α korijen. Primijetio da je I ideal. Sada po prethodnoj lemi znamo da postoji polinom $p = p(x) \in \mathbb{F}[x]$ takav da je $I = (p)$, pri ćemu možemo pretpostaviti da je p normiran. Tvrdimo da je polinom p i ireducibilan. Naime

ako bi postojali neki polinomi $g, h \in \mathbb{F}[x]$, oba stupnja strogo manjeg od $\deg(p)$, takvi da je $p = gh$, imali bismo da je $0 = p(\alpha) = g(\alpha)h(\alpha)$. To bi značilo da je ili $g(\alpha) = 0$ ili $h(\alpha) = 0$, odnosno da je ili $g \in I$ ili $h \in I$. No to bi značilo da p dijeli g ili h. Bez smanjenja općenitosti pretpostavimo da p dijeli g. No onda bi posebno bilo $\deg(p) \leq \deg(g)$ pa bi iz $p = gh$ slijedilo za stupnjeve da je

$$\deg(p) = \deg(gh) = \deg(g) + \deg(h) \geq \deg(p) + 1,$$

što je nemoguće. Tako zaključujemo da je p doista ireducibilan polinom.
Iz gornje argumentacije je jasno da za svaki polinom $f(x)$ kojemu je α korijen imamo da je $\deg(p) \leq \deg(f)$, kako smo i tvrdili. Nadalje, jasna je i jedinstvenost polinoma p. Naime, ako bi postojao neki polinom p_1 koji zadovoljava uvjete propozicije, posebno bismo imali da p dijeli p_1 i da su p i p_1 istog stupnja. No onda bi postojao neki konstantni polinom $k(x) = C \in \mathbb{F}^*$ takav da je $p_1 = Cp$. Kako su p i p_1 oba normirana, slijedi da je nužno $C = 1$, tj. vrijedi da je $p = p_1$. Time je naša propozicija dokazana. □

Primjerice može se pokazati da je broj $\frac{1+\sqrt{5}}{2}$, poznatiji pod nazivom zlatni rez, algebarski broj stupnja 2 nad poljem $\mathbb{Q}$ jer je nultočka polinoma $x^2 - x - 1 = 0$, a broj $\sqrt{2} + \sqrt{3}$ algebarski broj stupnja 4 nad poljem $\mathbb{Q}$ jer je nultočka polinoma $x^4 - 10x^2 + 1$.
U nastavku navodimo i dokazujemo lemu koja će dati karakterizaciju i pomoću koje ćemo moći provjeriti je li neki broj algebarski nad poljem $\mathbb{F}$.

Lema 3.1.3. *Ako su dana polja $\mathbb{F} \subseteq \mathbb{E}$ i element $\alpha \in \mathbb{E}$, onda su sljedeće dvije tvrdnje ekvivalentne.*

1. *Element α je algebarski nad $\mathbb{F}$.*
2. *Proširenje polja $\mathbb{F}(\alpha) \mid \mathbb{F}$ je konačno; tj., $[\mathbb{F}(\alpha) : \mathbb{F}] < \infty$.*

Dokaz. Ako je α algebarski broj nad poljem $\mathbb{F}$, onda prema propoziciji 3.1.2 postoji minimalni polinom $p \in \mathbb{F}[X]$ takav da vrijedi

$$p(\alpha) = \alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_1\alpha + a_0 = 0.$$

Gornju jednakost možemo zapisati kao

$$\alpha^d = -a_{d-1}\alpha^{d-1} - a_1\alpha - a_0$$

iz čega je jasno da se svaka potencija α^n može prikazati kao linearna kombinacija elemenata iz skupa $\{1, \alpha, \ldots, \alpha^{d-1}\}$. Drugim riječima, taj skup je baza od $\mathbb{F}(\alpha)$ gledanog kao vektorski prostor nad $\mathbb{F}$.

Ako je stupanj proširenja $[\mathbb{F}(\alpha) : \mathbb{F}]$ konačan, onda je po Propoziciji 1.3.9 proširenje polja $\mathbb{F}(\alpha) \mid \mathbb{F}$ algebarsko i onda je posebno element α algebarski nad $\mathbb{F}$. □

Stupanj proširenja ima vrlo važno multiplikativno svojstvo.

Propozicija 3.1.4. *Neka su $\mathbb{K}$, $\mathbb{L}$ i $\mathbb{M}$ polja za koja vrijedi $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$. Tada je $\mathbb{M}$ konačno proširenje nad $\mathbb{K}$ ako i samo ako je $\mathbb{M}$ konačno proširenje nad $\mathbb{L}$ i $\mathbb{L}$ konačno proširenje nad $\mathbb{K}$. U tom slučaju vrijedi*

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}]\,[\mathbb{L} : \mathbb{K}]\,.$$

Dokaz. Najprije pretpostavimo da je $[\mathbb{M} : \mathbb{K}] < \infty$ i onda da je $\{m_1, \ldots, m_n\}$ neki konačan skup izvodnica od $\mathbb{M}$ kao $\mathbb{K}$-vektorskog prostora. Jer je $\mathbb{K} \subseteq \mathbb{L}$ i onda je očito taj skup ujedno i skup izvodnica od $\mathbb{M}$ kao $\mathbb{L}$-vektorskog prostora. Slijedi da je $\dim_{\mathbb{L}}(\mathbb{M}) < \infty$, tj. $[\mathbb{M} : \mathbb{L}] < \infty$.

Isto tako, jer je $\mathbb{L}$ potprostor od $\mathbb{K}$-vektorskog prostora $\mathbb{M}$, očito imamo:

$$[\mathbb{M} : \mathbb{K}] < \infty \Rightarrow [\mathbb{L} : \mathbb{K}] < \infty.$$

Sada dokazujemo obratnu implikaciju. Da bi to dokazali pretpostavimo da je $[\mathbb{M} : \mathbb{L}] < \infty$ i $[\mathbb{L} : \mathbb{K}] < \infty$. Tada postoje konačne baze: baza $\mathcal{E} = (e_1, \ldots, e_n)$ od $\mathbb{M}$ kao $\mathbb{L}$-vektorskog prostora i $\mathcal{V} = (v_1, \ldots, v_d)$ od $\mathbb{L}$ kao $\mathbb{K}$-vektorskog prostora.

Tvrdimo da je skup

$$\mathcal{B} = \{e_i v_j \mid 1 \leq i \leq n, 1 \leq j \leq d\}$$

baza od $\mathbb{M}$ kao $\mathbb{K}$-vektorskog prostora. Da bismo to pokazali treba prvo vidjeti da je to skup izvodnica, a drugo da je $\mathcal{B}$ $\mathbb{K}$-linerarno nezavisan skup. Prvo uzmimo proizvoljan $x \in \mathbb{M}$. Tada postoje neki $a_i \in \mathbb{L}$ takvi da je

$$x = \sum_{i=1}^{n} a_i e_i.$$

Nadalje, za svaki indeks $1 \leq i \leq n$ postoji neki skalari $b_{ij} \in \mathbb{K}$ takvi da je

$$a_i = \sum_{j=1}^{d} b_{ij} v_j.$$

Ali onda je posebno

$$x = \sum_{i=1}^{n} \sum_{j=1}^{d} b_{ij} e_i v_j,$$

što pokazuje da je doista skup $\mathcal{B}$ skup izvodnica od $\mathbb{K}$-vektorskog prostora $\mathbb{M}$. Preostaje još samo pokazati linearnu nezavisnost skupa $\mathcal{B}$. Da bismo dokazali nezavisnost pretpostavimo da je

$$\sum_{i=1}^{n} \sum_{j=1}^{d} b_{ij} e_i v_j = 0,$$

što se ekvivalentno može zapisati i kao

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{d} b_{ij}v_j\right)e_i = 0.$$

Znamo da za svaki i

$$\sum_{j=1}^{d} b_{ij}v_j = 0$$

ako i samo ako je $b_{ij} = 0$ zbog toga što je skup $\mathcal{V}$ linearno nezavisan, s čime je propozicija je dokazana.

□

Sada dokazujemo sljedeći teorem, koji daje fundamentalnu opservaciju o algebarskim brojevima.

Teorem 3.1.5. *Neka su dana polja $\mathbb{F} \subseteq \mathbb{K}$, i definiramo skup*

$$\mathcal{A}(\mathbb{K}\,|\,\mathbb{F}) = \{\alpha \in \mathbb{K} \mid \alpha \textit{ je algebarski nad } \mathbb{F}\}.$$

Tada je $\mathcal{A}(\mathbb{K}\,|\,\mathbb{F})$ polje, odnosno imamo međupolje $\mathbb{F} \subseteq \mathcal{A}(\mathbb{K}\,|\,\mathbb{F}) \subseteq \mathbb{K}$. To se polje zove ***algebarsko zatvorenje*** *polja $\mathbb{F}$ u natpolju $\mathbb{K}$.*

Dokaz. Prema lemi 3.1.3 znamo da je $\alpha \in \mathcal{A}(\mathbb{K}\,|\,\mathbb{F})$ ako i samo ako je $[\mathbb{F}(\alpha) : \mathbb{F}]$ konačan. Pretpostavimo da su $\alpha, \beta \in \mathcal{A}(\mathbb{K}\,|\,\mathbb{F})$. Iskoristimo tezu propozicije 3.1 i zapišimo

$$[\mathbb{F}(\alpha,\beta) : \mathbb{F}] = [\mathbb{F}(\alpha,\beta) : \mathbb{F}(\alpha)]\,[\mathbb{F}(\alpha) : \mathbb{F}]\,.$$

Budući da je $\beta \in \mathcal{A}(\mathbb{K}\,|\,\mathbb{F})$ onda je sigurno i $\beta \in \mathcal{A}(\mathbb{K}\,|\,\mathbb{F}(\alpha))$ jer vrijedi $\mathbb{F} \subseteq \mathbb{F}(\alpha)$. Dakle prvi i drugi produkt na desnoj strani je konačan. Zaključujemo da je onda $[\mathbb{F}(\alpha,\beta) : \mathbb{F}]$ konačan broj, ali svaki od brojeva $\alpha+\beta, \alpha-\beta, \alpha\beta$ i $\frac{\alpha}{\beta}$ za $\beta \neq 0$ pripadaju skupu $\mathbb{F}(\alpha,\beta)$. Konačno zaključujemo da skup $\mathcal{A}(\mathbb{K}\,|\,\mathbb{F})$ ima strukturu polja. □

Napomena 3.1.6.

Posebno je zanimljiva situacija ako imamo neko polje $\mathbb{F}$ koje je potpolje nekog algebarski zatvorenog polja $\mathbb{K}$. Tada možemo gledati u gornjem teoremu definirano polje $\mathcal{A}(\mathbb{K}|\mathbb{F})$. Uz malo posla može se pokazati da je to polje zapravo algebarski zatvarač polja $\mathbb{F}$. Sjetimo se da smo u Teoremu 2.0.4 vidjeli da je algebarski zatvarač svakog polja do na izomorfizam jedinstven.
Naprimjer, možemo uzeti $\mathbb{F} = \mathbb{Q}$ i $\mathbb{K} = \mathbb{C}$. Tada je

$$\mathcal{A}(\mathbb{C}|\mathbb{Q})$$

polje koje je algebarski zatvoreno i njegovo proširenje nad $\mathbb{Q}$ je algebarsko. To je polje, koje se standardno označava s $\overline{\mathbb{Q}}$, **algebarski zatvarač** od $\mathbb{Q}$ i to je fundamentalan objekt u algebarskoj teoriji brojeva.
Primijetimo još jednu bitnu činjenicu, koju također navodimo bez dokaza. Ako je $\mathbb{F}$ neko polje algebarskih brojeva, onda je $\mathcal{A}(\mathbb{C}|\mathbb{F}) = \overline{\mathbb{Q}}$.

3.2 Algebarski cijeli brojevi

U prošlom odjeljku definirali smo i obradili osnovna svojstva algebarskih brojeva. Sada ćemo definirati poseban slučaj algebarskih brojeva koji ćemo u nastavku rada posebno istraživati. Navedimo za početak nekoliko definicija koja će nam trebati u nastavku poglavlja.

Definicija 3.2.1. *Kažemo da je cijeli broj a **kvadratno slobodan** ako je 1 najveći kvadrat prirodnog broja koji dijeli a.*

Tako su primjerice $\pm1, \pm2, \pm3, \pm5, \pm6, \ldots$ kvadratno slobodni brojevi.

Definicija 3.2.2. *Algebarski broj $\alpha \in \mathbb{C}$ je **algebarski cijeli broj** ako je njegov minimalni polinom s cjelobrojnim koeficijentima i istovremeno je normiran.*

Sada ćemo dokazati sljedeći važan rezultat, koji je jedan od centralnih u algebarskoj teoriji brojeva.

Teorem 3.2.3. Neka su $\alpha, \beta \in \mathbb{C}$ algebarski cijeli brojevi. Tada su $\alpha - \beta$ i $\alpha\beta$ također algebarski cijeli brojevi. Drugim riječima, ako definiramo skup

$$C = \text{skup svih algebarskih cijelih brojeva u } \mathbb{C},$$

onda je C potprsten od $\mathbb{C}$.

Naglasimo kako se iskaz još može formulirati u generalnijoj formi tako da umjesto $\mathbb{Z}$ gledamo bilo koju integralnu domenu R, umjesto $\mathbb{Q}$ *polje kvocijenata* $Q(R)$ od R, i umjesto $\mathbb{C}$ bilo koje algebarski zatvoreno polje koje sadrži $Q(R)$. Dokaz generalnije forme je u biti potpuno isti kao ovaj koji mi u nastavku dajemo.
Za dokaz gornjeg teorema treba nam sljedeća lema.

Lema 3.2.4. *Broj $\alpha \in \mathbb{C}$ je algebarski cijeli broj ako i samo ako postoji prirodan broj n i matrica $A \in M_n(\mathbb{Z})$ za koju je α svojstvena vrijednost.*

Dokaz. Ako je A cjelobrojna $n \times n$ matrica za koju je α svojstvena vrijednost, onda je α nultočka karakterističnog polinoma od A,

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

pri čemu primijetimo kako je očito $k_A(\lambda) \in \mathbb{Z}[\lambda]$ normiran polinom. Ali to po definiciji onda znači da je α algebarski cijeli broj.

Za obratnu implikaciju pretpostavimo da je α algebarski cijeli broj; tj.,

$$\alpha^n = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1},$$

za neke $c_i \in \mathbb{Z}$. Onda definiramo vektor $\boldsymbol{v} = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1})^T$, zapisan kao jednostupčana matrica. Isto tako definiramo matricu

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ c_0 & c_1 & c_2 & \cdots & c_{n-1} \end{pmatrix} \in M_n(\mathbb{Z}).$$

Tada je

$$\begin{aligned} A\boldsymbol{v} &= (\alpha, \alpha^2, \ldots, \alpha^{n-1}, c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1})^T \\ &= (\alpha, \alpha^2, \ldots, \alpha^n)^T = \alpha(1, \alpha, \ldots, \alpha^{n-1})^T = \alpha\boldsymbol{v}. \end{aligned}$$

Ali to znači da je α svojstvena vrijednost matrice A, za pripadni svojstveni vektor $\boldsymbol{v}$, što završava dokaz leme. □

Dokaz. Teorema 3.2.3 Neka su $\alpha, \beta \in C$, algebarski cijeli brojevi. Ideja je naći nenul vektor $\boldsymbol{w}$ i dvije matrice $A, B \in M_k(\mathbb{Z})$, za neki prirodan broj k, tako da je $A\boldsymbol{w} = \alpha\boldsymbol{w}$ i $B\boldsymbol{w} = \beta\boldsymbol{w}$. Kao jednostavnu posljedicu onda imamo da je

$$(A - B)\boldsymbol{w} = (\alpha - \beta)\boldsymbol{w}, \qquad (AB)\boldsymbol{w} = (\alpha\beta)\boldsymbol{w};$$

što po prethodnoj lemi znači da su $\alpha - \beta$ i $\alpha\beta$ također iz C.

Sada pretpostavimo da je, kao u lemi,

$$\alpha^n = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1},$$

i

$$\beta^m = d_0 + d_1\beta + \cdots + d_{m-1}\beta^{m-1},$$

za neke polinomijalne koeficijente $c_i, d_j \in \mathbb{Z}$. Onda definiramo vektor $\boldsymbol{w} \in \mathbb{C}^{mn}$ s

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

Sada promatrajmo vektor $\alpha\boldsymbol{w}$. Ako pažljivo pogledamo, uzevši u obzir gore napisanu jednakost $\alpha^n = \sum_i c_i\alpha^i$, lako vidimo da postoji matrica $A \in M_{mn}(\mathbb{Z})$ takva da je $A\boldsymbol{w} = \alpha\boldsymbol{w}$. Sasvim analogno zaključimo da postoji i $B \in M_{mn}(\mathbb{Z})$ takva da je $B\boldsymbol{w} = \beta\boldsymbol{w}$. Time je teorem dokazan. □

Primijetimo kako kvocijent dva algebarska cijela broja općenito neće biti algebarski cijeli broj. Primjerice, brojevi 5 i 6 su algebarski cijeli brojevi, ali broj $5/6$ to nije. Ta je konkretna činjenica direktna posljedica niže dane propozicije. No prije njezina dokaza, navedimo jedan dobro poznat rezultat, ali u malo generalnijoj formi negoli je to često potrebno.

Podsjetimo se da je neki prsten R **faktorijalan prsten**, ili **prsten jedinstvene faktorizacije**, ako se svaki element $x \in R$ može napisati u obliku $x = u\gamma_1 \cdots \gamma_k$, za neki invertibilan $u \in R^*$ i ireducibilne elemente $\gamma_i \in R$. I taj je rastav jedinstven, do na množenje invertbilinim elementom i do na poredak množenja ireducibilnih γ_i-ova. Uz malo se posla može pokazati da je u faktorijalnom prstenu R dobro definiran pojam najveće zajedničke mjere, kao i pojam relativno prostih elemenata. Malo slobodnije govoreći, dva su elementa, x i y iz R, relativno prosta ako je njihova najveća zajednička mjera invertibilan element. Dokaze svega navedenoga može se naći u [7].

Lema 3.2.5. *Neka je R faktorijalan prsten, neka je $\mathbb{K} = Q(R)$ pripadno polje kvocijenata, i neka je $\overline{\mathbb{K}}$ algebarski zatvarač od $\mathbb{K}$. Pretpostavimo da je dan polinom*

$$f(x) = c_n x^n + \cdots + c_1 x + c_0 \in R[x],$$

te da je $\gamma \in \overline{\mathbb{K}}$ njegova nultočka. Ako je štoviše $\gamma \in \mathbb{K}$, napisan kao razlomak a/b za neke relativno proste $a, b \in R$ pri čemu je $b \neq 0$, onda $b \mid c_n$ i $a \mid c_0$.

Dokaz. Ako je $\gamma = \frac{a}{b}$ korijen zadane jednadžbe, onda mora vrijediti

$$c_n\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\frac{a}{b} + c_0.$$

Pomnožimo li tu jednakost sa b^n dobivamo:

$$c_0 b^n = -c_n a^n - c_{n-1}a^{n-1}b - \cdots - c_1 a b^{n-1}.$$

Izlučimo $-a$ s desne strane jednakosti i dobivamo:

$$c_0 b^n = -a(c_n a^{n-1} + c_{n-1}a^{n-2}b + \cdots + c_1 b^{n-1}).$$

Sada vidimo da je $c_0 b^n$ djeljivo sa a. Budući da su a i b relativno prosti znamo da a nije djelitelj od b, pa niti od b^n. Stoga iz prethodne jednakosti zaključujemo da je a djelitelj od c_0.
Na sličan način se dokazuje da je b djelitelj od c_n. Sređivanjem gore dobivene jednakosti $c_n a^n + c_{n-1} a^{n-1} b + \cdots + c_1 a b^{n-1} + c_0 b^n = 0$ slijedi

$$c_n a^n = -c_{n-1} a^{n-1} b - \cdots - c_1 a b^{n-1} - c_0 b^n.$$

Izlučimo sada $-b$ s desne strane jednakosti i dobivamo:

$$c_n a^n = -b(c_{n-1} a^{n-1} + \cdots + c_1 a b^{n-2} + c_0 b^{n-1}).$$

Dakle, $a_n c^n$ je djeljivo sa b, no budući da smo pretpostavili da su a i b relativno prosti brojevi, slijedi da b nije djelitelj od a, a onda ni od a^n. Zaključujemo da je b djelitelj od c_n. □

Pokažimo sada jednu jednostavnu posljedicu gornje tvrdnje.

Korolar 3.2.6. *Među racionalnim brojevima jedini algebarski cijeli brojevi su upravo cijeli brojevi.*

Dokaz. Svaki $m \in \mathbb{Z}$ je algebarski cijeli broj jer je korijen normiranog polinoma $f(x) = x - m$. S druge strane, ako je $\frac{m}{q}$ algebarski cijeli broj, gdje su m i q relativno prosti cijeli brojevi, onda postoji normiran polinom

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

koji je minimalan polinom od $\frac{m}{q}$, ali onda po prethodnoj lemi slijedi da je $q \mid 1$, odnosno $q \in \{\pm 1\}$. Zaključujemo da vrijedi $\frac{m}{q} \in \mathbb{Z}$. □

Za racionalne brojeve ipak vrijedi jedna druga tvrdnja.

Lema 3.2.7. *Algebarski broj α nad $\mathbb{Q}$ je stupnja jedan ako i samo ako je $\alpha \in \mathbb{Q}$.*

Dokaz. Ako je $\alpha \in \mathbb{Q}$, onda je on korijen normiranog polinoma $f(x) = x - a$ iz $\mathbb{Q}[x]$. Dakle α je algebarski broj stupnja jedan.
Za pokazati obratnu implikaciju pretpostavimo da je $\alpha \in \mathbb{C}$ algebarski broj stupnja jedan. To znači da postoji normirani polinom $p(x) \in \mathbb{Q}[x]$ stupnja jedan čiji je α korijen. Ali to znači da je $p(x) = x + a_0$, za neki $a_0 \in \mathbb{Q}$, te da je $p(\alpha) = \alpha + a_0 = 0$. Zaključujemo da je $\alpha = -a_0 \in \mathbb{Q}$, što je i trebalo dokazati. □

U prošlom poglavlju bavili smo se općenito kvadratnim proširenjima polja gdje smo naveli i neke primjere. U nastavku ćemo promotriti kvadratna proširenja polja $\mathbb{Q}$. Prema teoremu 2.0.6 treba nam kvadratni polinom i zato ćemo pretpostaviti da je α nultočka ireducibilnog polinoma

$$f(x) = x^2 + bx + c, \quad b, c \in \mathbb{Q}.$$

Korištenjem poznate formule za rješenje kvadratne jednadžbe znamo da je α jednak

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Diskriminantu polinoma f označimo s d, i primijetio da vrijedi $\sqrt{d} \notin \mathbb{Q}$ jer je polinom f ireducibilan. Kvadratno proširenje je prema propoziciji 2.0.6 zadano s $\mathbb{K} = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$ što prema primjeru 1.3.5 možemo označiti s $\mathbb{Q}(\alpha)$.
Može se pokazati da je cijelo kvadratno proširenje zapravo jedinstveno određeno s diskriminatnom, a ne isključivo samo s nultočkama polinoma.

Lema 3.2.8. *Za ireducibilan kvadratni polinom $f(x) = x^2 + bx + c$, gdje su $b, c \in \mathbb{Q}$, kojem je α nultočka i d diskriminanta, vrijedi*

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d}).$$

Dokaz. Iz formule za rješenje kvadratne jednadžbe očito slijedi da vrijedi $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{d})$. Također iz formule zaključujemo da vrijedi $\sqrt{d} = \mp(b + 2\alpha)$ što pokazuje da je $\sqrt{d}$ element od $\mathbb{Q}(\alpha)$ i daje potrebnu inkluziju $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\alpha)$ iz koje slijedi tražena tvrdnja. □

Ako je $d > 0$ takvo proširenje nazivamo **realnim kvadratnim proširenjem**, a ako je $d < 0$ **imaginarnim kvadratnim proširenjem**.
Napomenimo samo da za $d = 0$ ili $d = 1$ dobivamo proširenje koje je jednako skupu $\mathbb{Q}$. Nas takva proširenja ovdje neće zanimati tako da u nastavku gdje pišemo d pretpostavljamo da je različit od 0 ili 1.
Koliko postoji kvadratnih proširenja? Ako postoje dva proširenja $\mathbb{Q}(\sqrt{d_1})$ i $\mathbb{Q}(\sqrt{d_2})$ kako možemo znati jesu li ta dva proširenja jednaka. To su samo neka od pitanja na koja ćemo u nastavku dati odgovor.

Propozicija 3.2.9. *Ako su kvadratna proširenja $K_1 = \mathbb{Q}(\sqrt{d_1})$ i $K_2 = \mathbb{Q}(\sqrt{d_2})$, onda je $K_1 = K_2$ ako i samo ako je $\frac{d_1}{d_2}$ kvadrat racionalnog broja.*

Dokaz. Ako je $\frac{d_1}{d_2} = r^2$, $r \in \mathbb{Q}$, onda je $d_1 = r^2 d_2$. Zato možemo pisati $a + b\sqrt{d_1} = a + b\sqrt{r^2 d_2} = a + br\sqrt{d_2}$. Slijedi da je $K_1 \subseteq K_2$ i $K_2 \subseteq K_1$, dakle $K_1 = K_2$.

Ako pretpostavimo da je $K_1 = K_2$ tada je $\sqrt{d_1} \in K_2$ i onda $\sqrt{d_1}$ možemo zapisati kao $\sqrt{d_1} = a + b\sqrt{d_2}$. Kvadriranjem dobivamo

$$d_1 = (a^2 + b^2 d_2) + 2ab\sqrt{d_2}.$$

To znači da je $d_1 = a^2 + b^2 d_2$ i $2ab = 0$. Dakle ili je $a = 0$ ili $b = 0$. Ako je $a = 0$, onda je $\frac{d_1}{d_2} = b^2$, dok ako je $b = 0$ onda je $d_1 = a^2$ što je u kontradikciji da je $\mathbb{Q}(\sqrt{d_1})$ kvadratno polje. □

Propozicija 3.2.10. *Ako je K kvadratno proširenje, onda je $K = \mathbb{Q}(\sqrt{d})$ gdje je d jedinstveno određen kvadratno slobodan broj.*

Dokaz. Po Teoremu 2.0.9 i Lemi 3.2.8 znamo da je $K = \mathbb{Q}(\sqrt{ab})$, za neke $a, b \in \mathbb{Z}$. No kako je $K = \mathbb{Q}(\sqrt{b^2(a/b)}) = \mathbb{Q}(\sqrt{ab})$ imamo da je $K = \mathbb{Q} = \sqrt{r}$, gdje smo stavili $r = ab \in \mathbb{Z}$. Ako r nije kvadratno slobodan onda postoji cijeli broj c takav da $c^2 \mid r$ i tada je $K = \mathbb{Q}(\sqrt{r/c^2})$. Daljnjim dijeljenjem broja r s kvadratom prirodnog broja u konačnom broju koraka dolazimo do kvadratno slobodnog broja d takvog da je $K = \mathbb{Q}(\sqrt{d})$.
Da bi dokazali jedinstvenost pretpostavimo da je $\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$ pri čemu možemo bez smanjenja općenitosti pretpostaviti da su d_1 i d_2 kvadratno slobodni. Prema propoziciji 3.2.9 znamo da je $d_1/d_2 = s^2$, $s \in \mathbb{Q}$, a iz toga lagano možemo zaključiti da d_1 i d_2 moraju biti istog predznaka. Označimo radi kraćega pisanja $s = u/v$, $d_1 v^2 = d_2 u^2$. Ako postoji prost broj p koji dijeli d_1, tada se p pojavljuje se parnim eksponentom u faktorizaciji na proste brojeve broja $d_1 v^2$ i broja $d_2 u^2$. To također znači da $p \mid d_2$. Istom argumentacijom dobivamo da svaki prost broj koji dijeli d_1 također dijeli d_2. Budući da su d_1 i d_2 kvadratno slobodni i istog predznaka zaključujemo da su jednaki. □

Od sada nadalje kada ćemo pisati $\mathbb{Q}(\sqrt{d})$ pretpostavit ćemo da je d kvadratno slobodan broj.
Na skupu $\mathbb{Q}(\sqrt{d})$ ćemo definirati operaciju $* : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$

$$(a + b\sqrt{d})^* = a - b\sqrt{d},$$

koju nazivamo **konjugiranje**. Sada imamo ovu jednostavnu lemu u kojoj iskazujemo svojstva definirane operacije i čiji dokaz ispuštamo.

Lema 3.2.11. *Neka su $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$. Tada vrijedi:*

$$(\alpha^*)^* = \alpha, \quad (\alpha \pm \beta)^* = \alpha^* \pm \beta^*, \quad (\alpha\beta)^* = \alpha^*\beta^*, \quad (\alpha^n)^* = (\alpha^*)^n, \, n \in \mathbb{N}$$

i za $\beta \neq 0$ vrijedi,

$$\left(\frac{\alpha}{\beta}\right)^* = \frac{\alpha^*}{\beta^*}.$$

Korištenjem gornjem leme lagano slijedi tvrdnja sljedeće propozicije.

Propozicija 3.2.12. *Ako za normiran polinom $p \in \mathbb{Z}[x]$ i $\alpha \in \mathbb{Q}(\sqrt{d})$ vrijedi $p(\alpha) = 0$, onda također vrijedi i $p(\alpha^*) = 0$*

Dokaz. Neka je

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Onda je

$$\begin{aligned} p(\alpha^*) &= (\alpha^*)^n + a_{n-1}(\alpha^*)^{n-1} + \cdots + a_1\alpha^* + a_0 \\ &= (\alpha^n)^* + (a_{n-1}\alpha^{n-1})^* + \cdots + (a_1\alpha)^* + a_0^* \\ &= (\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0)^* = (p(\alpha))^* = 0. \end{aligned}$$

□

Primijetimo da prošla propozicija zapravo tvrdi da ako je α algebarski cijeli broj, onda je α^* također algebarski cijeli broj.
Sada ćemo definirati dvije važne skalarne funkcije, koje ćemo u ovomu što slijedi često koristiti.

Definicija 3.2.13. *Za proizvoljno kvadratno proširenje $\mathbb{Q}(\sqrt{d})$ definiramo funkciju **trag** $T : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ s*

$$T(\alpha) = \alpha + \alpha^*,$$

*i funkciju **norma** $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ s*

$$N(\alpha) = \alpha\alpha^*.$$

Bitno je primijetiti da u realnim kvadratnim proširenjima, koja ćemo u ovom radu posebno istražiti, funkcija norma, za razliku od one na koju smo navikli u drugim granama matematike, može poprimiti i pozitivne i negativne vrijednosti. Tako primjerice postoji slučaj $N(1) = 1 \cdot 1 = 1$ i $N(\sqrt{d}) = \sqrt{d} \cdot -\sqrt{d} = -d$.
Sada imamo još jednu jednostavnu lemu u kojoj iskazujemo osnovna svojstva norme i traga i čiji dokaz ispuštamo.

Lema 3.2.14. *Ako su $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$, tada vrijedi*

$$T(\alpha \pm \beta) = T(\alpha) \pm T(\beta) \quad i \quad N(\alpha\beta) = N(\alpha)N(\beta).$$

Nadalje ako je $\beta \neq 0$, onda također vrijedi

$$N\left(\frac{\alpha}{\beta}\right) = \frac{N(\alpha)}{N(\beta)}.$$

Ako je $a + b\sqrt{d}$, za $a, b \in \mathbb{Q}$, algebarski cijeli broj, onda je on rješenje kvadratne jednadžbe oblika $x^2 + Ax + B = 0$, gdje su $A, B \in \mathbb{Z}$. Prema Osnovnom teoremu algebre znamo da navedeni polinom ima dvije nultočke. Jedna nultočka tog polinoma je $a + b\sqrt{d}$, dok je druga nultočka prema propoziciji 3.2.12 jednaka $a - b\sqrt{d}$.
Znači da je

$$x^2 + Ax + B = \left(x - (a + b\sqrt{d})\right)\left(x - (a - b\sqrt{d})\right).$$

Primjenom teorema o jednakosti polinoma na gornju jednakost zaključujemo da mora vrijediti

$$A = -2a \quad \text{i} \quad B = a^2 - db^2.$$

Dakle $-2a$ i $a^2 - db^2$ moraju biti cijeli brojevi. U biti vrijedi $a \in \mathbb{Z}$ ili $a + \frac{1}{2} \in \mathbb{Z}$.
U prvom slučaju

$$a \in \mathbb{Z} \Rightarrow a^2 \in \mathbb{Z}.$$

Budući da je $a^2 - db^2 \in \mathbb{Z}$ zaključujemo da je $db^2 \in \mathbb{Z}$.
Ako bi bilo $b^2 = \frac{m^2}{n^2}$ za m, n prirodne brojeve, tada bi d trebao biti djeljiv s n^2, a to nije moguće jer je d kvadratno slobodan. Zato zaključujemo da vrijediti $b^2 \in \mathbb{Z}$ i zato je onda $b \in \mathbb{Z}$.

U drugom slučaju $a + \frac{1}{2} \in \mathbb{Z}$, odnosno $2a$ je neparan broj, pa zato vrijedi $(2a)^2 \equiv 1 \pmod 4$. Budući da smo pretpostavili da vrijedi $a^2 - db^2 \in \mathbb{Z}$, onda je izraz $\frac{1}{4}\left((2a)^2 - d(2b)^2\right)$ također cijeli broj.
Zato možemo pisati

$$(2a)^2 - d(2b)^2 \equiv 0 \pmod 4.$$

Zaključujemo kako je onda

$$d(2b)^2 \equiv 1 \pmod 4$$

i korištenjem svojstva modularne aritmetike dobivamo:

$$d \equiv 1 \pmod 4 \text{ i } (2b)^2 \equiv 1 \pmod 4,$$

$$d \equiv 1 \pmod 4 \text{ i } (2b) \equiv 1 \pmod 2,$$

$$d \equiv 1 \pmod 4 \text{ i } b \in \frac{1}{2} + \mathbb{Z}.$$

S R_d ćemo označiti skup algebarskih cijelih brojeva u polju $\mathbb{Q}(\sqrt{d})$. Zbog svega gore navedenoga zaključujemo kako vrijedi tvrdnja sljedećeg teorema.

Teorem 3.2.15. *Ako je* $d \not\equiv 1 \pmod 4$*, tada vrijedi sljedeće:*

$$R_d = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

Dok za $d \equiv 1 \pmod 4$ *vrijedi*

$$R_d = \left\{ \frac{a + b\sqrt{d}}{2} \mid a, b \in \mathbb{Z}, a \equiv b \pmod 2 \right\}.$$

Skup R_d zove se prsten cijelih brojeva u polju $\mathbb{Q}(\sqrt{d})$.
Na kraju ovog poglavlja rješavamo jedan zadatak u čijem ćemo rješenju primijeniti do sada iskazanu teoriju.

Primjer 3.2.16. *Dokažite da je broj*

$$S = \sqrt{1001^2 + 1} + \sqrt{1002^2 + 1} + ... + \sqrt{2000^2 + 1}$$

iracionalan.

Uobičajeni način rješavanja ovakog tipa zadataka je da se pokuša dokazati da ne postoji $p, q \in \mathbb{N}$ takvi da je $S = p/q$. Budući da ne znamo kako eksplicitno odrediti S morat ćemo se poslužiti nekim drugim metodama rješavanja.

Dokažimo prvo da S nije prirodan broj. Lako se vidi da za svaki prirodni broj n vrijedi sljedeći niz nejednakosti

$$n^2 < n^2 + 1 < n^2 + 2 < n^2 + 2n\left(\frac{1}{n}\right) + \left(\frac{1}{n}\right)^2 = \left(n + \frac{1}{n}\right)^2,$$

što se ekvivalentno može zapisati kao

$$n < \sqrt{n^2 + 1} < n + \frac{1}{n}. \tag{3.1}$$

Služeći se sa nejednakošću (3.1) broj S možemo ocijeniti s

$$1001 + 1002 + \cdots + 2000 < S < 1001 + 1002 + \cdots + 2000 + \frac{1}{1001} + \frac{1}{1002} + \cdots + \frac{1}{2000}.$$

Također možemo zaključiti da vrijedi

$$0 < \frac{1}{1001} + \frac{1}{1002} + \cdots + \frac{1}{2000} < 1000 \cdot \frac{1}{1001} < 1.$$

Iz čega zaključujemo da $S \notin \mathbb{N}$.

Budući da je $\sqrt{n^2+1}$ algebarski cijeli broj za $n \in \{1001, 1002, \ldots, 2000\}$ jer je nultočka polinoma $f(x) = x^2 - n - 1$, a od ranije znamo da je zbroj dva algebarska cijela broja je opet algebarski cijeli broj i iz toga slijedi da je S također algebarski cijeli broj. Ali ako bi S bio racionalan broj, onda S također mora biti cijeli broj jer je algebarski cijeli broj, što je kontradikcija s gore dokazanim. Dakle zaključujemo kako je S iracionalan broj.

Poglavlje 4

Prsten cijelih brojeva

U ovom poglavlju bavit ćemo se strukturom prstena cijelih brojeva realnog kvadratnog proširenja i to posebice pojmovima kao što su invertibilni elementi, ideali, prosti ideali i faktorizacija. Za početak navedimo nekoliko osnovnih rezultata koji će nam trebati u ovom poglavlju.
Pritom se sjetimo da smo s R_d označavali prsten cijelih brojeva u polju $\mathbb{Q}(\sqrt{d})$.

Lema 4.0.1. *Ako je $\alpha \in R_d$, onda su norma $N(\alpha)$ i trag $T(\alpha)$ cijeli brojevi.*

Dokaz. Prema Propozciji 3.2.12 znamo da ako je $\alpha \in R_d$, da je tada također i $\alpha^* \in R_d$. Sjetimo se da smo $T(\alpha)$ definirali kao $\alpha + \alpha^*$, ali kako je zbroj dva algebarska cijela broja opet algebarski cijeli broj zaključujemo da je $T(\alpha) \in R_d$. Analogan slijed tvrdnji vrijedi i za $N(\alpha)$. Kako su $T(\alpha)$ i $N(\alpha)$ i elementi skupa $\mathbb{Q}$ zaključujemo da prema Propozciji 3.2.6 mora vrijediti da su $T(\alpha), N(\alpha) \in \mathbb{Z}$. □

Iako će nam i trag i norma biti važni, norma će igrati važniju ulogu. Razlog je taj što će nas zanimati multiplikativna pitanja poput faktorizacije, a norma multiplikativne odnose u R_d pretvara u multiplikativne odnose u $\mathbb{Z}$, gdje nam je jednostavnije donositi određene zaključke. Sljedeće dvije tvrdnje nam ilustriraju ovu ideju.

Propozicija 4.0.2. *Neka je γ algebarski cijeli broj u R_d. Tada je γ invertibilni element ako i samo ako je $N(\gamma) = \pm 1$.*

Dokaz. Ako je γ invertibilni element, onda je $N(\gamma)N\left(\frac{1}{\gamma}\right) = N(1) = 1$, pa budući da su $N(\gamma)$ i $N\left(\frac{1}{\gamma}\right)$ cijeli brojevi, slijedi da je $N(\gamma) = \pm 1$.
Obratno, ako je $N(\gamma) = \pm 1$, onda je $\gamma\gamma^* = \pm 1$, pa je $\frac{1}{\gamma} = \pm\gamma^*$ algebarski cijeli broj, što znači da je γ invertibilni element. □

Propozicija 4.0.3. *Ako $\alpha \in R_d$ ima normu koja je jednaka $\pm p$, gdje je p prost broj, tada je α ireducibilan element u R_d.*

Dokaz. Neka je $\alpha = \beta\gamma$, za neke $\beta, \gamma \in R_d$. Primjenom funkcije norma dobivamo jednakost u skupu $\mathbb{Z}$: $N(\alpha) = N(\beta)N(\gamma)$. Budući da je $N(\alpha)$ prost broj, to znači da je $N(\beta)$ ili $N(\gamma)$ jednako ± 1, a prema prethodnoj propoziciji to znači da je ili β ili γ invertibilni element u R_d. Dakle zaključujemo da je α ireducibilan u R_d. □

Ovdje primijetimo kako su negativni prosti brojevi također dozvoljeni, jer primjerice broj $1 + 2\sqrt{3}$ ima normu -11 i ireducibilan je u R_3.
U nastavku ćemo se posebno baviti invertibilnim elementima u prstenu R_d. Skup invertibilnih elemenata u R_d ćemo u nastavku označavati s U_d. Sjetimo se kako smo u uvodnom poglavlju napomenuli da takvi skupovi imaju strukturu multiplikativne grupe.

4.1 Invertibilni elementi

Korištenjem Propozicije 4.0.2 vrlo lako možemo provjeriti da primjerice već ranije spomenuti zlatni rez $\varphi = \frac{1+\sqrt{5}}{2}$ invertibilan element u prstenu R_5. Jer vrijedi $N\left(\frac{1+\sqrt{5}}{2}\right) = \left(\frac{1}{2}\right)^2 - \left(\frac{\sqrt{5}}{2}\right)^2 = -1$.
Dakle nas će zanimati svi elementi $x + y\sqrt{d}$ prstena R_d koji zadovoljavaju jednadžbu $x^2 - dy^2 = \pm 1$. Kako bi otkrili koji su to elementi podsjetimo se poznate jednadžbe iz teorije brojeva koja će nam pomoći riješiti navedeni problem.

Definicija 4.1.1. *Diofantska jednadžba*

$$x^2 - dy^2 = 1, \tag{4.1}$$

gdje je d prirodan broj koji nije kvadrat naziva se ***Pellova jednadžba****.*

Ako je d potpun kvadrat, $d = c^2$, $c \in \mathbb{Z}$ onda iz

$$x^2 - dy^2 = (x - cy)(x + cy) = 1$$

slijedi

$$(x - cy) = (x + cy) = \pm 1$$

U tom slučaju imamo trivijalna rješenja $x = \pm 1$, $y = 0$.

Definicija 4.1.2. *Diofantska jednadžba*

$$x^2 - dy^2 = N,$$

gdje je d prirodan broj koji nije potpun kvadrat i N cijeli broj različit od 0, naziva se ***pelovska jednadžba****.*

Jednadžba je dobila ime prema engleskom matematičaru *Johnu Pellu*, kojem je Euler, po svemu sudeći pogrešno, pripisao zasluge za njezino rješavanje. Neke pojedinačne jednadžbe ovog tipa nalaze se u tekstovima starogrčkih matematičara poput Arhimeda i Diofanta, no prvi su ih sustavno proučavali srednjovjekovni indijski matematičari. Od europskih matematičara, metode za rješavanje Pellovih jednadžbi dali su Brouncker, Fermat, Euler i Lagrange, koji je prvi dao i striktan dokaz korektnosti predložene metode. Pellova jednadžba uvijek ima netrivijalno rješenje, a dokaz te tvrdnje ispuštamo. Više detalja i dokaz tvrdnje koje ovdje navodimo može se naći u [3].

Teorem 4.1.3. *Neka je d prirodan broj koji nije potpun kvadrat. Tada Pellova jednadžba uvijek ima netrivijalno rješenje.*

Ovaj rezultat je jako bitan jer naprimjer najmanji prirodan x za koji postoji netrivijalno rješenje jednadžbe $x^2 - 1621y^2 = 1$ ima čak 76 znamenki, tako da bismo bez ovog rezultata vrlo lako mogli pomisliti da rješenje ne postoji.
Neka je (t, u) rješenje Pellove jednadžbe takvo da je $t > 0, u > 0$ i $t+u\sqrt{d}$ najmanje moguće s obzirom na standardni uređaj. To rješenje zovemo **fundamentalno rješenje** Pellove jednadžbe.
Vidimo da je problem pronalažnja invertibilnih elemenata usko povezan s rješavanjem Pellovih i pellovskih jednadžbi. Preciznije:

- ako je $d \equiv 2$ ili $3 \pmod 4$, tada je $u + v\sqrt{d}$ invertibilan element u prstenu R_d ako i samo ako vrijedi $u^2 - dv^2 = \pm 1$,
- ako je $d \equiv 1 \pmod 4$, tada je $\frac{u+v\sqrt{d}}{2}$ invertibilan element u prstenu R_d ako i samo ako vrijedi $u^2 - dv^2 = \pm 4$.

Stoga uz običnu Pellovu jednadžbu $x^2 - dy^2 = 1$ promatrat ćemo i pellovske jednadžbe $x^2 - dy^2 = -1$, $x^2 - dy^2 = \pm 4$.
Primijetimo da za razliku od Pellovih pelovske jednadžbe ne moraju nužno imati rješenje.

Primjer 4.1.4. *Pelovska jednadžba $x^2 - 7y^2 = -1$ nema rješenja.*

Ako bi svakoj strani jednadžbe dodali $8y^2+4$ dobili bi $x^2+y^2+4 = 8y^2+3$. Promatranjem dobivene jednadžbe modulo 4 dobivamo

$$x^2 + y^2 \equiv 3 \pmod 4.$$

Kako kvadrati cijelih brojeva prilikom dijeljenja s 4 daju ostatke 0 ili 1, zbroj ta dva ostatka nikako ne može biti jednak 3 i zato zaključujemo kako dana jednadžba nema rješenja.

Ipak za Pellovu jednadžbu oblika $x^2 - dy^2 = 4$ vrijedi sljedeći rezultat.

Propozicija 4.1.5. *Jednadžba*

$$x^2 - dy^2 = 4 \tag{4.2}$$

u prirodnim brojevima uvijek ima netrivijalno rješenje.

Dokaz. Ako je $(x, y) = (u, v)$ rješenje $x^2 - dy^2 = 1$, a prema Teoremu 4.1.3 znamo da ono postoji, onda je $(x, y) = (2u, 2v)$ rješenje $x^2 - dy^2 = 4$ i zaključujemo da je skup rješenja početne jednadžbe neprazan. □

Naprimjer neka rješenja jednadžbe $x^2 - 5y^2 = 1$ su $(x, y) = (9, 4), (161, 72)$ i onda zaključujemo kako su rješenja jednadžbe $x^2 - 5y^2 = 4$ su $(x, y) = (18, 8), (322, 144)$.
Napomenimo samo da se nažalost sva rješenja jednadžbe $x^2 - dy^2 = 4$ ne mogu pronaći na navedeni način jer na primjer ista jednadžba $x^2 - 5y^2 = 4$ ima i rješenja $(x, y) = (3, 1), (7, 3), (47, 21), (123, 55), (843, 377) \ldots$

Dakle zaključujemo da u svakom R_d za $d > 0$ postoji barem jedan invertibilan element. U nastavku ćemo istražiti koliko ih točno ima i kako ih sve možemo pronaći. U slučaju ako ih je prebrojivo mnogo, zanima nas možemo li ih nekako okarakterizirati.
Za početak pogledajmo konkretan primjer što je s invertibilnim elementima u prstenu R_2 i pokažimo da ne postoje invertibilni elementi između brojeva 1 i $1 + \sqrt{2}$.
Kako bi to dokazali pretpostavimo da je $\epsilon = x + y\sqrt{2}$ invertibilan element i vrijedi $x^2 - 2y^2 = \pm 1$, te je još

$$1 < x + y\sqrt{2} < 1 + \sqrt{2}. \tag{4.3}$$

Znamo također da vrijedi $x - y\sqrt{2} = \pm\frac{1}{x+y\sqrt{2}}$ i možemo zaključiti da vrijedi

$$-1 < x - y\sqrt{2} < 1. \tag{4.4}$$

Zbrajanjem nejednakosti (4.3) i (4.4) dobivamo da vrijedi $0 < x < 1.8$. Budući da je $x \in \mathbb{Z}$, jedino je moguće $x = 1$. Ali zato onda početna nejednakost glasi $1 < 1 + y\sqrt{2} < 1 + \sqrt{2}$ što nije moguće za niti jedan $y \in \mathbb{Z}$.
U nastavku ćemo pokazati da se svaki pozitivni invertibilan element u R_2 može zapisati u obliku $(1 + \sqrt{2})^k$, za neki $k \in \mathbb{N}$. Neka je $\lambda = 1 + \sqrt{2}$, a ϵ proizvoljni pozitivni invertibilni element.
Ako vrijedi $\lambda^n < \epsilon < \lambda^{n+1}$ tada je $1 < \epsilon\lambda^{-n} < 1 + \sqrt{2}$. Ali vrijedi $N(\epsilon\lambda^{-n}) = \frac{N(\epsilon)}{N(\lambda)^n} = 1$ budući da su ϵ i λ invertibilni elementi. Tada bi bilo da je $\epsilon\lambda^{-n}$ je invertibilni element između 1 i $1 + \sqrt{2}$ što je kontradikcija s ranije dokazanim. Dakle jedina mogućnost je $\epsilon = \lambda^n$ i zaključujemo da imamo prebrojivo mnogo pozitivnih invertibilnih elemenata u R_2 koje su generirane s jednim elementom.
Sljedeća propozicija pokazuje da su rezultati u R_2 zapravo posebni slučaj generalnog rezultata.

Propozicija 4.1.6. *Ako je $d > 0$, onda postoji jedinstveni $\gamma \in U_d$ takav da $\gamma > 1$ i svaki $\zeta \in U_d$ ima oblik $\pm\gamma^n$ za neki $n \in \mathbb{Z}$.*

Dokaz. Neka je η bilo koji invertibilan element u prstenu R_d koji je veći od 1.
Definiramo skup

$$U = \{\epsilon \in U_d \mid 1 < \epsilon \leq \eta\}.$$

Dokažimo prvo da je U konačan neprazan skup i onda će nam njegov najmanji element s obzirom na standardni uređaj biti traženi γ. Ako je $\epsilon \in U$, tada vrijedi $\epsilon\epsilon^* = \pm 1$ i $|\epsilon^*| = \frac{1}{|\epsilon|} < 1$. Također znamo da vrijedi $T(\epsilon) = \epsilon + \epsilon^* = \epsilon + |\epsilon^*|$ i iz toga možemo ocijeniti trag kao $0 < T(\epsilon) < \eta + 1$. Budući da je ϵ algebarski cijeli broj znamo da je $\epsilon^2 - T(\epsilon)\epsilon + N(\epsilon) = 0$ i $N(\epsilon) = \pm 1$. Korištenjem formule za rješenje kvadratne jednadžbe dobivamo da je traženi ϵ jednak

$$\epsilon = \frac{T(\epsilon) \pm \sqrt{T(\epsilon)^2 - 4N(\epsilon)}}{2} = \frac{t \pm \sqrt{t^2 \mp 4}}{2}, \text{ gdje je } t \text{ cijeli broj između 0 i } \eta + 1.$$

Kako t može poprimiti samo konačno mnogo vrijednosti onda također i ϵ može poprimiti samo konačno mnogo vrijednosti i onda zaključujemo da je U konačan skup. Tada iz teorije skupova znamo da u skupu U postoji najmanji element. Neka je γ najmanji element skupa U.
Sada pretpostavimo da je ξ proizvoljan element iz U_d. Za početak pretpostavimo da je $\xi > 0$. Znamo da postoji cijeli broj n takav da vrijedi:

$$n \leq \frac{\ln \xi}{\ln \gamma} < n + 1 \iff 0 \leq \frac{\ln \xi}{\ln \gamma} - n = \frac{\ln(\xi\gamma^{-n})}{\ln \gamma} < 1$$

što povlači da vrijedi $1 \leq \xi\gamma^{-n} < \gamma$. Budući da je $\xi\gamma^{-n}$ invertibilan element on prema prvom djelu ne može biti manji od γ, a veći od 1. Dakle onda mora vrijedi $\xi\gamma^{-n} = 1$ i zaključujemo da vrijedi $\xi = \gamma^n$. Ako je $\xi < 0$, onda je $-\xi$ pozitivani invertibilni element i vrijedi $-\xi = \gamma^n$ za neki n cijelu broj i zaključujemo kako je tada $\xi = -\gamma^n$. □

Grupa invertibilnih elemenata u realnom kvadratnom proširenju ima dva generatora: -1 i γ_d, gdje je $\gamma_d = a + b\sqrt{d}$ ili $\frac{a+b\sqrt{d}}{2}$, dok je $a + b\sqrt{d}$ fundamentalno rješenje jedne od Pellovih jednadžbi $x^2 - dy^2 = \pm 1, \pm 4$. Dakle, svaki se invertibilni element može zapisati u obliku $\pm\gamma_d$, $n \in \mathbb{Z}$. Generator γ_d zove se **fundamentalna jedinica** prstena R_d.

Pitanje je sada, kako naći fundamentalno rješenje. Nekada to možemo vrlo lako isprobavanjem vrijednosti za y, no već za malo veći d to može biti problematično. Osnovna metoda za nalaženje je metoda verižnih razlomaka gdje, ukratko rečeno, broj $\sqrt{d}$ razvijamo u verižni razlomak do trenutka dolaska u period i tada se točno zna kako izgleda fundamentalno rješenje. Više detalja može se pronaći u [6].

4.2 Faktorizacija

U nastavku ćemo generalizirati faktorizaciju na proste faktore u prstenu R_d, analogno kako to vrijedi u $\mathbb{Z}$ prema Osnovnom teoremu aritmetike. Jer znamo da se svaki cijeli broj može prikazati kao produkt jednog ili više prostih brojeva do redoslijeda faktora i prisutnosti jedinica ± 1 i to na jedinstven način. Takav pojam jedinstvene faktorizacije ne prenosi se dalje na svaki R_d, ali u nekim slučajevima to i dalje vrijedi. Kao ćemo vidjeti taj problem je uzrokovao velike probleme u povijesti. Za početak promotrimo malo povijesnih činjenica. Navedimo prvo bitan teorem koji je doprinio razvoju matematičkih struktura koje proučavamo u ovom radu.

Teorem 4.2.1. (Veliki Fermatov teorem) *Ne postoje prirodni brojevi a, b, c, n, takvi da je $n > 2$ i da vrijedi*

$$a^n + b^n = c^n.$$

Iako Veliki Fermatov teorem nema direktnu primjenu u teoriji brojeva, pokušaj dokazivanja teorema doveo je do snažnog razvoja teorije brojeva. Tako je u 19. stoljeću Kummer smatrao da ima dokaz Velikog Fermatovog teorema, ali njegov je dokaz ovisio o jedinstvenosti faktorizacije za koju se pokazalo da nije ispravna. Pokušavajući ispraviti tu grešku Kummer je razvio ideju o idealnim brojevima, koja je kasnije dovela Dedekinda do definicije ideala, a što je pak dovelo do temeljnih algebarskih struktura kao što su prsteni, polja, domene jedinstvene faktorizacije i Dedekindove domene. U lipnju 1995. engleski matematičar Wiles konačno dokazuje teorem, a način na koji je to učinjeno predstavljalo je znatno višu matematiku od one koja je bila javno poznata prije tog vremena.
Navedimo kriterij kada elementi skupa R_d nisu djeljivi.

Lema 4.2.2. *Neka su $\beta, \gamma \in R_d$. Ako vrijedi da $\beta \mid \gamma$, tada $N(\beta) \mid N(\gamma)$*

Dokaz. Ako $\beta \mid \gamma$, onda postoji $\delta = \frac{\gamma}{\beta} \in R_d$ i vrijedi $N(\gamma) = N(\beta)N(\delta)$. Budući da su β, γ, δ algebarski cijeli brojevi znamo da je njihova norma cijeli broj i onda zaključujemo da $N(\beta) \mid N(\gamma)$. □

Bitno je naglasiti da ako bi promatrali prsten algebarskih brojeva nad poljem $\mathbb{C}$, onda ne bi imali proste brojeve. Zato jer se svaki α algebarski broj može zapisati kao $\alpha = \sqrt{\alpha}\sqrt{\alpha}$. Ako je $p(x) \in \mathbb{Z}[x]$ polinom kojem je nultočka broj α tada je $\sqrt{\alpha}$ također algebarski broj jer je $p(x^2)$ polinom koji ga poništava, i $\sqrt{\alpha} \nmid \alpha$. Zato problem faktorizacije promatramo na skupu R_d zajedno s algebarskim cijelim brojevima na kojem takve probleme nemamo.

Propozicija 4.2.3. *Svaki algebarski cijeli broj α u R_d, koji nije invertibilan element, može se prikazati kao produkt ireducibilnih brojeva u R_d.*

Dokaz. Ako α nije ireducibilan, onda se može rastaviti na produkt $\beta\gamma$, gdje β i γ nisu invertibilni elementi. Nastavljajući ovaj postupak, faktoriziramo β i γ ako nisu ireducibilni. Ovaj proces faktorizacije mora završiti jer bismo inače dobili da α ima oblik $\beta_1\beta_2 \cdot \cdots \cdot \beta_n$, gdje je n po volji velik, a nijedan od β_j nije invertibilan element. To bi povlačilo da je

$$|N(\alpha)| = \prod_{j=1}^{n} |N(\beta_j)| \geq 2^n$$

jer je $|N(\beta_j)|$ prirodni broj veći od 1. No to je očito kontradikcija. □

Definicija 4.2.4. *Kažemo da kvadratno proširenje R_d ima svojstvo **jedinstvene faktorizacije** ako se svaki algebarski cijeli broj u R_d koji nije 0 ili invertibilan element, može faktorizirati na ireducibilne faktore jednoznačno, do na poredak faktora i zamjenu faktora asociranim brojevima.*

Iako smo pokazali da faktorizacija na ireducibilne faktore u R_d uvijek postoji, ona ne mora nužno biti jedinstvena.

Primjer 4.2.5. *Promotrimo broj 6 i njegove dvije faktorizacije u R_{10}:*

$$6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10}).$$

Pokažimo da su brojevi $2, 3, 4 \pm \sqrt{10}$ ireducibilni. Izračunajmo prvo $N(2) = 4$, $N(3) = 9$, $N(4 \pm \sqrt{10}) = 6$. Ono što odmah možemo primijetiti da brojevi 2 i $4 \pm \sqrt{10}$ nisu asocirani budući da imaju norme 4 i 6. Da bi dokazali da su ireducibilni dovoljno je pokazati da

$$a^2 - 10b^2 = \pm 2 \text{ ili } \pm 3$$

nema rješenja za $a, b \in \mathbb{Z}$. Kako bi to pokazali promotrit ćemo gornju jednadžbu modulo 10 iz koje zaključujemo da vrijedi

$$a^2 \equiv \pm 2 \text{ ili} \pm 3 \pmod{10},$$

što je ekvivalentno s

$$a^2 \equiv 2, 3, 7 \text{ ili } 8 \pmod{10}.$$

Kvadrati modulo 10 su redom $0, 1, 4, 9, 6, 5$. Na tom popisu se ne nalaze brojevi 2,3,7 i 8. Dakle zaključujemo kako su $2, 3, 4 \pm \sqrt{10}$ ireducibilni. Zaključujemo da faktorizacija na ireducibilne faktore nije jedinstvena u R_{10}. Na sličan način može se pokazati da faktorizacija nije jedinstvena u prstenima R_{15}, R_{26} i R_{30}. Jer naime vrijedi:

$$10 = 2 \cdot 5 = (5 + \sqrt{15})(5 - \sqrt{15}),$$

$$10 = 2 \cdot 5 = (6 + \sqrt{26})(6 - \sqrt{26}),$$
$$6 = 2 \cdot 3 = (6 + \sqrt{30})(6 - \sqrt{30}),$$

pri čemu se može pokazati da su svi popisani faktori ireducibilni elementi u odgovarajućem prstenu R_d. Sjetimo se da smo ranije pokazali da prsten R_2 ima prebrojivo mnogo invertibilnih elemenata, ali to predstavlja veliki problem kada promatramo razne faktorizacije koje nisu različite jer uključuju množenje invertibilnih elemenata.

Primjer 4.2.6. *Promotrimo broj 7 i njegove tri faktorizacije u R_2.*

$$7 = (3 - \sqrt{2})(3 + \sqrt{2}) = (-1)(1 - 2\sqrt{2})(1 + 2\sqrt{2}) = (5 - 3\sqrt{2})(5 + 3\sqrt{2})$$

Ipak ove tri faktorizacije su u R_2 jednake što možemo vidjeti kada brojeve podijelimo s invertibilnim elementom $1 + \sqrt{2}$. Naime, imamo

$$\frac{7}{1+\sqrt{2}} = \frac{(3-\sqrt{2})(3+\sqrt{2})}{1+\sqrt{2}} = \frac{(-1)(1-2\sqrt{2})(1+2\sqrt{2})}{1+\sqrt{2}} = \frac{(5-3\sqrt{2})(5+3\sqrt{2})}{1+\sqrt{2}} = -7+7\sqrt{2}.$$

Kasnije ćemo dokazati da prsten R_2 ima svojstvo jedinstvene faktorizacije.

Ako se vratimo na standardnu teoriju brojeva i proučimo dokaz jedinstvene faktorizacije u skupu $\mathbb{Z}$, ustanovit ćemo da dokaz u konačnici ovisi o Euklidovom algoritmu. Zato ako bismo mogli pronaći generaliziranu verziju tog algoritma unutar prstena R_d onda bismo možda mogli pokazati da R_d ima jedinstvenu faktorizaciju. To je doista tako.

Definicija 4.2.7. *Za prsten R_d kažemo da je **euklidski** ako je za algebarske cijele brojeve moguće provesti analogon Euklidovog algoritma, odnosno ako za $\alpha, \beta \in R_d$ i $\beta \neq 0$, postoji $\lambda \in R_d$ takav da vrijedi $|N(\alpha - \beta\lambda)| < |N(\beta)|$.*

U nastavku navodimo korisnu karakterizaciju koja će nam trebati u nastavku.

Lema 4.2.8. *R_d je euklidski ako i samo ako za svaki $\xi \in \mathbb{Q}(\sqrt{d})$ postoji $\gamma \in R_d$ tako da vrijedi $|N(\xi - \gamma)| < 1$.*

Dokaz. Neka je R_d euklidski, to znači da za $\alpha, \beta \in R_d$ i $\beta \neq 0$, postoji $\lambda \in R_d$ takav da vrijedi $|N(\alpha - \beta\lambda)| < |N(\beta)|$. Gornju nejednakost možemo zapisati kao:

$$\frac{|N(\alpha - \beta\lambda)|}{|N(\beta)|} = \left| N\left(\frac{\alpha}{\beta} - \lambda\right)\right| < 1.$$

Omjer α i β označimo kao $\xi \in \mathbb{Q}(\sqrt{d})$ jer smo ranije pokazali da omjer dva elementa iz R_d ne mora nužno biti u R_d, ali zato mora u $\mathbb{Q}(\sqrt{d})$. Dakle vrijedi $|N(\xi - \lambda)| < 1$ što je i trebalo dokazati. Obratna tvrdnja dokazuje se analognom argumentacijom. □

Propozicija 4.2.9. *Ako je R_d euklidski, onda je svaki ideal I nužno glavni.*

To je dobro poznat rezultat koji govori da je svaka Euklidska domena prsten glavnih ideala.
Kažemo da je R_d prsten glavnih ideala ako su svi njegovi ideali glavni. Poznato je da postoji točno 21 euklidsko polje R_d i to za sljedeće vrijednosti:

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

Hipoteza je da za $d > 0$ takvih polja ima prebrojivo mnogo.

Primjer 4.2.10. *Dokažimo da je prsten R_d, za $d = 2, 3$ euklidski.*

Dokaz. Neka je $\xi = x + y\sqrt{d},\ x, y \in \mathbb{Q}$. Tada sigurno postoje cijeli brojevi a i b za koje vrijedi $|x - a|, |y - b| \leq \frac{1}{2}$. Označimo $\delta = a + b\sqrt{d}$ i primijetimo da je $\delta \in R_d$.
Primjenom ideje iz leme 4.2.8 izračunajmo prvo normu elementa $\xi - \delta$ i dobivamo da je jednaka:

$$N(\xi - \delta) = N((x - a) + (y - b)\sqrt{d}) = (x - a)^2 - d(y - b)^2.$$

Najveća vrijednost gore dobivenoga izraza je $\frac{1}{4}$ jer vrijedi:

$$(x - a)^2 - d(y - b)^2 \leq \left(\frac{1}{2}\right)^2 - d(y - b)^2 \leq \frac{1}{4}.$$

Dok je minimalna vrijednost izraza jednaka $\frac{-d}{4}$ jer vrijedi:

$$(x - a)^2 - d(y - b)^2 \geq (x - a)^2 - d\left(\frac{1}{2}\right)^2 \geq \frac{-d}{4}.$$

Dakle zaključujemo da vrijedi

$$\frac{-d}{4} \leq N(\xi - \delta) \leq \frac{1}{4} \iff |N(\xi - \delta)| \leq \max\left(\frac{1}{4}, \frac{d}{4}\right) < 1, \text{za } d = 2, 3$$

Primjenom Leme 4.2.8 slijedi tražena tvrdnja.

□

4.3 Ideali

Sjetimo se na početku nekih pojmova i rezultata o idealima. Ako je R bilo koji prsten i ako su $I, J \trianglelefteq R$ ideali, definirajmo **produkt ideala** $IJ = \langle xy \mid x \in I, y \in J \rangle$, tj. IJ je najmanji ideal u R koji sadrži sve produkte elemenata xy, za $x \in I$ i $y \in J$. Lako se vidi da je

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \mid x_i \in I, y_i \in J \cup \{0_R\} \right\},$$

skup svih konačnih suma produkata $x_i y_i$. Nadalje definiramo **sumu ideala** $I + J = \langle I \cup J \rangle$, odnosno $I + J$ je najmanji ideal u R koji sadrži $I \cup J$.
Lako se vidi da je

$$I + J = \{x + y \mid x \in I, y \in J\}.$$

Lema 4.3.1. *Neka je $\alpha \in R_d$ i $J \trianglelefteq R_d$ ideal.*
Tada vrijedi

$$\langle \alpha \rangle J = \alpha J = \{\alpha\beta \mid \beta \in J\}.$$

Posebno ako je $\beta \in R_d$, tada imamo

$$\langle \alpha \rangle \langle \beta \rangle = \langle \alpha\beta \rangle.$$

Dokaz. Jer je $\alpha \in \langle \alpha \rangle$, onda je očito $\alpha J = \{\alpha\beta \mid \beta \in J\} \subseteq \langle \alpha \rangle J$. S druge strane, budući da je R_d komutativan prsten, onda je glavni ideal $\langle \alpha \rangle = \{\gamma\alpha \mid \gamma \in R\}$. Onda po gornjem opisu produkta ideala imamo da je svaki element iz produkta $\langle \alpha \rangle J$ oblika

$$\sum_{i=1}^{n} (\gamma_i \alpha) y_i = \alpha \left(\sum_{i=1}^{n} \gamma_i y_i \right), \quad \text{za neke } \gamma_i \in R_d, y_i \in J.$$

Ali kako je $y = \sum_{i=1}^{n} \gamma_i y_i \in J$, jer je J ideal u R_d, zaključujemo da je $\sum_{i=1}^{n} (\gamma_i \alpha) y_i = \alpha y \in \alpha J$.
Tada smo pokazali da je i $\langle \alpha \rangle J \subseteq \alpha J$.
Posebno ako su $\alpha, \beta \in R_d$, onda za glavni ideal $J = \langle \beta \rangle = \{\gamma\beta \mid \gamma \in R_d\}$ imamo da je

$$\langle \alpha \rangle \langle \beta \rangle = \langle \alpha \rangle J = \alpha J = \{\gamma\alpha\beta \mid \gamma \in R_d\} = \langle \alpha\beta \rangle.$$

□

Napomena 4.3.2. *Primijetimo da gornja lema vrijedi ako R_d zamijenimo s proizvoljnim komutativnim prstenom R.*

Sjetimo se da smo na $\mathbb{Q}(\sqrt{d})$ definirali operaciju konjugiranja $x \mapsto x^*$. Tu operaciju možemo podignuti i do operacije konjugiranja na idealima.

Definicija 4.3.3. *Ako je I ideal u R_d, onda je*

$$I^* = \{\alpha^* \mid \alpha \in I\}$$

*također ideal koji zovemo **konjugat** od I.*

Naime I^* je ideal jer je zatvoren u odnosu na zbrajanje i za svaki $c \in R_d$ i $\alpha \in I$ imamo $c\alpha^* = (c^*\alpha)^*$, gdje je $c^*\alpha \in I$.

Operacija konjugacija se ponaša očekivano u odnosu na dvije standardne operacije nad idealima. Naime za dva ideala I i J vrijedi

$$(I + J)^* = I^* + J^* \text{ i } (IJ)^* = I^* J^*.$$

Svaki ideal je aditivna podgrupa prstena R_d i prikladno je zato prvo klasificirati sve moguće podgrupe od R_d, a tek onda se pitati koje se strukture ideali.
Radi kraćeg pisanja definiramo oznaku $\tau = \sqrt{d}$ ako $d \not\equiv 1 \pmod 4$ i $\tau = \frac{1}{2}(1 + \sqrt{d})$ ako je $d \equiv 1 \pmod 4$. Primijetimo da se tada prsten R_d može zapisati kao

$$R_d = \{a + b\tau \mid a, b \in \mathbb{Z}\}.$$

Budući da radimo s kvadratnim proširenjima realno je očekivati da će se svaka podgrupa moći generirati s 2 elementa. Tu našu pretpostavku potvrđuje sljedeća propozicija.

Propozicija 4.3.4. *Neka je G aditivna podgrupa prstena R_d. Tada postoje cijeli brojevi a, m i n takvi da je $m, n \geq 0$ i*

$$G = \langle a + m\tau, n\rangle = \{u(a + m\tau) + vn \mid u, v \in \mathbb{Z}\};$$

tj., G je podgrupa od $(R_d, +)$ generirana dvočlanim skupom $\{a + m\tau, n\}$.

Dokaz. Proizvoljan element skupa G ima oblik $r + s\tau$, za neke $s, t \in \mathbb{Z}$. Promotrimo za početak skup

$$H = \{s \mid r + s\tau \in G\}.$$

Lagano se provjeri da je H podgrupa od $\mathbb{Z}$, a znamo da svaka takva podgrupa nužno ima oblik $m\mathbb{Z}$ za neki $m \geq 0$. Budući da je $m \in H$ onda postoji a takav da je $a + m\tau \in G$. Također $G \cap \mathbb{Z}$ je podgrupa od $\mathbb{Z}$ i zato možemo pisati $G \cap \mathbb{Z} = n\mathbb{Z}$, za neki $n \geq 0$ i $n \in G$. Tvrdimo da je $G = \langle a + m\tau, n\rangle$. Iz ranije napisanog očito je da vrijedi $\langle a + m\tau, n\rangle \subseteq G$. Neka je $r + s\tau$ proizvoljan element skupa G. Kako je $s \in H$ onda postoji $u \in \mathbb{Z}$ takav da $s = um$. Promotrimo sada $r - ua = r + s\tau - u(a + m\tau)$, a kako je to element iz $G \cap \mathbb{Z}$ tada je $r - ua = vn$, za neki $v \in \mathbb{Z}$. Onda imamo

$$r + s\tau = r - ua + u(a + m\tau) = vn + u(a + m\tau) \in \langle a + m\tau, n\rangle.$$

□

Korolar 4.3.5. *Ako je I netrivijalan ideal prstena R_d, tada postoje cijeli brojevi a, m i n gdje su $m, n > 0$ i vrijedi $I = \langle a + m\tau, n\rangle$.*

Dokaz. Neka je $\alpha \neq 0$ element od I. Bitno je primijetiti da je $N(\alpha) = \alpha\alpha^* \in I$ i zato zaključujemo $N(\alpha)\tau \in I$. Iz toga slijedi da skupovi H i $I \cap \mathbb{Z}$ iz gornjeg dokaza sadrže $N(\alpha)$ i da zato mora vrijediti $m > 0$ i $n > 0$. □

Pojam ideala uveo je njemački matematičar Ernst Eduard Kummer radi rješavanja problema nejedinstvene faktorizacije u poljima algebarskih brojeva. Naš sljedeći cilj je posvetiti se proučavanju ideala dokazujući da se svaki ideal može jedinstveno izraziti kao produkt prostih ideala. Započinjemo s definiranjem pojma norme ideala, ali prije toga navodimo sljedeći rezultat koji će biti temelj teorije koje navodimo u nastavku.

Lema 4.3.6. (Hurwitzova lema) *Neka su $\alpha, \beta \in R_d$ i $g \in \mathbb{N}$. Ako su brojevi $N(\alpha), N(\beta)$ i $T(\alpha\beta^*)$ djeljivi brojem g, onda su $\alpha\beta^*/g$ i $\alpha^*\beta/g$ elementi prstena R_d.*

Dokaz. Neka $\gamma = \alpha\beta^*/g$ i onda je $\gamma^* = \alpha^*\beta/g$. Ideja je pokazati da je $\gamma \in R_d$ jer će onda prema Propoziciji 3.2.12 slijediti da je također $\gamma^* \in R_d$. Da bi dokazali traženu tvrdnju iskoristit ćemo Lemu 4.0.1 s početka poglavlja.

$$T(\gamma) = \gamma + \gamma^* = \frac{\alpha\beta^* + \alpha^*\beta}{g} = \frac{T(\alpha\beta^*)}{g} \in \mathbb{Z}$$

$$N(\gamma) = \gamma\gamma^* = \frac{\alpha\beta^*\alpha^*\beta}{g^2} = \frac{\alpha\alpha^*}{g}\frac{\beta\beta^*}{g} = \frac{N(\alpha)}{g}\frac{N(\beta)}{g} \in \mathbb{Z}.$$

Zaključujemo da je $\gamma \in R_d$ i također $\gamma^* \in R_d$. □

U sljedećem korolaru pokazujemo kako ranije definiran pojam norme ima smisla i za ideale.

Korolar 4.3.7. *Ako je I ideal u R_d, tada je produkt ideala $II^* = \langle N \rangle$ za neki cijeli broj $N \geq 0$.*

Dokaz. Od prije znamo da je svaki ideal u R_d oblika $I = \langle \alpha, \beta \rangle$ za neke α i β, da vrijedi

$$II^* = \langle \alpha, \beta \rangle \langle \alpha^*, \beta^* \rangle = \langle \alpha\alpha^*, \alpha\beta^*, \beta\alpha^*, \beta\beta^* \rangle.$$

Zaključujemo kako racionalni brojevi $\alpha\alpha^* = N(\alpha)$, $\beta\beta^* = N(\beta)$ i $\alpha\beta^* + \alpha^*\beta = T(\alpha\beta)$ jesu elementi od II^*. Neka je N najveći zajednički djelitelj ta tri broja. Jasno je da $N \in II^*$ i onda $\langle N \rangle \subseteq II^*$. Budući da $N \mid N(\alpha)$, $N \mid N(\beta)$ i $N \mid T(\alpha\beta^*)$, onda prema Hurwitzovoj lemi znamo da $N \mid \alpha\beta^*$ i $N \mid \beta\alpha^*$. Dakle vrijedi $II^* \subseteq \langle N \rangle$ i zaključujemo da vrijedi $II^* = \langle N \rangle$. □

Definicija 4.3.8. *Neka je $I \trianglelefteq R_d$ ideal i neka je cijeli broj $N \geq 0$ takav da je $II^* = \langle N \rangle$, kao u prethodnom korolaru. Broj N zove se **norma ideala** I, i označavamo s $N(I)$.*

Norma ideala će dogovorno biti prirodan broj ili 0 jer znamo da vrijedi $\langle a \rangle = \langle -a \rangle$. Norma ideala je također jedinstveno definirana jer ako su $a, b \in \mathbb{Z}^+$ i vrijedi $\langle a \rangle = \langle b \rangle$, onda

$a = bu$ za neki $u \in U_d \cap \mathbb{Q} = \{\pm 1\}$. Dakle $u = 1$ jer su a i b pozitivni brojevi i slijedi $a = b$. Gornji rezultat daje nam sljedeću formulu:

$$N(\langle \alpha, \beta \rangle) = M(N(\alpha), N(\beta), T(\alpha\beta^*)),$$

gdje je $M(a, b, c)$ najveća zajednička mjera brojeva a, b, c.

Ako je $I = \langle \alpha \rangle$ glavni ideal, tada je $II^* = \langle \alpha\alpha^* \rangle$ i vrijedi $N(\langle \alpha \rangle) = |N(\alpha)|$. Općenitije ako je $\alpha \in I$, onda $\alpha^* \in I^*$ i $N(\alpha) = \alpha\alpha^* \in II^* = \langle N(I) \rangle$ i zaključujemo da $N(I) \mid N(\alpha)$. Norma ideala ima također svojstvo multiplikativnosti:

$$\langle N(IJ) \rangle = (IJ)(IJ)^* = IJI^*J^* = (II^*)(JJ^*) = \langle N(I) \rangle \langle N(J) \rangle = \langle N(I)N(J) \rangle,$$

i vrijedi $N(IJ) = N(I)N(J)$. Ako je $N(I) = 0$, onda je $N(\alpha) = \alpha\alpha^* = 0$ za svaki $\alpha \in I$ i zaključujemo kako je $I = \{0\}$. Također ako je $N(I) = 1$, tada je $II^* = \langle 1 \rangle = R_d$ i $I \supseteq II^* = R_d$ što pokazuje da je $I = R_d$. Dakle zaključujemo kako svi netrivijalni ideali imaju normu veću od 1. Navedimo još jedno svojstvo norme koje ćemo koristiti u nastavku.

Korolar 4.3.9. *Neka je I netrivijalan ideal u R_d. Svaki ideal koji je faktor od I ima normu koja je manja od $N(I)$.*

Dokaz. Neka je J faktor od I, odnosno $I = JK$ za $K \neq \langle 1 \rangle$. Budući da vrijedi $N(I) = N(J)N(K)$, gdje znamo da je $N(I) \neq 0$ i $N(K) > 1$, zaključujemo da je $N(J) < N(I)$. □

Ova opservacija će nam biti vrlo korisna u nastavku jer govori kako izračunati normu ideala.

Propozicija 4.3.10. *Neka je $I = \langle n, a + m\tau \rangle$ nenul ideal u R_d gdje su $m, n \in \mathbb{N}$ i $a \in \mathbb{Z}$. Tada je $N(I) = mn$.*

Dokaz. Neka je $\alpha = a + m\tau$,i zato $I = (n, \alpha)$ i $I^* = (n, \alpha^*)$. Također neka je N takav da vrijedi $N(I) = N$, odnosno $II^* = \langle N \rangle$. Tada zbog $n\alpha = an + mn\tau \in I^*I = \langle N \rangle$ slijedi da $N \mid an$ i $N \mid mn$. Da bi pokazali da je $N = nm$ dovoljno će nam biti pokazati da $mn \mid N$.
Tvrdimo da svaki element II^* ima oblik $A + Bmn\tau$, za neke $A, B \in \mathbb{Z}$. Kako je svaki element skupa II^* zapravo zbroj elementa oblika $\beta\gamma$ gdje je $\beta \in I, \gamma \in I^*$, dovoljno je pokazati da svaki element ima taj oblik. Ako uzmemo $\beta = rn + s\alpha$ i $\gamma = un + v\alpha^*$, onda je

$$\beta\gamma = run^2 + rvn\alpha^* + sun\alpha + sv\alpha\alpha^*.$$

□

Podsjetimo se iz teorije grupa definicije indeksa $(G : H)$ podgrupe H u grupi G kao broja lijevih (ili desnih) klasa H u G. Nije teško pokazati da je indeks od $I = \langle a + m\tau, n \rangle$ u

R_d jednak mn, jer su klase $(r + s\tau) + I$, gdje su $0 \leq r < n$ i $0 \leq s < m$. Normu ideala onda možemo računati i kao

$$N(I) = [R_d : I].$$

Sada se okrećemo dokazu jedinstvene faktorizacije ideala. Ideja za dokaz je ista kao u dokazu Osnovnog teorema aritmetike. Iz jednakosti dva produkta zaključimo da moraju postojati dva jednaka faktora i zatim poništiti taj faktor. Sada poništavanje faktora isto je kao i množenje s njegovim inverzom, ali problem je što nemamo inverz za ideale. Jer općenito za takvu tvrdnju ne moramo imati inverz s obzirom na množenje. Naime ako je G integralna domena, za nenul elemente $a, b, c \in G$ tada znamo da: $ac = bc \Rightarrow a = b$.

Propozicija 4.3.11. *Neka su I, J i K ideali u R_d. Tada za nenul ideal I i $IJ = IK$ vrijedi da je $J = K$.*

Dokaz. Pretpostavimo prvo da je $I = \langle\alpha\rangle$. Tada $IJ = \alpha J$ i onda je $J = \alpha^{-1}(IJ) = \{\alpha^{-1}\beta \mid \beta \in IJ\}$. Sličnom argumentacijom slijedi $K = \alpha^{-1}(IK) = \alpha^{-1}(IJ) = J$.
Pretpostavimo sada da je I bilo koji nenul ideal. Iz pretpostavke $IJ = IK$ slijedi

$$(II^*)J = (IJ)I^* = (IK)I^* = (II^*)K.$$

Ali kako je II^* glavni ideal, primjenom argumentacije iz prvog dijela dokaza slijedi da je $J = K$. □

Teorem 4.3.12. *Ako su I i J netrivijalni ideali u R_d, tada $I \mid J$ ako i samo ako $I \supseteq J$.*

Dokaz. Implikacija da $I \mid J$ povlači $I \supseteq J$ je jasna iz definicije djeljivosti na skupu ideala. Dokažimo onda suprotnu implikaciju. Ako vrijedi $I \supseteq J$, tada znamo da također $JI^* \subseteq II^* = \langle N(I)\rangle$. Tada je

$$K = \frac{1}{N(I)} JI^* = \{N(I)^{-1}\alpha : \alpha \in JI^*\} \subseteq R_d$$

i lagano se provjeri da je K ideal. Zato imamo

$$IK = \frac{1}{N(I)} I(JI^*) = \frac{1}{N(I)} J(II^*) = \frac{1}{N(I)} J\langle N(I)\rangle = J$$

i zaključujemo da $I \mid J$ što je i trebalo pokazati. □

Očita generalizacija gornjeg rezultata bila bi da ako je I ireducibilan i vrijedi $I \mid J_1 J_2 \dots J_k$, tada $I \mid J_j$ za neki j. Od sada ćemo naziv prost ideal koristiti kao sinonim za ireducibilan ideal. Prije nego dokažemo sljedeći važan teorem, navodimo jednu lemu.

Lema 4.3.13. *Neka je R proizvoljan prsten i neka su P, Q_1 i Q_2 prosti ideali u R. Ako je $P = Q_1 Q_2$, onda je $P = Q_1$ ili $P = Q_2$.*

Dokaz. ¸ Znamo da je ideal $P \trianglelefteq R$ prost ako je $P \neq R$ i ako iz inkluzije $IJ \subseteq P$, gdje su $I, J \trianglelefteq R$ ideali, slijedi da je $I \subseteq P$ ili $J \subseteq P$. Posebno iz $Q_1Q_2 = P$ imamo $Q_1 \subseteq P$ ili $Q_2 \subseteq P$.
S druge strane za bilo koje ideale $I, J \trianglelefteq R$ imamo da je $IJ \subseteq I \cap J$. Posebno je $P = Q_1Q_2 \subseteq Q_1 \cap Q_2$, i onda po definiciji presjeka imamo $P \subseteq Q_1$ i $P \subseteq Q_2$.
Kao zaključak imamo da je $P = Q_1$ ili $P = Q_2$, kako smo i trebali dokazati. □

Navedenu lemu naravno principom matematičke indukcije možemo poopćiti na $n \in \mathbb{N}$ ideala i tako dobiti generalniju tvrdnju.

Teorem 4.3.14. (Jedinstvena faktorizacija) *Svaki ideal može se prikazati kao produkt prostih ideala. Ta faktorizacija je jedinstvena do na poredak faktora.*

Dokaz. Neka su

$$I = P_1P_2 \dots P_r = Q_1Q_2 \dots Q_s$$

dvije faktorizacije ideala I u proste ideale. Dokaz provodimo metodom matematičke indukcije po broju prostih ideala. Ako je $r = 1$, onda je I prost i korištenjem gornje leme imamo da je $s = 1$ i $Q_1 = I = P_1$. Pretpostavimo da je $r > 1$. Ako $P_1 \mid Q_1Q_2 \dots Q_s$, tada $P_1 \mid Q_j$ za neki j. Element Q_j označimo kao Q_1 i tada vrijedi $P_1 \mid Q_1$. Budući da je Q_1 prost znamo da je $P_1 = Q_1$ i zato prema Propoziciji 4.3.11 vrijedi

$$P_2P_3 \dots P_r = Q_2Q_3 \dots Q_s.$$

Primjenom induktivne hipoteze slijedi tvrdnja teorema. □

Korolar 4.3.15. *Ako je ideal I čija je norma prost broj u skupu $\mathbb{Z}$, onda je I prost ideal.*

Dokaz. Neka je $N(I) = p$ prost broj. Ako je $I = JK$ primjenom norme dobivamo $p = N(J)N(K)$. Budući da je p prost broj tada ili J ili K ima normu 1, odnosno ili J ili K su jednaki cijelom prstenu. □

Obrat gornje tvrdnje općenito ne vrijedi, ali zato navodimo uz koju dodatnu pretpostavku to ipak vrijedi.

Korolar 4.3.16. *Svaki netrivijalan prost ideal u R_d ima normu p ili p^2, za $p \in \mathbb{N}$ prost broj.*

Dokaz. Neka je I netrivijalan prost ideal u R_d. Dakle postoji prost broj p takav da $I \mid \langle p \rangle$. Djelovanjem norme na zadnju jednakost dobivamo $N(I) \mid N(\langle p \rangle)$. Budući da je $N(\langle p \rangle) = |N(p)| = p^2$, broj $N(I)$ može poprimiti samo vrijednosti p ili p^2. □

Propozicija 4.3.17. *Neka je p prost broj i $P = \langle a + m\tau, n \rangle$ gdje su $a, m > 0$ i $n > 0$ cijeli brojevi. Tada je ideal P norme p ako i samo ako je $m = 1$, $n = p$ i $p \mid N(a + \tau)$.*

Dokaz. Pretpostavimo da je P ideal norme p. Prema Propoziciji 4.3.10 znamo da je $mn = p$. To je moguće samo u dva slučaja $m = p, n = 1$ ili $n = p, m = 1$. Ako je $m = p, n = 1$ znamo da $P = R_d$, a R_d nema normu p. Dakle vrijedi $m = 1, n = p$. Neka je $\alpha = a + \tau \in P$. Norma $N(\alpha) = \alpha\alpha^* \in PP^* = \langle p \rangle$ i vrijedi $p \mid N(\alpha)$.

Za obratnu implikaciju pretpostavimo da je $P = \langle a + \tau, p \rangle$ gdje vrijedi $p \mid N(a + \tau)$. Ako je P ideal on će sigurno imati normu p i zato je dovoljno pokazati da P ima strukturu ideala. Kako je P aditivna podgrupa od R_d sve što treba pokazati je $\beta\gamma \in P$ za $\beta \in P$ i $\gamma \in R_d$. Ali imamo $\beta = rp + s(a + \tau)$ i $\gamma = u + v\tau$ gdje su r, s, u i v cijeli brojevi. Tada vrijedi

$$\beta\gamma = rup + rvp\tau + su(a + \tau) + sv\tau(a + \tau).$$

Budući da je $p \in P$ i $a + \tau \in P$, dovoljno je pokazati da $p\tau \in P$ i $\tau(a + \tau) \in P$. No vrijedi

$$p\tau = p(a + \tau) - ap \in P$$

i

$$\tau(a + \tau) = (T(\tau) - \tau^*)(a + \tau) = (a + T(\tau) - a - \tau^*)(a + \tau) = (a + T(\tau))(a + \tau) - N(a + \tau) \in P$$

budući da $p \mid N(a + \tau)$.

□

Sada možemo odrediti sve proste ideale norme p. Lagano se može pokazati da vrijedi $\langle a + \tau, p \rangle = \langle b + \tau, p \rangle$ ako i samo ako $a \equiv b \pmod{p}$. Dakle broj ideala s normom p je broj različitih rješenja modulo p kongruencije

$$N(a + \tau) \equiv 0 \pmod{p}. \tag{4.5}$$

Rastavimo to na slučajeve u ovisnosti o vrijednosti parametra τ.
Ako je $d \equiv 2$ ili $3 \pmod 4$, tada je $\tau = \sqrt{d}$ i $N(a + \tau) = a^2 - d$. Onda (4.5) u tom slučaju postaje

$$a^2 \equiv d \pmod{p}.$$

Ako je $d \equiv 1 \pmod 4$, tada je $\tau = \frac{1}{2}(1 + \sqrt{d})$ i $N(a + \tau) = a^2 + a - \frac{1}{4}(d - 1)$. Da bi točno mogli odrediti koliko rješenja ima (4.5) podsjetimo se nekoliko definicija iz teorije brojeva.

Definicija 4.3.18. *Neka su a i m relativno prosti brojevi. Ako kongruencija $x^2 \equiv a \pmod m$ ima rješenja, onda kažemo da je a **kvadratni ostatak** modulo m. U protivnom kažemo da je a **kvadratni neostatak** modulo m.*

Uočimo da su kvadratni ostaci i neostaci definirani samo kada je ispunjen uvjet da su a i m relativno prosti. Tako, primjerice kongruencija $x^2 \equiv 0 \pmod m$ uvijek ima rješenja, ali 0 nije ni kvadratni ostatak ni kvadratni neostatak modulo m.

Definicija 4.3.19. *Neka je p neparni prost broj.* ***Legendreov simbol*** $\left(\frac{a}{p}\right)$ *je jednak 1 ako je kvadratni ostatak modulo p, jednak je -1 ako je kvadratni neostatak modulo p, a jednak je 0 ako* $p \mid a$.

Simbol je dobio ime po francuskom matematičaru Adrien-Marie Legendreu. Dakle, broj rješenja kongruencije $x^2 \equiv a \pmod{m}$ je jednak $1 + \left(\frac{a}{p}\right)$. Zaključujemo da

$$a^2 \equiv d \pmod{p}$$

ima 0,1 ili 2 rješenja ovisno od vrijednosti $\left(\frac{d}{p}\right) = \pm 1, 0$. U drugom slučaju imali smo kongruencijsku jednadžbu

$$a^2 + a - \frac{d-1}{4} \equiv 0 \pmod{p},$$

koja se može zapisati i na ovaj način:

$$4a^2 + 4a + 1 \equiv d \pmod{p}.$$

Gornji izraz možemo zapisati kao $b^2 \equiv d \pmod{p}$, gdje je $b = 2a + 1$ i zaključujemo kako dana jednadžba ima $1 + \left(\frac{d}{p}\right)$ rješenja.

4.3.1 Klase ideala

Ako je svaki ideal u R_d glavni, onda znamo da R_d ima svojstvo jedinstvene faktorizacije, ali u velikom broju slučajeva R_d nema samo glavne ideale.

Kažemo da su dva nenul ideala I i J u R_d **ekvivalenti** ako $I = \lambda J$ za neki $\lambda \in \mathbb{Q}(\sqrt{d})^*$ i pišemo $I \sim J$.

Očito su svaka dva nenul glavna ideala ekvivalentna.

Lema 4.3.20. *Relacija* $\sim$ *je relacija ekvivalencije na skupu ideala prstena* R_d.

Dokaz. Da bi pokazali da je relacija $\sim$ relacija ekivalencije trebamo pokazati svojstva refleksivnosti, simetričnosti i tranzitivnosti. Refeleksivnost lagano provjerimo jer za $\lambda = 1$ vrijedi $I = 1I$, što pišemo kao $I \sim I$.
Simetričnost isto lagano provjerimo jer ako vrijedi $I \sim J$, onda postoji λ takav da $I = \lambda J$. Budući da je $\mathbb{Q}(\sqrt{d})^*$ ima strukturu multiplikativne grupe znamo da postoji λ^{-1} i pišemo

$$\lambda^{-1} I = J$$

što je ekvivalentno zapisu $J \sim I$.
Napokon, relacije je i tranzitivna jer ako vrijedi $I \sim J$ i $J \sim K$, onda znamo da postoji $\lambda_1, \lambda_2 \in \mathbb{Q}(\sqrt{d})^*$ takvi da vrijedi $I = \lambda_1 J$, $J = \lambda_2 K$. Znamo da vrijedi $I \sim K$ jer $I = \lambda_1 J = \lambda_1 \lambda_2 K$.
Dakle zaključujemo kako je dana relacija relacije ekvivalencije. □

Skup

$$[I] = \{J \mid I \sim J\}$$

zovemo **klasa ekvivalencije** ideala I. Ideal I naziva se reprezentantom ili predstavnikom ove klase ekvivalencije. Uočimo da se ista klasa $[I]$ može predočiti i drugim predstavnicima jer iz opće teorije skupova znamo da vrijedi $[I] = [J] \iff I \sim J$. Sjetimo se također da je skup ideala u R_d disjunktna unija svih klasa ekvivalencije [I].

Definirajmo množenje klasa ekvivalencije na sljedeći način:

$$[I][J] = [IJ].$$

Definicija je sasvim prirodna: klase ekvivalencije određene reprezentantima I i J množimo tako da ideale I i J pomnožimo u polaznom prstenu R_d i onda umnožak $[I][J]$ definiramo kao klasu čiji reprezentant je upravo IJ. Problem s ovom definicijom je u tome što moramo pokazati da je konzistenta, tj. neovisna o izboru predstavnika pojedinih klasa.
Da bismo to učinili, odaberimo $I' \in [I]$ i $J' \in [J]$. Primijetimo da je tada $[I'] = [I]$ i $[J'] = [J]$. Sada je umnožak ovih dviju klasa definiran kao $[IJ]$, ali također i kao $[I'J']$, ako smo za reprezentante odabrali ideale I' i J'. Treba, dakle, vrijediti $[IJ] = [I'J']$, a to je ekvivalentno s $IJ \sim I'J'$, odnosno, po definiciji naše relacije postoji λ takav da $IJ = \lambda I'J'$. No, iz $I \sim I'$ i $J \sim J'$ imamo $I = \gamma_1 I'$ i $J = \gamma_2 J'$, pa slijedi $IJ = \gamma_1\gamma_2 I'J'$ i vrijedi $IJ \sim I'J'$. Time smo pokazali da je operacija množenja klasa ideala zaista dobra.

Za ovu operaciju množenja lagano se vidi da vrijedi svojstvo asocijativnosti i komutativnosti. Naime za svaki ideal I vrijedi $[I][R_d] = [I]$. Dakle $[R_d]$ je neutralni element. Također vrijedi i $[I][I^*] = [\langle N(I)\rangle] = [R_d]$. Iz svega ovdje navedenoga lagano slijedi tvrdnja sljedećeg teorema.

Teorem 4.3.21. *Skup klasa ideala od R_d ima strukturu Abelove grupe s obzirom na ranije definiranu operaciju množenja. Ova grupa, koju ćemo označiti s $Cl(R_d)$ naziva se* ***grupa klasa ideala*** *od R_d.*

U nastavku ćemo dokazati da je ta grupa uvijek konačna, ali prije toga dokažimo nekoliko pomoćnih tvrdnji.

Lema 4.3.22. *Ako je d kvadratno slobodan i $d \neq 1$, tada postoji konstanta C_d koja ovisi samo o vrijednosti broja d na način da za svaki nenul ideal I postoji nenul element $\alpha \in I$ takav da $|N(\alpha)| \leq C_d N(I)$.*

Dokaz. Neka je $N = N(I)$ i K najveći cijeli broj za koji vrijedi $K \leq \sqrt{N}$. Primjetimo da je prethodna nejednakost ekvivalentna s $K^2 \leq N < (K+1)^2$. Zapišimo ideal $I = \langle a + m\tau, n\rangle$,

gdje su $a, m, n \in \mathbb{Z}$ i $m > 0$, $n > 0$. Prema Propoziciji 4.3.10 znamo da je $N = nm$. Promotrimo sada skup

$$S = \{r + s\tau \mid r, s \in \mathbb{Z}, 0 \leq r \leq K, 0 \leq s \leq K\}$$

koji ima točno $(K+1)^2$ elemenata. Promotrimo sada podskupove $S_0, S_1, \ldots, S_{m-1}$ od S koji su definirani kao

$$S_j = \{r + s\tau \in S \mid s \equiv j \pmod{m}\}.$$

Budući da je S unija skupova $S_0, S_1, \ldots, S_{m-1}$ to znači da postoji barem jedan od skupova koji ima više od n elemenata. Neka je to S_j takav da vrijedi

$$S_j = \{r_1 + s_1\tau, r_2 + s_2\tau, \ldots, r_k + s_k\tau\}$$

gdje je $k > n$. $t_i = r_i - a\frac{(s_i - j)}{m}$. Napomenimo kako je t_i cijeli broj jer vrijedi $s_i \equiv j \pmod{m}$. Kako je $k > n$ tada znamo da mora postojati $i_1 < i_2$ takav da vrijedi $t_{i1} \equiv t_{i2} \pmod{n}$. Neka su $\alpha = r_{i1} + s_{i1}\tau$ i $\beta = r_{i2} + s_{i2}\tau$. Tada je $\alpha \neq \beta$, gdje su $\alpha, \beta \in S$ i možemo pisati

$$\begin{aligned}
\alpha - \beta &= r_{i_1} - r_{i_2} + (s_{i_1} - s_{i_2})\tau \\
&= r_{i_1} - r_{i_2} + (s_{i_1} - j - s_{i_2} + j)\tau \\
&= r_{i_1} - r_{i_2} + (s_{i_1} - j - s_{i_2} + j)\frac{a + m\tau}{m} - \frac{a}{m}((s_{i_1} - j) - (s_{i_2} - j)) \\
&= \frac{t_{i_1} - t_{i_2}}{n}n + \frac{s_{i_1} - s_{i_2}}{m}(a + m\tau) \in I.
\end{aligned}$$

Sada još samo trebamo procjeniti vrijednost $\gamma = \alpha - \beta$. Jer je $\gamma = u + v\tau$, gdje su $|u|, |v| \leq K$ i vrijedi

$$\begin{aligned}
|N(u + v\tau)| &= |(u + v\tau)(u + v\tau^*)| \\
&= |u^2 + uv(\tau + \tau^*) + v^2\tau\tau^*| \\
&\leq u^2 + |uvT(\tau)| + v^2|N(\tau)| \\
&\leq K^2(1 + |T(\tau)| + |N(\tau)|) \leq C_d N(I).
\end{aligned}$$

Zato, ovdje stavimo $C_d = 1 + |T(\tau)| + |N(\tau)|$ i zato slijedi tražena tvrdnja. □

Propozicija 4.3.23. *Ako je C_d definiran kao u prijašnjoj lemi, tada svaka klasa ideala u $Cl(R_d)$ sadrži ideal I za koji vrijedi $N(I) \leq C_d$.*

Dokaz. Neka je I ideal i $[I]$ klasa ideala. Prema zadnjoj Lemi znamo da ideal I^* sadrži nenul element α takav da vrijedi $|N(\alpha)| \leq C_d N(I^*)$. Budući da vrijedi $\langle\alpha\rangle \subseteq I^*$ znamo da prema Teoremu 4.3.12 vrijedi $I^* \mid \langle\alpha\rangle$ i pišemo $\langle\alpha\rangle = I^*J$ za neki ideal J. Budući je $[I^*][J] = [\langle\alpha\rangle] = [R_d]$ slijedi da je klasa $[J]$ inverzna klasi $[I^*]$, a kako je $[I^*]$ inverzna klasi $[I]$ i inverz u grupi je jedinstven, onda znamo da je $[I] = [J]$. Dakle $|N(\alpha)| = N\langle\alpha\rangle = N(I^*)N(J)$ i $N(I^*)N(J) \leq C_d N(I^*)$ i $N(J) \leq C_d$. □

Korolar 4.3.24. *Grupa $Cl(R_d)$ je konačna.*

Dokaz. Prema Propoziciji 4.3.23 svaka klasa ideala u R_d ima oblik $[I]$ u kojem vrijedi $N(I) \leq C_d$. No za svaku pojedinu normu $N \in \mathbb{N}$ postoji samo konačno mnogo ideala norme N, jer takav ideal mora biti produkt prostih ideala norme p ili p^2, gdje je p prost faktor broja N. Primijetimo da postoji konačno mnogo prostih ideala i ideala norme N. Dakle, postoji samo konačan broj ideala čija je norma manja ili jednaka broju C_d i zato postoji samo konačno mnogo klasa ideala. □

Red grupe $Cl(R_d)$ označavamo s $h(d)$ i zovemo **broj klasa** od R_d. Ako je $h(d) = 1$, onda je svaki ideal glavni. U tom slučaju je R_d domena glavnih ideala. Kako smo već spomenuli glasovitu Gaussovu hipotezu koja govori da postoji beskonačno mnogo pozitivnih brojeva d za koje je $h(d) = 1$. Drugim riječima da postoji beskonačno mnogo realnih kvadratnih proširenja čiji su pripadni prsteni cijeli R_d prsteni glavnih ideala.

Bibliografija

[1] R. Chapman, *Notes on algebraic numbers*, dostupno na `https://empslocal.ex.ac.uk/people/staff/rjchapma/notes/algn.pdf` (ožujak 2020.).

[2] K. Conrad, *Factoring in quadratic fields*, dostupno na `https://kconrad.math.uconn.edu/blurbs/gradnumthy/quadraticgrad.pdf` (lipanj 2020.).

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

[4] D. Tall I. Stewart, *Algebraic number theory*, Chapman and Hall, 1979.

[5] ———, *Algebraic number theory and Fermat's last theorem*, A K Peters. Ltd., 2002.

[6] H. C. Williams M. J. Jacobson Jr., *Solving the Pell equation*, CMS Books in Math, Canadian Math. Soc, Springer, 2009.

[7] W.J. Wickless, *A first graduate course in abstract algebra*, Marcel Dekker, 2004.

[8] B. Širola, *Algebarske strukture*, dostupno na `https://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf` (svibanj 2020.).

Sažetak

U ovom radu govorimo o kvadratnim proširenjima polja racionalnih brojeva, i to prvenstveno realnim kvadratnim proširenjima. Polazeći od definicije i elementarnih pojmova algebre, pokazujemo karakteristike i konstrukcije općenitih kvadratnih proširenja. Nadalje definiramo ključne pojmove algebarski broj i algebarskog cijelog broja i navodimo bitne rezultate vezane za njih. Na kraju navodimo neke strukturne rezultate za prsten cijelih brojeva kao što su jedinice, ideali, prosti ideali i faktorizacija.

Summary

In this thesis we consider quadratic field extensions of the field of rational numbers, and in particular real quadratic extensions. We begin by definitions and basic concepts of algebra, and then we characterize quadratic field extensions in general case. Furthermore we introduce the key notions of an algebraic number and algebraic integer, and for them we present some relevant results. Finally we prove certain structural results for the rings of integers of real quadratic extensions; e.g, some concerning units, ideals, prime ideals and factorization.

Životopis

Moje ime i prezime je Lovro Sindičić. Rođen sam 5. listopada 1995. u Zagrebu gdje sam pohađao Osnovnu školu Antuna Mihanovića, a 2011. upisao sam opći smjer III. gimnazije u istom gradu. Tijekom svojeg osnovnoškolskog i srednjoškolskog obrazovanja više puta sam sudjelovao na državnim i međunarodnim natjecanjima iz informatike.

Nakon završene srednje škole, 2015. sam upisao preddiplomski studij Matematika na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu. 2016. godine u časopisu Math.e u zajedničkoj suradnji s dr.sc. Tomislavom Burićem s Fakulteta elektrotehnike i računarstva iz Zagreba objavljujem stručni rad pod nazivom Harmonijski brojevi i Euler-Mascheronijeva konstanta. Titulu sveučilišnog prvostupnika (baccalaureus) matematike stekao sam 2018. godine te iste godine sam upisao željeni diplomski studiji Matematika i informatika; smjer: nastavnički, također na Matematičkom odsjeku.

U toku svojeg studija paralelno sam slušao i položio dodatne matematičke kolegije na Fakultetu elektrotehnike i računarstva i redovito volontirao na projektu Otvoreni dani PMF-a te predstavljao Matematički odsjek PMF-a na Smotri Sveučilišta u Zagrebu. Također tijekom studija držao sam instrukcije iz matematike učenicima osnovnih i srednjih škola u salezijanskoj župi na Jarunu, ali i radio razne druge studentske poslove. Uz sve to bio sam aktivan član atletske selekcije PMF-a i više puta pretrčao maratonsku dionicu u duljini od 42.195 km.

U zimskom semestru akademske godine 2019./2020. pohađao sam praksu iz informatike i matematike u Osnovnoj školi Vrbani u Zagrebu, dok u ljetnom semestru iste akademske godine, praksu iz istih predmeta pohađao sam u XV. gimnaziji u Zagrebu.

U zadnjoj godini svojeg studija bio sam demonstrator iz kolegija Programski jezici i oprema za nastavu programiranja u školama, te studentski predstavnik u Vijeću Matematičkog odsjeka i Vijeću voditelja studija Matematičkog odsjeka gdje u suradnji s kolegama predložio niz novih prijedloga.