Diplomski rad - Arijan Kovač - Algebarski brojevi

Kovač, Arijan

Supplement / Prilog

Sveučilište u Rijeci

Fakultet za matematiku

Sveučilišni diplomski studij Matematika

ARIJAN KOVAČ

ALGEBARSKI BROJEVI

Diplomski rad

Rijeka, rujan 2023.

Sveučilište u Rijeci

Fakultet za matematiku

Sveučilišni diplomski studij Matematika

ARIJAN KOVAČ

ALGEBARSKI BROJEVI

Mentor: doc.dr.sc. Ana Jurasić

Diplomski rad

Rijeka, rujan 2023.

SADRŽAJ

SAŽETAK

Algebarski brojevi su rješenja polinomnih jednadžbi s racionalnim koeficijentima, a proučavaju se u teoriji brojeva. Minimalni polinom algebarskog broja je ireducibilni normirani polinom s racionalnim koeficijentima najmanjeg stupnja koji ima taj broj kao korijen. Teorija brojeva proučava svojstva minimalnih polinoma i njihovu vezu sa svojstvima algebarskih brojeva. Algebarski brojevi igraju ključnu ulogu u kriptografiji, teoriji automata i teoriji grafova, kao i u ostalim granama matematike. Proučavanje algebarskih brojeva može donijeti brojna zanimljiva otkrića i primjene, potičući tako daljnji razvoj matematičkih teorija.

Ključne riječi: teorija brojeva, algebarski brojevi, algebarski cijeli brojevi

ABSTRACT

Algebraic numbers are solutions of polynomial equations with rational coefficients, which we study in Number Theory. The minimal polynomial of an algebraic number is an irreducible monic polynomial with rational coefficients of the smallest degree which has that number as a rooth. Number Theory studies the properties of minimal polynomials and their connection with the properties of algebraic numbers. Algebraic numbers play a key role in cryptography, automata theory and graph theory, as well as in other branches of mathematics. Studying algebraic numbers can bring numerous fascinating discoveries and applications, thus fostering further development of mathematical theories.

Key words: Number Theory, algebraic numbers, algebraic integers

1. UVOD

Algebarski brojevi su jedan od temeljnih koncepata u teoriji brojeva, koja proučava brojeve i njihova svojstva. Teorija brojeva je grana matematike koja proučava brojeve u njihovim različitim oblicima i svojstvima, a prvenstveno se bavi cijelim brojevima. Algebarski broj je kompleksan broj koji je korijen polinomne jednadžbe s koeficijentima u polju racionalnih brojeva. Drugim riječima, algebarski broj je broj koji se pojavljuje kao korijen polinomne jednadžbe s racionalnim koeficijentima. Algebarski brojevi su u potpunosti karakterizirani svojim minimalnim polinomom, koji je normirani polinom, najmanjeg stupnja, s racionalnim koeficijentima koji ima taj algebarski broj kao svoj korijen. Teorija brojeva proučava svojstva minimalnih polinoma i njihovu vezu sa svojstvima algebarskih brojeva.

Algebarski brojevi su važno i zanimljivo područje proučavanja u teoriji brojeva jer imaju niz zanimljivih svojstava. Na primjer, svaki algebarski broj može se jedinstveno izraziti kao zbroj racionalnog broja i transcendetnog broja, koji je broj koji nije algebarski.

Algebarski brojevi su iznimno važni u matematici jer omogućuju opisivanje mnogih drugih matematičkih koncepata, poput simetrija geometrijskih tijela, te su temelj u mnogim područjima matematike, poput algebre, analize i geometrije. Također, igraju ključnu ulogu u proučavanju eliptičkih krivulja, koje su temeljni objekti u algebarskoj geometriji. Jedna od važnih primjena algebarskih brojeva je u kriptografiji, gdje se koriste u kriptografskim sustavima poput RSA i Diffie – Hellman protokola. Algebarski brojevi igraju ključnu ulogu u teoriji automata te u teoriji grafova, gdje se koriste za modeliranje mnogih struktura, poput grupa simetrija grafova.

2. ALGEBARSKI BROJEVI U TEORIJI BROJEVA

U ovome poglavlju, objasnit će se kvadratna polja i polja algebarskih brojeva.

2.1. Kvadratna polja

Pitagorina jednadžba

$$x^2 + y^2 = z^2$$

može se riješiti na način da se zapiše drugačije, preciznije

$$y^2 = z^2 - x^2 = (z + x)(z - x).$$

Uređene trojke (x, y, z) prirodnih brojeva koje zadovoljavaju diofantsku jednadžbu $x^2 + y^2 = z^2$ nazivaju se **Pitagorine trojke**. Ako su x, y, z relativno prosti tada uređenu trojku (x, y, z) nazivamo **primitivna Pitagorina trojka**. Može se pokazati da su sve primitivne Pitagorine trojke dane sa:

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2$$

gdje su m i n relativno prosti prirodni brojevi, različite parnosti, za koje vrijedi $m > n$.

Promotrimo sada izraze $\frac{z+x}{2}$ i $\frac{z-x}{2}$. Primijetimo da su $z + x$ i $z - x$ parni. Ako z i x substituiramo gore navedenim jednakostima, dobivamo:

$$\frac{z + x}{2} = \frac{m^2 + n^2 + m^2 - n^2}{2} = \frac{2m^2}{2} = m^2,$$

$$\frac{z - x}{2} = \frac{m^2 + n^2 - m^2 + n^2}{2} = \frac{2n^2}{2} = n^2.$$

Spomenutom supstitucijom dobili smo da su $\frac{z+x}{2}$ i $\frac{z-x}{2}$ potpuni kvadrati. Navedeno vrijedi ako su x, y, z relativno prosti.

Na primjer, uzmimo Pitagorinu trojku $(5,12,13)$. Za nju vrijedi $5^2 + 12^2 = 13^2$. Ako promatramo $\frac{z+x}{2}$ i $\frac{z-x}{2}$ u ovom konkretnom slučaju imamo da je $\frac{13+5}{2} = 9$ i $\frac{13-5}{2} = 4$. Dobili smo da su $\frac{z+x}{2}$ i $\frac{z-x}{2}$ potpuni kvadrati, kao što smo gore pokazali za općeniti slučaj.

Pitanje je može li se zaključiti isto ako istu jednadžbu zapišemo u obliku

$$(x + yi)(x - yi) = z^2.$$

Drugim riječima, slijedi li da su $x + yi$ i $x - yi$ kvadrati u odgovarajućem proširenju prstena cijelih brojeva. Kod problema koji su potpuno formulirani u skupu cijelih brojeva, prirodno se nameće potreba promatranja proširenja prstena cijelih brojeva. To je dovelo do istraživanja polja algebarskih brojeva, od kojih su najjednostavnija kvadratna polja.

Navest ćemo nekoliko osnovnih tvrdnji vezanih za polinome, koje će nam u radu biti potrebne, bez ulaženja duboko u razmatranje polinoma. Neka je K integralna domena (često je to i polje). Skup polinoma jedne varijable s koeficijentima iz K, uz standardno definirane operacije zbrajanja i množenja polinoma, čini komutativni prsten s jedinicom i taj prsten ćemo označavati sa oznakom $K[x]$. Za polinom $p(x) \in K[x]$ stupnja n kažemo da je ireducibilan u prstenu polinoma $K[x]$ ako ne postoje polinomi $q(x)$ i $r(x)$ iz $K[x]$ stupnja barem jedan za koje vrijedi

$$p(x) = q(x) \cdot r(x).$$

Također, vrijedi i osnovni teorem o dijeljenju s ostatkom za polinome koji kaže da za svaki polinom $f \in K[x]$ kojemu je vodeći koeficijent invertibilan u K vrijedi da postoje jedinstveni polinomi $q, r \in K[x]$ za koje vrijedi

$$f = q \cdot g + r, \qquad \text{st}\, r < \text{st}\, g.$$

Definicija 2.1.1. Za kompleksni broj α kažemo da je **algebarski** broj ako postoji polinom $P(x)$ s racionalnim koeficijentima koji je različit od nul-polinoma i takav da vrijedi

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

Za kompleksni broj koji nije algebarski broj kažemo da je **transcendentan**.

Na primjer, broj i je algebarski broj zato što je nultočka polinoma $f(x) = x^2 + 1$. S druge strane, broj π je transcedentan jer nije algebarski broj zato što ne postoji polinom s racionalnim koeficijentima takav da mu je π nultočka.

Definicija 2.1.2. Za polinom

$$p(x) = a_d x^d + \cdots + a_1 x + a_0 \,,$$

za koji vrijede sljedeća svojstva:

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

$$a_d > 0, nzd(a_0, \dots, a_d) = 1,$$

$$p(\alpha) = 0,$$

ako je $p_0(x) \in \mathbb{Q}[x]$ za koji vrijedi $p_0(\alpha) = 0$, tada je $\frac{p_0(x)}{p(x)} \in \mathbb{Q}[x]$,

$p(x)$ je ireducibilan polinom nad poljem $\mathbb{Q}$,

kažemo da je **cjelobrojni minimalni polinom** algebarskog broja α. Minimalni polinom algebarskog broja α definira se kao

$$g(x) = \frac{1}{a_d} p(x).$$

Dakle, minimalni polinom algebarskog broja α je ireducibilni normirani polinom g s racionalnim koeficijentima za koji vrijedi

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

Stupanj algebarskog broja α definira se kao stupanj njegovog minimalnog polinoma.

Teorem 2.1.3. Za svaki algebarski broj α postoji jedinstveni polinom s cjelobrojnim koeficijentima

$$p(x) = a_d x^d + \cdots + a_1 x + a_0$$

opisan u definiciji 2.1.2

Dokaz. Neka je P skup svih polinoma iz $\mathbb{Q}[x]$, različitih od nul-polinoma, čiji je korijen α. Kako je skup stupnjeva svih polinoma iz skupa P zapravo podskup prirodnih brojeva, postoji minimalni element tog skupa. Neka je taj minimalni element m. Dakle, postoji $p_1(x) \in \mathbb{Q}[x]$ za kojeg vrijedi

$$\operatorname{st} P_1 = m,$$

$$p_1(\alpha) = 0.$$

Uzmimo da je A najmanji zajednički višekratnik nazivnika svih koeficijenata polinoma $p_1(x)$. Pomnožimo li $p_1(x)$ s A dobivamo polinom $Ap_1(x)$ koji u sebi sadrži cjelobrojne koeficijente. Označimo ga sa $p_2(x) = Ap_1(x)$. Uzmimo da je B najveći zajednički djelitelj svih koeficijenata polinoma $p_2(x)$. Podijelimo $p_2(x)$ s B i pomnožimo ga s -1 ako mu je vodeći koeficijent negativan. Time smo dobili polinom $p(x)$ za koji tvrdimo da zadovoljava uvjete teorema. Prva tri svojstva su očito zadovoljena. Neka je sada $p_0(x) \in \mathbb{Q}[x]$ takav da vrijedi

$$p_0(\alpha) = 0.$$

Ako podijelimo polinom $p_0(x)$ s $p(x)$, dobivamo

$$p_0(x) = p(x)q(x) + r(x),$$

gdje su $q(x), r(x) \in \mathbb{Q}[x]$ i

$$\operatorname{st} r(x) \leq m - 1.$$

Iz činjenice da vrijedi

$$p_0(\alpha) = p(\alpha) = 0,$$

slijedi

$$r(\alpha) = 0,$$

pa zbog minimalnosti od m, polinom $r(x)$ mora biti nul-polinom. Stoga, vrijedi da $p(x) | p_0(x)$.

Pokažimo da je $p(x)$ ireducibilan nad $\mathbb{Q}$. Pretpostavimo suprotno, odnosno, da $p(x)$ nije ireducibilan. U tom slučaju bi vrijedilo

$$p(x) = k_1(x)k_2(x),$$

gdje vrijedi

$$1 \leq \mathrm{st}\, k_i \leq m-1, \quad i = 1,2\,,$$

pa bismo imali

$$k_1(\alpha) = 0$$

ili

$$k_2(\alpha) = 0,$$

a to je protivno pretpostavci o minimalnosti stupnja od $p(x)$. Time smo dobili kontradikciju, odnosno, dobili smo da je $p(x)$ ireducibilan nad $\mathbb{Q}$.

Naposljetku, pokažimo jedinstvenost od $p(x)$. Neka je $e(x) \in \mathbb{Q}[x]$ polinom koji zadovoljava svih pet svojstava navedenih u definiciji 2.1.2. Tada postoji polinom $u(x)$ takav da vrijedi

$$e(x) = p(x)u(x).$$

Ireducibilnost od $e(x)$ povlači da je $u(x)$ konstanta, dok iz drugog svojstva slijedi da je

$$u(x) = 1$$

pa vrijedi: $e(x) = p(x)$. ■

U sljedećem teoremu navest ćemo glavno svojstvo skupa svih algebarskih brojeva, a to je da skup svih algebarskih brojeva čini polje. No, prije samog dokaza iskazat ćemo jedan korolar koji će nam biti potreban za dokaz Teorema 2.1.6.

Korolar 2.1.4.

Neka su $f(x)$ i $g(x)$ polinomi nad poljem K stupnja n, odnosno k, te neka su $\alpha_1, \ldots \ldots, \alpha_n$, odnosno $\beta_1, \ldots\ldots, \beta_k$ njihovi korijeni. Tada su:

$$h_1(x) = \prod_{j=1}^{k} \prod_{i=1}^{n} \left(x - \alpha_i - \beta_j\right),$$

$$h_2(x) = \prod_{j=1}^{k} \prod_{i=1}^{n} \left(x - \alpha_i \beta_j\right)$$

polinomi s koeficijentima iz K.

Primjer 2.1.5. Uzmimo neka dva algebarska broja, npr. $\alpha_1 = \sqrt{2},\ \beta_1 = i$. Za ta dva broja smo sigurni da su algebarski zato što postoje odgovarajući polinomi kojima su oni nultočke. Konkretno, $\sqrt{2}$ je nultočka polinoma $f(x) = x^2 - 2$, a i je nultočka polinoma $g(x) = x^2 + 1$. Ta dva polinoma imaju svaki po dva korijena, odnosno, imamo $\alpha_1 = \sqrt{2},\ \alpha_2 = -\sqrt{2},\ \beta_1 = i,\ \beta_2 = -i$. Korolar 2.1.4. kaže da polinomi

$$h_1(x) = (x - \sqrt{2} - i)(x - \sqrt{2} + i)(x + \sqrt{2} - i)(x + \sqrt{2} + i) \text{ i}$$

$$h_2(x) = \big(x - \sqrt{2}i\big)\big(x + \sqrt{2}i\big),$$

u svom standardnom obliku imaju koeficijente iz $\mathbb{Q}$, jer polinomi f, g imaju koeficijente iz $\mathbb{Q}$. I zaista, nakon što se „sredi“ svaki od ta dva polinoma, dobivamo

$$h_1(x) = \big(x - \sqrt{2} - i\big)\big(x - \sqrt{2} + i\big)\big(x + \sqrt{2} - i\big)\big(x + \sqrt{2} + i\big) = x^4 - 2x^2 + 9,$$

$$h_2(x) = \big(x - \sqrt{2}i\big)\big(x + \sqrt{2}i\big) = x^2 + 2,$$

odnosno, dobili smo da polinomi $h_1(x)$ i $h_2(x)$ imaju koeficijente iz $\mathbb{Q}$.

Teorem 2.1.6. Skup svih algebarskih brojeva čini polje.

Dokaz. Neka su α i $\beta \neq 0$ algebarski brojevi. Trebamo pokazati da su $\alpha + \beta$, $\alpha\beta$, $-\beta$ i β^{-1} algebarski brojevi. Neka su $f(x)$ i $g(x)$ minimalni polinomi od α i β. Možemo zaključiti da su $\alpha + \beta$ i $\alpha\beta$ algebarski brojevi jer su korijeni polinoma $h_1(x)$ i $h_2(x)$, opisanih u korolaru 2.1, s koeficijentima iz $\mathbb{Q}$. Broj $-\beta$ je algebarski jer je korijen polinoma $g(-x)$, dok je broj β^{-1} algebarski jer je korijen polinoma $x^m g\left(\frac{1}{x}\right)$, gdje je m stupanj od g. ■

Definicija 2.1.7. Za algebarski broj α kažemo da je **algebarski cijeli broj** ako njegov minimalni polinom ima cjelobrojne koeficijente. To znači da algebarski broj ima normirani cjelobrojni minimalni polinom.

Propozicija 2.1.8. U skupu racionalnih brojeva, jedini algebarski cijeli brojevi su cijeli brojevi.

Dokaz. Svaki cijeli broj m je algebarski broj jer poništava polinom

$$f(x) = x - m.$$

S druge strane, ako je $\frac{m}{q}$, gdje vrijedi

$$(m, q) = 1,$$

algebarski cijeli broj, tada vrijedi

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

gdje su $a_1, \ldots a_n$ cijeli brojevi. Ako pomnožimo navedenu jednakost s q^n, onda dobivamo

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

Dakle, $q | m^n$ i zato vrijedi

$$q = \pm 1,$$

što znači da je $\frac{m}{q}$ cijeli broj. ■

U nastavku ćemo definirati kvadratna polja.

Definicija 2.1.9. Za prirodan broj a kažemo da je **kvadratno slobodan** ako je 1 najveći kvadrat koji ga dijeli.

Definicija 2.1.10. Neka je d kvadratno slobodan cijeli broj takav da vrijedi

$$d \neq 1.$$

Kvadratno polje $\mathbb{Q}(\sqrt{d})$ definira se kao skup svih brojeva oblika $u + v\sqrt{d}$, gdje su u i v racionalni brojevi, s uobičajenim operacijama zbrajanja i množenja kompleksnih brojeva.

Ako se pretpostavi da broj d nije potpun kvadrat, neće se izgubiti općenitost jer vrijedi

$$\mathbb{Q}\left(\sqrt{dm^2}\right) = \mathbb{Q}\left(\sqrt{d}\right),$$

za racionalni broj m koji je različit od 0.

Za svaki element

$$\alpha = u + v\sqrt{d}$$

kvadratnog polja $\mathbb{Q}(\sqrt{d})$ definira se norma algebarskog broja α kao

$$N(\alpha) = u^2 - dv^2.$$

Dakle,

$$N(\alpha) = \alpha\bar{\alpha},$$

gdje je

$$\bar{\alpha} = u - v\sqrt{d}$$

konjugat od α.

Posebno, polje $\mathbb{Q}(\sqrt{-1})$ zove se polje Gaussovih brojeva koji su oblika $u + vi$. Lako se dokaže da je $\mathbb{Q}(\sqrt{d})$ polje. Za takve brojeve norma se definira kao

$$N(\alpha) = u^2 + v^2.$$

Teorem 2.1.11. Ako vrijedi

$$d \equiv 2(\text{mod } 4)$$

ili

$$d \equiv 3(\text{mod } 4),$$

tada algebarski cijeli brojevi u kvadratnom polju $\mathbb{Q}(\sqrt{d})$ imaju oblik $u + v\sqrt{d},$ gdje su $u, v \in \mathbb{Z}$. Ako vrijedi

$$d \equiv 1(\text{mod } 4),$$

tada su algebarski cijeli brojevi u kvadratnom polju $\mathbb{Q}\left(\sqrt{d}\right)$ oblika $s + t \cdot \frac{1+\sqrt{d}}{2}$, gdje su s i t cijeli brojevi.

Dokaz. Neka je

$$\alpha = u + v\sqrt{d}$$

algebarski cijeli broj u $\mathbb{Q}(\sqrt{d})$ te neka je

$$a = 2u,$$

$$b = 2v,$$

$$c = N(\alpha) = u^2 - dv^2.$$

Tada je α nultočka polinoma

$$f(x) = x^2 - ax + c.$$

Zaista, ako promatramo $f(\alpha)$, dobivamo

$$f(\alpha) = \left(u + v\sqrt{d}\right)^2 - 2u \cdot \left(u + v\sqrt{d}\right) + u^2 - dv^2$$

$$= u^2 + 2uv\sqrt{d} + v^2 d - 2u^2 - 2uv\sqrt{d} + u^2 - dv^2 = 0.$$

Prema tome, racionalni brojevi a i c moraju biti cijeli. Imamo

$$db^2 = a^2 - 4c$$

i budući da je d kvadratno slobodan, vidimo da je b također cijeli broj. Neka je sada

$$d \equiv 2 (\mathrm{mod}\ 4)$$

ili

$$d \equiv 3 (\mathrm{mod}\ 4).$$

Iz

$$db^2 = a^2 - 4c$$

slijedi

$$a^2 \equiv b^2 d (\mathrm{mod}\ 4).$$

Kako je općenito kvadrat cijelog broja ili djeljiv s 4 ili kod dijeljenja sa 4 daje ostatak 1, vrijedi

$$a^2 \equiv 0 (\mathrm{mod}\ 4)$$

ili

$$a^2 \equiv 1 (\mathrm{mod}\ 4).$$

Zatim, vrijedi jedna od sljedećih tri mogućnosti:

$$b^2d \equiv 0(\text{mod } 4),$$

$$b^2d \equiv 2(\text{mod } 4)$$

ili

$$b^2d \equiv 3(\text{mod } 4).$$

Te tri mogućnosti slijede iz činjenice da je $d \equiv 2(\text{mod } 4)$ ili je $d \equiv 3(\text{mod } 4)$ i činjenice da je kvadrat cijelog broja ili djeljiv s 4 ili kod dijeljenja sa 4 daje ostatak 1. Uzmimo prvi slučaj, a to je da je $d \equiv 2(\text{mod } 4)$ i b^2 je djeljiv sa 4. U tom slučaju b^2d će također biti djeljiv sa 4 jer je b^2 je djeljiv sa 4 i time smo dobili prvu mogućnost, odnosno, $b^2d \equiv 0(\text{mod } 4)$. Isto tako bi dobili i kada bi promatrali slučaj da je $d \equiv 3(\text{mod } 4)$ i b^2 je djeljiv s 4 jer svaki umnožak će biti djeljiv sa 4 ako mu je barem jedan od faktora djeljiv sa 4.

Druga mogućnost je da je $d \equiv 2(\text{mod } 4)$ i b^2 pri dijeljenju s 4 daje ostatak 1. To možemo zapisati kao: $d = 4k + 2$ i $b^2 = 4l + 1$, za neke cijele brojeve k, l. Tada imamo da nam je

$$b^2d = 16kl + 4k + 8k + 2.$$

Iz toga slijedi da je u tom drugom slučaju $b^2d \equiv 2(\text{mod } 4)$.

Treća mogućnost je da je $b^2d \equiv 3(\text{mod } 4)$ i b^2 pri dijeljenju s 4 daje ostatak 1. To možemo zapisati kao: $d = 4k + 3$ i $b^2 = 4l + 1$, za neke cijele brojeve k, l.

Tada imamo da nam je $b^2d = 16kl + 4k + 12k + 3$. Iz toga slijedi da je u tom drugom slučaju

$$b^2d \equiv 3(\text{mod } 4).$$

Kada bi a bio neparan broj, kongruencija $a^2 \equiv b^2d(\text{mod } 4)$ ne bi vrijedila. Dakle, a je paran pa je

$$a^2 \equiv 0(\text{mod } 4).$$

Ako bi b bio neparan, tada bi bilo $b^2d \equiv 2(\text{mod } 4)$ ili $b^2d \equiv 3(\text{mod } 4)$. Dakle b također mora biti paran broj. Budući su a i b parni brojevi, iz toga slijedi da su u i v cijeli brojevi. Ako je sada

$$d \equiv 1(\text{mod } 4),$$

onda vrijedi $b^2 d \equiv 0 (\mathrm{mod}\ 4)$ ako je b paran. U slučaju da je b neparan, $b^2 d \equiv 1 (\mathrm{mod}\ 4)$. Sada iz $a^2 \equiv b^2 d (\mathrm{mod}\ 4)$ slijedi da su a i b iste parnosti. Stoga je broj

$$u - v = \frac{1}{2}(a - b)$$

cijeli. Stavimo

$$s = u - v,$$

$$t = 2v.$$

Promotrimo sada izraz $s + t \cdot \frac{1+\sqrt{d}}{2}$. Kada bi u ovaj izraz substituirali varijable s i t gore navedenim jednakostima dobili bi

$$s + t \cdot \frac{1 + \sqrt{d}}{2} = u - v + 2v \cdot \frac{1 + \sqrt{d}}{2} = u - v + v + v\sqrt{d} = u + v\sqrt{d}.$$

Time smo dobili

$$u + v\sqrt{d} = s + t \cdot \frac{1 + \sqrt{d}}{2}.$$

■

Definicija 2.1.12. Invertibilni element (jedinica) u kvadratnom polju $\mathbb{Q}(\sqrt{d})$ je algebarski cijeli broj ε takav da je broj $\frac{1}{\varepsilon}$ algebarski cijeli broj.

Teorem 2.1.13. Vrijede sljedeća svojstva:

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

(2) vrijedi

$$N(\alpha) = 0$$

ako i samo ako vrijedi

$$\alpha = 0,$$

(3) ako je α algebarski cijeli broj u kvadratnom polju $\mathbb{Q}(\sqrt{d})$, onda je $N(\alpha)$ cijeli broj,

(4) ako je z algebarski cijeli broj u kvadratnom polju $\mathbb{Q}(\sqrt{d})$, onda je z invertibilni element ako i samo ako vrijedi

$$N(z) = \pm 1.$$

Dokaz. 1) Uzmimo dva proizvoljna elementa $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$. Iz toga slijedi da su α, β oblika

$$\alpha = a + b\sqrt{d}, \quad \beta = c + f\sqrt{d}, \quad a, b, c, f \in \mathbb{Q}.$$

Po definiciji norme imamo da je

$$N(\alpha\beta) = N\left(ac + bfd + (af + bc)\sqrt{d}\right) = (ac + bfd)^2 - (af + bc)^2\, d$$

$$= a^2c^2 + 2acbfd + b^2f^2d^2 - a^2f^2d - 2afbcd - b^2c^2d$$

$$= a^2c^2 + b^2f^2d^2 - a^2f^2d - b^2c^2d\,,$$

$$N(\alpha) = N\left(a + b\sqrt{d}\right) = a^2 - b^2d,$$

$$N(\beta) = N\left(c + f\sqrt{d}\right) = c^2 - f^2d.$$

Želimo pokazati da je $N(\alpha\beta) = N(\alpha)N(\beta)$. Dobivamo,

$$N(\alpha)N(\beta) = (a^2 - b^2d)(c^2 - f^2d) = a^2c^2 - a^2f^2d - b^2c^2d + b^2f^2d^2$$

i time smo pokazali da je $N(\alpha\beta) = N(\alpha)N(\beta)$.

2) Znamo da je $N\left(a + b\sqrt{d}\right) = a^2 - b^2d$, no kao što smo već prije spomenuli kod definiranja norme, normu nekog kompleksnog broja α možemo zapisati kao $N(\alpha) = \alpha\overline{\alpha}$.
Ako je najprije $N(\alpha) = 0$, iz toga slijedi da je $\alpha\overline{\alpha} = 0$. Ako je $\alpha\overline{\alpha} = 0$ onda iz toga slijedi da je $\alpha = 0$ jer ako je $\alpha \neq 0$ onda će biti i $\overline{\alpha} \neq 0$. Vrijedi i obrat, odnosno, ako je $\alpha = 0$ onda je i $N(\alpha) = 0$.

3) Dokazano u teoremu 2.1.11.

4) Neka je z jedinica, $z \in \mathbb{Q}(\sqrt{d})$. Po definiciji, ako je z jedinica, postoji z^{-1} takav da je

$$zz^{-1} = 1.$$

Ako djelujemo s normom na ovu jednakost, dobivamo $N(z)N(z^{-1}) = N(1) = 1$.
Budući su $N(z)$ i $N(z^{-1})$ cijeli brojevi, iz toga slijedi $N(z) = \pm 1$. Neka je $N(z) = \pm 1$.

Iz toga slijedi da je $z \cdot \overline{z} = \pm 1$, iz čega slijedi $\frac{1}{z} = \pm\, \overline{z}$ algebarski cijeli broj.

Time smo pokazali da je z jedinica. ■

Za kvadratno polje $\mathbb{Q}(\sqrt{d})$ kažemo da je **realno** ako je broj d pozitivan cijeli broj. U slučaju da je d negativan cijeli broj, tada takvo kvadratno polje nazivamo **imaginarnim**.

Teorem 2.1.14. Neka je d negativan kvadratno slobodan cijeli broj. Tada kvadratno polje $\mathbb{Q}(\sqrt{d})$ ima invertibilne elemente ± 1. To su jedini invertibilni elementi, osim u slučajevima kada vrijedi

$$d = -1$$

i

$$d = -3.$$

Invertibilni elementi u kvadratnom polju $\mathbb{Q}(i)$ su ± 1 i $\pm i$, dok su u kvadratnom polju $\mathbb{Q}(\sqrt{-3})$ invertibilni elementi ± 1, $\frac{1\pm\sqrt{-3}}{2}$ i $\frac{-1\pm\sqrt{-3}}{2}$.

Dokaz. Potrebno je pronaći sve algebarske cijele brojeve α takve da vrijedi

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

Ako vrijedi

$$d \equiv 2 (\mathrm{mod}\ 4)$$

ili

$$d \equiv 3 (\mathrm{mod}\ 4),$$

onda α ima oblik

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

gdje su x i y cijeli brojevi pa treba riješiti jednadžbe

$$x^2 - dy^2 = \pm 1.$$

Budući da je d negativan, to slučaj

$$x^2 - dy^2 = -1$$

otpada. Ako vrijedi

$$d \leq -2,$$

onda vrijedi

$$x^2 - dy^2 \geq 2y^2$$

pa su jedina rješenja $(x, y) = (\pm 1, 0)$, otkuda je

$$\alpha = \pm 1.$$

Ako je

$$d = -1,$$

onda imamo jednadžbu

$$x^2 + y^2 = 1$$

čija su rješenja (x, y) dana s

$$x = \pm 1, y = 0$$

i

$$x = 0, y = \pm 1,$$

odnosno

$$\alpha = \pm 1, \pm i.$$

Ako je

$$d \equiv 1 (\mathrm{mod}\ 4),$$

onda α ima oblik

$$x + y \cdot \frac{1 + \sqrt{d}}{2}$$

pa je

$$N(\alpha) = \left(x + \frac{y}{2}\right)^2 - \frac{1}{4}dy^2.$$

Ponovno, zbog

$$d < 0,$$

jednadžba

$$N(\alpha) = -1$$

nema rješenja. Ako je

$$d \leq -7,$$

onda je

$$\left(x + \frac{y}{2}\right)^2 - \frac{1}{4}dy^2 \geq \frac{7}{4}y^2$$

pa iz

$$N(\alpha) = 1$$

slijedi

$$y = 0, x = \pm 1,$$

odnosno

$$\alpha = \pm 1.$$

Ako je

$$d = -3,$$

onda imamo jednadžbu

$$\left(x + \frac{y}{2}\right)^2 + \frac{3}{4}y^2 = 1,$$

odnosno

$$x^2 + xy + y^2 = 1.$$

Iz

$$\left(x+\frac{y}{2}\right)^2+\frac{3}{4}y^2=1$$

slijedi

$$|y|\leq 1.$$

Ako je

$$y=0,$$

onda je

$$x=\pm 1, \qquad \alpha=\pm 1.$$

Ako je

$$y=1,$$

onda je

$$x=0 \text{ ili } x=-1$$

i

$$\alpha=\frac{1+\sqrt{-3}}{2} \text{ ili } \alpha=\frac{-1+\sqrt{-3}}{2}.$$

Ako je

$$y=-1,$$

onda je

$$x=0 \text{ ili } x=1$$

i

$$\alpha=\frac{1-\sqrt{-3}}{2} \text{ ili } \alpha=\frac{-1-\sqrt{-3}}{2}.$$

■

Realno kvadratno polje je polje koje proširuje polje racionalnih brojeva i sadrži kvadratni korijen određenog realnog broja. Invertibilni elementi u ovom polju su elementi koji imaju multiplikativni inverz. Prije nego što u sljedećem teoremu iskažemo jedno svojstvo vezano za invertibilne elemente, definirat ćemo pojam Pellove jednadžbe koji će nam biti potreban za dokaz tog teorema.

Definicija 2.1.15. Diofantsku jednadžbu

$$x^2 - dy^2 = 1,$$

gdje je d prirodan broj i nije potpun kvadrat, zovemo **Pellova jednažba**. Jednadžbu oblika

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

gdje su d i N prirodni brojevi i d nije potpun kvadrat, zovemo **pellovska jednadžba**.

Pellova jednadžba ima beskonačno mnogo rješenja, a o načinu rješavanja može se vidjeti u [3].

Teorem 2.1.16. U svakom realnom kvadratnom polju postoji beskonačno mnogo invertibilnih elemenata.

Dokaz. Brojevi

$$\alpha = x + y\sqrt{d}$$

gdje x, y algebarski cijeli brojevi su algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ s normom

$$N(\alpha) = x^2 - dy^2.$$

Ako vrijedi

$$x^2 - dy^2 = 1,$$

onda je α jedinica. No, jednadžba

$$x^2 - dy^2 = 1$$

je Pellova jednadžba i ona, za kvadratno slobodni broj

$$d > 1$$

ima beskonačno mnogo rješenja. ■

U grupi invertibilnih elemenata realnog kvadratnog polja postoji element koji djeluje kao identitet za množenje. Taj element je broj 1. Za svaki invertibilni element postoji drugi invertibilni element koji pomnožen s njim daje 1. Nije teško pokazati da invertibilni elementi u realnom kvadratnom polju tvore grupu u odnosu na množenje.

Kao što smo vidjeli, problem pronalaska invertibilnih elemenata u realnim kvadratnim poljima povezan je s Pellovim jednadžbama. Spomenimo još da je fundamentalno rješenje Pellove jednadžbe najmanje rješenje te jednadžbe u prirodnim brojevima.

Generatori grupe invertibilnih elemenata u realnom kvadratnom polju su elementi koji mogu generirati sve ostale elemente te grupe. U kontekstu realnog kvadratnog polja, generiranje se odnosi na korištenje potenciranja i množenja s generatorom kako bi se dobili svi ostali invertibilni elementi u polju.

Korolar 2.1.17. Grupa invertibilnih elemenata u realnom kvadratnom polju $\mathbb{Q}(\sqrt{d})$ ima dva generatora -1 i ϵ_d, gdje je

$$\epsilon_d = a + b\sqrt{d}$$

ili

$$\epsilon_d = \frac{a + b\sqrt{d}}{2},$$

gdje je $a + b\sqrt{d}$ fundamentalno rješenje jedne od Pellovih jednadžbi

$$x^2 - dy^2 = \pm 1$$

i

$$x^2 - dy^2 = \pm 4.$$

To znači da se svaki invertibilni element može zapisati u obliku $\pm\epsilon_d^n$, gdje je n cijeli broj. Za generator ϵ_d kažemo da je fundamentalna jedinica kvadratnog polja $\mathbb{Q}(\sqrt{d})$. Ako je $x_1 + y_1\sqrt{d}$ fundamentalno rješenje Pellove jednadžbe

$$x^2 - dy^2 = 1,$$

onda vrijedi

$$x_1 + y_1\sqrt{d} = \left(a + b\sqrt{d}\right)^{\upsilon},$$

gdje je $\upsilon \in \{1,2,3,6\}$.

Definicija 2.1.18. Neka su α i β algebarski cijeli brojevi kvadratnog polja $\mathbb{Q}(\sqrt{d})$. Za broj α kažemo da **dijeli** broj β ako postoji algebarski cijeli broj γ kvadratnog polja $\mathbb{Q}(\sqrt{d})$ za koji vrijedi

$$\beta = \alpha\gamma.$$

U takvom slučaju pišemo $\alpha \mid \beta$. Može se zaključiti da su invertibilni elementi djelitelji broja 1. Za brojeve α i β kažemo da su asocirani ili pridruženi ako je α/β invertibilni element.

Za algebarski cijeli broj α kvadratnog polja $\mathbb{Q}(\sqrt{d})$, koji nije nula niti jedinica u tom polju, kažemo da je ireducibilan ako je djeljiv samo s invertibilnim elementima i sebi asociranim brojevima. Za algebarski cijeli broj π kvadratnog polja $\mathbb{Q}(\sqrt{d})$ kažemo da je prost ako nije nula ni invertibilan element te ako ima svojstvo da ako vrijedi $\pi|\beta\gamma$, gdje su β i γ algebarski cijeli brojevi kvadratnog polja $\mathbb{Q}(\sqrt{d})$, onda vrijedi $\pi|\beta$ ili $\pi|\gamma$.

U skupu $\mathbb{Z}$ svaki prost broj je ujedno ireducibilan i obratno. U kvadratnom polju svaki prost broj je ireducibilan no obrat ne vrijedi, odnosno, ireducibilni element ne mora biti prost.

Primjer 2.1.19. Broj 2 je ireducibilan u $\mathbb{Q}(\sqrt{-5})$ jer iz

$$2 = \beta\gamma$$

slijedi

$$N(\beta)N(\gamma) = 4.$$

Budući da jednadžbe

$$x^2 + 5y^2 = \pm 2$$

nemaju cjelobrojnih rješenja, slijedi da vrijedi

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

ili

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

i onda je jedan od brojeva β i γ jedinica. S druge strane, broj 2 nije prost u $\mathbb{Q}(\sqrt{-5})$ jer 2 dijeli

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

ali 2 ne dijeli niti $1 + \sqrt{-5}$ niti $1 - \sqrt{-5}$. Naime:

$$N(2) = 4$$

ne dijeli

$$N(1 + \sqrt{-5}) = (1 - \sqrt{-5}) = 6.$$

Teorem 2.1.20. Ako je norma algebarskog cijelog broja α kvadratnog polja $\mathbb{Q}(\sqrt{d})$ jednaka $\pm p$, gdje je p prosti broj, onda je broj α ireducibilan.

Dokaz. Pretpostavimo da je $\alpha = \beta\gamma$, gdje su β i γ cijeli u $\mathbb{Q}(\sqrt{d})$. Prema teoremu 2.1.13 vrijedi

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

Iz činjenice da su $N(\beta)$ i $N(\gamma)$ cijeli brojevi slijedi da jedan od njih mora biti jednak ± 1. Dakle, slijedi da je ili β ili γ jedinica, a drugi da je asociran α. ■

Teorem 2.1.21. Svaki algebarski cijeli broj α kvadratnog polja $\mathbb{Q}(\sqrt{d})$, koji nije nula ni invertibilni element, može se zapisati u obliku produkta ireducibilnih brojeva kvadratnog polja $\mathbb{Q}(\sqrt{d})$.

Dokaz. Ako α nije ireducibilan element onda se može rastaviti kao umnožak $\beta\gamma$, gdje β i γ nisu invertibilni. Nastavljajući ovaj postupak, faktoriziramo β i γ ako nisu ireducibilni. Ovaj proces faktorizacije je konačan jer bismo inače dobili da je $\alpha = \beta_1\beta_2 \cdot \ldots \cdot \beta_n$, gdje je n po volji velik a nijedan od β_j nije jedinica. Iz toga bi slijedilo :

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

jer je $|N(\beta_j)|$ prirodni broj veći od 1, budući nijedan od β_j nije jedinica. Time smo dobili kontradikciju. ■

Ovime je pokazano da uvijek postoji faktorizacija na ireducibilne faktore u $\mathbb{Q}(\sqrt{d})$, no ona ne mora uvijek biti jedinstvena.

Primjer 2.1.22. Promotrimo broj 14 i njegove dvije faktorizacije u $\mathbb{Q}(\sqrt{-10})$:

$$14 = 2 \cdot 7 = (2 + \sqrt{-10})(2 - \sqrt{-10}).$$

Brojevi $2,7, 2 + \sqrt{-10},\ 2 - \sqrt{-10}$ su ireducibilni u $\mathbb{Q}(\sqrt{-10})$.

Definicija 2.1.23. Za kvadratno polje $\mathbb{Q}(\sqrt{d})$ kažemo da ima **svojstvo jedinstvene faktorizacije** ako se svaki algebarski cijeli broj kvadratnog polja $\mathbb{Q}(\sqrt{d})$, koji nije nula ni invertibilni element, može faktorizirati na ireducibilne faktore jednoznačno do na poredak faktora i zamjenu faktora asociranim brojevima.

Definicija 2.1.24. Za kvadratno polje kažemo da je euklidsko ako algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ zadovoljavaju Euklidov algoritam, odnosno ako za algebarske cijele brojeve α, β u $\mathbb{Q}(\sqrt{d})$, gdje je

$$\beta \neq 0,$$

postoje algebarski cijeli brojevi γ, δ iz $\mathbb{Q}(\sqrt{d})$ takvi da vrijedi

$$\alpha = \beta\gamma + \delta$$

i

$$|N(\delta)| < |N(\beta)|.$$

Teorem 2.1.25. Svako euklidsko kvadratno polje ima svojstvo jedinstvene faktorizacije.

Dokaz. Prvo ćemo pokazati da ako su α i β algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ koji nemaju zajedničkih djelitelja osim jedinica, onda postoje algebarski cijeli brojevi $x_0, y_0 \in \mathbb{Q}(\sqrt{d})$ takvi da je $\alpha x_0 + \beta y_0 = 1$.

Neka je M skup svih brojeva oblika $\alpha x + \beta y$, gdje x i y prolaze skupom svih algebarskih cijelih brojeva u $\mathbb{Q}(\sqrt{d})$. Brojevi $|N(\alpha x + \beta y)|$ su nenegativni cijeli brojevi, pa izaberimo element $e = \alpha x_1 + \beta y_1$ skupa M takav da $|N(e)|$ poprima najmanju pozitivnu vrijednost među brojevima $|N(\alpha x + \beta y)|$. Primjenom Euklidova algoritma na brojeve α i e dobivamo

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

Tada je $\delta = \alpha - \gamma(\alpha x_1 + \beta y_1) = \alpha(1 - \gamma x_1) + \beta(-\gamma y_1) \in M$. Prema definiciji od e imamo da je $N(\delta) = 0$ tj. $\delta = 0$. Dakle, $\alpha = e\gamma$ i $e \mid \alpha$. Slično se pokazuje da $e \mid \beta$ pa je e invertibilni element. Sada je i e^{-1} jedinica i imamo

$1 = e^{-1}e = e^{-1}(\alpha x_1 + \beta y_1) = \alpha(e^{-1}x_1) + \beta(e^{-1}y_1) = \alpha x_0 + \beta y_0.$ ■

Primjer 2.1.26. Sada dokazujemo da su kvadratna polja $\mathbb{Q}(\sqrt{d})$ za

$$d = -11, -7, -3, -2, -1, 2, 3, 5$$

euklidska. Neka su α i β algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$, gdje je

$$\beta \neq 0.$$

Tada vrijedi

$$\frac{\alpha}{\beta} = u + v\sqrt{d},$$

gdje su u i v racionalni brojevi. Odaberimo cijele brojeve x i y koji su najbliži brojevima u i v, odnosno

$$0 \leq |u - x| \leq \frac{1}{2},$$

$$0 \leq |v - y| \leq \frac{1}{2}.$$

Označimo

$$x + y\sqrt{d} = \gamma,$$

$$\alpha - \beta\gamma = \delta.$$

Brojevi γ i δ su cijeli u $\mathbb{Q}(\sqrt{d})$ i

$$N(\delta) = N(\alpha - \beta\gamma) = N(\beta)N\left(\frac{\alpha}{\beta} - \gamma\right) = N(\beta)N\left((u-x) + (v-y)\sqrt{d}\right)$$
$$= N(\beta)N((u-x)^2 - d(v-y)^2)$$

pa je

$$|N(\delta)| = |N(\beta)| \cdot |(u-x)^2 - d(v-y)^2|.$$

Ako je

$$d > 0,$$

onda je

$$-\frac{d}{4} \leq (u-x)^2 - d(v-y)^2 \leq \frac{1}{4},$$

a ako je

$$d < 0,$$

onda je

$$0 \leq (u-x)^2 + d(v-y)^2 \leq \frac{1}{4} + \frac{1}{4}(-d).$$

Prema tome, ako je

$$d = 2{,}3, -1, -2,$$

onda dobivamo

$$|N(\delta)| < |N(\beta)|$$

pa je za te vrijednosti od d polje $\mathbb{Q}(\sqrt{d})$ euklidsko. Za

$$d = -11, -7, -3{,}5$$

postupamo drugačije. Uočimo da je u svim ovim slučajevima

$$d \equiv 1 (\mathrm{mod}\ 4).$$

Neka su u i v definirani kao prije. Izaberemo cijeli broj z najbliži broju $2v$ i stavimo

$$s = v - \frac{1}{2}z.$$

U tom slučaju vrijedi

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

Nadalje, izaberimo cijeli broj x najbliži broju $u - \frac{1}{2}z$ i stavimo

$$k = u - x - \frac{1}{2}y.$$

U tom slučaju vrijedi

$$|k| \leq \frac{1}{2}.$$

Označimo

$$x + y \cdot \frac{1+\sqrt{d}}{2} = \gamma,$$

$$\alpha - \beta\gamma = \delta.$$

Iz toga slijedi da je

$$N(\delta) = N(\beta)(k^2 - ds^2).$$

Budući da je

$$|d| \leq 11,$$

imamo

$$|k^2 - ds^2| \leq \frac{1}{4} + 11 \cdot \frac{1}{16} < 1,$$

pa je

$|N(\delta)| < |N(\beta)|,$ što smo i htjeli dokazati. ■

Teorem 2.1.27. Neka kvadratno polje $\mathbb{Q}(\sqrt{d})$ ima svojstvo jedinstvene faktorizacije. Tada svakom ireducibilnom broju a kvadratnog polja $\mathbb{Q}(\sqrt{d})$ odgovara točno jedan prirodni prosti broj p za koji vrijedi $a| p$.

Dokaz. Ireducibilni broj a dijeli cijeli broj $N(a)$, dakle postoje prirodni brojevi koji su djeljivi s a. Neka je p najmanji takav broj. Pokazat ćemo da je p prost. Ako p nije prost tada bi vrijedilo $p = cd$ pa zbog svojstva jedinstvene faktorizacije $a \mid c$ ili $a \mid d$ što je kontradikcija jer je $1 < c,\ d < p$.

Pretpostavimo da a dijeli još neki prosti prirodni broj b. Tada je najmanji zajednički djelitelj od p i b jednak 1, pa postoje cijeli brojevi x, y takvi da je $px + by = 1$. Iz ovoga, dakle, slijedi da $a \mid 1$ što je kontradikcija i time smo pokazali da je prosti broj p jedinstven. ■

Teorem 2.1.26. Prosti brojevi kvadratnog polja $\mathbb{Q}(i)$ su prosti prirodni brojevi oblika

$$p = 4k + 3,$$

faktori π i π' iz faktorizacije

$$p = \pi\pi'$$

prostih prirodnih brojeva oblika

$$p = 4k + 1,$$

broj $1 + i$ te brojevi koji su asocirani prethodno navedenim brojevima. To znači svi brojevi koji se dobiju iz njih množenjem s ± 1 ili $\pm i$.

Ovaj teorem nećemo dokazivati, ali dokaz se može naći u [3], Teorem 12.13.

2.2. Polja algebarskih brojeva

Motivacija uvođenja polja algebarskih brojeva došla je iz rješavanja diofantskih jednadžbi, najviše zbog rješavanja Velikog Fermatovog teorema. To područje je središnja tema u algebarskoj teoriji brojeva.

Neka je α algebarski broj. Polje algebarskih brojeva $\mathbb{Q}(\alpha)$ generirano s elementom α je najmanje polje koje sadržava i element α i skup $\mathbb{Q}$. Za polje $\mathbb{Q}(\alpha)$ kažemo da je jednostavno algebarsko proširenje polja $\mathbb{Q}$. Iz definicije slijedi da je

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

odnosno $\mathbb{Q}(\alpha)$ je skup svih kvocijenata oblika $\frac{f(\alpha)}{g(\alpha)}$, gdje su f i g polinomi nad $\mathbb{Q}$ i $g(\alpha) \neq 0$. Sljedeći teorem pokazuje kako se na jedinstveni način može prikazati svaki element iz $\mathbb{Q}(\alpha)$. Dokaz se može naći u [3], Teorem 12.14.

Teorem 2.2.1. Svaki element β kvadratnog polja $\mathbb{Q}(\alpha)$ može se zapisati na jedinstven način kao

$$\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = p(\alpha),$$

gdje su $a_0, a_1, \dots, a_{n-1}$ racionalni brojevi i n stupanj algebarskog broja α.

Neka je $\mathbb{K} = \mathbb{Q}(\alpha)$. Stupanj od $\mathbb{K}$ je definiran kao stupanj minimalnog polinoma od α. Iz prethodnog teorema vidimo da je $\mathbb{K}$ vektorski prostor nad poljem $\mathbb{Q}$ dimenzije n koji ima bazu

$$\{1, \alpha, \dots \dots, \alpha^{n-1}\}.$$

Ako je c bilo koji algebarski broj takav da je $\mathbb{K} = \mathbb{Q}(c)$, onda je stupanj od c također jednak n.

Polje algebarskih brojeva $\mathbb{K}$ proširenje je polja racionalnih bojeva konačnog stupnja. Može se zaključiti da polje algebarskih brojeva sadrži skup racionalnih brojeva i ima konačnu dimenziju kao vektorski prostor nad skupom racionalnih brojeva.

Neka je skup $\{\alpha_1, \dots, \alpha_n\}$ baza polja algebarskih brojeva $\mathbb{K}$ nad $\mathbb{Q}$. Tada je $\mathbb{K} = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ najmanje polje koje sadrži skup racionalnih brojeva i algebarske brojeve $\alpha_1, \dots, \alpha_n$.

U sljedećem teoremu ćemo pokazati da se neko proizvoljno polje algebarskih brojeva $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ može dobiti kao jednostavno algebarsko proširenje algebarskog polja $\mathbb{Q}(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$. U iskazu teorema navest će se samo slučaj za $n = 2$ jer se onda opća tvrdnja može pokazati indukcijom.

Teorem 2.2.2. Neka vrijedi

$$k = \mathbb{Q}(\beta)$$

i

$$\mathbb{K} = k(\alpha) = \mathbb{Q}(\alpha, \beta).$$

Tada vrijedi

$$\mathbb{K} = \mathbb{Q}(\gamma),$$

gdje je

$$\gamma = u\alpha + v\beta$$

za neke cijele brojeve u i v.

Ovaj teorem nećemo dokazivati, no dokaz se može naći u [3], Teorem 12.16.

3. ALGEBARSKI CIJELI BROJEVI

U ovome poglavlju, objasnit će se algebarski cijeli brojevi, ideali te jedinice i klase ideala.

3.1. Algebarski cijeli brojevi

Za algebarski broj koji ima cijele brojeve za koeficijente minimalnog polinoma kažemo da je algebarski cijeli broj. Konjugati[1] algebarskog cijelog broja su algebarski cijeli brojevi. Može se zaključiti da su nultočke normiranih ireducibilnih polinoma s cijelim brojevima kao koeficijentima algebarski cijeli brojevi.

Skup svih algebarskih cijelih brojeva, uz standardne operacije zbrajanja i množenja kompleksnih brojeva, čini prsten. Takav prsten označava se s $\mathcal{O}$. Skup svih algebarskih cijelih brojeva polja algebarskih brojeva je također prsten.

Neka je α algebarski broj s minimalnim polinomom p. Nazivnik algebarskog broja α definira se kao najmanji prirodni broj a za koji polinom ap ima cjelobrojne koeficijente. Drugim riječima, broj a je najmanji zajednički višekratnik nazivnika koeficijenata polinoma p.

Lema 3.1.1. Neka je α algebarski broj i neka je a njegov nazivnik. Tada je $a\alpha$ algebarski cijeli broj. Drugim riječima, ako su $\alpha_1, \dots, \alpha_m$ različiti konjugati algebarskog broja α, onda je

$$a \cdot \alpha_1 \cdot \dots \cdot \alpha_m$$

algebarski cijeli broj.

Dokaz se može naći u [3], Lema 12.17.

Neka je $\mathcal{O}_{\mathbb{K}}$ prsten cijelih brojeva algebarskog polja $\mathbb{K}$. Za bazu prstena $\mathcal{O}_{\mathbb{K}}$ nad skupom cijelih brojeva kažemo da je integralna baza polja $\mathbb{K}$. Elementi $\omega_1, \dots, \omega_n$ prstena $\mathcal{O}_{\mathbb{K}}$ čine integralnu bazu polja $\mathbb{K}$ ako i samo ako se svaki element α prstena $\mathcal{O}_{\mathbb{K}}$ može zapisati u obliku

[1] Za $\alpha_1, \dots, \alpha_m$ kažemo da su konjugati od α ako su $\alpha_1, \dots, \alpha_m$ nultočke minimalnog polinoma g od α.

$$\alpha = u_1\omega_1 + \cdots + u_n\omega_n,$$

za cijele brojeve $u_1, \ldots, u_n$.

Teorem 3.1.2. Za svako polje algebarskih brojeva $\mathbb{K}$ postoji njegova integralna baza.

Dokaz se može naći u [3], Teorem 12.18.

Sada ćemo navesti teorem koji govori kako se svojstva algebarskih cijelih brojeva mogu iskoristiti za dobivanje rezultata o dekompozabilnosti polinoma.

Definicija 3.1.1. Za polinom $f \in \mathbb{C}[x]$ stupnja većeg od 1 kažemo da je nedekompozabilan nad $\mathbb{C}$ ako $f = g \circ h,\ \ g, h \in \mathbb{C}[x]$, povlači $\mathrm{st}\, g = 1$ ili $\mathrm{st}\, h = 1$.

Teorem 3.1.3. Neka je

$$f(x) \in \mathbb{Z}[x]$$

normiran i dekompozabilan polinom nad poljem $\mathbb{C}$. Tada je f dekompozibilan polinom nad $\mathbb{Z}$. To znači da je polinom f dekompozibilan kao kompozicija dva normirana polinoma.

Dokaz se može naći u [3], Teorem 12.19.

Teorem 3.1.4. Neka vrijedi

$$f(x) = x^n + ax^{n-1} + \cdots \in \mathbb{Z}[x].$$

Ako vrijedi

$$nzd(a, n) = 1,$$

onda je f nedekompozabilan polinom.

Dokaz se može naći u [3], Teorem 12.20.

3.2. Ideali

Iako Veliki Fermatov teorem nema direktnu primjenu u teoriji brojeva, pokušaj dokazivanja tog teorema doveo je do snažnog razvoja teorije brojeva. Tako je u devetnaestom

stoljeću Ernst Eduard Kummer smatrao da ima dokaz Velikog Fermatovog teorema, ali njegov dokaz je ovisio o jedinstvenosti faktorizacije za koju se pokazalo da nije ispravna. Pokušavajući ispraviti tu pogrešku, Kummer je razvio ideju o idealnim brojevima. Pojam ideala se ovdje uvodi zbog rješavanja problema nejedinstvene faktorizacije u poljima algebarskih brojeva. Navest ćemo samo osnovne tvrdnje koje su nam za to potrebne, nećemo ih dokazivati jer njihovi dokazi prelaze okvire ovoga rada. Dokazi svih navedenih teorema mogu se naći u [3].

Definicija 3.2.1. Neka je $\mathbb{K}$ polje algebarskih brojeva i $\mathcal{O}_{\mathbb{K}}$ njegov prsten cijelih brojeva. Za neprazan podskup $\mathfrak{a}$ skupa $\mathcal{O}_{\mathbb{K}}$ kažemo da je **ideal u polju algebarskih brojeva** $\mathbb{K}$ ako zadovoljava sljedeća svojstva:

(1) ako su α i β elementi skupa $\mathfrak{a}$, onda je $\alpha - \beta$ element skupa $\mathfrak{a}$,
(2) ako je α element skupa $\mathfrak{a}$ i β element skupa $\mathcal{O}_{\mathbb{K}}$, onda je $\alpha\beta$ element skupa $\mathfrak{a}$.

Teorem 3.2.2. Neka je $\mathfrak{a}$ ideal u polju algebarskih brojeva $\mathbb{K}$. Tada postoje elementi $\gamma_1, \dots, \gamma_n$ skupa $\mathfrak{a}$ za koje vrijedi da se svaki element α skupa $\mathfrak{a}$ može zapisati u obliku

$$\alpha = u_1\gamma_1 + \cdots + u_n\gamma_n,$$

gdje su $u_1, \dots, u_n$ cijeli brojevi.

Skup $\{\gamma_1, \dots, \gamma_n\}$, opisan u teoremu 3.2.2, naziva se **baza ideala $\mathfrak{a}$**.

Neka su $\mathfrak{a}$ i $\mathfrak{b}$ ideali polja algebarskih brojeva. Produkt ideala definira se kao ideal koji se sastoji od elemenata oblika $a_1b_1 + \cdots + a_jb_j$, gdje su $a_1, \dots, a_j$ elementi ideala $\mathfrak{a}$ i $b_1, \dots, b_j$ elementi ideala $\mathfrak{b}$.

Za elemente $\alpha_1, \dots, \alpha_m$ skupa $\mathcal{O}_{\mathbb{K}}$ skup svih brojeva oblika $\alpha_1\beta_1 + \cdots + \alpha_m\beta_m$, gdje su $\beta_1, \dots, \beta_m$ elementi skupa $\mathcal{O}_{\mathbb{K}}$, očito je jedan ideal, koji označavamo s

$$\mathfrak{a} = \langle \alpha_1, \dots, \alpha_m \rangle$$

te $\alpha_1, \dots, \alpha_m$ nazivamo generatorima od $\mathfrak{a}$.

Za ideal $\mathfrak{a}$ kažemo da dijeli ideal $\mathfrak{b}$ i pišemo $\mathfrak{a}|\mathfrak{b}$ ako postoji ideal $\mathfrak{c}$ takav da vrijedi

$$\mathfrak{b} = \mathfrak{a}\mathfrak{c}.$$

Za ideal $\mathfrak{a}$ kažemo da je maksimalan ideal ako je djeljiv samo sa samim sobom i s

$$\mathfrak{e} = \langle 1 \rangle.$$

Za ideal $\mathfrak{a}$ kažemo da je glavni ideal ako postoji element α prstena $\mathcal{O}_{\mathbb{K}}$ za koji vrijedi

$$\mathfrak{a} = \langle \alpha \rangle.$$

Teorem 3.2.3. Za svaki ideal $\mathfrak{a}$ postoji ideal $\mathfrak{b}$ takav da je $\mathfrak{ab}$ glavni ideal. Točnije, ideal $\mathfrak{b}$ se može odabrati tako da vrijedi

$$\mathfrak{ab} = \langle c \rangle,$$

gdje je c cijeli broj. To znači da ako je

$$\mathfrak{b} = \langle \beta_0, \dots, \beta_m \rangle$$

ideal, onda za ideal

$$\mathfrak{a}^{-1} = \langle \frac{\beta_0}{c}, \dots, \frac{\beta_m}{c} \rangle$$

vrijedi

$$\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{e}.$$

Korolar 3.2.4. Ako vrijedi

$$\mathfrak{ac} = \mathfrak{bc}$$

i

$$\mathfrak{c} \neq \langle 0 \rangle,$$

onda vrijedi

$$\mathfrak{a} = \mathfrak{b}.$$

Korolar 3.2.5. Vrijedi $\mathfrak{a}|\mathfrak{b}$ ako i samo ako vrijedi $\mathfrak{b} \subseteq \mathfrak{a}$.

Neka su $\mathfrak{a}$ i $\mathfrak{b}$ ideali polja algebarskih brojeva. Suma ideala označava se s $\mathfrak{a} + \mathfrak{b}$ i definira se kao skup koji se sastoji od elemenata oblika $a + b$, gdje je a element ideala $\mathfrak{a}$ i b element ideala $\mathfrak{b}$.

Za ideal $\mathfrak{p}$ za koji vrijedi

$$\mathfrak{p} \neq \mathfrak{e}$$

i

$$\mathfrak{p} \neq \langle 0 \rangle$$

kažemo da je prost ako za sve elemente γ i δ prstena $\mathcal{O}_{\mathbb{K}}$ iz $\gamma\delta \in \mathfrak{p}$ slijedi da je $\gamma \in \mathfrak{p}$ ili $\delta \in \mathfrak{p}$.

Lema 3.2.6. Neka su α i β elementi skupa $\mathcal{O}_{\mathbb{K}}$ i c element skupa $\mathbb{Z}\backslash\{0\}$. Tada se element α može zapisati u obliku

$$\alpha = c\beta + \gamma,$$

gdje je γ element konačnog skupa koji ovisi samo o c i ima $|c|^n$ elemenata te je n stupanj polja $\mathbb{K}$.

Lema 3.2.7. Svaki ideal ima konačno mnogo djelitelja.

Propozicija 3.2.8. Ideal $\mathfrak{p}$ za koji vrijedi

$$\mathfrak{p} \neq \mathfrak{e} \text{ i } \mathfrak{p} \neq \langle 0 \rangle$$

je maksimalan ideal ako i samo ako je prost ideal.

Sljedeći teorem je osnovni teorem ovog podpoglavlja. Dokaz ovog teorema temelji se na dokazu teorema koji govori da se svaki prirodni broj može rastaviti i na proste faktore te da je faktorizacija jedinstvena do na poredak faktora.

Teorem 3.2.9. Svaki ideal koji je različit od $\mathfrak{e}$ i od $\langle 0 \rangle$ može se prikazati kao produkt prostih ideala. Faktorizacija ideala je jedinstvena do na poredak faktora.

Za element α prstena $\mathcal{O}_{\mathbb{K}}$ kažemo da je djeljiv s idealom $\mathfrak{a}$ ako $\mathfrak{a} \mid < \alpha >$. Neka su α i β elementi skupa $\mathcal{O}_{\mathbb{K}}$ i $\mathfrak{a}|\alpha - \beta$. Tada vrijedi $\alpha \equiv \beta \pmod{\mathfrak{a}}$. Tako se dobiva relacija ekvivalencije na skupu $\mathcal{O}_{\mathbb{K}}$. Broj klasa ekvivalencije je konačan. Broj klasa modulo $\mathfrak{a}$ zovemo norma ideala $\mathfrak{a}$ i označavamo s $N(\mathfrak{a})$ ili s $N\mathfrak{a}$.

Teorem 3.2.10. Norma ideala je multiplikativna. Drugim riječima, vrijedi

$$N\mathfrak{a}N\mathfrak{b} = N(\mathfrak{a}\mathfrak{b}).$$

Neka je A prsten. **Lijevi modul** nad prstenom A ili **lijevi A-modul** je Abelova grupa $(M, +)$ takva da za sve $a,\ b \in A$ i $x, y \in M$ vrijede sljedeća svojstva:

$$(1)\ (a+b)x = ax + bx,$$

$$(2)\ a(x+y) = ax + ay.$$

Lako je provjeriti da iz definicije modula za $a \in A$, $x \in M$ direktno slijede sljedeća svojstva:

$$1x = x,$$

$$a(-x) = -ax,$$

$$0x = 0.$$

Ako umjesto prstena u definiciji modula uzmemo polje A, tada je M vektorski prostor nad A.

Neka je M A-modul. Za podskup S A-modula M kažemo da je **baza skupa** S ako vrijedi:

1. Skup S generira M kao A-modul.
2. Skup S je linearno nezavisan nad prstenom A.

U slučaju da je skup S baza za A-modul M, tada se svaki element $x \in M$ na jedinstven način može zapisati kao linearna kombinacija elemenata iz S. Za A-modul M kažemo da je **slobodan** ako ima bazu.

Propozicija 3.2.11. Neka je $\{\gamma_1, \dots, \gamma_n\}$ baza ideala $\mathfrak{a}$ i d diskriminanta polja algebarskih brojeva $\mathbb{K}$. Tada vrijedi

$$N\mathfrak{a} = \left(\frac{\Delta(\gamma_1, \dots, \gamma_n)}{d}\right)^{\frac{1}{2}}.$$

Lema 3.2.12. Za svaki ideal $\mathfrak{a}$ vrijedi $\mathfrak{a} | N\mathfrak{a}$.

Korolar 3.2.13. Za svaki prosti ideal $\mathfrak{p}$ postoji jedinstveni prosti prirodni broj p za koji vrijedi $\mathfrak{p} | p$.

Teorem 3.2.14. Neka je p prost prirodni broj čiji je rastav na produkt prostih ideala

$$< p >= \mathfrak{p}_1^{e_1} \cdot \dots \cdot \mathfrak{p}_r^{e_r}$$

te f_j stupanj ideala $\mathfrak{p}_j$, gdje je $j = 1, \dots, r$. Tada vrijedi

$$e_1 f_1 + \dots + e_r f_r = n.$$

5. ZAKLJUČAK

Proučavanje algebarskih brojeva je zanimljivo i bitno područje teorije brojeva. Ovi brojevi intrigiraju matematičare stoljećima i igraju ključnu ulogu u mnogim granama matematike, kao i u primjenama u drugim znanstvenim poljima. U ovome radu, bavili smo se temom algebarskih brojeva u teoriji brojeva. Proučavane su njihove osobine i važni koncepti povezani s njima.

Obradili smo kvadratna i algebarska polja. Ta polja imaju vrlo važnu ulogu u teoriji brojeva jer omogućuju proučavanje osobina algebarskih brojeva u općenitom kontekstu.

Nadalje, objašnjeni su algebarski cijeli brojevi. To su algebarski brojevi koji su rješenja polinoma s cjelobrojnim koeficijentima. Algebarski cijeli brojevi čine prsten koji se naziva prsten cijelih brojeva. U tom prstenu smo izučili ideale, koji omogućuju razmatranje dijeljenja i faktorizacije algebarskih cijelih brojeva.

LITERATURA

1. Chapman, Robin (1995.): Notes on Algebraic Numbers, https://empslocal.ex.ac.uk/people/staff/rjchapma/notes/algn.pdf,
2. Conrad, Keith (2002.): Factoring in Quadratic Fields, https://kconrad.math.uconn.edu/blurbs/gradnumthy/quadraticgrad.pdf,
3. Dujella, Andrej (2019.): Teorija brojeva, Školska knjiga, Hrvatska,
4. Janusz, Gerald (2005.): Algebraic Number Fields, American Mathematical Society, Sjedinjene Američke Države,
5. Stewart, Ian, Orme Tall, David (1979.): Algebraic Number Theory, Chapman and Hall, Nizozemska.