1 Kvadratna raširenja polja racionalnih brojeva

Definicija 1.1. Kvadratno raširenje polja $\mathbb{Q}$ je polje oblika

$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\},$$

pri čemu je $d \neq 1$ beskvadratan ceo broj (nije deljiv nijednim kvadratom osim sa 1).

Definicija 1.2. Element $a+b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ je integralan ako postoji moničan polinom $P(X)$ sa celobrojnim koeficijentima takav da je $P(a + b\sqrt{d}) = 0$. Skup svih ovakvih elementata polja $\mathbb{Q}[\sqrt{d}]$ zovemo prsten celih polja $\mathbb{Q}[\sqrt{d}]$.

Ako posmatramo polje racionalnih brojeva, skup svih integralnih brojeva é upravo biti skup svih celih brojeva $\mathbb{Z}$. Sledeće tvrđenje nam govori kako izgleda skup integralnih brojeva za ostala polja.

Tvrđenje 1.3. *Neka je $d \neq 1$ beskvadratan ceo broj. Tada je skup svih integralnih elemenata polja $\mathbb{Q}[\sqrt{d}]$ jednak $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ ako je $d \equiv 2, 3 \pmod 4$, i $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \{a + b\frac{1+\sqrt{d}}{2} \mid a, b \in \mathbb{Z}\}$ ako je $d \equiv 1 \pmod 4$.*

U skupu celih brojeva $\mathbb{Z}$, znamo da su jedini elementi koji imaju inverz 1 i -1. Uopšte, element $\varepsilon \in \mathbb{Z}[\alpha]$ zovemo jediničnim ako postoji $\varepsilon' \in \mathbb{Z}[\alpha]$ za koje je $\varepsilon\varepsilon' = 1$.

Primer 1.4. *Prsten $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ ima jedinice $1, -1, i, -i$. Ovaj prsten zovemo i Gausov prsten celih brojeva, a njegovi elementi su Gausovi celi brojevi (kompleksni brojevi sa celobrojnim koordinatama).*

Kao kod kompleksnih brojeva, možemo definisati normu i konjugat elementa u $\mathbb{Q}[\sqrt{d}]$:

Definicija 1.5. Konjugat elementa $z = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ je $\overline{z} = a - b\sqrt{d}$. Norma elementa $z = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ je $N(z) = |z \cdot \overline{z}| = |a^2 - db^2|$.

Budući je d ceo broj, norma nekog elementa je uvek prirodan broj. I pošto je $N(z_1z_2) = N(z_1)N(z_2)$, možemo pomoću norme naći jedinice prstena celih:

Tvrđenje 1.6. *Element prstena celih $a + b\sqrt{d}$ polja $\mathbb{Q}[\sqrt{d}]$ je jediničan ako i samo ako ima normu 1.*

1. Dokazati da za element $x + y\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ norme 2 važi $x^2 = 3y^2 - 2$.

Po definiciji, $N(x + y\sqrt{3}) = |x^2 - 3y^2| = 2$, pa je $x^2 - y^2 = \pm 2$. Sada, $3|3y^2$, a kvadratni ostaci modulo 3 su 0 i 1, pa $x^2 - 3y^2$ može biti ili 0 ili 1 modulo 3. Prema tome, $x^2 - y^2 = -2$, tj. $x^2 = y^2 - 2$.

2 Deljenje u $\mathbb{Z}[i]$

Kao i u prstenu celih, i u prstenu $\mathbb{Z}[i]$ postoji Euklidovo deljenje: Ako su $x, y \in \mathbb{Z}$ takvi da je $N(x) > N(y)$, tada postoje brojevi $q, r \in \mathbb{Z}[i]$ takvi da je $x = qy + r$ i $N(r) < N(y)$. Broj q je količnik, a r je ostatak pri deljenju x sa y. Kažemo da je x deljivo sa y ako je ostatak pri deljenju x sa y jednak nuli. Pošto relacija $\leqslant$ ne može da se proširi sa skupa realnih brojeva na skup kompleksnih brojeva, upoređuju se norme.

U $\mathbb{Z}[i]$ možemo definisati najveći zajednički delilac slično kao i u $\mathbb{Z}$, samo što sada kažemo da je d najveći zajednički delilac a i b ako je d najveće norme među svim brojevima koji dele i a i b, i pišemo $d = (a, b)$. Primetimo, $1, -1, i, -i$ dele svaki Gausov ceo broj, pa je najveći zajednički delilac neka dva broja jedinstven do na množenje jediničnim elementom.

Euklidski algoritam postoji i u $\mathbb{Z}[i]$, i ide isto kao u $\mathbb{Z}$: Neka je $N(a) > N(b)$. Kada podelimo a sa b, dobijamo

$$a = bq_1 + r_1,$$

gde je $N(r_1) < N(b)$. Zatim delimo b sa r_1:

$$b = r_1 q_2 + r_2,$$

gde je $N(r_2) < N(r_1)$. Sada delimo r_1 sa r_2, i tako delimo uzastopne ostatke, i pošto norme ostataka čine strogo opadajući niz prirodnoh brojeva, u jednom trenutku ćemo dobiti da r_{i+1} deli r_i. Sada uzmemo poslednji nenula ostatak, i to je najveći zajednički delilac a i b. Za dva broja kažemo da su uzajamno prosti ako je norma njihovog najvećeg zajdničkog delioca jednaka 1.

1. Odrediti najveći zajednički delilac brojeva $11 + 7i$ i $18 - i$.

Pošto je $N(11+7i) = |121+49| = 170 < N(18-i) = |324+1| = 325$, delimo $11+7i$ sa $18-i$: Tražimo q_1 i r_1 takve da je

$$18 - i = (11+7i)q_1 + r_1,$$

i $N(r_1) < N(11+7i) = 170$. Da bismo našli ove brojeve, uočimo sledeće: ako podelimo obe strane jednakosti $a = bq + r$ sa b, imamo da je $\frac{a}{b} = q + \frac{r}{b}$, pri čemu je $N(\frac{r}{b}) < 1$. Dakle, dovoljno je naći $q \in \mathbb{Z}[i]$ takvo da je $N(\frac{a}{b} - q) < 1$, tj. kompleksan broj q sa celobrojnim koeficijentima koji je najbliži razlomku (takvo q ne mora biti jedinstveno, može bilo koje takvo da se uzme, samo mora norma razlike između q i $\frac{a}{b}$ da bude manja od 1).

Dakle, imamo

$$\frac{18-i}{11+7i} = \frac{(18-i)(11-7i)}{170} = \frac{191}{170} - \frac{137}{170}i.$$

U ovom slučaju biramo $q_1 = 1 - i$. Sada se r_1 nalazi lako: $18 - i = (11 + 7i)(1-i) + r_1$, pa je $r_1 = 3i$. Sada delimo $11+7i$ sa $3i$, i tražimo q_2 i r_2:

$$\frac{11+7i}{3i} = \frac{7}{3} - \frac{11}{3}i,$$

pa uzimamo $q_2 = 2-4i$, i imamo $11+7i = 3iq_2 + r_2 = 3i(2-4i) + r_2$, odakle je $r_2 = -1+i$. Sada delimo $3i$ sa $-1+i$:

$$\frac{3i}{-1+i} = \frac{3-3i}{2} = \frac{3}{2} - \frac{3}{2}i,$$

pa uzimamo $q_3 = 1 - i$, i imamo $3i = (-1+i)(1-i) + r_3$, pa je $r_3 = 3i - (-1+i)(1-i) = i$. Pošto je $N(i) = 1$ ovde stajemo: i je jedinica, zbog čega deli sve Gausove cele brojeve, pa bi sledeći ostatak bio jednak nuli. Ovo smo takođe mogli da vidimo jer je niz normi ostataka strogo opadajući niz prirodnih brojeva. Dakle, $(11+7i, 18-i) = i$. Pošto je $N(i) = 1$, brojevi $11+7i$ i $18-i$ su uzajamno prosti.

2. Odrediti najveći zajednički delilac brojeva $11+3i$ i $1+8i$.

Kako je $N(11+3i) = 130 > 65 = N(1+8i)$, delimo $11+3i$ sa $1+8i$:

$$\frac{11+3i}{1+8i} = \frac{35-85i}{65}.$$

Najbliži Gausov ceo je $1-i$, pa je $11+3i=(1+8i)(1-i)+(2-4i)$. Sada:

$$\frac{1+8i}{2-4i}=\frac{-30+20i}{20}.$$

Ovome je najbliže $-1+i$, i imamo $1-8i=(2-4i)(-1+i)+(-1+2i)$. Opet delimo:

$$\frac{2-4i}{-1+2i}=-2.$$

Kako je $2-4i=(-1+2i)\cdot 2+0$, ovde stajemo. Poslednji nenula ostatak u ovom nizu je $-1+2i$, i zaključujemo da je $(11+3i,1+8i)=-1+2i$. Pošto je $N(-1+2i)=5$, brojevi $11+3i$ i $1+8i$ nisu uzajamno prosti.

3. Odrediti najveći zajednički delilac brojeva $13+2i$ i $4+5i$.

4. Odrediti najveći zajednički delilac brojeva $12+4i$ i $9-2i$.

3 Prosti elementi

Kao i u skupu celih brojeva, i u proizvoljnom prstenu sa jedinicom možemo uvesti koncep prostog broja:

Definicija 3.1. Element prstena $p\in R$ je prost ako i samo ako je deljiv samo sa 1 i sa samim sobom (do na množenje invertibilnih elementata).

Za dva elementa $x,y\in R$ kažemo da su asocirana ako postoji jedinični (invertibilni) element ε takav da je $x=\varepsilon y$.

Dakle, u skupu celih brojeva $\mathbb{Z}$, prost broj p je jedino deljiv sa $-p,-1,1$ i p. Kao i u skupu celih brojeva, možemo se pitati da li važi osnovna teorema aritmetike u prstenu oblika $\mathbb{Z}[\sqrt{d}]$ (tj. da li se svaki element $a+b\sqrt{d}$ može na jedinstven način predstaviti kao proizvod prostih elemenata). Ona će važiti u $\mathbb{Z}[i]$, ali ne i u svim prstenima ovog oblika (u nekim prstenima ovakva faktorizacija nije jedinstvena). Važe sledeće teoreme:

Teorema 3.2. *Element $x\in\mathbb{Z}[\sqrt{d}]$ je prost ako je $N(x)$ prost ceo broj*

Proof. Zaista, ako y deli x, tada norma y deli normu x, pa pošto su norme prirodni brojevi, i norma x je prost broj, ili je y norme 1 (dakle jedinični element), ili je iste norme kao i x. Ako su iste norme, tada je $\frac{x}{y}$ norme 1, dakle opet su asocirani. □

Teorema 3.3. *Neka je p prost ceo broj. Tada je p prost element $\mathbb{Z}[\sqrt{d}]$ ako i samo ako d nije kvadratni ostatak modulo p.*

Primer 3.4. *Broj 5 je prost element u $\mathbb{Z}[\sqrt{2}]$, pošto 2 nije kvadratni ostatak modulo 5 (tj. $\left(\frac{2}{5}\right) = -1$).*

U skupu Gausovih celih, možemo nabrojati proste brojeve. Prvo, važi sledeće:

Lema 3.5. *Neka je p prost prirodan broj veći od 2. Tada se p može prikazati kao zbir $p = a^2 + b^2$ ako i samo ako je $p \equiv 1 \pmod 4$.*

Ovo sada

Teorema 3.6. *Prosti elementi u $\mathbb{Z}[i]$ su, do na asocijaciju (množenje sa 1, -1, i, $-i$), svi elementi oblika:*

1. *Prost ceo broj p koji je kongruentan 3 modulo 4. Njegova norma je p^2, Gausov ceo broj $a + bi$ čija je norma $a^2 + b^2 = p$ ne postoji, jer p ne zadovoljava uslov prethodne leme.*

2. *Gausovi celi $a+bi$ čija norma a^2+b^2 je prost broj (po prethodnoj lemi, taj prost broj mora biti kongruentan 1 modulo 4, osim u slučaju kada je $N(a + bi) = 2$).*

3. *Gausovi celi brojevi norme 2 (dakle $1 + i$, $1 - i$,...).*

1. Odrediti faktorizaciju $3 + 4i \in \mathbb{Z}[i]$ na proste.

Norma ovog broja je $N(3 + 4i) = 25 = 5^2$. Ako je p prost Gausov ceo koji deli $3+4i$, njegova norma mora deliti normu $3+4i$, pa može biti 5 ili 25 (elementi norme 1 su jedinice). U slučaju da $3 + 4i$ ima prost faktor norme 25 to naravno znači da je on sam prost, pošto tada količnik ima normu 1, tj. $3 + 4i = \varepsilon p$, pa su asocirani.

Sada ćemo izbrojati proste faktore sa normom 5 (elementi norme 5 su svi prosti po teoremi), i videti da li je $3+4i$ deljiv sa nekim: $1+2i$, $-1-2i$, $2-i$, $-2+i$; i $-1+2i$, $1-2i$, $2+i$, $-2-i$. Prva četiri su međusobno asocirana kao i poslednja četiri. Ovde je dovoljno da uzmemo predstavnike asociranih elemenata i da vidimo da li je proizvod asociran sa $3+4i$. Prema tome, $(1+2i)(1-2i)=5$, $(1+2i)^2=-3+4i$ i $(1-2i)^2=-3-4i$, i vidimo da je

$$3+4i=-1(1-2i)^2.$$

2. Odrediti faktorizaciju $9+7i\in\mathbb{Z}[i]$ na proste.

Norma elementa $9+7i$ je $N(9+7i)=130=2\cdot 5\cdot 13$. Dakle prosti fakori mogu biti norme 2, 5 ili 13. Do na asocijaciju, ti prosti faktori su:

1. Norme 2: $1+i$;
2. Norme 5: $1+2i$ i $1-2i$;
3. Norme 13: $3+2i$ i $3-2i$.

Vidi se da je $\frac{9+7i}{1+i}=8-i$. Zatim, kada gledamo deljivost $8-i$ sa faktorima norme 5, dobijamo da je $\frac{8-i}{1+2i}=\frac{6-17i}{5}\notin\mathbb{Z}[i]$, i $\frac{8-i}{1-2i}=2+3i$. Dakle, imamo da je $9+7i=(1+i)(1-2i)(2+3i)$

3. Odrediti faktorizaciju $12+5i\in\mathbb{Z}[i]$ na proste.

4. Neka je $p>3$ prost prirodan broj. Kada je p prost element $\mathbb{Z}[\sqrt{p-2}]$?

Po jednoj od gornjih teorema, p je prosto ako i samo ako $p-2$ nije kvadrat modulo p. Tražimo kada je $\left(\frac{p-2}{p}\right)=-1$:

$$\left(\frac{p-2}{p}\right)=\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}=(-1)^{\frac{p^2+4p-5}{8}}$$

Ovaj izraz je jednak -1 ako i samo ako 2 ne deli $\frac{p^2+4p-5}{8}$, tj. ako i samo ako 16 ne deli p^2+4p-5.

5. Naći sve proste $p \in \mathbb{Z}$ koji su prosti i u $\mathbb{Z}[\sqrt{2}]$.

Kao i u prethodnom zadatku, gledamo kada je $\left(\frac{2}{p}\right) = -1$. No,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

pa gledamo kada 16 ne deli $(p-1)(p+1)$. Ako je $p = 4k+1$, tada je $p^2-1 = 8k(2k+1)$, pa $16 \nmid p^2-1$ ako i samo ako $2 \nmid k$ (dakle $k = 2n+1$), tj. p je oblika $8n+5$. Ako je p oblika $4k+3$, tada je $p^2-1 = 8(k+1)(2k+1)$, pa $16 \nmid p^2-1$ ako i samo ako $2 \nmid k+1$ (dakle, $k = 2n$), tj. p je oblika $8n+3$.