Algebarska teorija brojeva

Filip Najman

Prirodoslovno matematički fakultet, Matematički odsjek
2025/2026

Sadržaj

Poglavlje 1

Uvod

Glavna motivacija za algebarsku teoriju brojeva nam je rješavanje Diofanstkih jednadžbi, kao što su npr. $y^2+3=x^3$, $x^2+y^2=z^2$, $x^n+y^n=z^n$, itd. Ideja je ovakve jednadžbe *faktorizirati*:

$$(y+\sqrt{-2})(y-\sqrt{-2})=x^3, \quad (x+iy)(x-iy)=z^2,$$

$$(x-y)(x-\zeta_n y)(x-\zeta_n^2 y)\dots(x-\zeta_n^{n-1}y)=z^n, \quad \zeta_n=e^{\frac{2\pi i}{n}}.$$

Iako tražimo rješenja nad $\mathbb{Z}$, faktorizacija se odvija nad proširenjima od $\mathbb{Z}$. Faktoriziramo u $\mathbb{Z}\subset\mathcal{O}$, gdje je $\mathcal{O}$ *red*(ili poredak, eng. order), veći prsteni koji sadrži $\mathbb{Z}$.

Pojmovi grupa, prstena, ideala s kojima ste se susretali u algebri i algebarskim strukturama zapravo imaju povijesnu motivaciju iz teorije brojeva. Algebarsku teoriju brojeva možemo smatrati teorijom brojeva "u proširenjima od $\mathbb{Z}$". Vrijedit će sljedeće analogije:

$$\begin{aligned}
\mathbb{Z} &\longleftrightarrow \mathbb{Z}\subseteq\mathcal{O} - \text{ red}\\
\mathbb{Q} &\longleftrightarrow \mathbb{Q}\subseteq K - \text{polje algebarskih brojeva, tj. konačno proširenje od } \mathbb{Q}\\
a\mid b &\longleftrightarrow a\mid b \text{ u } \mathcal{O} \text{ znači } \exists c\in\mathcal{O} \text{ t.d. } b=ac,\\
\{\pm 1\}=\mathbb{Z}^\times &\longleftrightarrow \mathcal{O}^\times - \text{ obično beskonačna grupa,}\\
\text{prosti brojevi} &\longleftrightarrow \begin{cases}\text{prosti elementi, } 0\neq p\notin\mathcal{O}^\times, p|ab\Rightarrow p|a \text{ ili } p|b\\ \text{ireducibilni elementi, } 0\neq p\notin\mathcal{O}^\times, q|p\Rightarrow q\in\mathcal{O}^\times \text{ ili } q=up \text{ i } u\in\mathcal{O}^\times.\end{cases}
\end{aligned}$$

Osnovni teorem aritmetike (jedinstvena fakt. na proste br.) $\longleftrightarrow$? (općenito ne vrijedi).

Predznanje za koje se pretpostavlja da ga znate na kolegiju: gradivo iz Algebarskih struktura, Algebre 1 i 2; grupe, prsteni, ideali (prosti, maksimalni), domene glavnih ideala, domene jedinstvene faktorizacije, Kineski teorem o ostacima, proširenja polja, Galoisova teorija (iako ćemo nju ponoviti).

1.1 Uvod u faktorizaciju

Definicija 1.1.1

Definiramo da je prsten D *Euklidova domena* ako postoji funkcija $\varphi : D \setminus \{0\} \to \mathbb{N}$ takva da:

(i) $\varphi(z) \geq 0$, $\forall z \in D \setminus \{0\}$,

(ii) za sve $a \in D$ i $b \in D \setminus \{0\}$, postoje $g, r \in D$ takvi da $a = gb + r$, gdje je $r = 0$ ili $r \neq 0$ i $\varphi(r) < \varphi(b)$.

Propozicija 1.1.2

U integralnoj domeni D, svaki prost element je ireducibilan.

Dokaz. Pretpostavimo da $p \in D$ *nije* ireducibilan. Po definiciji to znači da možemo p napisati kao:

$$p = ab,$$

gdje su $a, b \in D$, a niti a niti b nisu invertibilni elementi u D.

Budući da je p prost, ako $p \mid ab$, tada prema definiciji imamo:

$$p \mid a \quad \text{ili} \quad p \mid b.$$

Bez smanjenja općenitosti, pretpostavimo da $p \mid a$. To znači da postoji element $d \in D$ takav da je $a = pd$. Uvrstimo $a = pd$ u $p = ab$:

$$p = (pd)b = p(db).$$

Budući da smo u integralnoj domeni i $p \neq 0$, možemo podijeliti obje strane s p, što daje:

$$1 = db.$$

Dakle, d i b su invertibilni elementi u D, što je kontradikcija s neinvertibilnošću od b. □

Sjetimo se karakterizacije prostih/ireducibilnih elemenata.

Teorem 1.1.3

Neka je D integralna domena i $0 \neq x \notin D^\times$.

1. x je ireducibilan ako i samo ako je (x) maksimalan u skupu glavnih ideala. Ideal (x) je maksimalan (u skupu svih ideala) ako i samo ako je $D/(x)$ polje.

2. x je prost ako i samo ako je (x) prost, ako i samo ako je $D/(x)$ integralna domena.

Dokaz. Dokazano na Algebarskim strukturama. □

Definicija 1.1.4

Prsten R se naziva **Noetherin prsten** ako zadovoljava jedno od sljedeća tri ekvivalentna svojstva:

1. Svaki ideal u R je konačno generiran.
2. Svaki uzlazni lanac ideala u R stabilizira se. To znači da za svaki niz ideala $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ postoji indeks n takav da za sve $m \geq n$ vrijedi $I_n = I_m$.
3. U svakom skupu ideala postoji maksimalan (u tom skupu), tj. ideal koji nije sadržan ni u jednom drugom.

Primjer prstena koji nije Noetherin: polinomi u beskonačno mnogo varijabli.

Definicija 1.1.5

Noetherin prsten koji je integralna domena zove se Noetherina domena.

Propozicija 1.1.6

Ako je D Noetherina domena, svaki ne-nul element se može napisati kao produkt ireducibilnih elemenata.

Dokaz. Pretpostavimo suprotno, te promotrimo skup S glavnih ideala (y), gdje se y ne može faktorizirati kao produkt ireducibilnih. Neka je (x) maksimalan ideal u tom skupu (takav postoji jer je D Noetherin)

Sada x nije ireducibilan, pa se može zapisati kao $x = a \cdot b$, gdje su a, b neinvertibilni, te se barem jedan od njih (bez smanjenja općenitosti a) ne može zapisati kao produkt ireducibilnih. Međutim sada imamo

$$(x) \subsetneq (a), \quad a \in S,$$

što je kontradikcija s maksimalnošću od (x). □

Primjer 1.1.7

U integralnoj domeni D postoji jedinstvena faktorizacija na ireducibilne ako i samo ako je svaki ireducibilan element prost u D.

Dokaz. Pokažimo samo jedan smjer, drugi ostavljamo za DZ. Neka je $\pi \in R$ ireducibilan. Razmotrimo glavni ideal (π). Ako je $(\pi) \subseteq (a)$ za neki a, onda vrijedi $\pi = ar$ za neki r. Budući da je π ireducibilan, ili je a jedinica ili je r jedinica; stoga vrijedi $(a) = (\pi)$ ili $(a) = R$. Dakle, (π) je maksimalan (nenul) ideal, a samim time i prost. Prema tome, π je prost element. □

Propozicija 1.1.8

Vrijedi:

(a) Svaka Euklidova domena je DGI (domena glavnih ideala),

(b) Svaka DGI je DJF (domena jedinstvene faktorizacije).

Dokaz. (a) Neka je D Euklidova domena s pripadajućom funkcijom φ, te pretpostavimo da $I \neq 0$ ideal u D. Odaberimo x takav da je $\varphi(x)$ jednak minimumu skupa $\{\varphi(a) : a \in I \backslash \{0\}\}$. Očito je da $(x) \subseteq I$.

Pokažimo obrnutu inkluziju. Neka je $a \in I$. Tada postoje $g, r \in D$ takvi da $a = gx + r$, gdje je $r = 0$ ili $r \neq 0$ i $\varphi(r) < \varphi(x)$. Kako je $r = a - gx \in I$, očito je da druga mogućnost nije moguća jer bi $\varphi(r)$ bila manja od $\varphi(x)$, što je u suprotnosti s definicijom od x. Dakle $a = gx \in (x)$, dakle $I \subset (x)$.

(b) Postojanje faktorizacije na ireducibilne faktore slijedi iz prethodne propozicije.
Dokažimo jedinstvenost rastava. Da su ireducibilni elementi prosti slijedi iz prethodnog primjera, a kad su svi ireducibilni elementi prosti, standardni argument za jedinstvenost faktorizacije vrijedi: ako

$$u \cdot p_1 p_2 \cdots p_n = v \cdot q_1 q_2 \cdots q_m$$

gdje su u, v invertibilni i svi p_i, q_j ireducibilni (dakle prosti), tada zbog svojstva prostosti možemo, nakon moguće permutacije i zamjene elemenata asociranim, spariti svaki p_i s nekim q_j. Stoga su faktorizacije jedinstvene do reda i asociranosti. □

Kombinirajući (i) i (ii) zaključujemo da je svaka DGI DJF.

1.2 Gaussovi cijeli brojevi

Proučavamo jednadžbu $x^2 + y^2 = z^2$, gdje su $x, y, z \in \mathbb{Z}$. Promotrimo polje Gaussovih racionalnih brojeva

$$\mathbb{Q}[i] = \mathbb{Q} + i\mathbb{Q} = \{x + iy \mid x, y \in \mathbb{Q}\}.$$

Za bilo koja dva Gaussova racionalna broja $\frac{x_1+iy_1}{x_2+iy_2}$, rezultat je:

$$\frac{x_1 + iy_1}{x_2 + iy_2} = \frac{x_1x_2 + y_1y_2 + i(x_2y_1 - x_1y_2)}{x_2^2 + y_2^2}.$$

Prsten Gaussovih cijelih brojeva je definiran kao

$$\mathbb{Z}[i] = \{x + iy \mid x, y \in \mathbb{Z}\}.$$

Funkcija norme $N : \mathbb{Z}[i] \to \mathbb{Z}$ definirana je s $N(x + iy) = x^2 + y^2 = |x + iy|^2$. Neka je $\alpha \in \mathbb{Q}[i]$, tada je norma $N(\alpha) = \alpha \cdot \bar{\alpha}$, i vrijedi:

$$N(ab) = N(a)N(b), \quad a, b \in \mathbb{Q}[i]$$

Vrijedi i $N(\mathbb{Z}[i]) \subseteq \mathbb{Z}$.

Lema 1.2.1

Vrijedi:

(i) Za $x \in \mathbb{Z}[i]$, vrijedi $x \in \mathbb{Z}[i]^\times \Leftrightarrow N(x) = 1$.

(ii) $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Dokaz. (i) Ako $x \in \mathbb{Z}[i]^\times$, tada postoji $y \in \mathbb{Z}[i]$ tako da $x \cdot y = 1$. Prema tome:

$$N(x \cdot y) = N(x)N(y) = N(1) = 1.$$

Norme $N(x)$ i $N(y)$ su nenegativni cijeli brojevi, stoga mora vrijediti $N(x) = 1$.

Obrnuto, Ako je

$$1 = N(a + bi) = a^2 + b^2 = (a + bi)(a - bi),$$

zaključujemo da je $(a + bi)^{-1} = a - bi$.
(ii) Očito je da $\{\pm 1, \pm i\} \subseteq \mathbb{Z}[i]^\times$. Dokažimo obratnu inkluziju: iz (i) vrijedi $N(a + bi) = 1$

$$\begin{aligned} \Rightarrow \quad a^2 + b^2 = 1 \quad a, b \in \mathbb{Z} \quad &\Rightarrow (a, b) \in \{(\pm 1, 0), (0, \pm 1)\} \\ &\Rightarrow \quad a + bi \in \{\pm 1, \pm i\} \end{aligned}$$

□

Propozicija 1.2.2

$\mathbb{Z}[i]$ je Euklidova domena.

Dokaz. Očito je da je $N(z) = |z|^2 \geq 0$ za sve $z \in \mathbb{Z}[i]$. Ako su $a, b \in \mathbb{Z}[i]$ i $b \neq 0$, tada vrijedi:

$$\frac{a}{b} \in \mathbb{Q}(i) \Rightarrow \exists g \in \mathbb{Z}[i] \text{ takav da } \left|\operatorname{Re}\frac{a}{b} - \operatorname{Re} g\right| \leq \frac{1}{2} \text{ i } \left|\operatorname{Im}\frac{a}{b} - \operatorname{Im} g\right| \leq \frac{1}{2}.$$

$$\begin{aligned} &\Rightarrow \left|\frac{a}{b} - g\right|^2 = \left|\left(\operatorname{Re}\frac{a}{b} - g\right) + i \operatorname{Im}\left(\frac{a}{b} - g\right)\right|^2 \\ &= \left|\operatorname{Re}\frac{a}{b} - \operatorname{Re} g\right|^2 + \left|\operatorname{Im}\frac{a}{b} - \operatorname{Im} g\right|^2 \\ &\leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \text{ (množimo s } |b|^2) \\ &\Rightarrow |a - gb|^2 \leq \frac{|b|^2}{2}, \text{ tj. } N(a - gb) \leq \frac{N(b)}{2}. \end{aligned}$$

Označimo $a - gb = r$. Sada imamo $a = gb + (a - gb) = gb + r$, gdje je $r \in \mathbb{Z}[i]$.

Ako $r \neq 0$, tada vrijedi $N(r) \leq \frac{N(b)}{2} < N(b)$ (vrijedi $N(b) > 0$ jer je $b \neq 0$). □

Korolar 1.2.3

$\mathbb{Z}[i]$ je domena jedinstvene faktorizacije.

Rješenje jednadžbe $x^2 + y^2 = z^2$, gdje su $x, y, z \in \mathbb{Z}$ (cijeli brojevi) nazivamo *Pitagorinom* (ili Pitagorejskom) trojkom. Primijetimo

$$NZD(x, y, z) = 1 \Leftrightarrow NZD(x, y) = NZD(x, z) = NZD(y, z) = 1.$$

Ako je najveći zajednički djelitelj od x, y i z jednak 1, tada kažemo da je Pitagorina trojka *primitivna*.

Promotrimo svojstva Pitagorinih trojki. Primijetimo da kvadrat bilo kojeg broja pri dijeljenju s 4 daje ostatak 0 ili 1. Zbog toga, ako su x i y različite parnosti, tada je z neparan.

Jednadžba $(x+yi)(x-yi) = z^2$ faktorizira se u $\mathbb{Z}[i]$ (Gaussovi cijeli brojevi), tako da su Gaussovi cijeli brojevi prirodno mjesto za promatranje Pitagorinih trojki.

Neka je (x, y, z) primitivna Pitagorina trojka:

$$x^2 + y^2 = z^2, \text{ tj. } (x + iy)(x - iy) = z^2, \quad (x, y) = (y, z) = (x, z) = 1,$$

Neka je $((x + iy), (x - iy)) = \pi$.

$$\begin{aligned} &\Rightarrow \pi | 2x, \quad \pi | 2iy \\ &\Rightarrow N(\pi) \left| 4x^2, N(\pi) \right| 4y^2 \\ &\Rightarrow N(\pi) \mid 4 \end{aligned}$$

Također, $N(\pi) \mid N(z) = z^2$, što je neparno.

$$\begin{aligned} \Rightarrow \quad & N(\pi) \mid 1 \quad \Rightarrow N(\pi) = 1 \\ \Rightarrow \quad & ((x + iy), (x - iy)) = 1 \\ \Rightarrow \quad & x + iy = v(m + iu)^2, m, u \in \mathbb{Z}, v \in \mathbb{Z}[i]^\times = \{\pm 1\} \\ \Rightarrow \quad & x + iy = v\left(m^2 + 2mui - u^2\right) \\ \Rightarrow \quad & \{x, y\} = \left\{\pm\left(m^2 - u^2\right), \pm 2mu\right\} \\ \Rightarrow \quad & z = \pm\left(m^2 + u^2\right), (m, u) = 1. \end{aligned}$$

1.3 Neki primjeri u drugim prstenovima

Primjer 1.3.1

Dokažite da prsten $\mathbb{Z}[\sqrt{-5}]$ nije DGI (domena glavnih ideala).

Rješenje: Vrijedi $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Ako pokažemo da su $2, 3, 1 \pm \sqrt{-5}$ ireducibilni, to znači da postoji više različitih faktorizacija u ireducibilne u $\mathbb{Z}[\sqrt{-5}]$.

Definirajmo normu $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ sa:

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

Tvrdnja: $N(xy) = N(x)N(y)$ za sve $x, y \in \mathbb{Z}[\sqrt{-5}]$.
Dokaz: Računski, DZ. □
Primjeri:

$$N(2) = 4, \quad N(3) = 9, \quad N(1+\sqrt{-5}) = N(1-\sqrt{-5}) = 6.$$

Tvrdnja: $x \in \mathbb{Z}[\sqrt{-5}]^\times \iff N(x) = 1$ i $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$.
Dokaz: Neka je: $x = a + b\sqrt{-5}$.
$\boxed{\Longleftarrow}$ Iz definicije vrijedi:

$$a^2 + 5b^2 = 1 \quad \iff \quad (a + b\sqrt{-5})(a - b\sqrt{-5}) = 1$$

Dakle, ako $N(x) = 1$, tada je x multiplikativno invertibilan i pripada $\mathbb{Z}[\sqrt{-5}]^\times$.
$\boxed{\Longrightarrow}$ Neka je $x \in \mathbb{Z}[\sqrt{-5}]^\times$

$$\begin{aligned} &\Longrightarrow \exists y \in \mathbb{Z}[\sqrt{-5}]^\times \text{t.d.} N(xy) = N(x)N(y) = N(1) \\ &\Longrightarrow N(x) = 1 \text{ jer } N(x), N(y) \in \mathbb{N}_0. \end{aligned}$$

Odmah zaključujemo da su jedini elementi s normom 1 upravo ± 1. □
Tvrdnja: $2, 3, 1 \pm \sqrt{-5}$ su ireducibilni elementi.
Dokaz: Pretpostavimo suprotno, tj. $2 = ab$, gdje $a, b \notin \mathbb{Z}[\sqrt{-5}]^\times$. Sada imamo:

$$N(2) = 4 = N(a)N(b),$$

što implicira da $N(a) = N(b) = 2$. Neka je $a = x_1 + y_1\sqrt{-5}$, tada:

$$x_1^2 + 5y_1^2 = 2$$

No, rješavanje ove jednadžbe mod 5 pokazuje da nema rješenja jer $x_1^2 \equiv 2 \pmod 5$ nije moguće. Analogno se dokaže i za $3, 1 \pm \sqrt{-5}$. □

Primijetimo da $2, 3, 1 \pm \sqrt{-5}$ nisu prosti elementi u $\mathbb{Z}[\sqrt{-5}]$: Pretpostavimo da je 2 prost. Vrijedi

$$2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5}) \Longrightarrow 2|(1+\sqrt{-5}) \text{ ili } 2|(1-\sqrt{-5})$$

$$\Longrightarrow 4 = N(2) \mid N(1 \pm \sqrt{-5}) = 6. \Rightarrow\!\Leftarrow$$

□.

Definicija 1.3.2

Neka je R prsten, te neka su $a_1, a_2, \ldots, a_n \in R$. *Najveći zajednički djelitelj* elemenata $a_1, a_2, \ldots, a_n$ u prstenu R je element $d \in R$, koji zadovoljava:

(a) $d \mid a_i$ za sve i.

(b) Ako neki element $c \in R$ dijeli svaki element a_i, tada vrijedi $c \mid d$.

Primjer 1.3.3

Elementi 6 i $2 + 2\sqrt{-5}$ u prstenu $\mathbb{Z}[\sqrt{-5}]$ nemaju najveći zajednički djelitelj.

Rješenje:

$$N(6) = 6^2 = 36, \quad N(2(1+\sqrt{-5})) = N(2) \cdot N(1+\sqrt{-5}) = 4 \cdot 6 = 24.$$

Pretpostavimo da $d = \gcd(6, 2(1+\sqrt{-5}))$ postoji, tj. da je d najveći zajednički djelitelj elemenata 6 i $2(1+\sqrt{-5}))$ u $\mathbb{Z}[\sqrt{-5}]$. Tada bi po (a) vrijedilo da $d \mid 6$ i $d \mid 2(1+\sqrt{-5})$. Vrijedi

$$2 \mid 6, \quad 2 \mid 2(1+\sqrt{-5}) \overset{(b)}{\Longrightarrow} 2|d,$$

$$(1+\sqrt{-5}) \mid 6, \quad (1+\sqrt{-5}) \mid 2(1+\sqrt{-5}) \overset{(b)}{\Longrightarrow} (1+\sqrt{-5})|d.$$

Napišimo $d = \pm y(1+\sqrt{-5})$, gdje $y|2$. Lako vidimo, promatrajući normu, da je 2 ireducibilan, pa zaključujemo da je $y = \pm 1$ ili ± 2. Pošto $2|d$, vidimo da je $y \neq \pm 1$, jer $2 \nmid (1+\sqrt{-5})$.

Pretpostavimo sada da je $d = \pm 2(1+\sqrt{-5})$.

$$\Longrightarrow 2(1+\sqrt{-5}) \mid 6 \Longrightarrow 24 = N(2(1+\sqrt{-5})) \mid N(6) = 36 \Rightarrow\Leftarrow .$$

Primjer 1.3.4

$\mathbb{Z}[\sqrt{3}]^\times$ je beskonačna.

Rješenje: Definiramo normu kao:

$$N(a+b\sqrt{3}) = (a+b\sqrt{3})(a-b\sqrt{3}) = a^2 - 3b^2.$$

Lako se dokaže, kao i prije da je element invertibilan ako i samo ako njegova norma iznosi 1, tj. $N(a+b\sqrt{3}) = 1$ (lako se vidi da je $N(a+b\sqrt{3}) = -1$ nemoguće). Pellova jednadžba $x^2 - 3y^2 = 1$ ima beskonačno mnogo rješenja. Generalna rješenja Pellove jednadžbe su:

$$x_n + y_n\sqrt{3} = (x_1 + y_1\sqrt{3})^n,$$

gdje je $(x_1, y_1) = (2, 1)$ prvi član. Vrijedi

$$N(x_1 + y_1\sqrt{3})^n = (x_1 + y_1\sqrt{3})^n(x_1 - y_1\sqrt{3})^n = 1,$$

pa je $(x_1 + y_1\sqrt{3})^n \in \mathbb{Z}[\sqrt{3}]^\times$. □
Može se pokazati i više, tj. da je $\mathbb{Z}[\sqrt{3}]^\times = \langle -1, 2 + \sqrt{3}\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Primjer 1.3.5

Odredite koji su od elemenata $1+i$, $2-7i$, 5, 7 i $12i$ ireducibilni u prstenu $\mathbb{Z}[i]$.

Rješenje:

- **Element** $1 + i$**:**
$$N(1 + i) = 1^2 + 1^2 = 2.$$
Norma 2 je prosta. Dakle, $1 + i$ je ireducibilan.

- **Element** $2 - 7i$**:**
$$N(2 - 7i) = 2^2 + (-7)^2 = 4 + 49 = 53.$$
Norma 53 je prosta. Dakle, $2 - 7i$ je ireducibilan.

- **Element** 5**:**
$$N(5) = 5^2 + 0^2 = 25.$$
Možemo napisati $5 = (2+i)(2-i)$, što pokazuje da 5 nije ireducibilan, jer su oba faktora neinvertibilna. Dakle, 5 je reducibilan.

- **Element** $12i$**:**
$$N(12i) = 0^2 + 12^2 = 144.$$
Norma 144 nije prosta (jer $144 = 12 \cdot 12$). Slično kao i prije, možemo pisati $12i = (3)(4i)$, gdje su oba faktora neinvertibilna. Dakle, $12i$ je reducibilan.

- **Element** 7**:**
$$N(7) = 7^2 + 0^2 = 49.$$
Pretpostavimo da 7 nije ireducibilan. Tada je $7 = z_1 z_2$, gdje je $N(z_i) = 7$ i $z_i = a_i + b_i$ za $i = 1, 2$. Međutim tada bi bilo $N(z_i) = a_i^2 + b_i^2 = 7$, što je nemoguće modulo 4. Dakle 7 je ireducibilan. Općenitije, vrijedi da je prost prirodan broj $p \equiv 3 \pmod 4$ ireduciblan u $\mathbb{Z}[i]$.

□

Primjer 1.3.6

Riješite (u $\mathbb{Z}$) jednadžbu $y^2 + 4 = z^3$.

Rješenje: Faktorizirajmo desnu stranu: $(y+2i)(y-2i) = z^3$. Neka je $\pi = \gcd((y+2i)(y-2i))$. Tada $\pi|(y+2i)$ i $\pi|(y-2i)$, pa $\pi|2y$ i $\pi|4i$. Dakle $N(\pi)|4y^2$, $N(\pi)|16$, te $N(\pi)|(y^2+4)$. Ako je y neparan, onda je ovaj zadnji izraz neparan, pa mora biti $\gcd((y+2i)(y-2i)) = 1$.

Riješimo prvo slučaj kada je $\boxed{\gcd((y+2i)(y-2i)) = 1}$.

Slijedi

$$y+2i = u(a+bi)^3, \quad y+2i = v(a-bi)^3, \text{ za neke } a,b \in \mathbb{Z},\ u,v \in \mathbb{Z}[i]^\times.$$

Primijetimo da je $\mathbb{Z}[i]^\times \simeq \mathbb{Z}/4\mathbb{Z}$, pa slijedi da su u i v kubovi u $\mathbb{Z}[i]^\times$, tj. možemo samo zapisati

$$\begin{aligned}
&y+2i = (a+bi)^3, \quad y-2i = (a-bi)^3 \\
&\Rightarrow y+2i = a^3+3a^2bi-3a^2b-b^3i, \quad y-2i = a^3-3a^2bi-3ab^2+b^3i \\
&\text{(oduzmemo ove dvije jednadžbe i pogledajmo imaginarni dio)} \\
&\Rightarrow 2 = 3a^2b-b^3 = b\left(3a^2-b^2\right) \Rightarrow \quad b = \pm 1 \text{ ili } b = \pm 2.
\end{aligned}$$

Pogledajmo prvo slučaj $b = \pm 1 \Rightarrow 2 = \pm 1\left(3a^2-1\right)$. Primijetimo da $3a^2-1 = -2$ nema rješenja, pa slijedi $a = \pm 1$. Uvrštavanjem dobijemo i $b = 1$ i dalje

$$\begin{aligned}
y = a^3-3ab^2 = \pm 1 \mp 3 \Rightarrow y = \pm 2 \\
\Rightarrow \boxed{(y,z) = (\pm 2, 2)}.
\end{aligned}$$

Promotrimo sada $b = 2$. Slijedi $3a^2-4 = 1$, tj. $3a^2 = 5$, što je nemoguće. Ostaje slučaj $b = -2$. Slijedi $3a^2-4 = -1$. Imamo

$$3a^2 = 3 \Rightarrow a = \pm 1 \Rightarrow y = \pm 1 \mp 12 \in \{-11, 11\} \Rightarrow \quad z = 5 \Rightarrow \boxed{(y,z) = (\pm 11, 5)}.$$

$\boxed{\gcd((y+2i)(y-2i)) > 1}$

Kao što smo već pokazali, y mora biti paran, pa imamo $y = 2t$, pa slijedi $4t^2+4 = z^3$; zaključujemo da je z paran, tj. $z = 2u$. Slijedi $4t^2+4 = 8u^3$, dakle $t^2+1 = 2u^3$. Faktorizirajmo lijevu stranu:

$$(t+i)(t-i) = 2u^3.$$

Neka $\pi \mid (t \pm i)$; slijedi

$$\pi \mid 2t, \quad \pi \mid 2i$$

$$\Rightarrow \pi|2 \Rightarrow \pi \in \{u, u(1+i), u \cdot 2\} \text{ za neki } u \in \mathbb{Z}[i]^\times.$$

Primijetimo sada da 2 ne dijeli $t+i$, jer bi u suprotnom bi bilo $2(a+bi) = t+i$, što je nemoguće za $a,b \in \mathbb{Z}$.

Ostaje jedino mogućnost $\gcd(t+i, t-i) = 1+i$ (sjetimo se da je gcd dobro definiran do na asociranost).

$$\Rightarrow t+i=(1+i)\cdot(a+bi)^3, \quad t-i=(1-i)(a-bi)^3$$
$$\Rightarrow t+i=(1+i)\left(a^3+3a^2bi-3ab^2i-b^3i\right)$$
$$=a^3+3a^2bi-3ab^2i-b^3i+a^3i-3a^2b+3ab^2+b^3$$
(pogledajmo imaginarni dio)
$$\Rightarrow 1=3a^2b-3ab^2-b^3+a^3=(a-b)^3+\left(6ab^2-6a^2b\right)=(a-b)^3-6ab(b-a)$$
$$=(a-b)\left(a^2-2ab+b^2+6ab\right)=(a-b)\left(a^2+4ab+b^2\right).$$

Pogledajmo prvo slučaj $a-b=1$, to jest $a=b+1$.

$$1=1\cdot\left((a+b)^2+2ab\right)=(2b+1)^2+2b(b+1)$$
$$=4b^2+4b+1+2b^2+2b=6b^2+6b+1$$
$$\Rightarrow b(6b+6)=0 \quad \Rightarrow \quad b=0,-1.$$

Ako $b=0$, tada $a=1$, pa $y=2$ i $z=2$, što je rješenje koje smo već dobili. Analogno $b=-1$ da je $y=-2$ i $z=2$, koje također već imamo.

Pogledajmo sada $a-b=-1$, to jest $a=b-1$. Imamo $-1=6b^2-6b+1$, te lako vidimo da to nema rješenja za $b\in\mathbb{Z}$. □

Poglavlje 2

Proširenja polja

Definicija 2.0.1

Element α se naziva **algebarski** nad poljem K ako:

$$\exists f(x) \in K[x] \text{ takav da } f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

gdje su $a_0, a_1, \ldots, a_n \in K$ i $a_n \neq 0$, a $f(\alpha) = 0$.
U suprotnom, ako ne postoji takav polinom, onda se α naziva **transcendentan** nad K.

Primijetimo da je ekvivalentna definicija: α je algebarski ako je skup $\{\alpha, \alpha^2, \ldots\}$ linearno zavisan nad K.

Ako kažemo samo da je α **algebarski** (bez specifikacije polja), uvijek mislimo algebarski nad $\mathbb{Q}$. Proširenje polja $L \supset K$ je **algebarsko** ako je svaki element u L algebarski nad K.

Propozicija 2.0.2

Neka su $F \supset L \supset K$ proširenja polja. Ako je L algebarsko nad K i F algebarsko nad L, tada je F algebarsko nad K.

Dokaz. DZ. □

Sljedeći teorem nećemo dokazivati.

Teorem 2.0.3

Neka je R domena jedinstvene faktorizacije. Tada je $R[x]$ domena jedinstvene faktorizacije.

Korolar 2.0.4

Neka je K polje. Prsten polinoma $K[x_1, \ldots, x_n]$ je domena jedinstvene faktorizacije.

Primijetimo da $K[x_1, x_2]$ nije DGI, te je ovo jednostavan primjer DJF koji nije DGI.

Neka je sada α algebarski nad K, te neka je $g \in K[x]$ t.d $g(\alpha) = 0$. Faktorizirajući g na ireducibilne dobijemo normiran ireducibilan polinom $f_\alpha \in K[x]$ takav da je $f_\alpha(\alpha) = 0$. Taj polinom zovemo **minimalni polinom** od α (nad K).

Propozicija 2.0.5

Neka je α algebarski nad K. Tada je njegov minimalni polinom nad K jedinstven.

Dokaz. Neka je $0 \neq h \in K[x]$ t.d. $h(\alpha) = 0$ i $f_\alpha \nmid h$. Pošto je f_α ireducibilan, to znači da su f_α i h relativno prosti, tj. postoje $g, k \in K[x]$ takvi da je

$$f_\alpha g + hk = 1.$$

Međutim, sada imamo

$$0 = f_\alpha(\alpha)g(\alpha) + h(\alpha)k(\alpha) = 1,$$

što je očito kontradikcija. □

Definicija 2.0.6

Neka je f_α minimalni polinom od α (nad K). Korijeni od f_α se zovu **konjugati** od α (nad K).

Neka je $n = \deg f_\alpha$. Vrijedi

$$K(\alpha) \simeq K[x]/(f_\alpha),$$

te je $\{1, \alpha, \ldots \alpha^{n-1}\}$ baza od $K(\alpha)$ nad K.

Definicija 2.0.7

Neka je K polje. Polinom $f(x) \in K[x]$ je separabilan ako su svi njegovi korijeni u $\overline{K}$ različiti, odnosno ako ne postoje dva ista korijena.
Proširenje L/K je **separabilno** ako su minimalni polinomi svakog elementa u L separabilni polinomi nad K.

Primjer 2.0.8

Neka je

$$K = \mathbb{F}_p(t)$$

polje racionalnih funkcija u jednoj varijabli t nad konačnim poljem $\mathbb{F}_p$, gdje je p prost broj. Promotrimo element

$$\alpha = t^{1/p}.$$

Onda je α korijen polinoma

$$f(x) = x^p - t \in K[x].$$

Derivacija polinoma je

$$f'(x) = px^{p-1} = 0,$$

jer smo u karakteristici p. Dakle, $f(x)$ nema različite korijene, tj. svi njegovi korijeni su višestruki. Polinom $f(x)$ je ireducibilan u $K[x]$, jer t nije p-ta potencija u K. Dakle, proširenje

$$L = K(\alpha) = \mathbb{F}_p(t^{1/p})$$

je neseparabilno proširenje stupnja $[L : K] = p$.

Neka su K, L polja, te neka je $f : K \to L$ homomorfizam prstena. Tada je $\ker f$ ideal u K, a jedini ideal u K je (0), pa zaključujemo da je f injektivan. Zato se homomorfizmi polja obično nazivaju **ulaganja** polja.

Definicija 2.0.9

Konačno proširenje $K/\mathbb{Q}$ (tj. K je konačno-dimenzionalni vektorski prostor nad $\mathbb{Q}$) se zove **polje algebarskih brojeva** (PAB).

Lema 2.0.10

Svi korijeni (u $\mathbb{C}$) ireducibilnog polinoma $f \in K[x]$, gdje je K polje algebarskih brojeva su različiti.

Dokaz. Pretpostavimo suprotno, tj. da f ima barem dvostruki korijen β. Tada je $f(\beta) = f'(\beta) = 0$. Vrijedi $\deg f' \leq \deg f - 1$, pa $(f') \not\subseteq (f)$. Pošto je (f) maksimalan slijedi $(f') + (f) = K[x]$, pa postoje $g, k \in K[x]$ takvi da je

$$fg + f'k = 1.$$

Međutim, sada imamo

$$0 = f(\beta)g(\beta) + f'(\beta)k(\beta) = 1,$$

što je očito kontradikcija.

□

Dakle sva proširenja PAB su separabilna. Pretpostavimo od sada nadalje da je $\mathbb{Q} \subset K \subset \mathbb{C}$. Sljedeći teorem je dokazan na Algebri.

Teorem 2.0.11

Neka su $K \subseteq L$ potpolja od $\mathbb{C}$. Tada se ulaganje $\sigma : K \hookrightarrow \mathbb{C}$ može proširiti na ulaganje $L \hookrightarrow \mathbb{C}$ na točno $[L : K]$ načina.

Definicija 2.0.12

Ulaganje od L u $\mathbb{C}$ koje fiksira K se zove K-ulaganje od L u $\mathbb{C}$.

Korolar 2.0.13

Postoji $[L : K]$ K-ulaganja L u $\mathbb{C}$.

Definicija 2.0.14

Neka je $K \subseteq L$. Ako vrijedi $L = K(\alpha)$, kažemo da je L/K **prosto proširenje**, te kažemo da je α **primitivni element** tog proširenja.

Primijetimo da je $[K(\alpha) : K] = \deg f_\alpha$.

Teorem 2.0.15: Teorem o primitivnom elementu

Neka su $K \subseteq L$ PAB. Tada je $L = K(\alpha)$ za neki $\alpha \in L$.

Dokaz. Indukcijom po stupnju proširenja $n = [L : K]$. Baza $n = 1$ je očita. Pretpostavimo da tvrdnja vrijedi za sva proširenja svakog PAB stupnja $< n$.

Neka je $\alpha \in L$. Ako je $L = K(\alpha)$, gotovi smo. Pretpostavimo $L \neq K(\alpha)$. Vrijedi

$$[L : K] = [L : K(\alpha)][K(\alpha) : K].$$

Po pretpostavci $L/K(\alpha)$ je prosto proširenje, pa slijedi $L = (K(\alpha))(\beta)$, tj. $L = K(\alpha, \beta)$. Neka je $a \in K^\times$ proizvoljan. Neka je $\gamma = \alpha + a\beta$. Ako je $L = K(\gamma)$, gotovi smo.

Pretpostavimo $K(\gamma) \subsetneq L$. Neka su σ_i, $i = 1, \ldots, n$ različita K-ulaganja od L u $\mathbb{C}$. Neka je f minimalni polinom od γ (nad K). Tada je $\deg f < n$. Promotrimo skup

$$\{\sigma_i(\gamma), i = 1, \ldots, n\}.$$

Vrijedi

$$f(\gamma) = 0, \text{ pa je } \sigma_i(f(\gamma)) = f(\sigma_i(\gamma)) = 0$$

(ovdje koristimo da je $f \in K[x]$). Zaključujemo da postoje $i \neq j$ takvi da je $\sigma_i(\gamma) = \sigma_j(\gamma)$, tj.

$$\sigma_i(\alpha) + \sigma_i(a\beta) = \sigma_j(\alpha) + \sigma_j(a\beta) \Longrightarrow \sigma_i(\alpha) - \sigma_j(\alpha) = a(\sigma_j(\beta) - \sigma_i(\beta)).$$

Mora vrijediti $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ ili $\sigma_j(\beta) \neq \sigma_i(\beta)$, jer bi u suprotnom K-ulaganja σ_i i σ_j bila identična. Međutim, ako vrijedi jedna nejednakost, vrijedi i druga.

Dakle

$$a \in S := \left\{ \frac{\sigma_i(\alpha) - \sigma_j(\alpha)}{\sigma_j(\beta) - \sigma_i(\beta)},\ 1 \leq i, j \leq n,\ i \neq j \right\}.$$

Zaključujemo da za $b \in K^\times \backslash S$ vrijedi da je $K(\alpha + b\beta) = L$, što uvijek možemo izabrati, pošto je S konačan, a $K^\times$ beskonačan. □

Definicija 2.0.16

Kažemo da je L **normalno proširenje** od K ako zadovoljava sljedeće: ako je $\alpha \in L$ korijen nekog $f \in K[x]$ tada su svi konjugati od α nad K sadržani u L.

Primjer 2.0.17

Polja $\mathbb{Q}(i)$, $\mathbb{Q}(\zeta_n)$ su normalna proširenja od $\mathbb{Q}$, međutim $\mathbb{Q}(\sqrt[3]{2})$ nije.

Sljedeći rezultati su dokazani na Algebri.

Teorem 2.0.18

Ekvivalentno je:

1. L/K je normalno proširenje,
2. Svako K-ulaganje $L \hookrightarrow \mathbb{C}$ je automorfizam od L,
3. L ima točno $[L : K]$ automorfizama koji fiksiraju K.

Dokaz. $\boxed{1) \Longrightarrow 2)}$: Neka je $L \supseteq K$ normalno i $\phi : L \hookrightarrow \mathbb{C}$ K-ulaganje. Tvrdimo $\phi(L) = L$. Za $\alpha \in L$, neka je f_α minimalni polinom od α. Vrijedi

$$0 = \phi(0) = \phi(f_\alpha(\alpha)) = f_\alpha(\phi(\alpha))$$

pošto ϕ djeluje kao identiteta na koeficijente of f_α Slijedi da je $\phi(\alpha)$ korijen od f_α, pa pošto je L normalno slijedi da je $\phi(\alpha) \in L$.

Slijedi $\phi(L) \subseteq L$, te onda pošto je $\dim_K \phi(L) = \dim_K L$, slijedi $\phi(L) = L$. Dakle ϕ je automorfizam.

$\boxed{2) \Longrightarrow 1)}$: Pretpostavimo da je svako K-ulaganje $L \hookrightarrow \mathbb{C}$ automorfizam od L. Neka je $\alpha \in L$, te β konjugat od α nad K.

Neka je ϕ K-ulaganje $\phi : K(\alpha) \hookrightarrow \mathbb{C}$ takvo da je $\phi(\alpha) = \beta$. Po ranije dokazanom teoremu, to ulaganje možemo proširiti na ulaganje $\tilde{\phi} : L \hookrightarrow \mathbb{C}$. Po pretpostavci vrijedi $\tilde{\phi}(L) = L$. Vrijedi

$$\beta = \phi(\alpha) = \tilde{\phi}(\alpha) \in L.$$

$\boxed{2) \Longrightarrow 3)}$: Znamo da postoji $[L : K]$ K-ulaganja L u $\mathbb{C}$. Dakle postoji barem $[L : K]$ automorfizama od L koji fiksiraju K. S druge strane ako komponiramo svaki taj automorfizam sa nekim fiksnim ulaganjem L u $\mathbb{C}$, dobijemo neko ulaganje L u $\mathbb{C}$, te su sva takva različita. Dakle, ima točno $[L : K]$ automorfizama od L koji fiksiraju K.

$\boxed{3) \Longrightarrow 2)}$: Kad bi imali neko K-ulaganje koje nije automorfizam, imali bi $\geq [L : K] + 1$ ulaganja $L \hookrightarrow \mathbb{C}$, što je kontradikcija s ranijim teoremom.

□

Teorem 2.0.19

Neka je $L = K(\alpha_1, \ldots, \alpha_n)$ i neka L sadrži sve konjugate nad K od $(\alpha_1, \ldots, \alpha_n)$. Tada je L normalno proširenje od K.

Dokaz. Neka je $\sigma : L \hookrightarrow \mathbb{C}$ K-ulaganje. Tada je

$$\sigma(L) = K(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) \subseteq L,$$

pošto su svi $\sigma(\alpha_1), \ldots, \sigma(\alpha_n) \in L$. Sada tvrdnja slijedi iz Teorema 2.0.18. □

Propozicija 2.0.20

Neka su $F \supset L \supset K$ proširenja polja. Ako je F normalno nad K. Tada je F normalno nad L.

Dokaz. Neka je $\phi : F \hookrightarrow \mathbb{C}$ L-ulaganje. Slijedi da je ϕ i K-ulaganje. Po Teoremu 2.0.18 je ϕ automorfizam od F, pa je opet po Teoremu 2.0.18 F normalno i nad L (pošto je svako L-ulaganje automorfizam). □

Primjer 2.0.21

Neka su $F \supset L \supset K$ proširenja polja. Ako je L normalno nad K i F normalno nad L, tada **ne mora vrijediti da je** F normalno nad K. Kontraprimjer je npr. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$.
Da bi to vidjeli primijetimo da je minimalni polinom od $\sqrt[4]{2}$ nad $\mathbb{Q}(\sqrt{2})$ jednak $x^2 - \sqrt{2}$, te su njegovi korijeni $\pm\sqrt[4]{2}$ sadržani unutar $\mathbb{Q}(\sqrt[4]{2})$.
S druge strane minimalni polinom od $\sqrt[4]{2}$ nad $\mathbb{Q}$ je $x^4 - 2$, te su konjugati (nad $\mathbb{Q}$) od $\sqrt[4]{2}$ jednaki $i^k \sqrt[4]{2}, k = 1, \ldots 4$, koji nisu svi sadržani u $\sqrt[4]{2} \subseteq \mathbb{R}$.

Korolar 2.0.22

Ako je $L \supseteq K$, tada postoji proširenje $M \supseteq L$ takvo da je M normalno nad K.

Napomena: Primijetimo da će M iz korolara biti normalan i nad L.

Dokaz. Neka je $L = K(\alpha)$, takav α postoji po teoremu o primitivnom elementu. Neka su $\alpha_1, \ldots, \alpha_n$ konjugati od α. Neka je $M = K(\alpha_1, \ldots, \alpha_n)$. Po Teoremu 2.0.19 slijedi da je M normalan nad K. □

Definicija 2.0.23

Neka je $L \supseteq K$. Najmanji $M \supseteq L$ koji je normalan nad K se zove **normalno zatvorenje** od L nad K.

Napomena: Mi pretpostavljamo cijelo vrijeme da radimo sa separabilnim i konačnim proširenjima!

Definicija 2.0.24

Neka je L/K normalno proširenje. Grupa od K-automorfizama od L se zove Galoisova grupa od L nad K i označava s $\mathrm{Gal}(L/K)$.

Napomena: Primijetimo da raniji teorem kaže $|\mathrm{Gal}(L/K)| = [L : K]$.

Definicija 2.0.25

Za $H \leq \mathrm{Gal}(L/K)$ definiramo **fiksno polje** od H, s oznakom L^H kao

$$L^H = \{\alpha \in L \mid \sigma(\alpha) = \alpha,\ \forall \sigma \in H\}.$$

Sada ćemo iskazati bez dokaza (pošto je već dokazano na Algebri) glavne rezultate Galoisove teorije.

Teorem 2.0.26

Neka je L/K normalno proširenje i $G = \mathrm{Gal}(L/K)$. Tada je K fiksno polje od G i K nije fiksno polje niti jedne druge podgrupe od G.

Teorem 2.0.27: Osnovni teorem Galoisove teorije

Neka je L/K normalno proširenje i $G = \mathrm{Gal}(L/K)$. Tada postoji bijekcija između podgrupa od G i međupolja $K \subseteq F \subseteq L$. Ta bijekcija u jednom smjeru šalje podgrupu H u fiksno polje od H, a u drugom šalje međupolje F u $\mathrm{Gal}(L/F)$.
Nadalje, međupolje F je normalno nad K ako i samo ako je $\mathrm{Gal}(L/F)$

normalna u $\mathrm{Gal}(L/K)$.

Dakle imamo:

$$\begin{aligned} \{F \text{ polje: } K \subseteq F \subseteq L\} &\longleftrightarrow \{H : H \leq G\} \\ F &\longmapsto \mathrm{Gal}(L/F) \leq G \\ L^H &\longmapsfrom H \leq G \end{aligned}$$

Teorem 2.0.28

Neka je L/K normalno proširenje, te neka je $E \supseteq K$ bilo koje proširenje. Označimo s EL polje generirano s $E \cup L$. Tada je $EL \supseteq E$ normalno i $\mathrm{Gal}(EL/E)$ se ulaže u $\mathrm{Gal}(L/K)$ restringirnajem na L. Ta restrikcija je izomorfizam ako i samo ako je $E \cap L = K$.

2.1 Ciklotomska polja

Definicija 2.1.1

Za pozitivan cijeli broj n, *n-to ciklotomsko polje* $K = \mathbb{Q}(\zeta_n)$ je proširenje polja racionalnih brojeva $\mathbb{Q}$, koje se dobije dodavanjem primitivnog n-tog korijena iz jedinice ζ_n. Ovaj korijen je kompleksni broj koji zadovoljava $\zeta_n^n = 1$, a ζ_n nije k-ti korijen iz jedinice za $k < n$.

Jedan primjer n-tog korijena iz jedinice je $e^{\frac{2\pi i}{n}}$.

Definicija 2.1.2

n-ti ciklotomski polinom $\Phi_n(x)$ je normirani polinom čiji su korijeni točno svi primitivni n-ti korijeni iz jedinice (ili analogno, minimalni polinom nekog primitivnog korijena jedinice). Drugim riječima, n-ti ciklotomski polinom $\Phi_n(x)$ je zadan kao

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} \left(x - \zeta_n^k\right),$$

gdje je $\zeta_n = e^{\frac{2\pi i}{n}}$ primitivni n-ti korijen iz jedinice, a produkt ide po svim k takvim da je $\gcd(k, n) = 1$, odnosno za sve k koji su relativno prosti s n.

Polinom $\Phi_n(x)$ zadovoljava sljedeću jednadžbu:

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

gdje produkt ide po svim djeliteljima n, a $\Phi_d(x)$ su ciklotomski polinomi za sve d. Ova jednadžba omogućuje rekurzivno računanje ciklotomskih polinoma. Vidimo da je stupanj od $\Phi_n(x)$ jednak $\varphi(n)$.

Na primjer, kada je $n = p$, gdje je p prost broj, n-ti ciklotomski polinom je

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Lema 2.1.3

Polinom $\Phi_p(x)$ je ireducibilan u $\mathbb{Q}[x]$.

Dokaz. Vrijedi

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}.$$

Uvedimo supstituciju $y = x - 1$. Sada imamo

$$g(y) := \Phi_p(y+1) = \frac{(y+1)^p - 1}{y} = \frac{y^p + \binom{p}{1}y^{p-1} + \ldots + \binom{p}{p-1}y}{y}$$

$$= y^{p-1} + py^{p-2} + \ldots p.$$

Upotrebom Eisensteinovog kriterija zaključujemo da je g ireducibilan. Slijedi da je i $\Phi_p(x)$ ireducibilan. □

Neka je $\zeta = \zeta_p$ primitivni p-ti korijen iz jedinice. Tada su nultočke od $\Phi_p(x)$ $\zeta, \zeta^2, \ldots \zeta^{p-1}$. Dakle (nad $\mathbb{Q}(\zeta_p)$) vrijedi

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = (x - \zeta)(x - \zeta^2)\ldots(x - \zeta^{p-1}).$$

Uvrštavanjem $x = 1$ dobivamo

$$\prod_{i=1}^{p-1}(1 - \zeta^i) = p.$$

2.2 Konstruktibilnost ravnalom i šestarom

Problem: S ravnalom i šestarom u konačno mnogo koraka riješite sljedeće probleme:

1. "Duplikacija kocke" - konstruirati kocku s duplo većim volumenom,
2. "Trisekcija kuta" - podijeliti zadani kut na 3 jednaka dijela,
3. "Kvadratura kruga" - Za zadani krug konstruirati kvadrat iste površine.

Neka je zadan skup E koji predstavlja skup točaka u ravnini. Definiramo D_E kao skup svih pravaca koji prolaze kroz dvije točke iz E. Također, definiramo C_E kao skup svih kružnica sa središtem u nekoj točki iz E i radijusom jednakim udaljenosti između nekih točaka iz E.

Točka u ravnini je konstruktibilna u jednom koraku iz E ako je:

1. presjek dvaju pravaca iz D_E,
2. presjek pravca iz D_E i kružnice iz C_E,
3. presjek dviju kružnica iz C_E.

Konstruktibilnost u n koraka iz E se definira induktivno.

Koordinatni sustav ćemo postaviti tako da su $O \in E$ i $(1,0)$ također iz E. Neka je $k = \mathbb{Q}(F)$, gdje je F skup svih koordinata točaka iz E u toj bazi.

Tada:

- Svaki pravac iz D_E ima jednadžbu:

$$ax + by + c = 0, \quad a, b, c \in k$$

- Svaka kružnica iz C_E ima jednadžbu:

$$x^2 + y^2 + ax + by + c = 0, \quad a, b, c \in k$$

Propozicija 2.2.1

Neka je $P = (p, q)$ točka u ravnini konstruktibilna u jednom koraku iz E. Tada je $k(p, q)$ ili jednako k, ili je kvadratno proširenje od k (vrijedi i obrat).

Dokaz. (a) Presjek dvaju pravaca:

$$ax + by + c = 0 \quad \text{i} \quad a'x + b'y + c' = 0$$

Pretpostavimo da ovi pravci nisu paralelni.

$\exists!(x, y) \in k^2$ koji zadovoljava ove 2 jednadžbe

$\Rightarrow \quad k(p, q) = k$

(b) Presjek pravca i kružnice:

$$x^2 + y^2 + ax + by + c = 0$$
$$a'x + b'y + c' = 0$$
$$\Rightarrow \quad x = \frac{-c' - b'y}{a'}$$

Uvrstimo u jednadžbu kružnice i dobijemo kvadratnu jednadžbu za y.

$[k(x, y) : k(y)] = 1$

$\Rightarrow [k(x, y) : k] = 1$ ili 2.

(c) Presjek dvije kružnice:

$$\begin{aligned} &y^2 + y^2 + ax + by + c = 0 \\ &x^2 + y^2 + a'x + b'y + c' = 0 \quad /- \\ &(a - a')\,x + (b - b')\,y + (c - c') = 0 \\ &\text{svodi se na} \qquad \text{(b)} \end{aligned}$$

□

Korolar 2.2.2

Neka je $P = (p, q)$ konstruktibilna iz E.

1. Tada postoji konačan niz polja $K_i, 0 \leq i \leq n$ takav da je svako K_i kvadratno proširenje od K_{i-1}, $K_0 = K$, $K_n \subseteq \mathbb{R}$, $K_n = K(p, q)$.
2. p i q su algebarski nad K i stupanj im je potencija od 2.

Riješimo sada probleme:

1. Neka je stranica kvadrata s vrhovima O i $(0, 1)$. Želimo naći kocku volumena 2. Tada bi kocka s volumenom 2 bez smanjenja općenitosti imala vrhove u O i $(0, \sqrt[3]{2})$. Međutim stupanj od $\sqrt[3]{2}$ je 3, pa točka $(0, \sqrt[3]{2})$ nije konstuktibilna. Ovo je dokazao Wantzel 1837.

2. Problem je ekvivalentan iz toga da iz zadanog $\cos 3\alpha$ dobijemo $\cos \alpha$. Međutim, lako dobijemo

$$\cos 3\alpha = 4\cos^3 \alpha - 3\cos \alpha.$$

Uzimanjem $x := \cos \alpha$ vidimo da zapravo tražimo korijen jednadžbe

$$4x^3 - 3x - \cos 3\alpha.$$

Npr. ako uzmemo $\alpha = 40°$, slijedi $\cos 3\alpha = -1/2$, te vidimo da je $4x^3 - 3x + 1/2$ ireducibilna nad $\mathbb{Q}$. Dakle x je stupnja 3 nad $\mathbb{Q}$. Dakle ne možemo ga konstruirati. Ovo je dokazao Wantzel 1837.

3. Radijus je bez smanjenja općenitosti 1, pa slijedi da je volumen jednak π. Dakle problem je ekvivalentan konstrukciji kvadrata sa stranicom duljine $\sqrt{\pi}$. Bez smanjenja općenitosti jedna stranica ima vrhove u O i $(0, \sqrt{\pi})$. Međutim π nije algebarski (Lindeman-Weierstrassov teorem, 1882.), tako da druga točka nije konstruktibilna.

2.3 Rješivost radikalima

Definicija 2.3.1

Polje $K \subseteq \mathbb{C}$ je **radikalno proširenje** od F ako postoji niz $(K_i)_{0\leq i\leq r}$ koji zovemo *radiklani toranj* t.d. za $i = 0, \ldots, r$ vrijedi:

1. $K_{i+1} \supset K_i,\ F = K_0,\ K_r = K.$
2. Za svaki $i \in \{1, \ldots, r\}$ postoje $n_i \in \mathbb{N},\ a_i \in K_{i-1}$ t.d: $K_i = K_{i-1}(\sqrt[n_i]{a_i})$.

Primjer 2.3.2

$$K = \mathbb{Q}\left(\sqrt[12]{\sqrt[3]{2+\sqrt[3]{-7}+\sqrt{5}}+\sqrt[3]{-7}}\right).$$

Vrijedi

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{-7}) \subset \mathbb{Q}(\sqrt[3]{-7}, \sqrt{5}) \subset \mathbb{Q}(\sqrt[3]{-7}, \sqrt{5}, \sqrt[5]{-7})$$

$$\subset \mathbb{Q}\left(\sqrt[3]{2+\sqrt[3]{-7}+\sqrt{5}}, \sqrt[3]{-7}, \sqrt[5]{-7}, \sqrt{5}\right) \subset K,$$

pa je K radikalno proširenje.

Definicija 2.3.3

Neka je $f \in F[x]$. Kažemo da je jednadžba $f(x) = 0$ rješiva u radikalima ako je polje cijepanja od f sadržano u nekom radikalnom proširenju od f.

Definicija 2.3.4

Grupa G je *rješiva* ako postoji niz normalnih podgrupa

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G,$$

takav da su kvocijentne grupe G_{i+1}/G_i Abelove za svaki $i = 0, 1, 2, \ldots, n-1$.

Primjer 2.3.5

S_3 je rješiva grupa, budući da imamo niz normalnih podgrupa

$$\{e\} \trianglelefteq A_3 \trianglelefteq S_3,$$

i obje kvocijentne grupe $A_3/\{e\} \cong \mathbb{Z}/3\mathbb{Z}$ i $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ su Abelove, zaključujemo da je S_3 rješiva grupa.

Lema 2.3.6: Galois

Ako je proširenje $F \subseteq K$ radikalno, tada je Galoisovo zatvorenje proširenja $F \subseteq K$ također radikalno.

Dokaz. Skica: normalno zatvorenje se dobije dodavanjem svih konjugata, a konjugati od m-tih korijena nekog elementa $a \in F$ su opet m-ti korijeni tog istog elementa. □

Napomena: (DZ) Ako je G rješiva grupa, tada su sve podgrupe i kvocijentne grupe od G rješive.

Teorem 2.3.7: Galois

Neka je $f \in F[x]$, i K polje cijepanja od f nad F. Tada je $f(x) = 0$ rješiva u radikalima $\iff$ $\mathrm{Gal}(K/F)$ je rješiva grupa.

Dokaz. Dajemo samo dokaz smjera $\implies$ (obrat je sličan). Po pretpostavci, postoji radikalno proširenje M/F t.d. $K \subseteq M$. Neka je L Galoisovo zatvorenje od M nad F. Dakle vrijedi $F \subseteq K \subseteq L$, pa je po Galoisovoj teoriji

$$\mathrm{Gal}(K/F) \simeq \mathrm{Gal}(L/F)/\,\mathrm{Gal}(L/K).$$

Po Napomeni prije teorema, dosta je dokazati da je $\mathrm{Gal}(L/F)$ rješiva (jer tada slijedi i da je $\mathrm{Gal}(K/F)$ rješiva).

Pošto je po Lemi L radikalno proširenje od F, postoji niz

$$F = L_0 \subseteq L_1 \subseteq \ldots L_s = L,$$

gdje je $L_{i+1} = L_i(\sqrt[n_i]{a_i})$. za neki $a_i \in L_i$, i $n_i \in \mathbb{N}$. Imamo 2 slučaja.

1) lakši slučaj: $\zeta_{n_i} \in F$ za sve $i = 1, \ldots, s$. Po Kummerovom teoremu vrijedi da je L_{i+1}/L_i cikličko proširenje, pa time i normalno.

Definirajmo $G_i := \mathrm{Gal}(L/L_i)$ i $G := \mathrm{Gal}(L/F)$. Po Galoisovoj teoriji vrijedi

$$1 = G_s \leq G_{s-1} \leq \ldots \leq G_1 \leq G_0 = G.$$

Pošto je L_{i+1}/L_i normalno proširenje, imamo da je $G_{i+1} \trianglelefteq G_i$, te je po Galoisovoj teoriji $\mathrm{Gal}(L_{i+1}/L_i) \simeq G_i/G_{i+1}$ ciklička grupa (a time i Abelova). Ovo

dokazuje prvi slučaj.

2) opći slučaj. Definirajmo $E := F(\zeta_{n_1}, \dots \zeta_{n_s})$. Vrijedi da je E/F Galoisovo, pa pošto je L/F Galoisovo, vrijedi da je EL/F Galoisovo. Pogledajmo sada niz

$$E \subseteq EL_0 \subseteq EL_1 \subseteq \ldots \subseteq EL.$$

Po prvom slučaju, vrijedi da je $\mathrm{Gal}(EL/E)$ rješiva. Također,

$$\mathrm{Gal}(E/F) \simeq \mathrm{Gal}(EL/F)/\mathrm{Gal}(EL/E)$$

Pošto je $\mathrm{Gal}(EL/E)$ rješiva, $\mathrm{Gal}(EL/E) \trianglelefteq \mathrm{Gal}(EL/F)$, i $\mathrm{Gal}(E/F)$ Abelova, slijedi da je $\mathrm{Gal}(EL/F)$ rješiva. Sada po Napomeni slijedi da je $\mathrm{Gal}(L/F)$ rješiva.

□

Mi nećemo to raditi na ovom kolegiju, ali može se lako dokazati da S_n nije rješiva grupa za $n \geq 5$, te da za svaki n postoji (beskonačno mnogo) polinoma čije polje cijepanja ima Galoisovu grupu S_n nad $\mathbb{Q}$, za svako $n \in \mathbb{N}$. Iz toga slijedi sljedeći važan teorem.

Teorem 2.3.8: Abel-Ruffini

Opća polinomijalna jednadžba stupnja ≥ 5 nije rješiva radikalima.

Poglavlje 3

Prsteni cijelih

Cilj: Izgradnja "teorije faktorizacije" u poljima algebarskih brojeva K (proširenja nad $\mathbb{Q}$, tj. $K/\mathbb{Q}$) i prstenima $\mathbb{Z} \subset \mathbb{Q}$.

Treba odabrati pravi potprsten R. Želimo:

1. "Smislena teorija faktorizacije."
2. Prsten R odgovara polju K kao što prsten $\mathbb{Z}$ odgovara polju $\mathbb{Q}$.
   a) K je polje razlomaka od R.
   b) (jače) $\forall \alpha \in K,\ \exists n \in \mathbb{Z}$ t.d. $n\alpha \in R$.
3. $R \cap \mathbb{Q} = \mathbb{Z}$

Primijetimo: Svojstvo 2 ne određuje R jedinstveno. Npr. neka je $S =$ pravi podskup prostih brojeva.

Definicija:

$$S^{-1}\mathbb{Z} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, \gcd(a,b) = 1, \text{ i svi prosti faktori od } b \text{ su iz } S \right\}$$

Npr. za $S = \{2\}$,

$$S^{-1}\mathbb{Z} = \left\{ \frac{a}{2^n} : a \in \mathbb{Z}, n \in \mathbb{N}_0 \right\}$$

Vidjeli smo da općenito faktorizacija na ireducibilne elemente u prstenima u poljima algebarskih brojeva nije jedinstvena. Ono što ćemo umjesto toga postići je jedinstvena faktorizacija proizvoljnog ideala na proste ideale.

Sada ćemo vidjeti da to ne možemo postići u svakom potprstenu polja algebarskih brojeva.

Primjer 3.0.1

Vrijedi $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Q}(\sqrt{d})$ je potprsten. Neka je $d = -3$. Vrijedi.

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

Elementi $1 \pm \sqrt{-3}$ su ireducibilni u prstenu $\mathbb{Z}[\sqrt{-3}]$.
Je li faktorizacija ideala na proste ideale jedinstvena u ovom prstenu? Pogledajmo primjer:

$$\begin{aligned} a &= (2, 1 + \sqrt{-3}) \quad \text{(nije glavni ideal)} \\ a^2 &= (2, 1 + \sqrt{-3})(2, 1 + \sqrt{-3}) = (4, 2(1 + \sqrt{-3}), -2 + 2\sqrt{-3}) \\ &= (4, 2 + 2\sqrt{-3}, -2 + 2\sqrt{-3}) = (4, 2 + 2\sqrt{-3}) \\ &= 2(2, 1 + \sqrt{-3}) = (2)a \end{aligned}$$

Imamo li jedinstvenu faktorizaciju ideala? Da je imamo, onda bismo imali $(2) = (2, 1 + \sqrt{-3})$, što nije istina.
Odabrali smo krivi prsten! Pravi prsten bi bio $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, i u njemu je jedinstvena faktorizacija na proste ideale.

Definicija 3.0.2

Neka je R integralna domena, $R \subset K$, gdje je K polje algebarskih brojeva. Element $\alpha \in K$ je **cijeli** nad R ako poništava normirani polinom iz $R[x]$. Kažemo da je R **integralno zatvoren** u K ako svaki element iz K, koji je cijeli nad R, leži u R.

Primjer 3.0.3

Neka je $R = \mathbb{Z}$, $K = \mathbb{Q}$, i neka je $\alpha = r/s$, gdje $(r, s) = 1$, poništava polinom $f \in \mathbb{Z}[x]$ oblika:

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

$$\Rightarrow \quad \left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\frac{r}{s} + a_0 = 0 \quad / s^n \neq 0$$

Imamo:

$$\begin{gathered} r^n + a_{n-1}r^{n-1}s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0, \\ \Rightarrow s(a_{n-1}r^{n-1} + \cdots + a_1 r s^{n-2} + a_0 s^{n-1}) = -r^n \\ \Rightarrow s \mid -r^n \Rightarrow s = 1. \end{gathered}$$

Dakle $\alpha \in \mathbb{Z}$.

Propozicija 3.0.4

Ako je K polje razlomaka od R, i ako je R DJF, tada je R integralno zatvoren u K.

Dokaz. Potpuno isto kao i u primjeru. □

Obrat ne vrijedi! Prsten $\mathbb{Z}[\sqrt{-5}] = R$ je integralno zatvoren u $K = \mathbb{Q}(\sqrt{-5})$, koje je polje razlomaka od R, ali R nije DJF.

Primjer 3.0.5

Da li je uvjet da je K polje razlomaka od R uvijek potreban? Promotrimo primjer $\mathbb{Z}[i] \subset \mathbb{Q}(i)$. Element $i \in \mathbb{Q}(i)$, jer polinom $f(x) = x^2 + 1$, zadovoljava $f(i) = 0$, što znači da je i cijeli nad $\mathbb{Z}$; dakle $\mathbb{Z}$ nije integralno zatvoren u $\mathbb{Q}(i)$.

Primjer 3.0.6

Neka je

$$R = \mathbb{Z}[\sqrt{-3}], \quad K = \mathbb{Q}(\sqrt{-3}), \quad f(x) = x^2 + x + 1 \in \mathbb{Z}[\sqrt{-3}][x].$$

Vrijedi $f(\alpha) = 0 \quad$ za $\quad \alpha = \frac{-1 \pm \sqrt{-3}}{2}$. Pošto $\alpha \notin R$ slijedi da R nije integralno zatvoren u K. Slijedi da $\mathbb{Z}[\sqrt{-3}]$ nije integralno zatvoren.

Definicija 3.0.7

Kažemo da je $\alpha \in \overline{\mathbb{Q}}$ **cijeli algebarski broj** ako postoji $f \in \mathbb{Z}[x]$ takav da je $f(\alpha) = 0$, pri čemu je f normiran polinom. Skup cijelih algebarskih brojeva označavamo s $\mathbb{A}$.

Napomena: Uvjeti

1. R je integralno zatvoren u K.
2. K je polje razlomaka od R.

osiguravaju da je R "dovoljno velik". Mi zapravo tražimo najmanji takav R.

Definicija 3.0.8

Neka je K polje, a R prsten. **Integralno zatvorenje** od R u K je podskup od K koji sadrži sve elemente koji su cijeli nad R.

Definicija 3.0.9

Neka je K polje algebarskih brojeva. Definiramo **prsten cijelih brojeva** $\mathcal{O}_K$ u K kao integralno zatvorenje $\mathbb{Z}$ u K. Dakle $\mathcal{O}_K = \mathbb{A} \cap K$.

Treba dokazati da je $\mathcal{O}_K$ prsten!

Propozicija 3.0.10

Neka je K polje algebarskih brojeva (PAB). Za $\alpha \in K$ sljedeće tvrdnje su ekvivalentne:

1. $\alpha \in \mathbb{A}$ (tj. $\alpha \in \mathcal{O}_K$).
2. Prsten $\mathbb{Z}[\alpha]$ je konačno generiran $\mathbb{Z}$-modul.
3. α pripada potprstenu $R \subset K$ koji je konačno generiran $\mathbb{Z}$-modul.
4. Postoji konačno generiran $\mathbb{Z}$-modul $R \subset K$ t.d. je $\alpha R \subset R$.

Dokaz. (1) $\Rightarrow$ (2): Postoji polinom $f_\alpha = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$ takav da je $f_\alpha(\alpha) = 0$. Vrijedi

$$\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/\left(f_\alpha\right).$$

Primijetimo da to znači da u $\mathbb{Z}[\alpha]$ vrijedi $\alpha^n = -a_{n-1}\alpha^{n-1} - \ldots - a_0$. Dakle, $\mathbb{Z}[\alpha]$ je konačno generiran kao $\mathbb{Z}$-modul sa generatorima $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, gdje je $n = \deg(f_\alpha)$.

(2) $\Rightarrow$ (3): Uzmimo $R = \mathbb{Z}[\alpha]$, koji je po pretpostavci konačno generiran.

(3) $\Rightarrow$ (4): Uzmemo opet R koji zadovoljava (3); on će zadovoljavati i (4).

(4) $\Rightarrow$ (1): Pretpostavimo da postoji $\mathbb{Z}$-modul $R \subset K$ koji je generiran s $a_1, a_2, \ldots, a_n \in R$, te $\alpha a_i \in R$ za $i = 1, \ldots, n$. Tada za sve $i = 1, \ldots, n$ vrijedi:

$$\alpha a_i = \sum_{j=1}^{n} b_{ij} a_j, \quad b_{ij} \in \mathbb{Z}, \quad i = 1, \ldots, n.$$

Zapišimo to kao:

$$\sum_{j=1}^{n} \left(\delta_{ij}\alpha - b_{ij}\right) a_j = 0.$$

Dakle, jednadžba

$$\sum_{j=1}^{n} \left(\delta_{ij}\alpha - b_{ij}\right) x_j = 0, \quad i = 1, \ldots, n.$$

ima netrivijalno rješenje. Definiramo matricu M:

$$M = \left(\delta_{ij}\alpha - b_{ij}\right)_{ij}.$$

Pošto jednadžba ima netrivijalno rješenje, slijedi da je

$$\det M = 0.$$

Međutim $\det M$ je normirani polinom u α:

$$\alpha^n + (b_{11} + b_{22} + \cdots + b_{nn})\,\alpha^{n-1} + \cdots = 0.$$

Iz ovoga zaključujemo da je $\alpha \in \mathcal{O}_K$.

□

Lema 3.0.11

Neka je $\alpha \in K$. Tada postoji $0 \neq q \in \mathbb{Z}$ takav da $q\alpha \in \mathcal{O}_K$.

Dokaz. Neka je $f_\alpha(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Q}[x]$ minimalni polinom od α. Postoji $q \in \mathbb{Z}$ takav da

$$qx^n + qa_{n-1}x^{n-1} + \cdots + qa_0 = qf_\alpha(x) \in \mathbb{Z}[x].$$

Definiramo polinom:

$$g(x) = \sum_{i=0}^{n} q^{n-i}a_i x^i \in \mathbb{Z}[x].$$

Vidimo i da je g normiran, dakle njegovi korijeni su cijeli. Vrijedi:

$$g(q\alpha) = q^n\alpha^n + q^n a_{n-1}\alpha^{n-1} + \cdots + q^n a_0 = q^n f(\alpha) = 0.$$

Dakle, $q\alpha \in \mathcal{O}_K$. □

Lema 3.0.12

Neka su $\alpha, \beta \in \mathcal{O}_K$. Tada je $\mathbb{Z}[\alpha, \beta]$ konačno generiran $\mathbb{Z}$-modul koji je sadržan u K. Općenito, $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ je konačno generiran podmodul od K za $\alpha_1, \ldots \alpha_n \in \mathcal{O}_K$.

Dokaz. Neka su $a_1, \ldots a_k$ generatori od $\mathbb{Z}[\alpha]$, a $b_1, \ldots b_l$ generatori od $\mathbb{Z}[\beta]$. Slijedi da $\{a_i b_j \mid 1 \leq i \leq k, 1 \leq j \leq l\}$ generira $\mathbb{Z}[\alpha, \beta]$. □

Teorem 3.0.13

$\mathcal{O}_K$ je prsten.

Dokaz. Neka su $\alpha, \beta \in \mathcal{O}_K$. Moramo dokazati da $\alpha + \beta, \alpha\beta \in \mathcal{O}_K$. Po prošloj lemi $\mathbb{Z}[\alpha, \beta]$ je konačno generiran $\mathbb{Z}$-modul, te slijedi da $\alpha + \beta, \alpha\beta \in \mathbb{Z}[\alpha, \beta]$. □

Propozicija 3.0.14

Neka je $f(x) \in \mathcal{O}_K[x]$ normiran, te je $\alpha \in K$ korijen od f. Tada slijedi da je $\alpha \in \mathcal{O}_K$, drugim riječima $\mathcal{O}_K$ je integralno zatvoren.

Dokaz. Neka je:

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{O}_K[x], \text{ gdje su } a_i \in \mathcal{O}_K.$$

Definirajmo $S = \mathbb{Z}[a_0, \ldots, a_{n-1}]$. Po lemi je to konačno generiran $\mathbb{Z}$-modul. Ako definiramo $S' := S[\alpha]$, tada je S' konačno generiran S-modul, a time i konačno generiran $\mathbb{Z}$-modul. Po propoziciji (3), slijedi da je $\alpha \in \mathcal{O}_K$. □

Zaključak je da vrijedi

$$\mathcal{O}_K = K \cap \mathbb{A} = \{\alpha \in K : \quad f_\alpha \in \mathbb{Z}[x]\} = \{\alpha \in K : \quad f_\alpha \in \mathcal{O}_K[x]\},$$

gdje zadnja jednakost slijedi iz integralne zatvorenosti od $\mathcal{O}_K$. Dakle $\mathcal{O}_K$ je "dovoljno velik prsten".

Neka je $K = \mathbb{Q}(\sqrt{d})$, gdje je $d \in \mathbb{Z}$ kvadratno slobodan. Odredimo $\mathcal{O}_K$.

Neka je $\alpha \in K \Rightarrow \alpha = a + b\sqrt{d}, \quad a, b \in \mathbb{Q} \quad b \neq 0$. Pretpostavimo da je $\alpha \notin \mathbb{Q}$ i $\alpha \in \mathcal{O}_K$. Minimalni polinom f_α od α je: $f_\alpha(x) = x^2 - 2ax + (a^2 - b^2 d)$, (DZ).

$$\alpha \in \mathcal{O}_k \quad \Leftrightarrow \quad f_\alpha \in \mathbb{Z}[x] \Leftrightarrow \quad 2a \in \mathbb{Z}; \quad a^2 - b^2 d \in \mathbb{Z}$$

Ako $a \in \mathbb{Z} \Rightarrow b^2 d \in \mathbb{Z}$, pa pošto je d kvadratno slobodan, slijedi da je $b^2 \in \mathbb{Z} \Rightarrow b \in \mathbb{Z}$.

$$\Rightarrow \quad \alpha \in \mathbb{Z}[\sqrt{d}].$$

Za $\alpha \in \mathbb{Z}[\sqrt{d}]$ slijedi $f_\alpha \in \mathbb{Z}[x]$, dakle $\alpha \in \mathcal{O}_K$. Dakle $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$.

Neka je sada $a \notin \mathbb{Z}$.

$$a \notin \mathbb{Z} \quad \overset{2a \in \mathbb{Z}}{\Longrightarrow} \quad a = \frac{a_1}{2}, \quad a_1 \in \mathbb{Z} \Longrightarrow \frac{a_1^2}{4} - b^2 d \in \mathbb{Z}$$

$$\Rightarrow \quad b = \frac{b_1}{2}, \quad b_1 \in \mathbb{Z}$$

Vidimo, pošto je a_1 neparan, da vrijedi $a_1^2 \equiv b_1^2 \equiv 1 \pmod 4$, pa slijedi $1 - d \equiv a_1^2 - b_1^2 d \equiv 0 \pmod 4$. Dakle, vrijedi $d \equiv 1 \pmod 4$

Dobili smo da je, ako $K = \mathbb{Q}(\sqrt{d})$, slijedi

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & \text{ako } d \equiv 1 \pmod 4, \\ \mathbb{Z}[\sqrt{d}], & \text{ako } d \equiv 2, 3 \pmod 4. \end{cases}$$

3.1 Trag i norma

Definicija 3.1.1

Neka je K polje algebarskih brojeva tako da $[K : \mathbb{Q}] = n$. Neka su $\sigma_1, \ldots, \sigma_n$ ulaganja $K \hookrightarrow \mathbb{C}$.
Za element $\alpha \in K$ definiramo:

$$T_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha), \quad \text{je trag od } \alpha \text{ nad } \mathbb{Q},$$
$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha), \quad \text{je norma od } \alpha \text{ nad } \mathbb{Q}.$$

Odmah slijedi iz definicija:

$$T(\alpha + \beta) = T(\alpha) + T(\beta),$$
$$N(\alpha\beta) = N(\alpha)N(\beta), \quad \forall \alpha, \beta \in K,$$

$$T(r\alpha) = rT(\alpha)$$
$$N(r\alpha) = r^n N(\alpha), \qquad r \in \mathbb{Q}, \alpha \in K,$$
$$T(r) = n \cdot r,$$
$$N(r) = r^n, \qquad \forall r \in \mathbb{Q}.$$

Neka je α element stupnja d nad $\mathbb{Q}$ ($[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$). Tada definiramo trag $t(\alpha)$ i normu $n(\alpha)$ kao zbroj (umnožak) konjugata od α nad $\mathbb{Q}$.

Lema 3.1.2

Vrijedi $T(\alpha) = \frac{n}{d} t(\alpha)$, i $N(\alpha) = n(\alpha)^{\frac{n}{d}}$.

Dokaz. Ovdje su $t(\alpha)$ i $n(\alpha)$ trag i norma od α u odnosu na proširenje $\mathbb{Q}(\alpha)/\mathbb{Q}$. Budući da se svako ulaganje iz $\mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$ može proširiti na točno $\frac{n}{d}$ ulaganja $K \hookrightarrow \mathbb{C}$, te je svako ulaganje od α određeno djelovanjem na $\mathbb{Q}(\alpha)$, lema slijedi. □

Korolar 3.1.3

$T(\alpha)$ i $N(\alpha) \in \mathbb{Q}$.

Dokaz. Dovoljno je prema Lemi 3.1.2 dokazati da $t(\alpha)$ i $n(\alpha) \in \mathbb{Q}$.
Neka je minimalni polinom od α nad $\mathbb{Q}$:

$$\begin{aligned} f(x) &= x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \\ &= (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d). \end{aligned}$$

Prema Vieteovim formulama,

$$t(\alpha) = -a_{d-1} \in \mathbb{Q},$$
$$n(\alpha) = (-1)^d a_0 \in \mathbb{Q}.$$

□

Korolar 3.1.4

Ako je $\alpha \in \mathcal{O}_K$, tada je $T(\alpha), N(\alpha) \in \mathbb{Z}$.

Dokaz. Budući da je $\alpha \in \mathcal{O}_K$ i da je $f(x) \in \mathbb{Z}[x]$, slijedi odmah $t(\alpha), n(\alpha) \in \mathbb{Z}$. □

Primjer 3.1.5

$$K = \mathbb{Q}(\sqrt{d})$$
$$T_{K/\mathbb{Q}}(a + b\sqrt{d}) = 2a$$
$$N_{K/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - db^2.$$

Lema 3.1.6

Za $u \in \mathcal{O}_K$ vrijedi

$$u \in \mathcal{O}_K^\times \quad \Longleftrightarrow \quad N(u) = \pm 1.$$

Dokaz. $\boxed{\Longrightarrow}$

$$\text{Postoji } v \in \mathcal{O}_K \text{ takav da} \quad uv = 1 \quad /N$$
$$N(uv) = 1^{[K:\mathbb{Q}]} = 1 \Longrightarrow \quad N(u)N(v) = 1.$$

Po Korolaru, $N(u), N(v) \in \mathbb{Z}$, pa $N(u) = \pm 1$.

$\boxed{\Longleftarrow}$ Neka je f minimalni polinom od u.

$$f(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + (-1)^d n(u) \in \mathbb{Z}[x],$$
$$0 = f(u) = u^d + a_{d-1}u^{d-1} + \ldots + (-1)^d n(u)$$
$$\Rightarrow u\left(u^{d-1} + a_{d-1}u^{d-2} + \ldots + a_1\right) = (-1)^{d+1} n(u) \in \{\pm 1\}$$
$$\Rightarrow \quad u \in \mathcal{O}_K^\times.$$

□

Primjer 3.1.7

Odredite $\mathcal{O}_K^\times$ za $K = \mathbb{Q}(\sqrt{-2})$.

Rješenje: Znamo da je $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$. Vrijedi $\alpha \in \mathcal{O}_K \Rightarrow \alpha = a + b\sqrt{-2}, \quad a, b \in \mathbb{Z}$. Vrijedi

$$N(\alpha) = a^2 + 2b^2, \text{ pa je}$$
$$N(\alpha) = \pm 1 \quad \Leftrightarrow \quad a^2 + 2b^2 = 1 \Leftrightarrow \quad a = \pm 1, \quad b = 0.$$

Zaključujemo $\mathcal{O}_K^\times = \{\pm 1\}$. □

Analogno vrijedi za sve $\mathbb{Q}(\sqrt{d})$, gdje je $d < 0$, osim za $d = -1, -3$. Za $K = \mathbb{Q}(i)$ smo već pokazali:$\mathcal{O}_K^\times = \{\pm 1, \pm i\}$.

Neka je sada $K = \mathbb{Q}(\sqrt{-3})$. Znamo da je $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Za $\alpha \in \mathcal{O}_K$ imamo $\alpha = a + b\frac{1+\sqrt{-3}}{2}, \quad a, b \in \mathbb{Z}$. Tada vrijedi:

$$\begin{aligned} N(\alpha) &= \left(a + \frac{b}{2}\right)^2 + \frac{3}{4}b^2 \\ &= a^2 + ab + b^2. \end{aligned}$$

Ako je $N(\alpha) = \pm 1$, tada imamo:

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

Zaključujemo:

$|b| \leq 1$,

$$b = -1 \Rightarrow 1 - a + a^2 = 1 \Rightarrow a \in \{0, 1\} \Rightarrow \alpha \in \left\{\frac{1-\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}\right\},$$

$$b = 0 \Rightarrow a^2 = 1 \Rightarrow \alpha \in \{\pm 1\},$$

$$b = 1 \Rightarrow 1 + a + a^2 = 1 \Rightarrow a \in \{-1, 0\} \Rightarrow \alpha \in \left\{\frac{1+\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}\right\}.$$

Dakle,

$$\mathcal{O}_K^\times = \left\{\pm 1, \frac{1 \pm \sqrt{-3}}{2}, \frac{-1 \pm \sqrt{-3}}{2}\right\}.$$

(4) U slučaju kada je $K = \mathbb{Q}(\sqrt{2})$, imamo

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{2}],$$
$$\alpha = a + b\sqrt{2}, \quad a, b \in \mathbb{Z},$$
$$N(\alpha) = \pm 1 \Leftrightarrow a^2 - 2b^2 = \pm 1.$$

Vrijedi: $N(1 + \sqrt{2}) = -1, \quad N((1 + \sqrt{2})^n) = (-1)^n$. Dakle $\mathcal{O}_K^\times$ je beskonačna grupa. Iz teorije brojeva zapravo možemo zaključiti

$$\mathcal{O}_K^\times = \{(1 + \sqrt{2})^n, n \in \mathbb{Z}\}.$$

Norma se može koristiti da se pokaže da je element $\alpha \in \mathcal{O}_K$ ireducibilan ako je $N(\alpha) = \pm$ prost broj. Očito to implicira da je α ireducibilan.

1. $9+\sqrt{10}$ je ireducibilan u $\mathbb{Z}[\sqrt{10}]$, jer je $N(9+\sqrt{10}) = 81-10 = 71$, što je prost broj
2. Neka je $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Tada $\mathcal{O}_K$ ne sadrži elemente čija je norma $\equiv \pm 2 \pmod 5$ pošto
$$a^2 + 5b^2 = \pm 2 \pmod 5,$$
nema rješenja. Slijedi da su npr. elementi $2, 3, 1+\sqrt{-5}$ ireducibilni (pošto ne postoje elementi norme $\pm 2, \pm 3$ u $\mathcal{O}_K$).

Norma i trag elementa se mogu definirati općenitije. Neka je L/K proširenje polja, gdje je $[L:K] = n$, a $\sigma_1, \ldots, \sigma_n$ su K-ulaganja $L \hookrightarrow \mathbb{C}$.

Definiramo trag $T_{L/K}(\alpha)$ kao:
$$T_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$
i normu $N_{L/K}(\alpha)$ kao:
$$N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$
Lako se vidi sljedeće:

Propozicija 3.1.8

Neka je $\alpha \in L$, te L/K proširenje. Vrijedi $T_{L/K}(\alpha) \in K$, te $N_{L/K}(\alpha) \in K$. Ako je $\alpha \in \mathcal{O}_L$, tada je $T_{L/K}(\alpha) \in \mathcal{O}_K$, te $N_{L/K}(\alpha) \in \mathcal{O}_K$.

Teorem 3.1.9

Neka su $K \subset L \subset M$ polja algebarskih brojeva. Tada za $\alpha \in M$ vrijedi:
$$T_{L/K}\left(T_{M/L}(\alpha)\right) = T_{M/K}(\alpha),$$
$$N_{L/K}\left(N_{M/L}(\alpha)\right) = N_{M/K}(\alpha).$$

Dokaz. Neka su $\sigma_1, \ldots, \sigma_n$ K-ulaganja $L \hookrightarrow \mathbb{C}$ i neka su $\tau_1, \ldots, \tau_m$ L-ulaganja $M \hookrightarrow \mathbb{C}$. σ_j-eve možemo proširiti na K-ulaganja $\tilde{M} \hookrightarrow \mathbb{C}$, gdje je $\tilde{M}$ normalno zatvorenje od M nad K (neće biti bitan izbor ulaganja).

Tada imamo:
$$\begin{aligned} T_{L/K}\left(T_{M/L}(\alpha)\right) &= T_{L/K}\left(\sum_{i=1}^{m} \tau_i(\alpha)\right) \\ &= \sum_{j=1}^{n} \sigma_j \left(\sum_{i=1}^{m} \tau_i(\alpha)\right) \\ &= \sum_{i,j} \sigma_j \tau_i(\alpha). \end{aligned}$$

gdje $\sigma_j\tau_i$ K-ulaganja M u $\mathbb{C}$, te ih ima $m \cdot n = [M : K]$. Treba pokazati da su sva različita, to jest

$$\sigma_i\tau_j = \sigma_u\tau_v \quad \Leftrightarrow \quad i = u, \quad j = v.$$

Neka je $\sigma_i\tau_j = \sigma_u\tau_v$

$$\begin{aligned} &\Rightarrow \quad \sigma_i\tau_j|_L = \sigma_u\tau_v|_L \\ &\Rightarrow \quad \sigma_i|_L = \sigma_u|_L \end{aligned}$$

pošto je τ_j, τ_v identiteta na L. Dakle $i = u$. Uvrštavanjem gore dobijemo

$$\tau_j|_M = \tau_v|_M \Rightarrow \tau_j = \tau_v \Rightarrow j = v.$$

□

3.2 Diskriminanta

Definicija 3.2.1

Neka je K PAB i neka je $[K : \mathbb{Q}] = n$. Označimo sa $\sigma_1, \ldots, \sigma_n$, ulaganja $K \hookrightarrow \mathbb{C}$, i neka su $\alpha_1, \ldots, \alpha_n \in K$. **Diskriminanta** $\Delta(\alpha_1, \ldots, \alpha_n)$ je kvadrat determinante matrice $(\sigma_i(\alpha_j))_{i,j}$.

Primjer 3.2.2

Neka je $K = \mathbb{Q}(\sqrt{2})$. Tada:

$$\Delta\left(1, \sqrt{2}\right) = \left|\begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix}\right|^2 = (-2\sqrt{2})^2 = 8.$$

Lema 3.2.3

Neka su oznake kao i iznad. Tada vrijedi

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det\left(T_{K/\mathbb{Q}}(\alpha_i\alpha_j)\right)_{ij}.$$

Dokaz. Neka je $A = (\sigma_i(\alpha_j))_{ij}$. Pošto je $\det(A) = \det(A^\tau)$, vrijedi

$$\begin{aligned} \Delta(\alpha_1, \ldots, \alpha_n) &= (\det(A))^2 = \det(A^\tau A) \\ &= \det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right) \\ &= \det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j)\right) \\ &= \det\left(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)\right)_{ij} \end{aligned}$$

□

Primjer 3.2.4

$$\Delta(1,\sqrt{2}) = \left|\begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}\right| = 8.$$

Korolar 3.2.5

$\Delta(\alpha_1,\ldots,\alpha_n) \in \mathbb{Q}$, i ako su $\alpha_1,\ldots,\alpha_n \in \mathcal{O}_K$, tada je $\Delta(\alpha_1,\ldots,\alpha_n) \in \mathbb{Z}$.

Teorem 3.2.6

$\Delta(\alpha_1,\ldots,\alpha_n) = 0 \Leftrightarrow \alpha_1,\ldots,\alpha_n$ su linearno zavisni nad $\mathbb{Q}$.

Dokaz. $\boxed{\Longleftarrow}$ Ako su $\alpha_1,\ldots,\alpha_n$ linearno zavisni, tada postoji relacija

$$\alpha_1 = \sum_{i=2}^{n} a_i\alpha_i.$$

Onda imamo matricu:

$$\begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{vmatrix} = \sum_{i=2}^{n} a_i \begin{vmatrix} \sigma_1(\alpha_i) & \ldots & \sigma_1(\alpha_i) & \ldots \\ \sigma_2(\alpha_i) & \ldots & \sigma_2(\alpha_i) & \ldots \\ \ldots & \ldots & \ldots & \ddots \end{vmatrix} = 0.$$

Dakle imamo 2 ista stupca, pa je $\Delta(\alpha_1,\ldots,\alpha_n) = 0$.

$\boxed{\Longrightarrow}$ Neka je $\Delta(\alpha_1,\ldots,\alpha_n) = 0$ i pretpostavimo suprotno, tj, $\alpha_1,\ldots,\alpha_n$ linearno nezavisni nad $\mathbb{Q}$.

Označimo s $R_1,\ldots,R_n$ retke matrice

$$A = \mathrm{Tr}(\alpha_i\alpha_j)_{ij}.$$

Vrijedi $\det A = \Delta(\alpha_1,\ldots,\alpha_n) = 0$.

$\Rightarrow$ $R_1,\ldots,R_n$ su linearno zavisni nad $\mathbb{Q}$, pa postoji relacija:

$$a_1R_1 + a_2R_2 + \ldots + a_nR_n = 0, \quad \text{gdje su } a_i \in \mathbb{Q}, \quad \text{i nisu svi } a_i = 0$$

pa pošto suma u j-tom stupcu mora biti 0 vrijedi:

$$\sum_{i=1}^{n} a_i \,\mathrm{Tr}\,(\alpha_i\alpha_j) = 0, \quad \forall j = 1,\ldots,n.$$

Neka je $\alpha = a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n \Rightarrow \alpha \neq 0$.

Pogledajmo

$$\mathrm{Tr}(\alpha\alpha_j) = \mathrm{Tr}\left(\sum_{i=1}^{n} a_i\alpha_i\alpha_j\right) = \sum_{i=1}^{n} a_i\,\mathrm{Tr}(\alpha_i\alpha_j) = 0, \quad \forall j = 1,\ldots,n.$$

$$\Rightarrow \quad \mathrm{Tr}(\alpha\beta) = 0, \quad \forall \beta \in K.$$

Međutim

$$n = \mathrm{Tr}(1) = \mathrm{Tr}\left(\alpha \cdot \frac{1}{\alpha}\right) = 0,$$

dakle dobili smo kontradikciju. □

Propozicija 3.2.7

Neka je K PAB s bazom (nad $\mathbb{Q}$) $\alpha_1,\ldots,\alpha_n \in \mathcal{O}_K$. Neka su $a_i \in \mathbb{Q}$ takvi da je $a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n \in \mathcal{O}_K$. Tada je $\Delta(\alpha_1,\ldots,\alpha_n)\cdot a_i \in \mathbb{Z}$.

Dokaz. Neka je $\Delta := \Delta(\alpha_1,\ldots,\alpha_n)$.

Neka su $\sigma_1,\ldots,\sigma_n$ ulaganja $K \hookrightarrow \mathbb{C}$. Promotrimo sustav

$$\sigma_i(\alpha) = a_1\sigma_i(\alpha_1) + a_2\sigma_i(\alpha_2) + \ldots + a_n\sigma_i(\alpha_n).$$

Možemo ga promatrati kao sustav s n "nepoznanica" a_i. Može se zapisati u matrici oblika:

$$\begin{bmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{bmatrix} = \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{bmatrix} \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}.$$

Pošto je $\Delta \neq 0$, slijedi da postoji jedinstveno rješenje. Po Cramerovom pravilu: $a_i = \frac{\gamma_i}{\delta}$, gdje je γ_i determinanta matrice dobivene zamjenom i-tog stupca sa stupcem $\begin{bmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{bmatrix}$, a δ je determinanta matrice jednadžbe. Pošto ulaganje σ_i šalje α_j u neki njegov konjugat, slijedi da su $\delta, \gamma_i \in \mathcal{O}_K$, te

$$\Delta a_i = \frac{\gamma_i\delta^2}{\delta} = \gamma_i\delta \in \mathcal{O}_K.$$

Slijedi $\Delta a_i \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$. □

Teorem 3.2.8

Neka je K konačno proširenje polja $\mathbb{Q}$ stupnja $[K:\mathbb{Q}] = n$. Tada je prsten cijelih brojeva $\mathcal{O}_K$ slobodan $\mathbb{Z}$-modul ranga n.

Dokaz. Neka je $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ baza od K nad $\mathbb{Q}$ s $\alpha_i \in \mathcal{O}_K$; takva postoji po Lemi 3.0.11, te

$$\mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n \subseteq \mathcal{O}_K,$$

slijedi da je rang od $\mathcal{O}_K$ veći ili jednak od n.

Po prošloj propoziciji vrijedi:

$$\mathcal{O}_K \subseteq \frac{1}{\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)} \left(\mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n\right),$$

pa slijedi da je rang $\mathcal{O}_K$ manji ili jednak od n. □

Korolar 3.2.9

$\mathcal{O}_K$ je Noetherin prsten.

Dokaz. Po prošlom teoremu možemo zapisati

$$\mathcal{O}_K = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$$

za neke $\alpha_1, \ldots, \alpha_n$.

Dakle, postoji surjektivni homomorfizam

$$\mathbb{Z}[x_1, \ldots, x_n] \to \mathbb{Z}[\alpha_1, \ldots, \alpha_n].$$

Pošto je $\mathbb{Z}[x_1, \ldots, x_n]$ Noetherin prsten, te pošto je slika homomorfizma iz Noetherinog prstena opet Noetherin prsten, slijedi da je i $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ Noetherin prsten. □

3.3 Dedekindove domene

Definicija 3.3.1: Dedekindova domena

Integralnu domenu R nazivamo *Dedekindovom domenom* ako zadovoljava sljedeće uvjete:

- R je Noetherin prsten (svaki ideal u R je konačno generiran),
- R je integralno zatvoren u svojem polju razlomaka,
- Svaki nenul prosti ideal je maksimalan.

Lema 3.3.2

Neka je a ideal u $\mathcal{O}_K$ (prstenu cijelih brojeva PAB K), gdje $a \neq (0)$. Tada vrijedi $a \cap \mathbb{Z} \neq \{0\}$.

Dokaz. Neka je $\alpha \in a$. Tvrdimo da

$$N_{K/\mathbb{Q}}(\alpha) \in a \cap \mathbb{Z}.$$

Treba dokazati da $N_{K/\mathbb{Q}}(\alpha) \subseteq a$.

Neka je $\sigma : K \hookrightarrow \mathbb{C}$ neko ulaganje, te $\alpha_1, \alpha_2, \ldots, \alpha_n$ svi konjugati elementa α nad $\mathbb{Q}$. Neka je bez smanjenja općenitosti $\alpha_1 = \sigma(\alpha)$. Tada vrijedi:

$$N_{K/\mathbb{Q}}(\alpha) = \alpha_1 \alpha_2 \cdots \alpha_n,$$

te definirajmo $\alpha' := \alpha_2 \cdots \alpha_n$. Primijetimo da su svi konjugati od α cijeli algebarski brojevi, pa je i α' cijeli algebarski broj.

Slijedi

$$\alpha' = \frac{N_{K/\mathbb{Q}}(\alpha)}{\alpha_1} \in \mathcal{O}_K.$$

Neka je α'' takva da je $\alpha'' := \sigma^{-1}(\alpha')$.

Budući da je a ideal, zaključujemo da $\alpha'' \alpha \in a$. Konačno imamo:

$$\alpha'' \cdot \alpha = \sigma^{-1}(\alpha') \cdot \sigma^{-1}(\alpha_1) = \sigma^{-1}(\alpha_1 \cdot \ldots \cdot \alpha_n) = N_{K/\mathbb{Q}}(\alpha).$$

Dakle $\alpha'' \cdot \alpha \in \mathbb{Z} \cap a$, te smo gotovi. □

Propozicija 3.3.3

$\mathcal{O}_K$ je Dedekindova domena.

Dokaz. Tvrdimo da je svaki nenul prosti ideal u $\mathcal{O}_K$ maksimalan ideal.

Neka je P neki nenul prosti ideal, pa po Lemi 3.3.2 postoji $m \in \mathbb{Z} \cap P$. Dakle, $(m) \subseteq P$.

Pogledajmo preslikavanje $\varphi : \mathcal{O}_K/(m) \to \mathcal{O}_K/P$ zadano sa

$$a + (m) \mapsto a + P.$$

Očito je surjekcija.

Ako je $[K : \mathbb{Q}] = n$, tada je

$$|\mathcal{O}_K/(m)| = |(\mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \ldots + \mathbb{Z}\alpha_n)/(m)| = m^n < +\infty,$$

za neke $\alpha_1, \ldots, \alpha_n$.

Slijedi da je $\mathcal{O}_K/P$ konačna integralna domena. Međutim, svaka konačna integralna domena je polje (DZ - pogledajte potencije od x, pa zbog konačnosti postoji neki m takav da je $x^m = x$, pa slijedi da je $x^{m-1} = x^{-1}$.) Slijedi da je P maksimalan ideal. □

3.4 Jedinstvena faktorizacija u Dedekindovim domenama

Lema 3.4.1

Neka je A ideal u Dedekindovoj domeni R. Tada postoje prosti ne-nul ideali $p_1, \ldots, p_n$ t.d $p_1 \cdot \ldots \cdot p_n \subseteq A$.

Dokaz. Pretpostavimo suprotno, neka postoje ideali za koje to ne vrijedi, te nazovimo skup takvih ideala S. Pošto je R Noetherin, postoji maksimalni element u tom skupu; nazovimo ga B. Pošto je B iz S, on nije prost.

Dakle postoje $\alpha, \beta \in R$ takvi da $\alpha\beta \in B$, ali $\alpha \notin B$ i $\beta \notin B$.

Pošto je B maksimalan u S, slijedi da $B + (\alpha)$ i $B + (\beta)$ nisu iz S. Sada imamo

$$(B + (\alpha))(B + (\beta)) = B \cdot B + B(\alpha) + B(\beta) + (\alpha)(\beta).$$

Vidimo da su svi sumandi iz B, pa je i suma iz B.

Međutim, pošto $B + (\alpha)$ i $B + (\beta)$ nisu iz S, slijedi da postoje ideali p_i, q_j takvi da

$$B + (\alpha) \supseteq p_1 \cdot \ldots \cdot p_k,$$
$$B + (\beta) \supseteq q_1 \cdot \ldots \cdot q_l,$$

pa je

$$p_1 \cdot \ldots \cdot p_k q_1 \cdot \ldots \cdot q_l \subseteq (B + (\alpha))(B + (\beta)) \subseteq B,$$

što je kontradikcija s našom pretpostavkom. □

Lema 3.4.2

Neka je $A \neq 0$ ideal u Dedekindovoj domeni R, i neka je $A \neq R$. Neka je K polje razlomaka od R. Tada postoji element $\gamma \in K$ takav da je $\gamma A \subseteq R$ i $\gamma \notin R$.

Dokaz. Neka je $0 \neq \alpha \in A$ proizvoljan. Sada po prošloj lemi postoje prosti nenul ideali $p_1, \ldots, p_k$ takvi da je

$$(\alpha) \supseteq p_1 \cdot \ldots \cdot p_k$$

takvi da je k minimalan. Pošto je prsten R Noetherin, A je sadržan u nekom maksimalnom idealu P. Vrijedi

$$P \supseteq A \supseteq (\alpha) \supseteq p_1 \cdot \ldots \cdot p_k.$$

S druge strane, pošto je R DD, slijedi da su $p_1, \ldots, p_k$ maksimalni. Dakle bez smanjenja općenitosti vrijedi $P = p_1$; ovo vrijedi jer je P prost, pa ako sadrži produkt, onda mora sadržati i jedan faktor. Primijetimo da ako je $k = 1$, tada je $p_2 \cdot \ldots \cdot p_k = R$.

Po pretpostavci minimalnosti od k, slijedi da α ne sadrži produkt $k - 1$ prostih ideala. Dakle postoji $\beta \in p_2 \cdot \ldots \cdot p_k$ takav da $\beta \notin (\alpha)$.

Neka je $\gamma := \frac{\beta}{\alpha}$. Tvrdimo da γ zadovoljava lemu. Vrijedi

1. $\gamma \notin R$ jer $\beta \notin (\alpha)$
2. Za svaki $\alpha' \in A$, slijedi da je $\beta\alpha' \in p_1 \cdot p_2 \cdot \ldots \cdot p_k$, pošto je $\alpha' \in p_1$, a $\beta \in p_2 \cdot \ldots \cdot p_k$. Dakle $\beta\alpha' \in p_1 \cdot \ldots \cdot p_k \subseteq (\alpha)$. Slijedi da je

$$\gamma \cdot \alpha' = \frac{\beta\alpha'}{\alpha} \in \frac{1}{\alpha}(\alpha) = R.$$

□

Propozicija 3.4.3

Neka je $A \neq 0$ ideal u DD (Dedekindovoj domeni) R. Tada postoji ideal $B \subseteq R$ t.d je AB glavni ideal.

Dokaz. Neka je $0 \neq \alpha \in A$ i neka je

$$B := \{\beta \in R | \beta A \subseteq (\alpha)\}.$$

Pošto je $\alpha \in B$, slijedi da $B \neq (0)$. Također, lako se provjeri da je B ideal. Nadalje, po definiciji od B slijedi da je

$$AB \subseteq (\alpha).$$

Tvrdimo da je $AB = (\alpha)$. Promotrimo $C := \frac{1}{\alpha}AB \subseteq R$. Vrijedi

$$AB = (\alpha) \iff C = R.$$

Pošto su A i B ideali u R, slijedi i da je C ideal u R.

Pretpostavimo suprotno, tj. da je $C \neq R$. Po Lemi 3.4.2, postoji $\gamma \in K$ takav da $\gamma \notin R$ takav da je $\gamma C \subseteq R$.

Mi ćemo pokazati da je γ nultočka normiranog polinoma iz $R[x]$, iz čega će slijediti da je $\gamma \in R$, pošto je R integralno zatvoren. To će međutim biti kontradikcija s našom pretpostavkom na γ.

Primijetimo da za svaki $\beta \in B$ vrijedi

$$\beta = \frac{1}{\alpha}\alpha\beta \in C,$$

pa je $B \subseteq C$. Imamo

$$\gamma B \subseteq \gamma C \subset R.$$

Sada tvrdimo: $\boxed{\gamma B \subseteq B}$. Neka je $\beta \in B$ proizvoljan. On zadovoljava $\beta\alpha' \in (\alpha)$ za sve $\alpha' \in A$. Želimo dokazati:

$$\forall \alpha' \in A, \quad \gamma\beta\alpha' \in (\alpha).$$

Fiksirajmo $\alpha' \in A$. Vrijedi

$$\beta\alpha' \in (\alpha) \quad \text{(po definiciji od } B\text{)},$$

$$\implies \beta\alpha' = \alpha\delta, \quad \text{za neki } \delta \in R$$
$$\implies \delta = \frac{1}{\alpha}\alpha'\beta \in C$$
$$\implies \gamma\delta \in \gamma C \subseteq R$$
$$\implies \gamma\beta\alpha' = \alpha\gamma\delta \in (\alpha) \quad \text{pošto je } \gamma\delta \in R.$$
$$\implies \gamma\beta \in B \implies \gamma B \subseteq B.$$

Imamo da je B ideal u R, pa pošto je R Noetherin, B je konačno generiran kao R-modul, tj. $B = R[b_1, \ldots, b_n]$. Ako promotrimo množenje s γ to je "linearni operator" u B, pa možemo djelovanje na bazu $\{b_1, \ldots, b_n\}$ zapisati s nekom matricom M s koeficijentima iz R. Po Hamilton-Cayleyevom teoremu postoji normirani polinom iz $R[x]$ koji poništava γ, pošto je γ svojstvena vrijednost od matrice M. □

Lema 3.4.4

Neka su A, B, C ideali u Dedekindovoj domeni R i neka je $A \neq \{0\}$. Tada $AB = AC$ povlači da je $B = C$.

Dokaz. Neka je $A' \subseteq R$ ideal takav da je $AA' = (\alpha)$ glavni ideal; takav postoji po Propoziciji 3.4.3.

Pošto je $AB = AC$, slijedi da je

$$AA'B = AA'C,$$

pa je

$$(\alpha)B = (\alpha)C, \text{to jest } \alpha B = \alpha C.$$

Slijedi da je $B = C$. □

Definicija 3.4.5

Za ideale A, B u Dedekindovoj domeni R kažemo da B *dijeli* A ako postoji ideal C u R takav da je $A = BC$.

Primijetimo da ako B dijeli A, tada $B \supseteq A$. Dokažimo da u Dedekindovoj domeni vrijedi i obrat ovoga.

Lema 3.4.6

Neka su A, B ideali u Dedekindovoj domeni R. Tada B dijeli A ako i samo ako $B \supseteq A$.

Dokaz. $\boxed{\implies}$ Ovo je očito.
$\boxed{\impliedby}$ Neka je $B \supseteq A$, B' ideal takav da $BB' = (\beta)$. Neka je

$$C = \frac{1}{\beta}B'A \subset R.$$

Ovo je ideal u R pošto je $B \supseteq A$. Slijedi

$$BC = \frac{1}{\beta} BB'A = \frac{1}{\beta}\beta A = A.$$

□

Definicija 3.4.7

Kažemo da se ideal $A \subseteq R$ *faktorizira u proste ideale* ako se može zapisati kao $A = P_1 P_2 \dots P_k$, gdje su $P_i \neq 0$ prosti ideali u R. Kažemo da se A *jedinstveno faktorizira u proste ideale* ako je faktorizacija od A u proste ideale jedinstvena do na poredak P_i-ova.

Teorem 3.4.8: Teorem o jedinstvenoj faktorizaciji u Dedekindovim domenama

Svaki nenul ideal u Dedekindovoj domeni R ima jedinstvenu faktorizaciju u proste ideale.

Dokaz. Dokažimo prvo da se svaki nenul ideal faktorizira u proste ideale. Neka je S skup pravih ideala koji se ne faktoriziraju u proste ideale. Pretpostavimo $S \neq \emptyset$.

Pošto je R Noetherin, slijedi da S ima maksimalni element A (primijetimo da ovo ne znači da je A maksimalan ideal). Slijedi da je $A \subseteq P$ za neki maksimalan ideal P. Slijedi da je P prost ideal. Po Lemi 3.4.6 slijedi da P dijeli A, pa je $A = PB$ za neki ideal B u R.

Pokažimo da $A \neq B$. Pretpostavimo suprotno, tj. $A = B$. Podijelimo $B = A = PB$ s B; dobijemo $P = R$, što je kontradikcija.

Dakle imamo $A \subseteq B$, $A \neq B$, tj. $A \subsetneq B$. Slijedi da $B \notin S$, dakle B se faktorizira na proste ideale

$$B = P_1 \dots P_t.$$

Slijedi da se A faktorizira u proste ideale

$$A = PP_1 \dots P_t,$$

što je kontradikcija.

Dokažimo sada jedinstvenost faktorizacije. Pretpostavimo

$$Q_1 \dots Q_s = A = P_1 \dots P_r,$$

za neke proste ideale Q_i, P_j. Slijedi $P_1 | Q_1 \dots Q_s$, pa je $P_1 \supseteq Q_1 \dots Q_s$. Pošto je P_1 prost, slijedi da $P_1 \supseteq Q_i$ za neki $i \in \{1, \dots s\}$. Bez smanjenja općenitosti možemo pretpostaviti da je $i = 1$. Imamo $P_1 \supseteq Q_1$, te je Q_1 maksimalan, pošto smo u DD. Dakle slijedi $P_1 = Q_1$. Dijeljenjem s $P_1 = Q_1$, te ponavljanjem ovog postupka dokazujemo teorem. □

Primjer 3.4.9

Pogledajmo faktorizaciju 6 u $\mathbb{Z}[\sqrt{-5}]$. Neka je

$$P_1 = (2, 1+\sqrt{-5}), \quad P_2 = (3, 1+\sqrt{-5}), \quad P_3 = (3, 1-\sqrt{-5}).$$

Sada imamo

$$(P_1^2)(P_2P_3) = (2)(3) = (6) = (1+\sqrt{-5})(1-\sqrt{-5}) = (P_1P_2)(P_1P_3).$$

Iako faktorizacija elemenata u ireducibilne nije jedinstvena, faktorizacija u proste ideale je.

3.5 Određivanje $\mathcal{O}_K$

Sjetimo se da je slobodna Abelova grupa ranga n generirana s $\{x_1, \ldots, x_n\}$.

Lema 3.5.1

Neka je G slobodna Abelova grupa ranga n s bazom $\{x_1, \ldots, x_n\}$. Pretpostavimo da je $A = (a_{ij})$ $n \times n$ matrica, s $a_{ij} \in \mathbb{Z}$. Tada su elementi

$$y_i = \sum_{j=1}^{n} a_{ij}x_j, \quad i = 1, \ldots, n$$

baza za G ako i samo ako $\det A = \pm 1$.

Dokaz. $\boxed{\Longrightarrow}$ Imamo

$$y_i = \sum_{j=1}^{n} a_{ij}x_j, \quad i = 1, \ldots, n,$$

pa pošto y_i-evi čine bazu, imamo i

$$x_i = \sum_{j=1}^{n} b_{ij}y_j, \quad i = 1, \ldots, n,$$

za neke b_{ij}-eve. Neka je $B = (b_{ij})$. Slijedi

$$y_i = \sum_{j=1}^{n} a_{ij} \sum_{k=1}^{n} b_{jk}y_k = \sum_{k=1}^{n} (\sum_{j=1}^{n} a_{ij}b_{jk})y_k.$$

Dakle imamo $AB = I_n$, pa je $\det(AB) = \det A \det B = 1$. Pošto su $\det A, \det B \in \mathbb{Z}$, slijedi $\det A \in \{\pm 1\}$.
$\boxed{\Longleftarrow}$ Neka je $\det A \in \{\pm 1\}$. Primijetimo da to implicira da su y_i-evi linearno

nezavisni. Vrijedi $A^{-1} = (\det A)^{-1}\tilde{A}$, te su koeficijenti od $\tilde{A}$ iz $\mathbb{Z}$. Slijedi da su koeficijenti od A^{-1} iz $\mathbb{Z}$. Neka je $B = A^{-1} = (b_{ij})$. Imamo da je

$$x_i = \sum_{j=1}^{n} b_{ij} y_j,$$

pa slijedi da y_j-evi generiraju G (pošto možemo generirati sve x_i-eve.) □

Sjetimo se $\Delta(\{\alpha_1, \ldots, \alpha_n\}) = (\det(\sigma_i(\alpha_j))_{ij})^2$. Uzmimo neki skup $\{\beta_1, \ldots \beta_n\}$ takav da

$$\beta_k = \sum_{i=1}^{n} c_{ik}\alpha_i,$$

za neke $c_{ik} \in K$, te neka je $C = (c_{ij})$.

Tada vrijedi (ostavljamo dokaz za DZ):

$$\Delta(\{\beta_1, \ldots, \beta_n\}) = (\det C)^2 \Delta(\{\alpha_1, \ldots, \alpha_n\}). \tag{3.1}$$

Definicija 3.5.2

Diskriminanta Δ_K od PAB K je $\Delta(\{\alpha_1, \ldots, \alpha_n\})$, gdje je $\{\alpha_1, \ldots, \alpha_n\}$ baza od $\mathcal{O}_K$ kao $\mathbb{Z}$-modula.

Teorem 3.5.3

Neka je G aditivna podgrupa od $\mathcal{O}_K$ ranga $[K : \mathbb{Q}] = n$ sa $\mathbb{Z}$-bazom $\{\alpha_1, \ldots, \alpha_n\}$. Tada $|\mathcal{O}_K/G|^2$ (ovdje $\mathcal{O}_K$ promatramo kao aditivnu grupu) dijeli $\Delta(\{\alpha_1, \ldots, \alpha_n\})$.

Dokaz. Vrijedi (DZ): Postoji baza $\{\beta_1, \ldots \beta_n\}$ od $\mathcal{O}_K$ takva da je $\{\mu_1\beta_1, \ldots, \mu_n\beta_n\}$ $\mathbb{Z}$-baza od G, gdje su $\mu_i \in \mathbb{Z}$. Sada je po (3.1)

$$\Delta(\{\alpha_1, \ldots, \alpha_n\}) = (\mu_1 \cdot \ldots \cdot \mu_n)^2 \Delta(\{\beta_1, \ldots, \beta_n\}) = |\mathcal{O}_K/G|^2 \Delta_K.$$

Sada tvrdnja teorema slijedi iz $\Delta_K \in \mathbb{Z}$. □

Propozicija 3.5.4

Neka je $G \subsetneq \mathcal{O}_K$ aditivna podgrupa sa $\mathbb{Z}$-bazom $\{\alpha_1, \ldots, \alpha_n\}$. Tada postoji $x \in \mathcal{O}_K$ oblika

$$0 \neq x = \frac{1}{p}(\lambda_1\alpha_1 + \ldots \lambda_n\alpha_n),$$

gdje su $0 \leq \lambda_i \leq p-1, \lambda_i \in \mathbb{Z}$, i p je prost broj takav da $p^2 | \Delta(\{\alpha_1, \ldots, \alpha_n\})$.

Dokaz. Ako je $G \subsetneq \mathcal{O}_K$, slijedi da je $|\mathcal{O}_K/G| > 1$, pa postoji prost p koji dijeli $|\mathcal{O}_K/G|$ i element $G \neq U \in \mathcal{O}_K/G$ takav da $pU = G$.

Dakle postoji $x \in \frac{1}{p}G$, pa se on može zapisati kao

$$x = \frac{1}{p}(\lambda_1\alpha_1 + \dots \lambda_n\alpha_n).$$

Možemo (ako je potrebno, nakon dodavanja elemenata iz G) pretpostaviti $0 \leq \lambda_i \leq p-1$. □

Primjer 3.5.5

Dokažite da za $K = \mathbb{Q}(\sqrt{5})$ vrijedi $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Rješenje:

Pošto su generatori od $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ cijeli algebarski brojevi, očito je da $\mathcal{O}_K \supseteq \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Treba samo provjeriti da $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ nije strogo manji od $\mathcal{O}_K$.

Baza za $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ (nad $\mathbb{Z}$) je $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$, te je

$$\Delta\left(\left\{1, \frac{1+\sqrt{5}}{2}\right\}\right) = \begin{vmatrix} 2 & 1 \\ 1 & 3 \end{vmatrix} = 5$$

(ovdje smo računali diskriminantu preko traga). Pošto je $\Delta\left(\left\{1, \frac{1+\sqrt{5}}{2}\right\}\right)$ kvadratno slobodan, slijedi $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Primjer 3.5.6

Odredite $\mathcal{O}_K$ za $K = \mathbb{Q}(\sqrt[3]{5})$.

Rješenje: Neka je $\theta = \sqrt[3]{5}$. Očito je $\{1, \theta, \theta^2\}$ $\mathbb{Z}$-baza od $\mathbb{Z}[\sqrt[3]{5}]$, koji je ranga $[K : \mathbb{Q}]$. Imamo 3 ulaganja $\sigma_i : K \hookrightarrow \mathbb{C}$, za $i = 0, 1, 2$, gdje je $\sigma_i(\theta) = \zeta^i\theta$, gdje je ζ treći korijen iz jedinice.

Sada imamo

$$\Delta(\{1, \theta, \theta^2\}) = \begin{vmatrix} 1 & \theta & \theta^2 \\ 1 & \zeta\theta & \zeta^2\theta^2 \\ 1 & \zeta^2\theta & \zeta\theta^2 \end{vmatrix}^2 = (\theta^3)^2 \begin{vmatrix} 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta \end{vmatrix}^2 = 5^2 3^2 (\zeta^2 - \zeta)^2 = -3^3 5^2.$$

Dakle, zaključujemo $[\mathcal{O}_K : \mathbb{Z}\left[\sqrt{5}\right]] \in \{1, 3, 5, 15\}$.

Ako $\mathbb{Z}[\sqrt[3]{5}] \neq \mathcal{O}_K$ tada postoji $\alpha \in \mathcal{O}_K$ gdje vrijedi jedna od sljedećih mogućnosti:

(1) $0 \neq \alpha = \frac{1}{3}(\lambda_1 + \lambda_2\theta + \lambda_3\theta^2)$, gdje su $0 \leq \lambda_i \leq 2$, ili

(2) $0 \neq \alpha = \frac{1}{5}(\lambda_1 + \lambda_2\theta + \lambda_3\theta^2)$, gdje su $0 \leq \lambda_i \leq 4$.

Pokažimo da (2) nije moguće, dok (1) ostavljamo za DZ. Pošto je $1+\zeta+\zeta^2 = 0$ slijedi da je $T(\alpha) = 3/5\lambda_1 \in \mathbb{Z}$, pa slijedi $\lambda_1 = 0$. Računamo $N(a\theta + b\theta^2) = \ldots = 5a^3 + 25b^3$. Dakle imamo

$$N(\alpha) = \frac{\lambda_2^3 + 5\lambda_3^3}{25} \in \mathbb{Z}.$$

Slijedi

$$\lambda_2^3 + 5\lambda_3^3 \equiv 0 \pmod{25}. \tag{3.2}$$

Primijetimo

$$\lambda_2 \equiv 0 \pmod 5 \iff \lambda_3 \equiv 0 \pmod 5,$$

i ako je to istina, dobijemo $\alpha = 0$, pa možemo ovaj slučaj odbaciti.

Neka je sada $\lambda_3 \not\equiv 0 \pmod 5$; sada iz (4.4) slijedi da je

$$\left(\frac{-\lambda_2}{\lambda_3}\right) \equiv 5 \pmod{25},$$

pa slijedi

$$\left(\frac{-\lambda_2}{\lambda_3}\right) \equiv 0 \pmod 5,$$

što je očito kontradikcija jer implicira $\lambda_2 \equiv 0 \pmod 5$.

Primjer 3.5.7

Neka je $K = \mathbb{Q}(\zeta_p)$. Pokažimo da je $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.

Rješenje:
Očito je $\mathcal{O}_K \supseteq \mathbb{Z}[\zeta_p]$. Vrijedi

$$T(\zeta_p) = \zeta_p + \zeta_p^2 + \ldots + \zeta_p^{p-1} = -1.$$

Također $T(\zeta_p^i) = T(\zeta_p) = -1$ za sve $1 \leq i \leq p-1$. Vrijedi $T(1) = p-1$. Također

$$T(1-\zeta_p) = T(1-\zeta_p^i) = p \text{ za sve } 1 \leq i \leq p-1.$$

Sjetimo se da je

$$\Phi_p(x) = (1 + x + \ldots + x^{p-1}) = \prod_{1 \leq i \leq p-1} (x - \zeta^i),$$

pa slijedi

$$p = \Phi_p(1) = \prod_{1 \leq i \leq p-1} (1 - \zeta^i) = N(1 - \zeta_p^i) \tag{3.3}$$

za sve $1 \leq i \leq p-1$.

Dovršit ćemo dokaz primjera (do kraja poglavlja) s nekoliko rezultata.

Lema 3.5.8

Vrijedi $p\mathbb{Z} = (1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z}$.

Dokaz. Primijetimo da $(1-\zeta_p)|p$ (u $\mathcal{O}_K$) pa je $p\mathbb{Z} \subseteq (1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z}$. Pretpostavimo da ne vrijedi jednakost. Tada pošto je $(1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z}$ ideal u $\mathbb{Z}$ i $p\mathbb{Z}$ je maksimalan u $\mathbb{Z}$, slijedi $(1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z} = \mathbb{Z}$.

Dakle $1 \in (1-\zeta_p)\mathcal{O}_K$, to jest postoji $\alpha \in \mathcal{O}_K$ takav da je $1 = (1-\zeta_p)\alpha$. Međutim tada bi moralo vrijediti $N(1-\zeta_p) = \pm 1$, što smo vidjeli da ne vrijedi. □

Korolar 3.5.9

Za svaki $\alpha \in \mathcal{O}_K$ vrijedi $T((1-\zeta_p)\alpha) \in p\mathbb{Z}$.

Dokaz. Neka su σ_i takvi da je $\sigma_i(\zeta_p) = \zeta_p^i$.

$$T((1-\zeta_p)\alpha) = \sigma_1((1-\zeta_p)\alpha) + \ldots + \sigma_{p-1}((1-\zeta_p)\alpha)$$

$$= (1-\zeta_p)\sigma_1(\alpha) + (1-\zeta_p^2)\sigma_2(\alpha) + \ldots (1-\zeta_p^{p-1})\sigma_{p-1}(\alpha).$$

Primijetimo da je

$$\frac{1-\zeta_p^i}{1-\zeta_p} = 1 + \zeta_p + \zeta_p^2 + \ldots + \zeta_p^{i-1} \in \mathcal{O}_K,$$

pa $(1-\zeta_p)|T((1-\zeta_p)\alpha)$. Dakle, imamo

$$T((1-\zeta_p)\alpha) \in (1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}.$$

□

Propozicija 3.5.10

$\mathcal{O}_K = \mathbb{Z}[\zeta_p] \simeq \mathbb{Z}[x]/\phi_p$.

Dokaz. Znamo $\mathbb{Z}[\zeta_p] \subseteq \mathcal{O}_K$. Neka je $\alpha \in \mathcal{O}_K$. Tada je

$$\alpha = a_0 + a_1\zeta_p + \ldots + a_{p-2}\zeta_p^{p-2}, \quad a_i \in \mathbb{Q}.$$

Pomnožimo sve s $(1-\zeta_p)$; dobijemo

$$\alpha(1-\zeta_p) = a_0(1-\zeta_p) + a_1(\zeta_p - \zeta_p^2) + \ldots a_{p-2}(\zeta_p^{p-2} - \zeta_p^{p-1}).$$

Slijedi

$$T(\alpha(1-\zeta_p)) = T(a_0(1-\zeta_p)) + T(a_1\zeta_p) - T(a_1\zeta_p^2) + T(a_2\zeta_p^2) - T(a_2\zeta_p^3) +$$

$$\ldots + T(a_{p-2}\zeta_p^{p-2}) - T(a_{p-2}\zeta_p^{p-1}).$$

Sada pošto je $T(a_i\zeta_p^i) = T(a_i\zeta_p^j)$ za svaki $1 \leq i \leq p-1$, slijedi

$$T(\alpha(1-\zeta_p)) = T(a_0(1-\zeta_p)) = a_0T((1-\zeta_p)) = a_0p.$$

Pošto je po Korolaru 3.5.9 $T(\alpha(1-\zeta_p)) \in p\mathbb{Z}$, zaključujemo da je $a_0 \in \mathbb{Z}$.

Imamo da je $\alpha - a_0 \in \mathcal{O}_K$, te slijedi

$$\beta := (\alpha - a_0)\zeta_p^{-1} = (\alpha - a_0)\zeta_p^{p-1} = a_1 + a_2\zeta_p + \ldots a_{p-2}\zeta_p^{p-3} \in \mathcal{O}_K$$

Ponavljanjem istog postupka za β, tj. promatranjem $T(\beta(1-\zeta_p))$, dobijemo $a_1 \in \mathbb{Z}$, i analogno za ostale a_i-eve. □

Poglavlje 4

Faktorizacija ideala u poljima algebarskih brojeva

Želimo vidjeti kako se (n) faktorizira u $\mathcal{O}_K$ za PAB K. Vidjeli smo da se u $\mathbb{Z}[\sqrt{-5}]$ ideal (6) faktorizira kao $(6) = P_1^2 P_2 P_3$.

Pogledajmo kako se (n) faktorizira u $\mathcal{O}_K$ za $n \in \mathbb{N}$.. Primijetimo da vrijedi

$$(n) = (p_1) \dots (p_k) \quad \text{gdje } n = \prod_i^k p_i.$$

Dakle, treba samo odrediti kako se (p_i)-evi faktoriziraju. Vidjeli smo na primjer $(5) = (2+i)(2-i)$ u $\mathbb{Z}[i]$. Može se i općenitije promatrati: kako se za proširenje PAB L/K faktoriziraju prosti ideali $P\mathcal{O}_K$ u $\mathcal{O}_L$, tj. koja je faktorizacija u proste ideale od $P\mathcal{O}_L$.

Lema 4.0.1

Neka je K PAB i $\mathfrak{p}$ prost ideal u $\mathcal{O}_K$. Tada postoji prost broj $p \in \mathbb{Z}$ takav da je $p \in \mathbb{Z} \cap \mathfrak{p}$.

Dokaz. Prema Lemi 3.3.2 imamo $\mathfrak{p} \cap \mathbb{Z} \neq \{0\}$. Očito je i $\mathfrak{p} \cap \mathbb{N} \neq \{0\}$. Neka je $n = \min \mathfrak{p} \cap \mathbb{N}$. Tvrdimo da je n prost. Pretpostavimo suprotno. Neka je $n = ab$, gdje $a, b \in \mathbb{N} \backslash \{1\}$. Pošto je $n \in \mathfrak{p}$, vrijedi da je $ab \in \mathfrak{p}$, pa pošto je $\mathfrak{p}$ prost, slijedi da je ili $a \in \mathfrak{p}$ ili $b \in \mathfrak{p}$. □

Posljedica je da se svaki prosti ideal u nekom $\mathcal{O}_K$ može naći kao faktor nekog (p) za $p \in \mathbb{Z}$. Dakle, trebamo vidjeti kako se faktorizira $p\mathcal{O}_K$.

Pogledajmo sada jednostavniji slučaj kada je $\mathcal{O}_K = \mathbb{Z}[\alpha]$, za neki $\alpha \in \mathcal{O}_K$. **Ovo ne mora vrijediti općenito!** Neka je $f = f_\alpha$ minimalni polinom od α.

Imamo

$$\begin{array}{ccc} \mathcal{O}_K & \longrightarrow & \mathcal{O}_K/p\mathcal{O}_K \\ \downarrow\sim & & \downarrow\sim \\ \mathbb{Z}[x]/(f) & \longrightarrow & \mathbb{Z}[x]/(p,f) \simeq \mathbb{F}_p[x]/(\overline{f}) \end{array},$$

gdje su vertikalne strelice izomorfizmi, a $\overline{f}$ označava redukciju od f modulo p.

Pogledajmo prvo slučaj kada je f stupnja 2. Onda dakle mora i $\overline{f}$ biti stupnja 2, jer je f normiran. Polinom f je ireducibilan, ali $\overline{f}$ ne mora biti. Imamo 3 mogućnosti:

1. $\overline{f}$ je ireducibilan
2. $\overline{f} = gh$, gdje su $g, h \in \mathbb{F}_p[x]$ stupnja 1, te nisu međusobno asocirani.
3. $\overline{f} = g^2$, gdje je $g \in \mathbb{F}_p[x]$ stupnja 1.

Pogledajmo sada što se dogodi u svakom od slučaja:

1) $\overline{f}$ je ireducibilan $\iff$ $(\overline{f})$ je maksimalan ideal u $\mathbb{F}_p[x] \iff \mathbb{F}_p[x]/(\overline{f})$ je polje $\iff \mathcal{O}_K/p\mathcal{O}_K$ je polje $\iff p\mathcal{O}_K$ je maksimalan $\iff p\mathcal{O}_K$ je prost.

2) $\overline{f} = gh \implies$

$$\mathbb{F}_p[x]/(\overline{f}) \simeq \mathbb{F}_p[x]/(\overline{g}) \times \mathbb{F}_p[x]/(\overline{h}) \simeq \mathbb{F}_p \times \mathbb{F}_p.$$

Pogledajmo homomorfizam

$$\varphi : \mathcal{O}_K \to \mathbb{F}_p[x]/(\overline{f}) \simeq \mathbb{F}_p[x]/(\overline{g}) \times \mathbb{F}_p[x]/(\overline{h}),$$

$$\alpha \mapsto (x + (\overline{f})) \mapsto (x + (g), x + (h)).$$

Vidimo da je jezgra tog preslikavanja $p\mathcal{O}_K$. Stavimo $\varphi(\alpha) = (\varphi_1(\alpha), \varphi_2(\alpha))$. Tada će biti $\ker\varphi_1 = (p, \tilde{g}(\alpha))$ i $\ker\varphi_2 = (p, \tilde{h}(\alpha))$, gdje su $\tilde{g}, \tilde{h} \in \mathbb{Z}[X]$ bilo koji polinomi takvi da su njihove redukcije modulo p jednake g i h. Dakle, imamo $\ker\varphi = \ker\varphi_1 \cap \ker\varphi_2$. Pošto su $(p, \tilde{g}(\alpha))$ i $(p, \tilde{h}(\alpha))$ relativno prosti (jer su g i h), tj. $(p, \tilde{g}(\alpha)) + (p, \tilde{h}(\alpha)) = (1)$, vrijedi

$$p\mathcal{O}_K = \ker\varphi = \ker\varphi_1 \cap \ker\varphi_2 = \ker\varphi_1 \cdot \ker\varphi_2 = (p, \tilde{g}(\alpha)) \cdot (p, \tilde{h}(\alpha)),$$

tj. $p\mathcal{O}_K$ je produkt 2 različita prosta ideala.

3) U ovom slučaju analogno dobijemo $p\mathcal{O}_K = (p, g(\alpha))^2$.

Primjer 4.0.2

Pogledajmo faktorizaciju $2, 3, 5$ u $\mathbb{Z}[i] \simeq \mathbb{Z}[x]/(x^2+1)$.

$$x^2 + 1 \equiv (x+1)^2 \pmod 2 \implies (2) = (2, 1+i)^2 = (1+i)^2.$$

$$x^2 + 1 \text{ je ireducibilan u } \mathbb{F}_3 \implies (3) \text{ je prost u } \mathbb{Z}[i].$$

$$x^2+1 \equiv (x-2)(x+3) \pmod 5 \implies (5) = (5, i-2)(5, i-3) = (2+i)(2-i).$$

Notacija: $K = \mathbb{Q}(\sqrt{d})$, gdje je d kvadratno slobodan, $\mathcal{O}_K$ prsten cijelih K, $\mathcal{O}_K = \mathbb{Z}[\alpha]$, $f = f_\alpha$ je minimalni polinom od α, a $\bar{f}$ je redukcija polinoma f modulo p.

Za prost broj p postoje tri moguće situacije za faktorizaciju $\bar{f}(x)$:

1. $\bar{f}(x)$ je ireducibilan, te je tada $p\mathcal{O}_K$ prost.
2. $\bar{f}(x) = g(x)^2$, gdje je g linearni polinom, tada $p\mathcal{O}_K = (p, g(\alpha))^2$.
3. $\bar{f}(x) = g_1(x)g_2(x)$, gdje su g_1 i g_2 linearni polinomi. Tada je $p\mathcal{O}_K = (p, g_1(\alpha))(p, g_2(\alpha))$.

Definicija 4.0.3

U slučaju (1), kažemo da je p inertan $\mathcal{O}_K$. U slučaju (2), kažemo da se p grana (ili ramificira) u $\mathcal{O}_K$. U slučaju (3), kažemo da se p cijepa u $\mathcal{O}_K$.

Sjetimo se

$$f_\alpha(x) = \begin{cases} x^2 - d & \text{ako je } d \equiv 2, 3 \pmod 4, \\ x^2 - x + \frac{1-d}{4} & \text{ako je } d \equiv 1 \pmod 4. \end{cases}$$

Propozicija 4.0.4

Ako je $d \equiv 1 \pmod 4$, tada se p grana u $\mathbb{Q}(\sqrt{d})$ ako i samo ako p dijeli d. Ako je $d \equiv 2, 3 \pmod 4$, tada se p grana u $\mathbb{Q}(\sqrt{d})$ ako i samo ako $p = 2$ ili $p|d$.

Dokaz. Promotrimo prvo slučaj $d \equiv 2, 3 \pmod 4$. Vrijedi da se p grana ako i samo ako postoji $a \in \mathbb{F}_p$ takav da je $x^2 - d = (x-a)^2 \pmod p$, što je ekvivalentno s:

$$x^2 - d \equiv x^2 - 2ax + a^2 \pmod p.$$

Oduzimajući x^2 s obje strane, dobivamo:

$$2ax - d \equiv a^2 \pmod p.$$

Ovo je kongruencija polinoma koja je ekvivalentna s

$$2a \equiv 0 \pmod p, \quad a^2 \equiv -d \pmod p.$$

Prva jednadžba je zadovoljena ako i samo ako $p \mid 2$ ili $p \mid a$. Za $p = 2$ očito postoji $a \equiv a^2 \equiv -d \pmod 2$. Ako je $p \mid a$, slijedi $d \equiv 0 \pmod p$, dakle $p \mid d$.

Obrnuto, ako $p|d$ onda uzmemo $x^2 - d \pmod x^2 \pmod p$, pa se p grana.

Neka je sada $d \equiv 1 \pmod 4$ i označimo s $f = f_\alpha$. Korijeni od $\bar{f}$ su

$$x_{1,2} = \frac{1 \pm \sqrt{d}}{2}.$$

Primijetimo da se p grana ako i samo ako su korijeni isti, što je ekvivalentno s tim da je $\sqrt{d} = 0$ u $\mathbb{F}_p$. Za $p \neq 2$, to je ekvivalentno s $d \equiv 0 \pmod{p}$, tj. $p \mid d$.

Za $p = 2$, $\overline{f}$ ima linearni član, pa nije kvadrat ($x^2 + a^2 \equiv (x+a)^2 \pmod{2}$), dakle 2 se ne grana. □

Propozicija 4.0.5

Neka je $K = \mathbb{Q}(\sqrt{d})$, gdje je 2 kvadratno slobodan. Tada

a) 2 se grana u $\mathcal{O}_K$ ako i samo ako $d \equiv 2, 3 \pmod{4}$,

b) 2 se cijepa u $\mathcal{O}_K$ ako i samo ako $d \equiv 1 \pmod{8}$,

c) 2 je inertan u $\mathcal{O}_K$ ako i samo ako $d \equiv 5 \pmod{8}$.

Dokaz. a) slijedi iz prethodne propozijcije. Neka je sada $d \equiv 1 \pmod{4}$; tada je $f_\alpha = x^2 - x - \frac{1-d}{4}$. Neka je $\frac{1-d}{4} = t$. Tada je

$$\overline{f_\alpha} = x^2 + x + t.$$

Vidimo da je $\overline{f_\alpha}$ ireducibilan ako je $t = 1$ (što je ekvivalentno s $d \equiv 5 \pmod{8}$), te da je $\overline{f_\alpha}$ produkt 2 različita polinoma ako je $t = 0$ (što je ekvivalentno s $d \equiv 1 \pmod{8}$), pa se u tom slučaju 2 cijepa. □

Primjer 4.0.6

Neka je $d = -5$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Faktorizirajmo prvih nekoliko prostih cijelih brojeva u $\mathcal{O}_K$.

$$\begin{aligned}
&x^2 + 5 \equiv x^2 + 1 = (x+1)^2 \pmod 2,\\
&\implies 2\mathcal{O}_K = \left(2, \sqrt{-5}+1\right)^2 \implies 2 \text{ se grana},\\
&x^2 + 5 \equiv x^2 + 2 \equiv (x+1)(x+2) \pmod 3,\\
&\implies 3\mathcal{O}_K = (2, \sqrt{-5}+1)(2, \sqrt{-5}+2),\\
&5\mathcal{O}_K = (5, \sqrt{-5})^2 = (\sqrt{-5})^2, \implies 5 \text{ se grana},\\
&x^2 + 5 \equiv (x+3)(x+4) \pmod 7.\\
&\implies 7\mathcal{O}_K = (7, \sqrt{-5}+3)(7, \sqrt{-5}+4) \implies 7 \text{ se cijep},
\end{aligned}$$

Pogledajmo $p = 11$: $x^2 + 5$ je ireducibilan u $\mathbb{F}_{11}[x]$, jer:

$x \pmod{11}$	0	1	2	3	4	5
$x^2 + 5 \pmod{11}$	5	6	9	3	10	8

pa zaključujemo da x^2+5 nema nultočaka u $\mathbb{F}_{11}$, pa je ireducibilan. Stoga je 11 inertan u $\mathcal{O}_K$.
Pogledajmo $p = 17$. Promatramo $x^2 \equiv -5 \pmod{17}$.
Međutim, provjerimo da je $\left(\frac{-5}{p}\right) = -1$, pa je 17 inertan.

Definicija 4.0.7

Neka je $p \neq 2$ prost broj. Definiramo *Legendreov simbol* kao funkciju:

$$\left(\frac{\bullet}{p}\right) : \mathbb{Z}/p\mathbb{Z} \to \{0, \pm 1\},$$

gdje vrijedi:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ako je } a \neq 0 \text{ kvadratni ostatak modulo } p,\\ 0, & \text{ako } a = 0,\\ -1, & \text{inače.} \end{cases}$$

Često pišemo $\left(\frac{a}{p}\right)$ i za $a \in \mathbb{Z}$, gdje se onda zapravo uzima kompozicija s redukcijom modulo p.

Korolar 4.0.8

Neka je $p \neq 2$ prost broj i $\mathcal{O}_K$ prsten cijelih nekog kvadratnog polja $K = \mathbb{Q}(\sqrt{d})$. Tada vrijedi:

- p se cijepa u $\mathcal{O}_K \iff \left(\frac{d}{p}\right) = 1$,
- p je inertan u $\mathcal{O}_K \iff \left(\frac{d}{p}\right) = -1$,
- p se grana u $\mathcal{O}_K \iff \left(\frac{d}{p}\right) = 0$.

Dokaz. Promotrimo $d \equiv 2, 3 \pmod 4$. $p \mid d \iff p$ se grana. Ako $p \nmid d$, tada se $x^2 - d$ faktorizira kao produkt linearnih polinoma u $\mathbb{F}_p[x]$ ako i samo ako $x^2 \equiv d \pmod p$ ima rješenje

$$\iff \left(\frac{d}{p}\right) = 1.$$

Ako je $d \equiv 1 \pmod 4$, tada su korijeni od f_α jednaki

$$x_{1,2} = \frac{1 \pm \sqrt{d}}{2}.$$

Dakle f_α se faktorizira u $\mathbb{F}_p[x]$ postoji $\Leftrightarrow x_{1,2} \in \mathbb{F}_p \Leftrightarrow \sqrt{d} \in \mathbb{F}_p \Leftrightarrow \left(\frac{d}{p}\right) = 1$. □

4.1 Konačna polja

Definicija 4.1.1

Kažemo da je polje **konačno** ako ima konačno mnogo elemenata.

Neka je F konačno polje i neka je $f : \mathbb{Z} \to F$ homomorfizam prstenova takav da $f(1) = 1$. Pošto je F konačno, f ima netrivijalnu jezgru, dakle $\ker f = m\mathbb{Z}$ za neki $m \in \mathbb{N}$. Dakle $\mathbb{Z}/m\mathbb{Z}$ se ulaže u F. Slijedi da $\mathbb{Z}/m\mathbb{Z}$ mora biti integralna domena, dakle m mora biti prost. Pišemo p umjesto m da bismo to naglasili. Dakle vrijedi $\operatorname{char} F = p$. Dakle F je proširenje polja $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Dakle F je vektorski prostor nad $\mathbb{F}_p$. Neka je $[F : \mathbb{F}_p] = n$. Slijedi $|F| = p^n$.

Teorem 4.1.2

Neka je $\mathbb{F}_q$ konačno polje s $q = p^n$ elemenata, gdje je p prost broj, a $n \geq 1$. Multiplikativna grupa $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ je ciklička.

Dokaz. Neka $\mathbb{F}_q^\times$ označava multiplikativnu grupu svih nenul elemenata u $\mathbb{F}_q$. Ta grupa ima $q - 1$ elemenata jer $|\mathbb{F}_q| = q$. Očito je grupa $\mathbb{F}_q^\times$ konačna Abelova grupa.

Dakle

$$\mathbb{F}_q^\times \simeq \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z},$$

pa slijedi da je $x^{m_k} - 1$ za svaki $x \in \mathbb{F}_q^\times$. Međutim, $x^{m_k} - 1$ ima najviše m_k nultočaka u $\mathbb{F}_q^\times$, pa onda vrijedi da je $k = 1$ $|\mathbb{F}_q^\times| = m_k$, tj. $\mathbb{F}_q^\times$ je ciklička. □

Posljedica je da za konačno polje F karakteristike p vrijedi $F = \mathbb{F}_p[\alpha]$, gdje je α generator od $\mathbb{F}^\times$.

Označimo sa $\sigma : F \to F$, definiran sa $\sigma(x) = x^p$. Ovo preslikavanje je očito multiplikativno. Također

$$\sigma(x+y) = (x+y)^p = x^p + y^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i} = x^p + y^p,$$

pošto je $\binom{p}{i} = 0$ u karakteristici p ta $i = 1, \ldots, p-1$. Dakle σ je automorfizam od F, pošto je injekcija, i F je konačan, pa je i surjekcija. σ se često naziva *Frobeniusovo preslikavanje* ili *Frobenius*.

Sjetimo se da je $\beta^p = \beta$ za svaki $\beta \in \mathbb{F}_p$ (Mali Fermatov teorem). Također znamo da $x^p - x$ ima $\leq p$ korijena u F. Zaključujemo da su nultočke $x^p - x$, tj. fiksne točke od σ upravo elementi od $\mathbb{F}_p$.

Također $\beta^{p^n-1} = 1$ za sve $\beta \in F^\times$, pa je $\beta^{p^n} = \beta$, tj. $\sigma^n = id|_F$. Primijetimo da σ^k, za $1 \leq k \leq n-1$ vrijedi $\sigma^k \neq id|_F$, jer $\sigma^k(\alpha) = \alpha^{p^k} \neq \alpha$, pošto je α reda $p^n - 1$. Također $\sigma^i \neq \sigma^j$ za $1 \leq i < j \leq n-1$, jer bi u suprotnom bilo $\sigma^{j-1} = id|_F$.

Dakle imamo

$$\operatorname{Aut} F \supseteq \{id, \sigma, \sigma^2, \ldots \sigma^{n-1}\}.$$

Tvrdimo da vrijedi jednakost. Neka je $\varphi \in \operatorname{Aut} F$. Zbog $\varphi(1) = 1$, vrijedi $\varphi(k) = k$ za $k \in \mathbb{F}_p$, dakle $\varphi|_{\mathbb{F}_p} = id|_{\mathbb{F}_p}$. Primijetimo da su $\sigma^i(\alpha)$ nultočke od f_α, te da su sve različite, tj.

$$f_\alpha(x) = \prod_{i=0}^{n-1} (x - \sigma^i(\alpha)).$$

S druge strane $\varphi(\alpha)$ je također nultočka od f_α, dakle mora biti $\varphi(\alpha) = \sigma^i(\alpha)$ za neki $1 \leq i \leq n-1$. Pošto α generira $F^\times$, slijedi da je $\varphi = \sigma^i$.

Slijedi

$$\operatorname{Aut} F = \operatorname{Gal}(F/\mathbb{F}_p) = \langle \sigma \rangle \simeq \mathbb{Z}/n\mathbb{Z}. \tag{4.1}$$

Napomena: Svi rezultati koje smo dokazivali iz Galoisove teorije vrijedi i za proširenja $F/\mathbb{F}_p$.

Primijetimo da to povlači da za svaki djelitelj $d \mid n$, $n = dm$, vrijedi da postoji jedinstvena podgrupa $H \leq \operatorname{Gal}(F/\mathbb{F}_p)$ reda d, pošto je $\operatorname{Gal}(F/\mathbb{F}_p)$ ciklička, pa po Galoisovoj teoriji, postoji jedinstveno potpolje K od F takvo da je $[F : K] = d$, tj. $|K| = p^m$.

Propozicija 4.1.3

Postoji jedinstveno, do na izomorfizam, polje s p^n elemenata.

Oznaka: Polje s p^n elemenata označavamo s $\mathbb{F}_{p^n}$.

Dokaz. Neka je $f_n(x) := x^{p^n} - x \in \mathbb{F}_p[x]$ i neka je F skup korijena od f_n. Kako f_n nema višestrukih točaka, slijedi da F ima p^n elemenata. Lako se provjeri da je umnožak i zbroj korijena, te inverz elementa, opet korijen, pa slijedi da je F polje (s p^n elemenata).

Primijetimo da je svaki element od F korijen polinoma $f(x) = x^{p^n} - x$, koji ima najviše p^n korijena, dakle F je polje cijepanja od f. Sada tvrdnja slijedi iz jedinstvenosti polja cijepanja nekog polinoma. □

Primjer 4.1.4

Konstruirajmo polje s 9 elemenata. Zapisat ćemo ga kao $\mathbb{F}_9 := \mathbb{F}_3[x]/(x^2+1)$; to možemo pošto je x^2+1 ireducibilan u $\mathbb{F}_3[x]$. Dakle elementi od $\mathbb{F}_9$ su $\{ax+b | a, b \in \mathbb{F}_3\}$. Množenje se radi modulo x^2+1, npr. $x(x+1) = x^2 + x = x + 2$.

4.2 Dalje o faktorizaciji

Neka je sada K općenito polje algebarskih brojeva.

Definicija 4.2.1

Ako je $\mathfrak{p}$ ideal u $\mathcal{O}_K$, te $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, kažemo da $\mathfrak{p}$ *leži nad* p, te p *leži ispod* $\mathfrak{p}$.

Definicija 4.2.2

Neka je $p \in \mathbb{Z}$ prost. Tada je

$$p\mathcal{O}_K = \prod_{\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}} \mathfrak{p}^{e(\mathfrak{p}/p)},$$

gdje produkt ide po različitim prostim idealima $\mathfrak{p}$. Tada se $e(\mathfrak{p}/p)$ zove *stupanj grananja* od $\mathfrak{p}$ nad p.

Neka je $n := [K : \mathbb{Q}]$.Pošto je $\mathcal{O}_K = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$, vrijedi

$$|\mathcal{O}_K / p\mathcal{O}_K| = p^n,$$

te

$$\mathcal{O}_K / p\mathcal{O}_K \simeq \mathcal{O}_K / \mathfrak{p}_1^{e(\mathfrak{p}_1/p)} \times \ldots \times \mathcal{O}_K / \mathfrak{p}_r^{e(\mathfrak{p}_r/p)}$$

za neki prirdan broj r. Primijetimo da je za prost ideal $\mathfrak{p}$, $\mathcal{O}_K/\mathfrak{p}$ uvijek polje, pa je $|\mathcal{O}_K/\mathfrak{p}| = p^{f(\mathfrak{p}/p)}$, za neki $f(\mathfrak{p}/p)$.

Definicija 4.2.3

Vrijednost $f(\mathfrak{p}/p)$ takva da je $|\mathcal{O}_K/\mathfrak{p}| = p^{f(\mathfrak{p}/p)}$ zove se *stupanj inercije* od $\mathfrak{p}$ nad p.

Definicija 4.2.4

Neka je A ideal u $\mathcal{O}_K$. Definiramo *normu* $N_{K/\mathbb{Q}}(A)$ od A kao $N_{K/\mathbb{Q}}(A) := |\mathcal{O}_K/A|$.

Primijetimo da ako je $\mathfrak{p}$ prost, tada je $N_{K/\mathbb{Q}}(\mathfrak{p}) = p^{f(\mathfrak{p}/p)}$.

Lema 4.2.5

Norma ideala je multiplikativna, tj., $N_{K/\mathbb{Q}}(AB) = N_{K/\mathbb{Q}}(A)N_{K/\mathbb{Q}}(B)$.

Dokaz. Ako su A i B relativno prosti, tada tvrdnja odmah slijedi iz

$$\mathcal{O}_K/AB \simeq \mathcal{O}_K/A \times \mathcal{O}_K/B.$$

Treba samo dokazati da je

$$N_{K/\mathbb{Q}}(\mathfrak{p}^m) = N_{K/\mathbb{Q}}(\mathfrak{p})^m,$$

za prost ideal $\mathfrak{p}$. Prvo primijetimo da po 3. teoremu o izomorfizmu (za grupe!) vrijedi

$$|\mathcal{O}_K/\mathfrak{p}^m| = |\mathcal{O}_K/\mathfrak{p}| \cdot |\mathfrak{p}/\mathfrak{p}^2| \cdot \ldots |\mathfrak{p}^{m-1}/\mathfrak{p}^m|.$$

Sada tvrdimo da je homomorfizam grupa

$$|\mathfrak{p}^k/\mathfrak{p}^{k+1}| = |\mathcal{O}_K/\mathfrak{p}| \text{ za sve } k = 1, \ldots m-1.$$

Neka je $\gamma \in \mathfrak{p}^k \backslash \mathfrak{p}^{k+1}$. Primijetimo da takav γ postoji jer $\mathfrak{p}^k \neq \mathfrak{p}^{k+1}$ zbog jedinstvene faktorizacije u proste ideale.

Definirajmo za $k = 1, \ldots, m-1$ preslikavanje

$$\mathcal{O}_K \to \mathfrak{p}^k/\mathfrak{p}^{k+1}, \quad \alpha \mapsto \alpha(\gamma + \mathfrak{p}^{k+1}).$$

Lako se vidi da je ovo surjekcija, te da je jezgra upravo $\mathfrak{p}$, te smo dokazali da je

$$\mathfrak{p}^k/\mathfrak{p}^{k+1} \simeq \mathcal{O}_K/\mathfrak{p}.$$

□

Propozicija 4.2.6

Neka je K PAB, $[K:\mathbb{Q}]=n$, te p prost broj. Neka je

$$p\mathcal{O}_K=\prod_{i=1}^{r}\mathfrak{p}_i^{e(\mathfrak{p}_i/p)}$$

faktorizacija od $p\mathcal{O}_K$ na proste ideale. Označimo s $f_i := f(\mathfrak{p}_i/p)$, te $e_i := e(\mathfrak{p}_i/p)$. Tada je $\sum_{i=1}^{r} e_i f_i = n$.

Dokaz. Imamo

$$p^n = N_{K/\mathbb{Q}}(p\mathcal{O}_K) = N_{K/\mathbb{Q}}(\prod_{i=1}^{r}\mathfrak{p}_i^{e_i}) = \prod_{i=1}^{r} N(\mathfrak{p}_i)^{e_i} = \prod_{i=1}^{r}(p^{f_i})^{e_i} = p^{\sum_{i=1}^{r} f_i e_i}.$$

□

Teorem 4.2.7

Neka je $\mathcal{O}_K=\mathbb{Z}[\alpha]$ za neki $\alpha\in K$. Neka je p prost broj, $f := f_\alpha \in \mathbb{Z}[x]$ minimalni polinom od α i neka je

$$\overline{f} := g_1(x)^{e_1}\cdot g_2(x)^{e_2}\dots g_r(x)^{e_r}, \quad g_i\in\mathbb{F}_p[x]$$

faktorizacija $\overline{f}$ na ireducibilne polinome. Tada je

$$p\mathcal{O}_K=\prod_{i=1}^{r}(p,g_i(\alpha))^{e_i}$$

faktorizacija od $p\mathcal{O}_K$ na proste ideale.

Dokaz. Neka je $s_i=\deg g_i$, pa slijedi $\sum_{i=1}^{r} s_i e_i = n$. Sjetimo se da je

$$\mathcal{O}_K/\mathfrak{p}_i \simeq \mathbb{Z}[\alpha]/(p,g_i(\alpha)) \simeq \mathbb{Z}[x]/(f(x),p,g_i(x)) \simeq \mathbb{F}_p[x]/(\overline{f}(x),g_i(x)) \simeq$$

$$\simeq \mathbb{F}_p[x]/(g_i(x)).$$

Primijetimo prvo iz ovoga da je $\mathfrak{p}_i$ prost pošto je $g_i(x)$ ireducibilan u $\mathbb{F}_p[x]$. Također slijedi da je pa slijedi da je s_i jednak stupnju inercije $f(\mathfrak{p}_i/p)$ od $\mathfrak{p}_i$.

Promotrimo sada preslikavanje redukcija modulo p

$$\varphi : \mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K.$$

Očito vrijedi $\ker\varphi = p\mathcal{O}_K$, te

$$\begin{aligned}\mathcal{O}_K/p\mathcal{O}_K &\simeq \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/(p,f(x)) \simeq \mathbb{F}_p[x]/(\overline{f}(x)) \\ &\simeq \mathbb{F}_p[x]/(g_1(x)^{e_1}) \times \ldots \times \mathbb{F}_p[x]/(g_r(x)^{e_r}).\end{aligned} \tag{4.2}$$

Neka je ψ sada izomorfizam iz (4.2) zadan s

$$\alpha \mapsto (x, \ldots, x).$$

gdje označavamo s ψ_i preslikavanje na i-tu koordinatu.

$$\ker \psi_i = (p, g_i(\alpha)^{e_i}),$$

pa je

$$p\mathcal{O}_K = \ker \psi = \prod_{i=1}^{r} (p, g_i(\alpha)^{e_i}).$$

Imamo

$$(p, g_i(\alpha))^{e_i} = (p^{e_i}, p^{e_i-1} g_i(\alpha), \ldots, p g_i(\alpha)^{e_i-1}, g_i(\alpha)^{e_i}) \subseteq (p, g_i(\alpha)^{e_i})$$

pošto p dijeli sve članove u izrazu osim $g_i(\alpha)^{e_i}$. Ideali $(p, g_i(\alpha)^{e_i})$ su relativno prosti (jer su g_i-evi relativno prosti u $\mathbb{F}_p[x]$).

Sada imamo

$$pO_K = \prod_{i=1}^{r} (p, g_i(\alpha)^{e_i}) \text{ dijeli } \prod_{i=1}^{r} (p, g_i(\alpha))^{e_i}.$$

Imamo da je $N_{K/\mathbb{Q}}(pO_K) = p^n$, te je $\prod_{i=1}^{r} (p, g_i(\alpha))^{e_i} = p^{\sum_{i=1}^{r} e_i f_i} = p^n$, pošto je $f_i = \deg g_i$ i $\prod g_i^{e_i} = \overline{f}$. Imamo 2 ideala iste norme, gdje jedan sadržan u drugom, pa moraju biti jednaki.

Dakle, pokazali smo

$$p\mathcal{O}_K = \ker \psi = \prod_{i=1}^{r} (p, g_i(\alpha))^{e_i} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}.$$

□

Primjer 4.2.8

Neka je α korijen od $f(x) = x^3 + 2x + 1$ i $K = \mathbb{Q}(\alpha)$. Vrijedi (DZ) $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Faktorizirajmo $2\mathcal{O}_K$.
Vrijedi

$$x^3 + 2x + 1 \equiv (x+1)(x^2 + x + 1) \pmod 2,$$

gdje je drugi faktor ireducibilan, pa slijedi

$$2\mathcal{O}_K = (2, \alpha + 1)(2, \alpha^2 + \alpha + 1).$$

Neka je

$$\mathfrak{p}_1 := (2, \alpha + 1), \quad \mathfrak{p}_2 := (2, \alpha^2 + \alpha + 1).$$

Primijetimo da je

$$\mathcal{O}_K/\mathfrak{p}_1 \simeq \mathbb{F}_2, \quad \mathcal{O}_K/\mathfrak{p}_2 \simeq \mathbb{F}_4.$$

Dakle vrijedi, koristeći oznake kao i ranije, $r = 2$, $e_1 = e_2 = 1$, $f_1 = 1$, $f_2 = 2$.
Faktorizirajmo $3\mathcal{O}_K$. Primijetimo da $f(x)$ nema nultočke modulo 3, pa vrijedi da je $\mathcal{O}_K/(3) \simeq \mathbb{F}_{27}$, tj. $r = 1, e = 1, f = 3$.
Modulo 17, $f(x)$ ima tri nultočke $3, 5, 9$, te je

$$17\mathcal{O}_K = (17, \alpha - 3)(17, \alpha - 5)(17, \alpha - 9),$$

pa je $r = 3$, $e_i = f_i = 1$, za $i = 1, 2, 3$.

Sada proširujemo definiciju "ležati nad" i na relativna proširenja (tj. kada manje polje nije $\mathbb{Q}$).

Definicija 4.2.9

Ako je $\mathfrak{p}$ ideal u $\mathcal{O}_K$ i $\mathfrak{q}$ ideal u $\mathcal{O}_L$, te $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$, kažemo da $\mathfrak{q}$ *leži nad* $\mathfrak{p}$, te $\mathfrak{q}$ *leži ispod* $\mathfrak{p}$.

Lema 4.2.10

Neka je L/K Galoisovo proširenje i neka je $\mathfrak{p}$ prost ideal u $\mathcal{O}_K$. Neka su $P_1, \ldots, P_r$ prosti ideali od L koji leže iznad $\mathfrak{p}$. Tada $\mathrm{Gal}(L/K)$ djeluje tranzitivno na ovom skupu prostih ideala; to jest, za sve i, j, postoji $\sigma \in \mathrm{Gal}(L/K)$ takav da $\sigma(P_i) = P_j$.

Dokaz. Fiksirajmo različite proste ideale P i P' koji leže iznad $\mathfrak{p}$. Pretpostavimo da $\sigma(P) \neq P'$ za svaki $\sigma \in \mathrm{Gal}(L/K)$. Koristeći ovu pretpostavku, prema Kineskom teoremu o ostatku, možemo pronaći $\alpha \in \mathcal{O}_L$ takav da:

$$\alpha \equiv 0 \pmod{P'}$$

i

$$\alpha \equiv 1 \pmod{\sigma(P)} \quad \text{za sve } \sigma \in \mathrm{Gal}(L/K).$$

Promotrimo $N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha) \in \mathcal{O}_K$. Budući da $\alpha \in P'$, ova norma mora biti u $P' \cap \mathcal{O}_K = \mathfrak{p}$.

S druge strane, budući da je $\alpha \equiv 1 \pmod{\sigma(P)}$ za sve σ, $\alpha \notin \sigma(P)$. Sada zapišimo normu kao

$$N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma^{-1}(\alpha).$$

Budući da niti jedan od faktora nije u P, a P je prost ideal, to implicira da $N_{L/K}(\alpha) \notin P$. Imamo $N_{L/K}(\alpha) \notin P \cap \mathcal{O}_K = \mathfrak{p}$, što je kontradikcija, čime se dokazuje lema. □

Primijetimo da analogne tvrdnje onima koje smo dokazali za faktorizaciju $p\mathcal{O}_K$, za prost p, vrijede ako imamo proširenje L/K te promatramo faktorizaciju nekog prostog ideala $\mathfrak{p}$ od $\mathcal{O}_K$ u $\mathcal{O}_L$, tj. faktorizaciju od $\mathfrak{p}\mathcal{O}_L$. Tj. vrijedi

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{q}^{e(\mathfrak{q}/\mathfrak{p})},$$

za neke $e(\mathfrak{q}/\mathfrak{p})$. Broj $e(\mathfrak{q}/\mathfrak{p})$ se zovu stupanj grananja od $\mathfrak{q}$ nad $\mathfrak{p}$. Također definiramo stupanj inercije $f(\mathfrak{q}/\mathfrak{p})$ od $\mathfrak{q}$ nad $\mathfrak{p}$ s $f(\mathfrak{q}/\mathfrak{p}) := [(\mathcal{O}_L/\mathfrak{q}) : (\mathcal{O}_K/\mathfrak{p})] = \frac{e(\mathfrak{q}/p)}{e(\mathfrak{p}/p)}$; ovdje ulažemo i $(\mathcal{O}_L/\mathfrak{q})$ i $(\mathcal{O}_K/\mathfrak{p})$ u neko fiksno algebarsko zatvorenje od $\mathbb{F}_p$, gdje je p karakteristika oba ova polja.

Korolar 4.2.11

Neka je L/K Galoisovo proširenje stupnja n, i neka je $\mathfrak{p}$ prosti ideal od $\mathcal{O}_K$. Neka je:

$$\mathfrak{p}\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$$

faktorizacija $\mathfrak{p}$ u $\mathcal{O}_L$, i neka je $f_i = f(P_i/\mathfrak{p})$. Tada vrijedi:

$$f_1 = f_2 = \cdots = f_r$$

i

$$e_1 = e_2 = \cdots = e_r.$$

Također vrijedi $re_if_i = n$ za sve i.

Dokaz. Ako je $r = 1$, korolar je trivijalan, pa pretpostavljamo $r \geq 2$. Dokazat ćemo da $e_1 = e_2$ i $f_1 = f_2$; općeniti slučaj je isti. Prema Lemi 4.2.10 možemo pronaći $\sigma \in \mathrm{Gal}(L/K)$ takav da $\sigma(P_1) = P_2$. Primjenom σ na našu faktorizaciju i koristeći činjenicu da $\sigma(\mathfrak{p}) = \mathfrak{p}$ jer σ fiksira K, zaključujemo da:

$$\mathfrak{p}\mathcal{O}_L = \sigma(P_1)^{e_1}\sigma(P_2)^{e_2} \cdots \sigma(P_r)^{e_r}.$$

S obzirom na to da je $\sigma(P_1) = P_2$, slijedi $e_1 = e_2$.

Također primijetimo da je $\sigma : \mathcal{O}_L/P_1 \to \mathcal{O}_L/P_2$, $x + P_1 \mapsto \sigma(x) + P_2$ izomorfizam (svaki homomorfizam polja je injektivan, te pošto je σ automorfizam od $\mathcal{O}_L$, očito je i surrjektivno), pa slijedi da je $\mathcal{O}_L/P_1 \simeq \mathcal{O}_L/P_2$, pa je i $f_1 = f_2$. □

4.3 Karakteri, norma i Hilbertov teorem 90

Definicija 4.3.1

Neka je K/F konačno proširenje polja tako da je K normalno nad F. Kažemo da je **cikličko/Abelovo** proširenje ako je $\mathrm{Gal}(K/F)$ ciklička/Abelova grupa.

Definicija 4.3.2

Neka je G grupa, a L polje. **Karakter** grupe G sa vrijednostima u L je homomorfizam $\chi : G \to L^\times$.

Lema 4.3.3

Neka su $\chi_1, \chi_2, \ldots, \chi_n$ različiti karakteri grupe G sa vrijednostima u L. Oni su linearno nezavisni nad L, tj. vrijedi

$$\sum_{i=1}^{n} a_i \chi_i(g) = 0, \quad \text{za sve } g \in G,$$

tada je $a_i = 0$ za sve $i = 1, \ldots, n$.

Dokaz. Pretpostavimo suprotno i neka je n najmanji takav da postoji n linearno zavisnih karaktera. Neka je $a_1\chi_1 + a_2\chi_2 + \ldots + a_n\chi_n = 0$. Očito je da $n \geq 2$, te možemo pretpostaviti da je $a_1 \neq 0$. Pošto su karakteri χ_i međusobno različiti, postoji $g \in G$ takav da $\chi_1(g) \neq \chi_n(g)$. Sada imamo

$$a_1\chi_1(x) + \ldots + a_n\chi_n(x) = 0, \quad \forall x \in G, \tag{4.3}$$

pa vrijedi i

$$a_1\chi_1(gx) + \ldots + a_n\chi_n(gx) = 0, \quad \forall x \in G, \tag{4.4}$$

to jest

$$a_1\chi_1(g)\chi_1(x) + \ldots + a_n\chi_n(g)\chi_n(x) = 0, \quad \forall x \in G. \tag{4.5}$$

Pomnožimo (4.3) s $\chi_n(g)$ i oduzmimo (4.5) pa dobivamo

$$\sum_{i=1}^{n-1} a_i(\chi_n(g) - \chi_i(g))\chi_i(x) = 0, \quad \forall x \in G.$$

Budući da je $\chi_n(g) - \chi_1(g) \neq 0$ i $a_1 \neq 0$, dobili smo linearnu zavisnost $\leq n-1$ karaktera, što je u kontradikciji s našom pretpostavkom. □

Korolar 4.3.4

Neka su K, L polja i neka su $\sigma_1, \ldots, \sigma_n$ ulaganja od K u L. Tada su $\sigma_1, \ldots, \sigma_n$ linearno nezavisni nad L.

Dokaz. Primijenimo prethodnu lemu na $G := K^\times$. □

Lema 4.3.5

Neka je K/F konačno normalno proširenje. Tada za svaki $\sigma \in \mathrm{Gal}(K/F)$ i $\alpha \in K^\times$ imamo

$$N\left(\frac{\sigma(\alpha)}{\alpha}\right) = 1.$$

Dokaz.

$$N\left(\frac{\sigma(\alpha)}{\alpha}\right) = 1 \iff N(\sigma(\alpha))\, N\left(\frac{1}{\alpha}\right) = 1 \iff N(\sigma(\alpha)) = N(\alpha)$$

$$\iff \prod_{\tau \in \mathrm{Gal}(K/F)} \tau(\sigma(\alpha)) = \prod_{\tau \in \mathrm{Gal}(K/F)} \tau(\alpha),$$

što očito vrijedi. □

Teorem 4.3.6: Hilbertov teorem 90

Neka je K/F konačno cikličko proširenje, $\mathrm{Gal}(K/F) = \langle \sigma \rangle$. Tada za svaki $\beta \in K^\times$ takav da je $N(\beta) = 1$ postoji $\alpha \in K$ takav da je

$$\beta = \frac{\sigma(\alpha)}{\alpha}.$$

Dokaz. Neka je $n := [K : F] = |\mathrm{Gal}(K/F)| = |\sigma|$. Definirajmo $\phi : K \to K$ s

$$\phi(x) = \frac{x}{\beta} + \frac{\sigma(x)}{\beta\sigma(\beta)} + \frac{\sigma^2(x)}{\beta\sigma(\beta)\sigma^2(\beta)} + \ldots + \frac{\sigma^{n-1}(x)}{\beta\sigma(\beta)\ldots\sigma^{n-1}(\beta)}.$$

Zbog linearne nezavisnosti $id, \sigma, \ldots, \sigma^{n-1}$ vrijedi $\phi \neq 0$. Dakle, postoji θ takav da je $\phi(\theta) \neq 0$. Neka je $\alpha := \phi(\theta)$. Tvrdimo da je $\beta = \frac{\sigma(\alpha)}{\alpha}$.

Vrijedi

$$\alpha = \frac{\theta}{\beta} + \frac{\sigma(\theta)}{\beta\sigma(\beta)} + \frac{\sigma^2(\theta)}{\beta\sigma(\beta)\sigma^2(\beta)} + \ldots + \frac{\sigma^{n-1}(\theta)}{\beta\sigma(\beta)\ldots\sigma^{n-1}(\beta)},$$

te

$$\sigma(\alpha) = \frac{\sigma(\theta)}{\sigma(\beta)} + \frac{\sigma^2(\theta)}{\sigma(\beta)\sigma^2(\beta)} + \frac{\sigma^3(\theta)}{\sigma(\beta)\sigma^2(\beta)\sigma^3(\beta)} + \ldots + \frac{\sigma^n(\theta)}{\sigma(\beta)\ldots\sigma^{n-1}(\beta)\sigma^n(\beta)}.$$

Primijetimo sada da je zadnji član ove sume jednak θ zbog $\sigma^n = id$ i jer je nazivnik jednak $N(\beta) = 1$. Podijelimo ovu jednakost s β, pa dobijemo

$$\frac{\sigma(\alpha)}{\beta} = \frac{\sigma(\theta)}{\beta\sigma(\beta)} + \frac{\sigma^2(\theta)}{\beta\sigma(\beta)\sigma^2(\beta)} + \frac{\sigma^3(\theta)}{\beta\sigma(\beta)\sigma^2(\beta)\sigma^3(\beta)} + \ldots + \frac{\theta}{\beta} = \alpha.$$

$$\frac{\sigma(\alpha)}{\beta} = \alpha.$$

□

Lema 4.3.7

Neka je p prost, ζ_p primitivni p-ti korijen iz 1, te $\zeta_p \notin F$. Tada je $F(\zeta_p)$ normalno proširenje i $\mathrm{Gal}(F(\zeta_p)/F) \leq (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

Dokaz. Analogno kao i za $F = \mathbb{Q}$. □

Primijetimo da je općenito $K(\zeta_{n_1}, \zeta_{n_2}) = K(\zeta_{NZV(n_1 n_2)})$, te da je

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times,$$

a $\mathrm{Gal}(K(\zeta_n)/K)$ je podgrupa od $(\mathbb{Z}/n\mathbb{Z})^\times$.

Teorem 4.3.8: Kummer

Neka je F polje algebarskih brojeva, $n \in \mathbb{N}$ i pretpostavimo da je $\zeta_n \in F$. Tada

a) Neka je K/F normalno proširenje takvo da je $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/n\mathbb{Z}$. Tada je $K = F(\sqrt[n]{a})$ za neki $a \in F$, tj. $K = F(\alpha)$ za neki $\alpha \in K$ takav da je $\alpha^n \in F$.

b) Ako je $K = F(\sqrt[n]{a})$ za neki $a \in F$, tada je K/F normalno i $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/d\mathbb{Z}$ za neki $d \mid n$.

Dokaz. a) Neka je $\zeta_n \in F$, $N : K \to F$ norma, $\langle\sigma\rangle = \mathrm{Gal}(K/F)$. Budući da je $\zeta_n \in F$, slijedi

$$N_{K/F}(\zeta_n) = \prod_{\tau \in \mathrm{Gal}(K/G)} \tau(\zeta_n) = \zeta_n^n = 1.$$

Po Hilbertovom teoremu 90 slijedi da postoji $\alpha \in K$ takav da je $\zeta_n = \frac{\sigma(\alpha)}{\alpha}$. Dalje slijedi

$$\sigma(\alpha) = \alpha\zeta_n,$$

$$\Longrightarrow \sigma^i(\alpha) = \sigma^{i-1}(\sigma(\alpha)) = \sigma^{i-1}(\alpha\zeta_n) = \sigma^{i-1}(\alpha)\sigma^{i-1}(\zeta_n) = \sigma^{i-1}(\alpha)\zeta_n =$$

$$\sigma^{i-2}(\sigma(\alpha))\zeta_n = \sigma^{i-2}(\alpha\zeta_n)\zeta_n = \ldots = \alpha\zeta_n^i, \quad \text{za } i = 0, \ldots, n-1.$$

Slijedi da je $|\{\sigma^i(\alpha) : i = 0, \ldots, n-1\}| = n$. Slijedi da pošto su svi konjugati od α različiti, je $\deg f_\alpha = n$ i da je $K = F(\alpha)$. Ostaje dokazati da je $\alpha^n \in F$.

Vrijedi

$$\sigma(\alpha^n) = (\sigma(\alpha))^n = (\alpha\zeta_n)^n = \alpha^n,$$

pa slijedi $\sigma^i(\alpha^n) = \sigma^{i-1}(\sigma(\alpha^n)) = \sigma^{i-1}(\alpha^n) = \ldots = \alpha^n$, dakle α^n je iz fiksnog polja od $\mathrm{Gal}(K/F)$, tj. iz F.

b) Neka je $b := \sqrt[n]{a}$. Slijedi da

$$f_b \mid x^n - a = (x-b)(x-\zeta_n b)\ldots(x-\zeta_n^{n-1}b),$$

pa slijedi da su $\{b\zeta_n^i : i = 0, \ldots, n-1\}$ svi konjugati od b. Pošto su oni svi u $F(b) = K$, slijedi da je K normalno nad F. Definirajmo preslikavanje

$$\phi : \mathrm{Gal}(K/F) \to \mathbb{Z}/n\mathbb{Z}, \quad (b \mapsto \zeta_n^i b) \mapsto i.$$

Lako se vidi da je ϕ homomorfizam grupa, te da je injektivan. Slijedi $\mathrm{Gal}(K/F) \simeq \mathrm{Im}\,\phi \leq \mathbb{Z}/n\mathbb{Z}$, pa je $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/d\mathbb{Z}$, za neki $d \mid n$. □

4.4 Relativna faktorizacija

Prvo ćemo izreći nekoliko lako dokazivih činjenica, čije dokaze ostavljamo za vježbu.

Propozicija 4.4.1

Neka je L/K proširenje polja algebarskih brojeva stupnja n i neka je $\mathfrak{p}$ nenul prosti ideal od $\mathcal{O}_K$. Tada vrijedi:

$$\#(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = (\#(\mathcal{O}_K/\mathfrak{p}))^n.$$

Korolar 4.4.2

Neka je L/K proširenje polja algebarskih brojeva stupnja n i neka je $\mathfrak{a}$ nenul ideal od $\mathcal{O}_K$. Tada

$$N_{L/\mathbb{Q}}(\mathfrak{a}\mathcal{O}_L) = N_{K/\mathbb{Q}}(\mathfrak{a})^n.$$

Korolar 4.4.3

Neka je K polje algebarskih brojeva stupnja n i neka je α u $\mathcal{O}_K$. Tada

$$N_{K/\mathbb{Q}}(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|.$$

Sada proširujemo naše ranije rezultate faktorizacije na proizvoljna proširenja polja brojeva. Neka je L/K proširenje polja brojeva stupnja n. Najprije moramo proširiti pojam prostog broja iz $\mathcal{O}_L$ koji leži iznad prostog broja iz $\mathcal{O}_K$.

Lema 4.4.4

Neka je $\mathfrak{p}$ nenul prost ideal u $\mathcal{O}_K$ i neka je $\mathfrak{P}$ nenul prost ideal u $\mathcal{O}_L$. Sljedećih pet uvjeta su ekvivalentni.

1. $\mathfrak{P}$ dijeli $\mathfrak{p}\mathcal{O}_L$;
2. $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}_L$;
3. $\mathfrak{P} \supseteq \mathfrak{p}$;
4. $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$;
5. $\mathfrak{P} \cap K = \mathfrak{p}$.

Nadalje, ako je bilo koji od gornjih uvjeta zadovoljen, tada je $\mathfrak{p} \cap \mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$.

Dokaz ostavljamo za vježbu.

Ako $\mathfrak{p}$ i $\mathfrak{P}$ zadovoljavaju bilo koji od ekvivalentnih uvjeta iz ove leme, kažemo da $\mathfrak{P}$ leži iznad $\mathfrak{p}$ i da $\mathfrak{p}$ leži ispod $\mathfrak{P}$. Svaki prost iz $\mathcal{O}_L$ leži iznad jednog jedinstvenog prostog iz $\mathcal{O}_K$, i da svaki prost iz $\mathcal{O}_K$ leži ispod najmanje jednog prostog iz $\mathcal{O}_L$. Primijetimo također da su prosti ideali koji leže iznad $\mathfrak{p}$ upravo oni prosti koji se pojavljuju u faktorizaciji od $\mathfrak{p}\mathcal{O}_L$ na proste ideale.

Sada, neka su $\mathfrak{p}$ i $\mathfrak{P}$ kao gore i pretpostavimo da $\mathfrak{P}$ leži iznad $\mathfrak{p}$. Označavamo s $e(\mathfrak{P}/\mathfrak{p})$ točnu potenciju od $\mathfrak{P}$ koja dijeli $\mathfrak{p}\mathcal{O}_L$; ona se naziva indeks grananja od $\mathfrak{P}/\mathfrak{p}$. Tako možemo pisati

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{P}\cap\mathcal{O}_K=\mathfrak{p}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}.$$

Nadalje, neka je p jedinstveni pozitivni racionalni prost sadržan u $\mathfrak{p}$ i $\mathfrak{P}$. Tada su $\mathcal{O}_K/\mathfrak{p}$ i $\mathcal{O}_L/\mathfrak{P}$ konačna polja karakteristike p. Štoviše, prirodna injekcija $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ inducira injekciju

$$\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P},$$

budući da je $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ prema Lemi 4.4.4. Tako je $\mathcal{O}_L/\mathfrak{P}$ polje proširenja od $\mathcal{O}_K/\mathfrak{p}$. Definiramo stupanj inercije $f(\mathfrak{P}/\mathfrak{p})$ kao stupanj $[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$ ovog proširenja. Primijetimo da

$$N_{L/\mathbb{Q}}(\mathfrak{P}) = N_{K/\mathbb{Q}}(\mathfrak{p})^{f(\mathfrak{P}/\mathfrak{p})}.$$

Sada možemo iskazati i dokazati naš temeljni rezultat.

Teorem 4.4.5

Neka je L/K proširenje polja algebarskih brojeva stupnja n i neka je $\mathfrak{p}$

prost u $\mathcal{O}_K$. Neka je

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

faktorizacija od $\mathfrak{p}\mathcal{O}_L$ u proste ideale od $\mathcal{O}_L$. Postavimo $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. Tada

$$\sum_{i=1}^{r} e_i f_i = n.$$

Dokaz. Uzimajući norme ideala s obje strane faktorizacije od $\mathfrak{p}\mathcal{O}_L$, nalazimo da

$$N_{L/\mathbb{Q}}(\mathfrak{p}\mathcal{O}_L) = N_{L/\mathbb{Q}}(\mathfrak{P}_1)^{e_1} \cdots N_{L/\mathbb{Q}}(\mathfrak{P}_r)^{e_r} = N_{K/\mathbb{Q}}(\mathfrak{p})^{f_1 e_1} \cdots N_{K/\mathbb{Q}}(\mathfrak{p})^{f_r e_r}$$

prema definiciji od f_i. Prema Korolaru 4.4.2 znamo da $N_{L/\mathbb{Q}}(\mathfrak{p}\mathcal{O}_L) = N_{K/\mathbb{Q}}(\mathfrak{p})^n$, iz čega teorem sada neposredno slijedi. □

Završimo ovaj odjeljak s nekim dodatnim činjenicama i terminologijom. Prije svega, neka su $M/L/K$ polja algebarskih brojeva, neka je $\mathfrak{p}_K$ prost u $\mathcal{O}_K$, neka je $\mathfrak{p}_L$ prost u $\mathcal{O}_L$ koji leži iznad $\mathfrak{p}_K$, i neka je $\mathfrak{p}_M$ prost u $\mathcal{O}_M$ koji leži iznad $\mathfrak{p}_L$. Tada očito $\mathfrak{p}_M$ leži iznad $\mathfrak{p}_K$, i neposredno iz definicija slijedi da imamo

$$e(\mathfrak{p}_M/\mathfrak{p}_K) = e(\mathfrak{p}_M/\mathfrak{p}_L)e(\mathfrak{p}_L/\mathfrak{p}_K)$$

i

$$f(\mathfrak{p}_M/\mathfrak{p}_K) = f(\mathfrak{p}_M/\mathfrak{p}_L)f(\mathfrak{p}_L/\mathfrak{p}_K).$$

Vratimo se sada na slučaj proširenja L/K stupnja n i neka je $\mathfrak{p}$ prost u $\mathcal{O}_K$. Neka je

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

faktorizacija od $\mathfrak{p}\mathcal{O}_L$ u proste od $\mathcal{O}_L$. Postavimo $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. Ako bilo koji od e_i nije jednak 1, kažemo da se $\mathfrak{p}$ grana u L/K. (Važna je činjenica da se samo konačno mnogo prostih grana u proširenju, a koji su to prosti i koliko se oni jako granaju je bitna invarijanta proširenja.) Ako je $r = 1$ i $e_1 = n$ (tako da je $f_1 = 1$), tada kažemo da se $\mathfrak{p}$ potpuno grana u L/K:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^n.$$

Ako je $r = 1$ i $e_1 = 1$ (tako da je $f_1 = n$), kažemo da je $\mathfrak{p}$ inertan ili ostaje prost u L/K; to je slučaj gdje je $\mathfrak{p}\mathcal{O}_L$ još uvijek prost. Konačno, ako je $e_i = f_i = 1$ za sve i, kažemo da se $\mathfrak{p}$ potpuno cijepa u L/K:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_n.$$

Sljedeći rezultat će nam biti koristan za određivanje cijepanja prostih ideala u kompozitumima polja algebarskih brojeva.

Definicija 4.4.6

Neka je $\mathfrak{p}$ ideal u $\mathcal{O}_K$. Tada je $k_\mathfrak{p} := O_K/\mathfrak{p}$ *polje ostataka* od $\mathfrak{p}$.

Napomena: $k_{\mathfrak{p}}$ nije tipfeler - malo slovo k nema veze s poljem K.

Propozicija 4.4.7

Neka su K_1 i K_2 polja algebarskih brojeva, $L = K_1K_2$ njihov kompozitum, te p prost broj. Neka su f_1 i f_2 stupnjevi inercije broja p u K_1, odnosno K_2 za fiksirani prost ideal $\mathfrak{P} \subset \mathcal{O}_L$ (te odgovarajuće ideale $\mathfrak{p}_1, \mathfrak{p}_2$ ispod njega). Tada vrijedi:

1. $\text{lcm}(f_1, f_2)$ dijeli f_L.
2. $f_L \leq f_1 \cdot f_2$.

Dokaz. **1. Dokaz donje granice ($\text{lcm}(f_1, f_2) \mid f_L$):**
Promatrajmo polja ostataka (konačna polja):

$$\mathbb{F}_p \subseteq \mathcal{O}_{K_1}/\mathfrak{p}_1 \subseteq \mathcal{O}_L/\mathfrak{P}$$

Stupanj proširenja $\mathbb{F}_p \subseteq \mathcal{O}_{K_1}/\mathfrak{p}_1$ je po definiciji f_1. Iz multiplikativnosti stupnja proširenja polja slijedi da f_1 dijeli stupanj $f_L = [\mathcal{O}_L/\mathfrak{P} : \mathbb{F}_p]$. Isto vrijedi i za f_2 promatrajući put kroz K_2. Budući da $f_1 \mid f_L$ i $f_2 \mid f_L$, tada i njihov najmanji zajednički višekratnik mora dijeliti f_L.

2. Dokaz gornje granice ($f_L \leq f_1 \cdot f_2$):

Za polje ostataka $k_{\mathfrak{P}} := \mathcal{O}_L/\mathfrak{P}$ je kompozitum polja ostataka $k_{\mathfrak{p}_1}$ i $k_{\mathfrak{p}_2}$ (ostavljamo za DZ):

$$k_{\mathfrak{P}} = k_{\mathfrak{p}_1} \cdot k_{\mathfrak{p}_2}.$$

Znamo da su $k_{\mathfrak{p}_1}$ i $k_{\mathfrak{p}_2}$ konačna polja reda p^{f_1} i p^{f_2}. Kompozitum dvaju konačnih polja reda p^{f_1} i p^{f_2} unutar nekog fiksiranog algebarskog zatvorenja je jedinstveno konačno polje reda $p^{\text{lcm}(f_1,f_2)}$. Stoga je stupanj tog kompozituma nad $\mathbb{F}_p$ točno $\text{lcm}(f_1, f_2)$.

□

Propozicija 4.4.8

Neka su K_1 i K_2 dva brojevna polja i neka je $L = K_1K_2$ njihov kompozitum. Neka je $p \in \mathbb{Z}$ prost broj, te neka su e_1 i e_2 indeksi grananja broja p u poljima K_1, odnosno K_2. Tada vrijedi:

1. Najmanji zajednički višekratnik $\text{lcm}(e_1, e_2)$ dijeli indeks grananja e_L broja p u polju L.
2. Indeks grananja e_L je manji ili jednak produktu $e_1 \cdot e_2$.

Dokaz. Sada ćemo dokazati samo prvi dio, pošto dokaz drugog dijela zahtijeva teoriju lokalnih polja koju ćemo raditi kasnije. Dokaz je zapravo analogan dokazu prvog dijela prethodnog teorema.

Promatrajmo toranj proširenja $\mathbb{Q} \subset K_1 \subset L$. Ako je $\mathfrak{P}$ prost ideal u L iznad $\mathfrak{p}$ u K_1, a $\mathfrak{p}$ iznad p u $\mathbb{Q}$, tada vrijedi:

$$e(L/\mathbb{Q}) = e(L/K_1) \cdot e(K_1/\mathbb{Q})$$

Budući da je $e(K_1/\mathbb{Q}) = e_1$ po definiciji, slijedi da e_1 dijeli $e(L/\mathbb{Q})$.

Analogno, promatrajući toranj $\mathbb{Q} \subset K_2 \subset L$, dobivamo:

$$e(L/\mathbb{Q}) = e(L/K_2) \cdot e(K_2/\mathbb{Q})$$

odakle slijedi da e_2 dijeli $e(L/\mathbb{Q})$. Budući da je $e(L/\mathbb{Q})$ zajednički višekratnik brojeva e_1 i e_2, on mora biti djeljiv i s njihovim najmanjim zajedničkim višekratnikom $\text{lcm}(e_1, e_2)$.

□

Primjer 4.4.9: Dekompozicija prostog broja $p = 5$ u $L = \mathbb{Q}(i, \sqrt{2}, \sqrt{5})$

Promatramo multikvadratno proširenje $L = \mathbb{Q}(i, \sqrt{2}, \sqrt{5})$ nad $\mathbb{Q}$. Stupanj ovog proširenja je $[L : \mathbb{Q}] = 8$. Da bismo odredili ponašanje prostog broja $p = 5$, analiziramo ga kroz tri kvadratna podpolja.
Promotrimo prvo ponašanje prostog broja p u kvadratnom polju $\mathbb{Q}(\sqrt{d})$:

- $\mathbb{Q}(i)$**:** Budući da je $5 \equiv 1 \pmod 4$, broj 5 se cijepa. Indeksi su: $e_1 = 1, f_1 = 1, g_1 = 2$.
- $\mathbb{Q}(\sqrt{2})$**:** Imamo $\left(\frac{2}{5}\right) = -1$, pa je5 ovdje inertan. Indeksi su: $e_2 = 1, f_2 = 2, g_2 = 1$.
- $\mathbb{Q}(\sqrt{5})$**:** Budući da 5 dijeli diskriminantu polja, 5 se grana. Indeksi su: $e_3 = 2, f_3 = 1, g_3 = 1$.

Po Propozicijama 4.4.7 i 4.4.8

- **Ukupni indeks grananja (e):** $2 = \text{lcm}(e_1, e_2, e_3) \leq e \leq e_1 \cdot e_2 \cdot e_3 = 2$.
- **Ukupni rstupanj inercije (f):** $2 = \text{lcm}(f_1, f_2, f_3) \leq f \leq f_1 \cdot f_2 \cdot f_3 = 2$.

Koristeći jednakost $e \cdot f \cdot r = [L : \mathbb{Q}]$, dobivamo broj prostih ideala g:

$$2 \cdot 2 \cdot r = 8 \implies \mathbf{r = 2}$$

Dakle, u polju L, prost broj 5 se rastavlja na **dva prosta ideala**, svaki s indeksom grananja 2 i stupnjem inercije 2.
Faktorizacija ideala (5) u prstenu cijelih brojeva polja L glasi:

$$(5) = (\mathfrak{P}_1 \mathfrak{P}_2)^2$$

gdje su $\mathfrak{P}_1$ i $\mathfrak{P}_2$ prosti ideali norme $5^f = 5^2 = 25$.

4.5 Još o ciklotomskim poljima

Neka je $K = \mathbb{Q}(\zeta_m)$ ciklotomsko polje i neka je p racionalan prost broj. Neka je $\mathfrak{p}$ bilo koji prosti ideal od $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$ koji leži iznad p. Želimo odrediti $e = e(\mathfrak{p}/p)$ i $f = f(\mathfrak{p}/p)$. Primijetimo da su, prema Korolaru 4.2.11 ovi brojevi neovisni o izboru prostog ideala $\mathfrak{p}$. Drugim riječima, u $\mathbb{F}_p[x]$ polinom $\Phi_m(x)$ faktorizira se kao

$$\Phi_m(x) = (g_1(x) \cdots g_r(x))^e$$

gdje je $\deg g_i = f$ za svaki i i vrijedi $efr = \varphi(m)$.

Započinjemo s slučajem kada p ne dijeli m. Budući da $x^m - 1$ nema ponovljenih faktora u $\mathbb{F}_p[x]$, isto vrijedi i za $\Phi_m(x)$; posebno, mora vrijediti $e = 1$. Preostaje nam odrediti f i r. Prije nego što riješimo opći slučaj, razmotrimo poseban slučaj $f = 1$ kako bismo ilustrirali ideju. Ako je $f = 1$, tada se $\Phi_m(x)$ u potpunosti rastavlja na linearne faktore u $\mathbb{F}_p[x]$, što znači da $\Phi_m(x)$ ima korijene u $\mathbb{F}_p$. To implicira da $\mathbb{F}_p$ sadrži primitivne m-te korijene jedinice. No, $\mathbb{F}_p^\times$ je ciklička grupa reda $p-1$, pa ima elemente točno reda m ako i samo ako m dijeli $p-1$, odnosno ako i samo ako

$$p \equiv 1 \pmod{m}.$$

Vidimo da vrijedi i obrat, pa smo pokazali da se prost broj p potpuno cijepa u $\mathbb{Q}(\zeta_m)$ ako i samo ako p ne dijeli m i $p \equiv 1 \pmod{m}$.

U općem slučaju moramo proširiti polje $\mathbb{F}_p$ kako bismo pronašli primitivni m-ti korijen jedinice. Neka je $g(x)$ jedan od ireducibilnih faktora $\Phi_m(x)$ u $\mathbb{F}_p[x]$; tada $g(x)$ ima stupanj f. Neka je α korijen polinoma $g(x)$ i definirajmo $F = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(g(x))$; ovo je proširenje polja $\mathbb{F}_p$ stupnja f. Primijetimo da je α primitivni m-ti korijen jedinice, budući da poništava $g(x)$, a samim time i $\Phi_m(x)$. Nadalje, F je očito najmanje proširenje $\mathbb{F}_p$ koje sadrži primitivni m-ti korijen jedinice (jer je jednostavno $\mathbb{F}_p$ kojem je pridružen m-ti korijen jedinice), pa smo pokazali da je f stupanj najmanjeg proširenja $\mathbb{F}_p$ koje sadrži primitivni m-ti korijen jedinice.

Sada ćemo ovo proširenje odrediti na drugi način. Neka je F_i jedinstveno proširenje polja $\mathbb{F}_p$ stupnja i. Tada je multiplikativna grupa $F_i^\times$ ciklička reda $p^i - 1$, pa sadrži primitivni m-ti korijen jedinice ako i samo ako m dijeli $p^i - 1$. Dakle, najmanje proširenje od $\mathbb{F}_p$ koje sadrži primitivni m-ti korijen jedinice bit će F_i, gdje je i najmanji pozitivan cijeli broj takav da vrijedi

$$p^i \equiv 1 \pmod{m}.$$

Drugim riječima, i je red broja p u multiplikativnoj grupi $(\mathbb{Z}/m\mathbb{Z})^\times$. Kombinirajući ovo s našim ranijim argumentima, dobivamo sljedeći rezultat.

Dokazali smo:

Propozicija 4.5.1

Neka je p racionalan prost broj koji ne dijeli m, i neka je $\mathfrak{p}$ prosti ideal od $\mathbb{Z}[\zeta_m]$ koji leži iznad p. Tada vrijedi:

a) $e(\mathfrak{p}/p) = 1$,

b) $f(\mathfrak{p}/p)$ je red broja p u grupi $(\mathbb{Z}/m\mathbb{Z})^\times$,

c) Ukupno postoji $\varphi(m)/f(\mathfrak{p}/p)$ prostih ideala u $\mathbb{Z}[\zeta_m]$ koji leže iznad p.

Propozicija 4.5.2

Neka je p racionalan prost broj i $n = p^k \cdot \prod q_i^{\alpha_i}$ faktorizacija od n, gdje $q_i \neq p$. Neka je $K = \mathbb{Q}(\zeta_n)$ i neka je $\mathfrak{p}$ prost ideal od K nad p. Tada je $e(\mathfrak{p}/p) = \varphi(p^k)$.

Dokaz. Kao i u za $\mathbb{Q}(\zeta_p)$, na isti način se dokaže da za $L = \mathbb{Q}(\zeta_{p^k})$ vrijedi $p\mathcal{O}_L = (1-\zeta_{p^k})^{\varphi(p^k)}$, tj. p se potpuno grana u K. Sada rezultat slijedi primjenom Propozicije 4.4.8. □

4.6 Primjene na kvadratna polja i Gaussov zakon reciprociteta

Postoje vrlo zanimljive primjene aritmetike ciklotomskih polja na kvadratna polja. Razmotrimo polje $\mathbb{Q}(\zeta_p)$ za neki neparni prost broj p. Podsjetimo da je ovo Galoisovo proširenje od $\mathbb{Q}$ s Galoisovom grupom izomorfnom $(\mathbb{Z}/p\mathbb{Z})^\times$, gdje je automorfizam koji odgovara $\sigma_a \in (\mathbb{Z}/p\mathbb{Z})^\times$ definiran kao

$$\sigma_a(\zeta_p) = \zeta_p^a.$$

Budući da je $(\mathbb{Z}/p\mathbb{Z})^\times$ ciklička grupa reda $p-1$, ona sadrži jedinstvenu podgrupu indeksa 2, koja se sastoji od svih kvadrata u $(\mathbb{Z}/p\mathbb{Z})^\times$. Ovu podgrupu označimo s S. Neka je K fiksno polje od S, tj. K je potpolje od $\mathbb{Q}(\zeta_p)$ čiji su svi elementi fiksni pod djelovanjem svih elemenata S. Galoisova teorija nam govori da je $[K : \mathbb{Q}] = 2$, dakle K je kvadratno polje. Ostaje nam odrediti koje je točno kvadratno polje.

Možemo to učiniti razmatranjem ramifikacije. Podsjetimo da je p potpuno ramificiran u $\mathbb{Q}(\zeta_p)$; to jest, postoji jedinstven prosti ideal $\mathfrak{P}$ od $\mathbb{Q}(\zeta_p)$ koji leži iznad p, te vrijedi

$$(p) = \mathfrak{P}^{p-1}.$$

Neka je $\mathfrak{p}$ bilo koji prosti ideal od K koji leži iznad p. Tada $\mathfrak{P}$ leži iznad $\mathfrak{p}$ (budući da je $\mathfrak{P}$ jedini prosti ideal od K koji leži iznad p) i vrijedi

$$e(\mathfrak{P}/p) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/p).$$

Budući da je $e(\mathfrak{P}/p) = p-1$ i da su ramifikacijski indeksi ograničeni stupnjevima proširenja, to implicira da je

$$e(\mathfrak{P}/\mathfrak{p}) = \frac{p-1}{2} \quad \text{i} \quad e(\mathfrak{p}/p) = 2.$$

Posebno, $\mathfrak{p}$ je jedini prosti ideal od K koji leži iznad p, te je potpuno ramificiran.

Neka je $\mathfrak{Q}$ bilo koji drugi prosti ideal od $\mathbb{Q}(\zeta_p)$, neka je $\mathfrak{q}$ prosti ideal od K koji leži iznad njega, i neka je q prosti ideal od $\mathbb{Z}$ koji leži ispod njega. Sličan

argument, koristeći činjenicu da je $e(\mathfrak{Q}/q) = 1$, pokazuje da je $e(\mathfrak{q}/q) = 1$, što znači da $\mathfrak{q}$ nije ramificiran u K. Zaključujemo da je p jedini prosti broj iz $\mathbb{Z}$ koji se ramificira u K.

Sada, već smo odredili ramifikaciju u svakom kvadratnom polju, i jedino kvadratno polje u kojem se samo p ramificira jest $\mathbb{Q}(\sqrt{\varepsilon p})$, gdje je $\varepsilon = \pm 1$ takav da vrijedi

$$\varepsilon p \equiv 1 \pmod 4.$$

Možemo uzeti $\varepsilon = (-1)^{(p-1)/2}$. Time smo dokazali sljedeću netrivijalnu činjenicu.

Propozicija 4.6.1

Polje $\mathbb{Q}(\zeta_p)$ sadrži kvadratno polje $\mathbb{Q}(\sqrt{\varepsilon p})$, gdje je $\varepsilon = (-1)^{(p-1)/2}$. Posebno, $\sqrt{\varepsilon p}$ može se napisati kao racionalna linearna kombinacija p-tih korijena jedinice.

Teorem 4.6.2: Gaussov kvadratni zakon reciprociteta

Neka su p i q različiti, pozitivni neparni prosti brojevi. Tada vrijedi $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Dokaz. Pokazali smo iznad da $\sqrt{\varepsilon p} \in \mathbb{Q}(\zeta_p)$. Označimo taj element s τ. Razmotrimo automorfizam $\sigma_q \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$; on je definiran s $\sigma_q(\zeta_p) = \zeta_p^q$. Budući da su konjugati od τ jednostavno $\pm\tau$, moramo imati

$$\sigma_q(\tau) = \pm\tau.$$

Nadalje, neka je S podgrupa od $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ definirana sa $\sigma(\tau) = \tau$ ako i samo ako $\sigma \in S$. (To je zato što je $\mathbb{Q}(\tau)$ fiksno polje od S po definiciji.) Pod identifikacijom $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ i $(\mathbb{Z}/p\mathbb{Z})^\times$, S odgovara podgrupi kvadrata; kombinirajući sve ovo, vidimo da je $\sigma_q(\tau) = \tau$ ako i samo ako je q kvadrat u $(\mathbb{Z}/p\mathbb{Z})^\times$; odnosno,

$$\sigma_q(\tau) = \left(\frac{q}{p}\right)\tau.$$

Sada neka je $\mathfrak{q}$ prost ideal u $\mathcal{O}_K$ iznad q. Zapišimo $\tau = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$ gdje su $a_i \in \mathbb{Z}$. (Primijetimo da je τ očito algebarski cijeli broj.) Koristeći da je $\sigma_q(\zeta_p) = \zeta_p^q$ i $a^q = a$ za sve $a \in \mathbb{F}_q$, nalazimo da je

$$\begin{aligned}
\sigma_q(\tau) &= a_0 + a_1\zeta_p^q + a_2\zeta_p^{2q} + \cdots + a_{p-2}\zeta_p^{(p-2)q} && (4.6)\\
&\equiv a_0^q + a_1^q\zeta_p^q + a_2^q\zeta_p^{2q} + \cdots + a_{p-2}^q\zeta_p^{(p-2)q} \pmod{\mathfrak{q}} && (4.7)\\
&\equiv (a_0 + a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-2}\zeta_p^{p-2})^q \pmod{\mathfrak{q}} && (4.8)\\
&\equiv \tau^q \pmod{\mathfrak{q}}. && (4.9)
\end{aligned}$$

Kombinirajući ovo s našim drugim izrazom za $\sigma_q(\tau)$ dobivamo

$$\left(\frac{q}{p}\right)\tau \equiv \tau^q \pmod{\mathfrak{q}}.$$

Budući da je $\mathfrak{q}$ prost i očito imamo $\tau \notin \mathfrak{q}$, možemo skratiti τ modulo $\mathfrak{q}$; zaključujemo da

$$\left(\frac{q}{p}\right) \equiv \tau^{q-1} \equiv (\varepsilon p)^{(q-1)/2} \pmod{\mathfrak{q}}.$$

Prema Eulerovom kriteriju, ovo pokazuje da

$$\left(\frac{q}{p}\right) \equiv \left(\frac{\varepsilon p}{q}\right) \pmod{\mathfrak{q}}.$$

Po definiciji, to znači da

$$\left(\frac{q}{p}\right) - \left(\frac{\varepsilon p}{q}\right) \in \mathfrak{q};$$

budući da su $\left(\frac{q}{p}\right)$ i $\left(\frac{\varepsilon p}{q}\right)$ cijeli brojevi, ta razlika je zapravo sadržana u $\mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}$. Zapravo, $\left(\frac{q}{p}\right)$ i $\left(\frac{\varepsilon p}{q}\right)$ su samo ± 1, pa je razlika sigurno manja od $\pm q$. Iz toga slijedi da zapravo imamo jednakost

$$\left(\frac{q}{p}\right) = \left(\frac{\varepsilon p}{q}\right).$$

Činjenica da je $\left(\frac{\varepsilon}{q}\right) = \left(\frac{(-1)^{(p-1)/2}}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ dovršava dokaz. □

4.7 Natrag na ciklotomska polja

Dokažimo još nekoliko rezultata o ciklotomskim poljima. Dokažimo prvo neke opće rezultate.

Definicija 4.7.1

Neka je $f(x) = \prod(x - \alpha_i) \in K(x)$, gdje su $\alpha_i \in \overline{K}$. Tada je *diskriminanta* $\Delta(f)$ od f jednaka

$$\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2.$$

Propozicija 4.7.2

Neka je $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Tada je $\Delta_K = \Delta(f_\alpha)$.

Dokaz. Neka je K stupnja n. Po pretpostavci $\{\alpha^i | i = 0, \dots n-1\}$ čine bazu od $\mathcal{O}_K$, pa je po definiciji

$$\Delta_K = \det(1, \alpha, \dots \alpha^{n-1}) = \det[\sigma_i(\alpha^{j-1})]_{ij} = \prod(\sigma_i(\alpha) - \sigma_j(\alpha))^2 = \Delta(f_\alpha),$$

gdje predzadnja jednakost vrijedi pošto je $[\sigma_i(\alpha^{j-1})]_{ij} = [\sigma_i(\alpha)^{j-1}]_{ij}$ Vandermondeova matrica.

□

Propozicija 4.7.3

Neka je $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Tada se u $\mathcal{O}_K$ granaju samo prosti brojevi $\in \mathbb{Z}$ koji dijele Δ_K.

Dokaz. Neka je f_α minimalni polinom od α, $p \in \mathbb{Z}$ prost i $p\mathcal{O}_K = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$, $\mathfrak{p}_i \neq \mathfrak{p}_j$ za $i \neq j$. Ovo je ekvivalentno sa $\overline{f_\alpha}(x) \equiv \prod_{i=1}^r g_i(x)^{e_i}$, $g_i \neq g_j$ za $i \neq j$. Kad bi bio neki $e_i > 1$, to bi značilo da se neki korijen od $\overline{f_\alpha}$ (u $\overline{\mathbb{F}}_p$) ponavlja.

Ovo je ekvivalentno sa tim da je $\Delta(\overline{f_\alpha(x)}) = 0$, što je ekvivalentno sa $\Delta(f(x)) \equiv 0 \pmod p$, što je po prethodnoj propoziciji ekvivalentno sa $p|\Delta_K$.

□

Propozicija 4.7.4

Neka je K stupnja n, $\mathcal{O}_K = \mathbb{Z}[\alpha]$ i f_α minimalni polinom od α. Tada je $\Delta_K = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'_\alpha(\alpha))$.

Dokaz. Neka su $\alpha_1, \dots \alpha_n$ konjugati od α. Vrijedi

$$f_\alpha(x) = \prod_{i=1}^n (x - \alpha_i), \quad f'_\alpha(x) = \sum_{j=1}^n \left(\prod_{i \neq j} (x - \alpha_i) \right).$$

Slijedi da je

$$f'_\alpha(\alpha_j) = \prod_{i \neq j} (\alpha_j - \alpha_i)),$$

pa je

$$N_{K/\mathbb{Q}}\left(f'_\alpha(\alpha_j)\right) = \prod_{j=1}^n (f'_\alpha(\alpha_j)) = \prod_{i \neq j} (\alpha_j - \alpha_i).$$

Pogledajmo koliko se puta za fiksni i, j, $i \neq j$ javlja u Δ_K, a koliko u $N_{K/\mathbb{Q}}(f'_\alpha(\alpha))$: u Δ_K se kao faktor javlja $(\alpha_i - \alpha_j)^2$, dok se u $N_{K/\mathbb{Q}}(f'_\alpha(\alpha))$ javlja $(\alpha_i - \alpha_j)(\alpha_j - \alpha_i) = -(\alpha_i - \alpha_j)^2$. Vidimo da se u $N_{K/\mathbb{Q}}(f'_\alpha(\alpha))$ pojavi ukupno $\binom{n}{2}$ minusa, što dokazuje našu tvrdnju. □

Propozicija 4.7.5

$\Delta_{\mathbb{Q}(\zeta_p)} = (-1)^{\frac{p-1}{2}} p^{p-2}$.

Dokaz. Po prošloj propoziciji imamo da je

$$\Delta_{\mathbb{Q}(\zeta_p)} = (-1)^{\frac{(p-1)(p-2)}{2}} N(\Phi_p'(\zeta_p)).$$

Vrijedi

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} \Longrightarrow \Phi_p'(x) = \frac{(x-1)px^{p-1} - (x^p - 1)}{(x-1)^2}$$

$$\Longrightarrow \Phi_p'(\zeta_p) = \frac{(\zeta_p - 1)p\zeta_p^{p-1}}{(\zeta_p - 1)^2} = \frac{p\zeta_p^{p-1}}{\zeta_p - 1}.$$

Slijedi da je

$$N(\Phi_p'(\zeta_p)) = \frac{N(p)N(\zeta_p^{p-1})}{N(\zeta_p - 1)} = \frac{p^{p-1} \cdot 1}{p} = p^{p-2}.$$

□

primijetimo da smo opet na drugi način dokazali da je p jedini prost broj koji se grana u $\mathbb{Q}(\zeta_p)$.

4.8 Dekompozicijska i inercijska grupa

Neka je K polje algebarskih brojeva, te neka je L/K konačno Galoisovo proširenje od K stupnja n. Neka je $\mathfrak{p}$ fiksan prost ideal od $\mathcal{O}_K$ i neka je njegova faktorizacija u $\mathcal{O}_L$

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e,$$

gdje svi $\mathfrak{P}_i$-ovi imaju isti stupanj inercije f. Sjetimo se da vrijedi $ref = n$, te da grupa $\mathrm{Gal}(L/K)$ djeluje na skup $\{\mathfrak{P}_1, \cdots, \mathfrak{P}_r\}$. To djelovanje je tranzitivno, tj. za svaki $\mathfrak{P}_i$ i $\mathfrak{P}_j$ postoji $\sigma \in \mathrm{Gal}(L/K)$ takav da je $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$.

Kada grupa djeluje na skup, tada se često promatra stabilizatorska podgrupa nekog elementa, tj. podgrupa elemenata grupe koji trivijalno djeluju na taj element skupa.

Definicija 4.8.1

Uz notaciju kao i prije, definiramo *dekompozicijsku grupu* $D(\mathfrak{P}_i/\mathfrak{p})$ elementa $\mathfrak{P}_i$

$$D(\mathfrak{P}_i/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\} \leq \mathrm{Gal}(L/K).$$

Primijetimo sljedeće: neka su $\mathfrak{P}_i$ i $\mathfrak{P}_j$ takvi da je $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Tada se lako provjeri da je

$$D(\mathfrak{P}_j/\mathfrak{p}) = \sigma D(\mathfrak{P}_i/\mathfrak{p})\sigma^{-1}.$$

Dakle, sve dekompozicijske grupe su konjugirane. Pošto je $D(\mathfrak{P}_i)$ po definiciji stabilizatorska podgrupa elementa $\mathfrak{P}_i$, te je djelovanje grupe tranzitivno (tj. orbita od $\mathfrak{P}_i$ je duljine r), po teoremu o orbiti i stabilizatoru da je

$$\#D(\mathfrak{P}_i/\mathfrak{p}) = n/r = ef.$$

Primjer 4.8.2

Promotrimo proširenje $\mathbb{Q}(\zeta_{15})/\mathbb{Q}$; to je proširenje stupnja $\phi(15) = 8$, vrijedi $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q}) \simeq (\mathbb{Z}/15\mathbb{Z})^\times$. Elemente $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q})$ prikazujemo kao $\sigma_i(\zeta_{15}) = \zeta_{15}^i$, gdje je $i \in (\mathbb{Z}/15\mathbb{Z})^\times$. Također, vrijedi da je prsten cijelih brojeva u $\mathbb{Q}(\zeta_{15})$ jednak $\mathbb{Z}[\zeta_{15}]$.
Promotrimo faktorizaciju elemenata $2, 3, 5$ i 31 u $\mathbb{Z}(\zeta_{15})$. Neka su

$$\begin{aligned}
\mathfrak{p}_2 &= (2, \zeta_{15}^4 + \zeta_{15} + 1),\\
\mathfrak{p}_3 &= (3, \zeta_{15}^4 + \zeta_{15}^3 + \zeta_{15}^2 + \zeta_{15} + 1),\\
\mathfrak{p}_5 &= (5, \zeta_{15}^2 + \zeta_{15} + 1)\\
\mathfrak{p}_{31} &= (31, \zeta_{15} + 3)
\end{aligned}$$

Prikažimo u sljedećoj tablici vrijednosti r, e i f za navedene proste brojeve.

	r	e	f
$\mathfrak{p}_2$	2	1	4
$\mathfrak{p}_3$	1	2	4
$\mathfrak{p}_5$	1	4	2
$\mathfrak{p}_{31}$	8	1	1

Izračunajmo sada dekompozicijsku grupu svakog od ovih prostih elemenata. Očito je $D(\mathfrak{p}_3/3) = D(\mathfrak{p}_5/5) = \mathrm{Gal}(L/K)$, pošto su $\mathfrak{p}_3$ i $\mathfrak{p}_5$ jedini prosti brojevi iznad 3 i 5. Također, očito vrijedi $\#D(\mathfrak{p}_{31}/31) = n/r = 1$. Dakle, jedini zanimljivi slučaj je $D(\mathfrak{p}_2/2)$. To je grupa reda $ef = 4$. Promotrimo preslikavanje

$$\mathbb{Z}[\zeta_{15}] \to \mathbb{Z}[\zeta_{15}]/\mathfrak{p}_2 = \mathbb{F}_2[x]/(x^4 + x + 1),$$

koji šalje ζ_{15} u x. Vrijedi

$$\sigma_i((2, \zeta_{15}^4 + \zeta_{15} + 1)) = (2, \sigma(\zeta_{15}^4 + \zeta_{15} + 1)) = (2, \zeta_{15}^{4i} + \zeta_{15}^i + 1).$$

Zaključujemo da će σ biti u $D(\mathfrak{p}_2/2)$ ako i samo ako je $\zeta_{15}^{4i} + \zeta_{15}^i + 1$ u $\mathfrak{p}_2$, ili ekvivalentno, da $x^4 + x + 1$ dijeli $x^{4i} + x^i + 1$ u $\mathbb{F}_2[x]$. Sada eksplicitnim računom možemo provjeriti da je

$$D(\mathfrak{p}_2/2) = \{\sigma_1, \sigma_2, \sigma_4, \sigma_8\}.$$

Dekompozicijska grupa nam je važna jer fiksira polje ostataka. Neka je $\mathfrak{P}$ prost broj iznad $\mathfrak{p}$, te neka je $\sigma \in D(\mathfrak{P}/\mathfrak{p})$. Pošto je $\sigma(\mathfrak{P}) = \mathfrak{P}$, slijedi da σ inducira automorfizam polja $\mathcal{O}_L/\mathfrak{P}$. Ovaj automorfizam svakako fiksira $\mathcal{O}_K/\mathfrak{p}$, te slijedi da smo dobili preslikavanje

$$D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})), \tag{4.10}$$

koje lako provjerimo da je homomorfizam.

Definicija 4.8.3

Inercijska grupa $I(\mathfrak{P}/\mathfrak{p})$ je jezgra preslikavanja (4.10), tj.

$$I(\mathfrak{P}/\mathfrak{p}) = \ker\left(D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))\right).$$

Eksplicitnije, vrijedi da je

$$I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in D(\mathfrak{P}/\mathfrak{p}) | \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}} \text{ za sve } \alpha \in \mathcal{O}_L\}.$$

Po definiciji inercijske grupe i prvom teoremu o izomorfizmu grupa, slijedi da je

$$D(\mathfrak{P}/\mathfrak{p})/I(\mathfrak{P}/\mathfrak{p}) \simeq \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})).$$

Kao i za dekompozicijske grupe, inercijske grupe prostih ideala koje leže nas istim prostim idealom od $\mathcal{O}_K$ su međusobno konjugirane, te se lako vidi da je $\#I(\mathfrak{P}/\mathfrak{p}) = e$. Drugim riječima, inercijska grupa $I(\mathfrak{P}/\mathfrak{p})$ je trivijalna ako i samo ako je $\mathfrak{P}/\mathfrak{p}$ nerazgranat.

Primjer 4.8.4

Izračunajmo inercijske grupe iz prethodnog primjera. Očito su $I(\mathfrak{p}_2/2)$ i $I(\mathfrak{p}_{31}/31)$ trivijalne. Grupa $I(\mathfrak{p}_3/3)$ je reda 2. Promotrimo preslikavanje

$$\mathbb{Z}[\zeta_{15}]/\mathfrak{p}_3 \simeq \mathbb{F}_3[x]/(x^4 + x^3 + x^2 + x + 1).$$

Element σ_i iz $D(\mathfrak{p}_3/3)$ će biti u $I(\mathfrak{p}_3/3)$ ako i samo ako je $\sigma_i(\zeta_{15}) = \zeta_{15}$ pošto je očito $\sigma_i(1) = 1$, a 1 i ζ_{15} su generatori od $\mathbb{Z}[\zeta_{15}]$, pa time i $\mathbb{Z}[\zeta_{15}]/\mathfrak{p}_3$. To je ekvivalentno da je

$$\sigma_i(x) = x^i \equiv x \pmod{x^4 + x^3 + x^2 + x + 1}.$$

Drugim riječima, pitamo se kada $x^4 + x^3 + x^2 + x + 1$ dijeli $x^i - x$. Vidimo da je to istina za $i = 11$, te onda pošto je $I(\mathfrak{p}_3/3)$ grupa reda 2, zaključujemo da je

$$I(\mathfrak{p}_3/3) = \{\sigma_1, \sigma_{11}\}.$$

Analogno možemo izračunati

$$I(\mathfrak{p}_5/5) = \{\sigma_1, \sigma_4, \sigma_7, \sigma_{13}\}.$$

Definicija 4.8.5

Pretpostavimo da je $\mathrm{Gal}(L/K)$ Abelova. Definiramo *inercijsko polje* L^I od $\mathfrak{P}/\mathfrak{p}$ kao fiksno polje od $I(\mathfrak{P}/\mathfrak{p})$, te *dekompozicijsko polje* L^D od $\mathfrak{P}/\mathfrak{p}$ kao fiksno polje od $D(\mathfrak{P}/\mathfrak{p})$.

Teorem 4.8.6: Teorem o slojevima

Neka je $\mathfrak{p}$ netrivijalni ideal od $\mathcal{O}_F$, gdje je K/F Abelovo proširenje. Tada se $\mathfrak{p}$ potpuno cijepa u K^D, te ideali iznad $\mathfrak{p}$ ostaju inertni u K^I/K^D, te se potpuno granaju u K/K^D.

Poglavlje 5

Grupa klasa ideala

5.1 Razlomljeni ideali

Ideali prstena cijelih brojeva ne čine grupu, jer nemaju inverze. Razlomljeni ideali, s druge strane, tvore grupu; odnos između razlomljenih ideala i običnih ideala vrlo je sličan odnosu između polja brojeva i njegovog prstena cijelih brojeva.

Neka je K polje brojeva s prstenom cijelih brojeva $\mathcal{O}_K$. Neka je $\mathfrak{r}$ neprazan podskup od K koji je $\mathcal{O}_K$-modul; odnosno, $\mathfrak{r}$ je zatvoren na zbrajanje i množenjem elementima iz $\mathcal{O}_K$. Za takav $\mathfrak{r}$ kažemo da je razlomljeni ideal ako postoje $\gamma_1, \ldots, \gamma_m \in r$ takvi da je

$$\mathfrak{r} = \{\alpha_1\gamma_1 + \cdots + \alpha_m\gamma_m \mid \alpha_i \in \mathcal{O}_K\};$$

odnosno, $\mathfrak{r}$ je generiran nad $\mathcal{O}_K$ pomoću γ_i. (Ključna stvar ovdje je da je $\mathfrak{r}$ konačno generiran nad $\mathcal{O}_K$. Nisu svi $\mathcal{O}_K$-podmoduli od K takvi).

Postoje dva osnovna primjera razlomljenih ideala. Prije svega, svaki neprazan ideal $\mathfrak{a}$ od $\mathcal{O}_K$ također je razlomljeni ideal: $\mathfrak{a}$ je $\mathcal{O}_K$-modul po definiciji i ima konačni skup generatora jer je $\mathcal{O}_K$ Noetherin. Da bismo izbjegli zabunu, od sada ćemo ideale od $\mathcal{O}_K$ nazivati cjelobrojnim idealima.

Druga vrsta primjera su razlomljeni ideali oblika $\gamma\mathcal{O}_K$ za neki $\gamma \in K^*$. (Lako se provjeri da je $\gamma\mathcal{O}_K$ $\mathcal{O}_K$-modul, i ima samo jedan generator γ.) Takav razlomljeni ideal naziva se glavni razlomljeni ideal. Primjećujemo da su glavni ideali od $\mathcal{O}_K$ upravo cjelobrojni glavni razlomljeni ideali.

Općenitije, neka je $\mathfrak{a}$ bilo koji ideal od $\mathcal{O}_K$ i neka je γ bilo koji element iz K^*. Tada je $\gamma\mathfrak{a}$ razlomljeni ideal. ($\gamma\mathfrak{a}$ ima konačni skup generatora jer ako $\alpha_1, \ldots, \alpha_m$ generiraju $\mathfrak{a}$, onda $\gamma\alpha_1, \ldots, \gamma\alpha_m$ generiraju $\gamma\mathfrak{a}$.) I obrat ove tvrdnje vrijedi.

Lema 5.1.1

Neka je $\mathfrak{r}$ $\mathcal{O}_K$-podmodul od K. Tada je $\mathfrak{r}$ razlomljeni ideal ako i samo ako postoji $\gamma \in K^*$ takav da je $\gamma\mathfrak{r}$ cjelobrojni ideal. (Zapravo, može se uzeti da je γ racionalni cijeli broj.)

Dokaz. Vidjeli smo gore da ako je $\mathfrak{a}$ cjelobrojni ideal i $\gamma \in K^*$, onda je $\gamma\mathfrak{a}$ razlomljeni ideal. Obratno, ako je $\mathfrak{r}$ razlomljeni ideal, možemo pisati

$$\mathfrak{r} = \{\alpha_1\gamma_1 + \ldots + \alpha_m\gamma_m \mid \alpha_i \in \mathcal{O}_K\}$$

za neke $\gamma_1, \ldots, \gamma_m \in \mathfrak{r}$. Po ranije dokazanom postoje $a_1, \ldots, a_m \in \mathbb{Z}$ takvi da je $a_i\gamma_i \in \mathcal{O}_K$. Lako se provjeri da je $a_1 \cdots a_m\mathfrak{r}$ cjelobrojni ideal, što dokazuje lemu s $\gamma = a_1 \cdots a_m$. □

Označit ćemo s I_K skup svih razlomljenih ideala od K. Ako su $\mathfrak{r}, \mathfrak{s} \in I_K$, definiramo produkt $\mathfrak{rs}$ kao $\mathcal{O}_K$-modul generiran svim produktima parova elemenata iz $\mathfrak{r}$ i $\mathfrak{s}$. Primijetimo da ako je $\mathfrak{r}$ generiran s $\gamma_1, \ldots, \gamma_m$ i $\mathfrak{s}$ je generiran s $\delta_1, \ldots, \delta_k$, onda je $\mathfrak{rs}$ generiran produktima $\gamma_i\delta_j$. Posebno, $\mathfrak{rs}$ je također razlomljeni ideal.

Teorem 5.1.2

Skup I_K je Abelova grupa pod množenjem razlomljenih ideala.

Dokaz. Vidjeli smo gore da je I_K zatvoren pod množenjem. Jasno je da je ovo množenje komutativno i asocijativno. Lako se provjerava da je jedinični element jedinični ideal $\mathcal{O}_K$. Preostaje pronaći inverze. Dakle, neka je $\mathfrak{r}$ razlomljeni ideal i odaberimo $\gamma \in K^*$ takav da je $\gamma\mathfrak{r}$ cjelobrojni ideal. Prema Propoziciji 3.4.3 postoji cjelobrojni ideal $\mathfrak{b}$ takav da je $\gamma\mathfrak{rb}$ glavni, recimo generiran s $\alpha \in O_K^*$. Uzmimo $\mathfrak{s} = \frac{\gamma}{\alpha}\mathfrak{b}$. Tada je $\mathfrak{s}$ razlomljeni ideal, i imamo

$$\mathfrak{rs} = \frac{\gamma\mathfrak{rb}}{\alpha} = \mathcal{O}_K.$$

Tako je $\mathfrak{s}$ inverz od $\mathfrak{r}$ u I_K. □

primijetimo da je iz dokaza Propozicije 3.4.3 jasno da ako je $\mathfrak{r}$ razlomljeni ideal, onda je njegov inverz dan s

$$\mathfrak{r}^{-1} = \{\gamma \in K^* \mid \gamma\mathfrak{r} \subseteq \mathcal{O}_K\}.$$

Također možemo karakterizirati razlomljene ideale u smislu jedinstvene faktorizacije ideala.

Propozicija 5.1.3

Svaki razlomljeni ideal $\mathfrak{r}$ može se zapisati kao

$$\mathfrak{r} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

gdje su $\mathfrak{p}_i$ različiti prosti ideali od $\mathcal{O}_K$ i e_i su cijeli brojevi. (Primijetimo da dopuštamo da e_i budu negativni.) Ovaj izraz je jedinstven do na promjenu redoslijeda faktora. Dakle, I_K je slobodna Abelova grupa na skupu

$$\{\mathfrak{p} \mid \mathfrak{p} \text{ je prost ideal od } \mathcal{O}_K\}.$$

Konačno, $\mathfrak{r}$ je cjelobrojni ideal ako i samo ako je svaki e_i nenegativan.

Dokaz. Neka je $\mathfrak{r}$ razlomljeni ideal i odaberimo nenul racionalni cijeli broj $a \in \mathbb{Z}$ takav da je $a\mathfrak{r}$ cjelobrojni ideal. Tada možemo pisati (jedinstveno do na promjenu redoslijeda i dodavanje faktora s nul eksponentom)

$$aO_K = \mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_r^{e_r'}$$

$$a\mathfrak{r} = \mathfrak{p}_1^{e_1''} \cdots \mathfrak{p}_r^{e_r''};$$

ovdje dopuštamo da neki e_i' i e_i'' budu nula. Tako, budući da je I_K grupa,

$$\mathfrak{r} = \mathfrak{p}_1^{e_1''-e_1'} \cdots \mathfrak{p}_r^{e_r''-e_r'}.$$

Ovo pokazuje da $\mathfrak{r}$ ima takav izraz; činjenica da je on jedinstven slijedi iz činjenice da su faktorizacije od aO_K i $a\mathfrak{r}$ jedinstvene. Činjenica da je $\mathfrak{r}$ cjelobrojni ideal ako i samo ako je svaki e_i pozitivan jasna je iz jedinstvene faktorizacije ideala. □

Primijetimo da je ova dekompozicija razlomljenih ideala u smislu prostih ideala potpuno analogna dekompoziciji racionalnih brojeva u smislu racionalnih prostih brojeva.

5.2 Grupa klasa ideala

Neka je K polje brojeva s prstenom cijelih brojeva $\mathcal{O}_K$. Vidjeli smo da $\mathcal{O}_K$ možda nije domena jedinstvene faktorizacije, iako će imati jedinstvenu faktorizaciju ideala. Također smo vidjeli da je $\mathcal{O}_K$ DJF ako i samo ako je DGI; odnosno, ako i samo ako je svaki ideal glavni. Nadalje, čak i kad $\mathcal{O}_K$ nije DGI, često je korisno znati kada su ideali glavni.

Ove činjenice sugeriraju da bi bilo korisno imati neki način da se odredi je li ideal glavni. Iako je to u praksi često prilično teško, možemo apstraktno dosta toga dokazati. Definirajmo P_K kao podgrupu od I_K koja se sastoji od glavnih razlomljenih ideala. Primijetimo da su cjelobrojni ideali u P_K upravo glavni ideali od $\mathcal{O}_K$.

Definicija 5.2.1

Definiramo *grupu klasa ideala* C_K od K kao kvocijent

$$C_K = I_K/P_K.$$

Grupa C_K će nam biti korisna za promatranje ranije postavljenih pitanja. Prije svega, C_K je trivijalna grupa ako i samo ako je $I_K = P_K$; odnosno, ako i samo ako je svaki razlomljeni ideal od K zapravo glavni. Budući da su cjelobrojni ideali u P_K upravo glavni ideali, ovo je ekvivalentno tome da je $\mathcal{O}_K$ DGI, što je pak ekvivalentno tome da je $\mathcal{O}_K$ DJF. Odnosno, C_K je trivijalna ako i samo ako je $\mathcal{O}_K$ DJF. Drugo, primijetimo da je razlomljeni ideal $\mathfrak{r}$ glavni ako i samo ako se preslikava u 0 u C_K.

Zvat ćemo elemente od C_K klasama ideala; tako je klasa ideala A jednostavno koskup od P_K. Po definiciji C_K, dva razlomljena ideala $\mathfrak{a}$ i $\mathfrak{b}$ leže u istoj klasi ideala ako i samo ako postoji neki $\gamma \in K^*$ s

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

Pisat ćemo ovu relaciju kao $a \sim b$.

Sljedeća reinterpretacija Leme 5.1.1 pokazuje da razlomljeni ideali zapravo nisu esencijalni za definiciju grupe idealnih klasa.

Lema 5.2.2

Neka je A klasa ideala. Tada postoji cjelobrojni ideal a u koskupu A.

Dokaz. Neka je $\mathfrak{r}$ bilo koji razlomljeni ideal u A. Tada postoji $\gamma \in K^*$ takav da je $\gamma\mathfrak{r}$ cjelobrojni ideal. Budući da je $\gamma\mathcal{O}_K \in P_K$, imamo $\gamma\mathfrak{r} \in A$, što dokazuje lemu. □

Primjer 5.2.3

Uzmimo $K = \mathbb{Q}(\sqrt{-5})$ i razmotrimo ideale

$$\mathfrak{p}_1 := (2, 1-\sqrt{-5}), \quad \mathfrak{p}_2 := (3, 1+\sqrt{-5}), \quad \mathfrak{p}_3 := (3, 1-\sqrt{-5}).$$

Možemo direktno izračunati da je $(2, 1-\sqrt{-5}) = \gamma(3, 1+\sqrt{-5})$ gdje je

$$\gamma = -\frac{\sqrt{-5}}{3} + \frac{1}{3}.$$

Dakle, $(2, 1-\sqrt{-5}) \sim (3, 1+\sqrt{-5})$. Također, možemo primijetiti i da je

$(6) := \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$, $\mathfrak{p}_1^2 = (2)$, $\mathfrak{p}_2\mathfrak{p}_3 = (3)$, $\mathfrak{p}_1\mathfrak{p}_2 = (1+\sqrt{-5})$, $\mathfrak{p}_1\mathfrak{p}_3 = (1-\sqrt{-5})$,

pa zaključujemo da je

$$\mathfrak{p}_1 \sim \mathfrak{p}_2 \sim \mathfrak{p}_3, \text{ te je } \quad [\mathfrak{p}_1] \text{ reda 2.}$$

5.3 Konačnost grupe klasa ideala

Činjenica da je grupa klasa ideala konačna pokazuje da jedinstvena faktorizacija nikada ne "propada previše" u prstenima cijelih brojeva polja algebarskih brojeva i možda je najvažnija činjenica u algebarskoj teoriji brojeva. U ovom ćemo odjeljku dati iznenađujuće jednostavan dokaz.

Teorem 5.3.1

Neka je K polje algebarskih brojeva. Postoji broj λ_K, koji ovisi samo o K, takav da svaki nenul ideal $\mathfrak{a}$ od $\mathcal{O}_K$ sadrži nenul element α sa svojstvom:

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \lambda_K N_{K/\mathbb{Q}}(\mathfrak{a}).$$

Dokaz. Neka je $\alpha_1, \ldots, \alpha_n$ integralna baza za $\mathcal{O}_K$ i neka su $\sigma_1, \ldots, \sigma_n$ ulaganja polja K u $\mathbb{C}$. Pokazat ćemo da možemo uzeti

$$\lambda_K = \prod_{i=1}^{n} \left(\sum_{j=1}^{n} |\sigma_i(\alpha_j)| \right).$$

Neka je $\mathfrak{a}$ nenul ideal od $\mathcal{O}_K$ i neka je m jedinstven pozitivni cijeli broj takav da vrijedi

$$m^n \leq N_{K/\mathbb{Q}}(\mathfrak{a}) < (m+1)^n.$$

Razmotrimo skup od $(m+1)^n$ elemenata:

$$\left\{ \sum_{j=1}^{n} m_j \alpha_j \,\middle|\, 0 \leq m_j \leq m,\ m_j \in \mathbb{Z} \right\}.$$

Budući da kvocjentni prsten $\mathcal{O}_K/\mathfrak{a}$ ima manje od $(m+1)^n$ elemenata, dva gore navedena elementa moraju biti kongruentna modulo $\mathfrak{a}$. Oduzimanjem ta dva elementa dobivamo element

$$\alpha = \sum_{j=1}^{n} m'_j \alpha_j \in \mathfrak{a}$$

sa svojstvom $|m'_j| \leq m$. Računamo sada normu:

$$\begin{aligned}
|N_{K/\mathbb{Q}}(\alpha)| &= \prod_{i=1}^{n} |\sigma_i(\alpha)| \\
&= \prod_{i=1}^{n} \left| \sigma_i \left(\sum_{j=1}^{n} m'_j \alpha_j \right) \right| \\
&= \prod_{i=1}^{n} \left| \sum_{j=1}^{n} m'_j \sigma_i(\alpha_j) \right| \\
&\leq \prod_{i=1}^{n} \sum_{j=1}^{n} |m'_j| |\sigma_i(\alpha_j)| \\
&\leq \prod_{i=1}^{n} \sum_{j=1}^{n} m |\sigma_i(\alpha_j)| \\
&= m^n \lambda_K \leq \lambda_K N_{K/\mathbb{Q}}(\mathfrak{a}).
\end{aligned}$$

□

Korolar 5.3.2

Neka je A klasa ideala u C_K. Tada A sadrži integralni ideal norme $\leq \lambda_K$.

Dokaz. Neka je $\mathfrak{b}$ neki integralni ideal u A^{-1}. Po prethodnom teoremu možemo pronaći $\beta \in \mathfrak{b}$ takav da vrijedi

$$|N_{K/\mathbb{Q}}(\beta)| \leq \lambda_K N_{K/\mathbb{Q}}(\mathfrak{b}).$$

Glavni ideal $\beta\mathcal{O}_K$ sadržan je u $\mathfrak{b}$, a ranije smo dokazali da onda mora postojati integralni ideal $\mathfrak{a}$ takav da vrijedi $\mathfrak{a}\mathfrak{b} = \beta\mathcal{O}_K$. Budući da je $\beta\mathcal{O}_K$ glavni ideal, imamo $\mathfrak{a} \in A$, te računamo

$$N_{K/\mathbb{Q}}(\mathfrak{a}) = \frac{|N_{K/\mathbb{Q}}(\beta)|}{N_{K/\mathbb{Q}}(\mathfrak{b})} \leq \lambda_K.$$

□

Korolar 5.3.3

Grupa klasa ideala C_K je konačna.

Dokaz. Prema prethodnom korolaru svaka klasa ideala sadrži ideal norme najviše λ_K. Postoji samo konačno mnogo ideala s normom $\leq \lambda_K$, što znači da svaka klasa ideala sadrži jedan od konačnog skupa ideala. Konkretno, C_K mora biti konačna. □

5.4 Teorija Minkowskog

Počet ćemo s nekim osnovnim pojmovima iz linearne algebre koji na prvi pogled možda ne djeluju povezano s našom temom. No, strategija je primijeniti linearne algebarske koncepte, posebno pojam rešetke, na ideale Dedekindovih prstenova kako bismo dobili osjećaj za "veličinu" ideala. To će nam omogućiti da ograničimo veličinu ideala i konačno dokažemo da je broj klasa konačan.

Definicija 5.4.1

Neka je V n-dimenzionalan $\mathbb{R}$-vektorski prostor. Rešetka u V je podskup oblika

$$\Gamma = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \cdots + \mathbb{Z}v_m,$$

gdje su $v_1, \ldots, v_m$ linearno nezavisni vektori u V. Skup $\{v_1, \ldots, v_m\}$ naziva se baza rešetke, a skup

$$\Phi = \{x_1v_1 + \cdots + x_mv_m \mid x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

naziva se fundamentalna domena rešetke. Rešetka je potpuna ako je $m = n$.

Budući da radimo u Euklidskom prostoru, imamo na raspolaganju pojam volumena. Ako su $v_1, \ldots, v_n$ bazni vektori rešetke, tada je volumen temeljnog paralelopipeda definiran kao

$$\mathrm{vol}(\Phi) = |\det A|,$$

gdje je A matrica promjene baze od ortonormirane baze od $\mathbb{R}^n$ do $v_1, \ldots, v_n$. Označimo $\mathrm{vol}(\Gamma) := \mathrm{vol}(\Phi)$.

Sada smo spremni izreći i dokazati Minkowskijev teorem o točkama na rešetci.

Teorem 5.4.2: Minkowskijev teorem o točkama na rešetci

Neka je Γ potpuna rešetka u Euklidskom vektorskom prostoru V, a neka je X centralno simetričan (oko ishodišta) i konveksan podskup od V za koji vrijedi

$$\mathrm{vol}(X) > 2^n \,\mathrm{vol}(\Gamma).$$

Tada X sadrži barem jednu točku $0 \neq \gamma \in \Gamma$.

Dokaz. Pretpostavimo prvo da postoje $\gamma_1, \gamma_2 \in \Gamma$ takvi da je

$$\left(\frac{1}{2}X + \gamma_1\right) \cap \left(\frac{1}{2}X + \gamma_2\right) \neq \emptyset. \tag{5.1}$$

Dakle postoje $x_1, x_2 \in X$ takvi da

$$y = \frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2.$$

Tada slijedi da je

$$\gamma_1 - \gamma_2 = \frac{1}{2}(x_2 - x_1),$$

pa je $\gamma_1 - \gamma_2$ polovište dužine između x_2 i $-x_1$. Pošto je X centralno-simetričan oko ishodišta, imamo da je $-x_1 \in X$, te pošto je X konveksan, slijedi da $\gamma_1 - \gamma_2$ pripada skupu X. Budući da su γ_1 i γ_2 elementi rešetke Γ (koja je grupa), razlika $\gamma_1 - \gamma_2$ također pripada Γ. Time smo dokazali da je $(\gamma_1 - \gamma_2) \in \Gamma \cap X$.

Ostaje dokazati da postoje $\gamma_1, \gamma_2 \in \Gamma$ koji zadovoljavaju (5.1).

Pogledajmo kolekciju skupova

$$\left\{\frac{1}{2}X + \gamma \mid \gamma \in \Gamma\right\}.$$

Pretpostavimo da su svi ti skupovi međusobno disjunktni. Tada to vrijedi i za njihove presjeke $\Phi \cap (\frac{1}{2}X + \gamma)$ s fundamentalnom domenom Φ od Γ. Dakle imamo

$$\mathrm{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \mathrm{vol}\left(\Phi \cap \left(\frac{1}{2}X + \gamma\right)\right)$$

Translacija skupa $\Phi \cap \left(\frac{1}{2}X + \gamma\right)$ za $-\gamma$ daje skup $(\Phi - \gamma) \cap \frac{1}{2}X$ istog volumena. S druge strane, skup

$$\{\Phi - \gamma \mid \gamma \in \Gamma\}$$

prekriva cijeli prostor V, pa i $\frac{1}{2}X$. Dakle, mi dobivamo

$$\mathrm{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \mathrm{vol}\left((\Phi - \gamma) \cap \frac{1}{2}X\right) = \mathrm{vol}\left(\frac{1}{2}X\right) = \frac{1}{2^n}\,\mathrm{vol}(X),$$

što je kontradikcija s našom pretpostavkom.

□

Sada ćemo primijeniti teoriju rešetki na polja algebarskih brojeva $K/\mathbb{Q}$ stupnja n. Razmatramo preslikavanje

$$j : K \to K_{\mathbb{C}} = \prod_{i=1}^{n} \mathbb{C},$$

koje svakoj vrijednosti $x \in K$ pridružuje njen niz ulaganja

$$j(x) = (\tau_1(x), \ldots, \tau_n(x)).$$

Iako je K_C vektorski prostor nad $\mathbb{C}$, što nam daje pojam udaljenosti, prilično ga je teško geometrijski vizualizirati. Bilo bi mnogo "bolje" kada bismo mogli preslikati K u Euklidski prostor bez gubitka informacija iz kompleksnih ulaganja. Da bismo to učinili, moramo primijetiti tri stvari: Prvo, realna ulaganja već preslikavaju K u $\mathbb{R}$, tako da trenutno možemo zanemariti ta ulaganja. Drugo, kompleksna ulaganja mogu se promatrati kao ulaganja u $\mathbb{R}^2$ razdvajanjem ulaganja na njihov realni i imaginarni dio. Konačno, kompleksna ulaganja dolaze u parovima kompleksnih konjugata. Dakle, ako imamo samo polovicu kompleksnih ulaganja, odnosno jedan iz svakog para kompleksnih konjugata, ne gubimo nikakve informacije. To nas dovodi do opisa prostora Minkowskog:

Svako ulaganje od K u $\mathbb{C}$ je ili realno ili kompleksno. Neka su $\rho_1, \ldots, \rho_r$ realna ulaganja. Kao što je upravo spomenuto, kompleksna ulaganja dolaze u parovima. Neka su $\sigma_1, \overline{\sigma}_1, \ldots, \sigma_s, \overline{\sigma}_s$ kompleksna ulaganja. Od sada nadalje će nam r biti broj realnih ulaganja, a $2s$ broj kompleksnih ulaganja. Iz svakog para kompleksnih ulaganja, odabiremo jedno fiksno ulaganje. Zatim dopuštamo da ρ varira preko realnih ulaganja, a σ preko odabranih kompleksnih ulaganja.

Definicija 5.4.3

Prostor Minkowskog $K_{\mathbb{R}}$ definiran je kao

$$K_{\mathbb{R}} = \{(z_\tau) \in K_{\mathbb{C}} \mid z_\rho \in \mathbb{R}, z_{\overline{\sigma}} = \bar{z}_\sigma\},$$

gdje τ varira kroz svih n ulaganja polja K u $\mathbb{C}$, te gdje su ρ realna ulaganja, a σ kompleksna.

primijetimo da je $j(K) \subseteq K_{\mathbb{R}}$. Na taj način možemo polje K interpretirati kao n-dimenzionalni Euklidski prostor, a njegove prstenove cijelih brojeva i ideale kao rešetke u prostoru Minkowskog.

Da bismo prostor Minkowskog zamislili geometrijski, moramo ga uložiti u $\mathbb{R}^n$. Sljedeći rezultat se lako dokazuje (ostavljamo za vježbu).

Propozicija 5.4.4

Preslikavanje

$$f : K_{\mathbb{R}} \to \prod_{\tau} \mathbb{R} = \mathbb{R}^{r+2s}, \tag{5.2}$$

dano s $(z_\tau) \mapsto (x_\tau)$, gdje je

$$x_\rho = z_\rho, \quad x_\sigma = \mathrm{Re}(z_\sigma), \quad x_{\overline{\sigma}} = \mathrm{Im}(z_\sigma), \tag{5.3}$$

je izomorfizam. Ovaj izomorfizam pretvara kanonsku metriku $\langle \cdot, \cdot \rangle$ u skalarni produkt

$$\langle x, y \rangle = \sum_{\tau} \alpha_\tau x_\tau \overline{y_\tau},$$

gdje je $\alpha_\tau = 1$ ako je τ realan, a $\alpha_\tau = 2$ ako je τ kompleksan.

Može se dosta jednostavno pokazati da je $\mathrm{vol}(X) = 2^s \,\mathrm{vol}_{\text{Lebesgue}} f(X)$
Da bismo ilustrirali ovaj koncept, predstavljamo jednostavan primjer.

Primjer 5.4.5

Neka je $K = \mathbb{Q}[\sqrt[3]{2}]$. $K/\mathbb{Q}$ je proširenje stupnja 3. Stoga postoje tri kanonska ulaganja od K u $\mathbb{C}$, koja ćemo označiti τ_1, τ_2 i τ_3. Preslikavanja su jedinstveno definirana njihovim djelovanjem na $\sqrt[3]{2}$, pa pišemo

$$\tau_1(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \tau_2(\sqrt[3]{2}) = \sqrt[3]{2}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right), \quad \tau_3(\sqrt[3]{2}) = \sqrt[3]{2}\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right).$$

Vidimo da je τ_1 realno ulaganje i da je $\tau_2 = \overline{\tau_3}$. Stoga, koristeći gornji izomorfizam, tri nova ulaganja u $\mathbb{R}^3$ su

$$\sigma_1(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \sigma_2(\sqrt[3]{2}) = -\frac{\sqrt[3]{2}}{2}, \quad \sigma_3(\sqrt[3]{2}) = \frac{\sqrt[3]{2}\sqrt{3}}{2}.$$

Definicija 5.4.6

Neka je $\mathfrak{a}$ ideal u $\mathcal{O}_K$. Definiramo *diskriminatu* $\Delta(\mathfrak{a})$ od $\mathfrak{a}$ kao $\Delta(\alpha_1, \ldots, \alpha_n)$, gdje je $\alpha_1, \ldots, \alpha_n$ baza od $\mathfrak{a}$ kao $\mathbb{Z}$-modula.

Sada kada možemo razmišljati o K kao n-dimenzionalnom euklidskom prostoru, možemo tumačiti prsten cijelih brojeva od K i njegove ideale kao rešetke u prostoru Minkowskog K_R, koristeći sljedeću lemu.

Lema 5.4.7

Neka je K konačno proširenje $\mathbb{Q}$, a $\mathfrak{a}$ nenul ideal prstena $\mathcal{O}_K$. Tada je $\Gamma = j(\mathfrak{a})$ potpuna rešetka u $K_{\mathbb{R}}$ kojem fundamentalna domena ima volumen

$$\mathrm{vol}(\Gamma) = \sqrt{|\Delta_K|}[O_K : \mathfrak{a}].$$

Dokaz. Neka je $\alpha_1, \ldots, \alpha_n$ $\mathbb{Z}$-baza od $\mathfrak{a}$. Tada je $\Gamma = \mathbb{Z}j(\alpha_1) + \cdots + \mathbb{Z}j(\alpha_n)$. Neka su $\tau_1, \tau_2, \ldots, \tau_n$ ulaganja od K u $\mathbb{C}$. Definiramo matricu

$$A = \begin{pmatrix} \tau_1(\alpha_1) & \tau_2(\alpha_1) & \cdots & \tau_n(\alpha_1) \\ \tau_1(\alpha_2) & \tau_2(\alpha_2) & \cdots & \cdots \\ \vdots & \vdots & \ddots & \vdots \\ \tau_1(\alpha_n) & \cdots & \cdots & \tau_n(\alpha_n) \end{pmatrix}.$$

Ako su $\mathfrak{b} \subseteq \mathfrak{b}'$ dva nenul konačno generirana $\mathcal{O}_K$-podmodula od K, tada je $[\mathfrak{b}' : \mathfrak{b}]$ konačan i $\Delta(\mathfrak{b}) = [\mathfrak{b}' : \mathfrak{b}]^2\Delta(\mathfrak{b}')$ (prema ranije dokazanom).

Stoga imamo

$$\Delta(\mathfrak{a}) = \Delta(\alpha_1, \ldots, \alpha_n) = (\det A)^2 = [\mathcal{O}_K : \mathfrak{a}]^2\Delta(\mathcal{O}_K) = [\mathcal{O}_K : \mathfrak{a}]^2\Delta_K.$$

Sada imamo

$$\mathrm{vol}(\Gamma) = |\det A| = \sqrt{|\Delta_K|}[\mathcal{O}_K : \mathfrak{a}],$$

što je i trebalo dokazati. □

Teorem 5.4.8

Neka je $K/\mathbb{Q}$ konačno proširenje, i neka je $\mathfrak{a} \neq 0$ ideal od $\mathcal{O}_K$. Neka je $c_\tau > 0$, za τ ulaganje K u $\mathbb{C}$, realan broj takav da je $c_\tau = c_{\overline{\tau}}$ i

$$\prod_\tau c_\tau > A[\mathcal{O}_K : \mathfrak{a}],$$

gdje je $A = (2/\pi)^s\sqrt{|\Delta_K|}$. Tada postoji nenul $\alpha \in \mathfrak{a}$ takav da

$$|\tau(\alpha)| < c_\tau \text{ za sve } \tau \in \mathrm{Hom}(K, \mathbb{C}).$$

Dokaz. Neka je

$$X = \{(z_\tau) \in K_{\mathbb{R}} \mid |z_\tau| < c_\tau\}.$$

Ovaj skup je centralno simetričan, budući da je $|z_\tau| = |-z_\tau|$, i konveksan je jer ako je $|z_\tau|, |w_\tau| < c_\tau$, tada je

$$\left|\frac{1}{t}z_\tau + \frac{1}{1-t}w_\tau\right| \leq \frac{1}{t}|z_\tau| + \frac{1}{1-t}|w_\tau| \leq \max\{|z_\tau|, |w_\tau|\} < c_\tau.$$

Izračunavamo volumen koristeći preslikavanje (5.2). Ispada da je 2^s puta volumen slike

$$f(X) = \left\{ (x_\tau) \in \prod_\tau \mathbb{R} \mid |x_\rho| < c_\rho, x_\sigma^2 + x_{\overline{\sigma}}^2 < c_\sigma^2 \right\}.$$

Ovo daje

$$\mathrm{vol}(X) = 2^s \mathrm{vol}(f(X)) = 2^s \prod_\rho (2c_\rho) \prod_\sigma (\pi c_\sigma^2) = 2^{r+s}\pi^s \prod_\tau c_\tau.$$

Sada imamo

$$\mathrm{vol}(X) > 2^{r+s}\pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|}[\mathcal{O}_K : \mathfrak{a}] = 2^n \mathrm{vol}(j(\mathfrak{a})).$$

Nejednakost slijedi iz pretpostavke, a jednakost iz Leme 5.4.7.

Dakle, prema Minkowskom teoremu o točki rešetke, postoji točka rešetke $j(\alpha) \in X$, $\alpha \neq 0$, $\alpha \in \mathfrak{a}$. To jest, $|\tau(\alpha)| < c_\tau$, što je i trebalo dokazati. □

Lema 5.4.9

U svakom idealu $\mathfrak{a} \neq 0$ od $\mathcal{O}_K$ postoji $\alpha \in \mathfrak{a}$, $\alpha \neq 0$, takav da

$$\left|N_{K/\mathbb{Q}}(\alpha)\right| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|} N(\mathfrak{a}).$$

Dokaz. Za svaki $\varepsilon > 0$, možemo odabrati pozitivne realne brojeve c_τ za $\tau \in \mathrm{Hom}(K, \mathbb{C})$ takve da $c_\tau = c_{\overline{\tau}}$ i

$$\prod_\tau c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|} N(\mathfrak{a}) + \varepsilon.$$

Tada prema Teoremu 5.4.8 nalazimo element $\alpha \in \mathfrak{a}$, $\alpha \neq 0$, koji zadovoljava $|\tau(\alpha)| < c_\tau$. Stoga

$$\left|N_{K/\mathbb{Q}}(\alpha)\right| = \prod_\tau |\tau(\alpha)| < \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|} N(\mathfrak{a}) + \varepsilon.$$

Budući da je $|N_{K/\mathbb{Q}}(\alpha)|$ pozitivan cijeli broj, te tvrdnja vrijedi za svaki $\epsilon > 0$ očito slijedi da postoji $\alpha \in \mathfrak{a}$, $\alpha \neq 0$, takav da

$$\left|N_{K/\mathbb{Q}}(\alpha)\right| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} N(\mathfrak{a}).$$

□

Sada smo spremni dokazati konačnost broja klasa.

Teorem 5.4.10

Neka je $K/\mathbb{Q}$ polje algebarskih brojeva. Tada je *broj klasa* od K (ili od $\mathcal{O}_K$), $h_K := [I_K : P_K]$ konačan.

Dokaz. Kao što smo komentirali i ranije, postoji samo konačan broj ideala od $\mathcal{O}_K$ s ograničenom apsolutnom normom $N(\mathfrak{a}) \leq M$.

Stoga će biti dovoljno pokazati da svaka klasa ideala $[\mathfrak{a}]$ iz C_K sadrži ideal $\mathfrak{a}_1$ od $\mathcal{O}_K$ takav da

$$N(\mathfrak{a}_1) \leq M = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|}.$$

Da bismo to pokazali, biramo proizvoljnog predstavnika klase $\mathfrak{a}$ i nenul element $\gamma \in \mathcal{O}_K$ takav da je $\mathfrak{b} = \gamma\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. Prema Lemi 5.4.9, možemo naći nenul element $\alpha \in \mathfrak{b}$ takav da

$$N\left(\alpha\mathfrak{b}^{-1}\right) = N\left((\alpha)\mathfrak{b}^{-1}\right) = \left|N_{K/\mathbb{Q}}(\alpha)\right| N(\mathfrak{b})^{-1} \leq M.$$

Primijetimo da $N(\mathfrak{b})|N(\alpha)$, pa slijedi da je $a\mathfrak{b}^{-1}$ cijeli ideal, pošto mu je norma cjeloborjna. Dakle, ideal $\alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a} \in [\mathfrak{a}]$ ima željeno svojstvo. □

Važna činjenica iz dokaza koju ćemo zapisati kao posebnu propoziciju je sljedeća:

Propozicija 5.4.11

Svaka klasa iz C_K sadrži ideal $\mathfrak{a}_1$ od $\mathcal{O}_K$ takav da

$$N(\mathfrak{a}_1) \leq M = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|}.$$

Najbolja ograda koja se može dobiti za općeniti n je sljedeća (i koju mi nećemo dokazivati):

Teorem 5.4.12: Minkowski

Neka je $\mu_K = \sqrt{|\Delta_K|}\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}$, gdje je $[K : \mathbb{Q}] = n$. Tada postoji integralni ideal I u svakoj klasi u C_K takav da je $\mathbb{N}(I) \leq \mu_K$.

Primjer 5.4.13

Neka je $K = \mathbb{Q}(\sqrt{-5})$. Budući da je $-5 \equiv 3 \pmod 4$, znamo da je $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ i $\delta_K = -20$. Prema Propoziciji 5.4.11 znamo da svaka klasa ideala sadrži ideal $\mathfrak{a}$ takav da

$$N(\mathfrak{a}) \leq \left(\frac{2}{\pi}\right)\sqrt{20} \approx 2.85.$$

Stoga moramo naći sve ideale s apsolutnom normom 2. Pretpostavimo da je $\mathfrak{a}$ ideal takav da je $N(\mathfrak{a}) = 2$. Ranije smo komentirali da se prosti ideal norme p^k mora naći u faktorizaciji od $p\mathcal{O}_K$.
Također smo vidjeli da je $2\mathcal{O}_K = \mathfrak{b}^2$, gdje je $\mathfrak{b} = (\sqrt{-5} + 1, 2)$. Pokazat ćemo da $\mathfrak{b}$ nije glavni, i stoga da nije u istoj klasi ideala kao (2). Pretpostavimo da je $\mathfrak{b}$ glavni, tako da je $\mathfrak{b} = (b)$ za neki $b \in \mathbb{Z}[\sqrt{-5}]$. Tada

$$N_{K/\mathbb{Q}}(b) \mid N_{K/\mathbb{Q}}(2) = 4$$

i

$$N_{K/\mathbb{Q}}(b) \mid N_{K/\mathbb{Q}}(\sqrt{-5} + 1) = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$$

Stoga je $N_{K/\mathbb{Q}}(b) = 2$. Pa ako je $b = x + y\sqrt{-5}$, onda

$$N_{K/\mathbb{Q}}(b) = x^2 + 5y^2 = 2.$$

Nema cjelobrojnih rješenja za x i y, pa $\mathfrak{b}$ ne može biti glavni.
Pokazali smo da sve klase ideale imaju predstavnika norme ≤ 2, te smo vidjeli da postoji jedinstveni ideal norme $\mathfrak{b}$ koji nije glavni. Zaključujemo $h_K = 2$, te $C_K = \{[(1)], [\mathfrak{b}]\}$

Primjer 5.4.14

Neka je $K = \mathbb{Q}(\zeta_5)$. Pokazali smo da je $\Delta_K = 5^3$. Imamo

$$\mu_K = \left(\frac{4}{\pi}\right)^2 \sqrt{125}\frac{4!}{4^4} \sim 1.669921.$$

Zaključujemo da svaka klasa ima u sebi ideal (1), dakle $h_K = 1$. Dakle K je domena jedinstvene faktorizacije.

Primjer 5.4.15

Neka je $K = \mathbb{Q}(\sqrt{-7})$. Imamo

$$\mu_K = \left(\frac{2}{\pi}\right)^1 \sqrt{7} \simeq 1.861,$$

pa zaključujemo kao i prije da je $h_K = 1$ i da je K domena jedinstvene faktorizacije.

Primjer 5.4.16

Neka je $K = \mathbb{Q}(\zeta_7)$. Imamo

$$\mu_K = \left(\frac{4}{\pi}\right)^3 \sqrt{7^5}\frac{6!}{6^6} \sim 4.129.$$

Dakle, ako postoji klasa ideala koja nije glavna, onda se ona mora naći u faktorizaciji od ideala $2O_K$ i $3O_K$.
Element 2 je reda 3 u $(\mathbb{Z}/7\mathbb{Z})^\times$, pa slijedi da je

$$2O_K = \mathfrak{p}_1\mathfrak{p}_2,$$

gdje je $N(\mathfrak{p}_i) = 8$.
Element 3 je reda 6 pa je $3O_K$ prost i norme 3^6. Zaključujemo da je $h_K = 1$ i K je domena jedinstvene faktorizacije.

Primjer 5.4.17

Neka je $K = \mathbb{Q}(\sqrt{-14})$. Imamo

$$\mu_K = \frac{4\sqrt{56}}{\pi} \sim 4.76.$$

Dakle, treba samo promotriti faktorizaciju od 2 i 3. Imamo

$$2\mathcal{O}_K = (2, \sqrt{-14})^2,$$

$$3\mathcal{O}_K = (3, 1+\sqrt{-14})(3, 2+\sqrt{-14}).$$

Dakle svakako imamo $h_K \leq 4$.
Prvo želimo vidjeti je li $\mathfrak{p}_2 = (2, \sqrt{-14})$ glavni. Dakle pitamo se je li postoji $a \in \mathcal{O}_K$ takav da $a|2$ $a\sqrt{-14}$. Dakle

$$N(a)|(N(2), N(\sqrt{-14})) = (4, 14) = 2.$$

Neka je $a = x + y\sqrt{-14}$. tada bi moralo biti $x^2 + 14y^2 = 2$, što je očito nemoguće. Dakle $\mathfrak{p}_2$ nije glavni.
Neka je $\mathfrak{a} = (3, 1+\sqrt{-14})$. Analogno kao i gore, pokažemo da $\mathfrak{a}^2$ nije glavni. Dakle $[\mathfrak{a}]$ je reda ≥ 4. Zaključujemo da je

$$h_K = 4, \quad C_K \simeq \mathbb{Z}/4\mathbb{Z}, \quad C_K = \{[(1)], [\mathfrak{p}_2], [\mathfrak{a}], [\mathfrak{a}^3]\}.$$

Primjer 5.4.18

Neka je $K = \mathbb{Q}(\sqrt{-163})$. Dobijemo $\mu_K \sim 8.127$. Računamo

$$\left(\frac{-163}{3}\right) = \left(\frac{-163}{5}\right) = \left(\frac{-163}{7}\right) = -1.$$

Dakle, $p\mathcal{O}_K$ su inertni za $p = 3, 5, 7$. Dakle ne postoje ideali norme $3, 5, 7$ u $\mathcal{O}_K$. Ostaje odrediti faktorizaciju od $2\mathcal{O}_K$.
Sjetimo se da je $\mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$, te je minimalni polinom od $\frac{1+\sqrt{-163}}{2}$ jednak x^2-x+41. Taj polinom je ireducibilan modulo 2, pa slijedi da je 2 inertan u K. Dakle $2\mathcal{O}_K$ je jedini pravi ideal norme $< \mu_K$, te je on očito glavni. Slijedi da je $h_K = 1$.

Recimo malo i o povijesti proučavanja broja klasa imaginarnih kvadratnih polja. Gauss je izrekao slutnju (bila je zato poznata kao Gaussova slutnja) da $h_{\mathbb{Q}(\sqrt{-d})} \to \infty$ kako $d \to \infty$. To je dokazao Heilbronn 1934. godine.

Postoji samo 9 imaginarnih kvadratnih polja K s $h_K = 1$. To su $\mathbb{Q}(\sqrt{d})$ za

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Ovo je dokazao Stark 1967. godine, koristeći prethodne rezultate Bakera i Heeg-

nera. Važno otvoreno pitanje je postoji li beskonačno mnogo realnih kvadratnih polja $K = \mathbb{Q}(\sqrt{d})$, $d > 0$ s $h_K = 1$. Slutnja je da postoji.

Nastavimo sada promatrati $K = \mathbb{Q}(\sqrt{-163})$.

Lema 5.4.19

Neka je $p \leq 37$ prost broj. Tada je p inertan u $K = \mathbb{Q}(\sqrt{-163})$.

Dokaz. Pretpostavimo da nije, da se neki pO_K cijepa za $p \leq 37$. Neka je $\alpha = \frac{1+\sqrt{-163}}{2}$. Pošto je $h_K = 1$, slijedi da je

$$p\mathcal{O}_K = (a)(b), \qquad \text{za neke } a, b, \in \mathcal{O}_K$$

Tada je $a = x + y\alpha,\ x, y \in \mathbb{Z}$ takav da je $N(a) = p$. Međutim, imamo

$$N(a) = N\left(\left(x + \frac{y}{2}\right) + \left(x + \frac{y\sqrt{-163}}{2}\right)\right) = \left(x + \frac{y}{2}\right)^2 + \frac{163}{4}y^2.$$

Pošto mora biti $a \notin \mathbb{Z}$, mora biti $y \neq 0$, pa slijedi $N(a) > \frac{163}{4}$, što je kontradikcija. □

Ova činjenica ima jednu vrlo zanimljivu posljedicu.

Propozicija 5.4.20

Neka je $f(x) = x^2 - x + 41$. Tada je $f(x_0)$ prost za sve prirodne brojeve $x_0 \in x_0 \leq 40$.

Naravno, ova propozicija se lako računski dokaže, ali mi ćemo dati ljepši dokaz.

Dokaz. Neka je x_0 kao u pretpostavkama propoziciji. Neka je p neki prosti djelitelj od $x_0^2 - x_0 + 41$. Tada je

$$x_0^2 - x_0 + 41 \equiv 0 \pmod{p},$$

$$\implies (2x_0 - 1)^2 \equiv -163 \pmod{p}$$

$$\left(\frac{-163}{p}\right) = 1$$

za $p \neq 163$. Kada bi to bilo istina za $p \leq 37$, tada bi se taj p cijepao u $\mathbb{Q}(\sqrt{-163})$, a vidjeli smo da je to nemoguće.

Ako uvrstimo $f(40) = 1601 < 41^2$, pa slijedi da kada $f(x_0)$ ne bi bio prost za neki $x_0 \leq 40$, tada bi imao prostog djelitelja < 41, što smo vidjeli da je nemoguće. □

Primjer 5.4.21

Neka je $K = \mathbb{Q}(\sqrt{82})$. Pokažimo da je grupa klasa cikličkа grupa reda 4.

Rješenje: Ovdje je $n = 2$, $r_2 = 0$, $\text{disc}(K) = 4 \cdot 82$, pa je Minkowskijeva ograda ≈ 9.055. Pogledajmo proste ideale koji dijele 2, 3, 5 i 7.

Sljedeća tablica opisuje kako se (p) faktorizira iz načina na koji se $T^2 - 82$ faktorizira modulo p.

p	$T^2 - 82 \bmod p$	(p)
2	T^2	$\mathfrak{p}_2^2$
3	$(T-1)(T+1)$	$\mathfrak{p}_3\mathfrak{p}_3'$
5	ireducibilno	prost
7	ireducibilno	prost

Dakle, grupa klasa od $\mathbb{Q}(\sqrt{82})$ je generirana s $[\mathfrak{p}_2]$ i $[\mathfrak{p}_3]$, gdje su $\mathfrak{p}_2^2 = (2) \sim (1)$ i $\mathfrak{p}_3' \sim \mathfrak{p}_3^{-1}$.

Budući da je $N_{K/\mathbb{Q}}(10 + \sqrt{82}) = 18 = 2 \cdot 3^2$, i $10 + \sqrt{82}$ nije djeljivo s 3, $(10 + \sqrt{82})$ je djeljivo samo s jednim od $\mathfrak{p}_3$ i $\mathfrak{p}_3'$. Neka je $\mathfrak{p}_3$ taj prosti ideal, tako da je $(10 + \sqrt{82}) = \mathfrak{p}_2\mathfrak{p}_3^2$. Stoga $\mathfrak{p}_2 \sim \mathfrak{p}_3^{-2}$, pa je grupa klasa od K generirana s $[\mathfrak{p}_3]$ i imamo formule

$$[\mathfrak{p}_2]^2 = 1, \quad [\mathfrak{p}_3]^2 = [\mathfrak{p}_2].$$

Dakle, $[\mathfrak{p}_3]$ ima red koji dijeli 4.

Pokazat ćemo da $\mathfrak{p}_2$ nije glavni ideal, tako da $[\mathfrak{p}_3]$ ima red 4, i stoga K ima grupu klasa $\langle[\mathfrak{p}_3]\rangle \cong \mathbb{Z}/4\mathbb{Z}$.

Ako je $\mathfrak{p}_2 = (a + b\sqrt{82})$, onda je $a^2 - 82b^2 = \pm 2$, tako da je 2 ili $-2 \equiv \square \bmod 41$. Ovo nije kontradikcija, jer je $2 \equiv 17^2 \bmod 41$. Potrebna nam je drugačija ideja.

Ideja je koristiti poznatu činjenicu da je $\mathfrak{p}_2^2$ glavni ideal. Ako je $\mathfrak{p}_2 = (a + b\sqrt{82})$, onda je $(2) = \mathfrak{p}_2^2 = ((a + b\sqrt{82})^2)$, tako da je

$$2 = (a + b\sqrt{82})^2 u,$$

gdje je u jedinica.

Uzimajući norme ovdje, $N(u)$ mora biti pozitivna, pa je $N(u) = 1$. Grupa jedinica od $\mathbb{Z}[\sqrt{82}]$ je $\pm(9 + \sqrt{82})^{\mathbb{Z}}$, a $9 + \sqrt{82}$ ima normu -1. Stoga su pozitivne jedinice norme 1 integralne potencije od $(9 + \sqrt{82})^2$, koji su svi kvadrati. Kvadrat jedinice može se apsorbirati u izraz $(a + b\sqrt{82})^2$, pa moramo moći riješiti $2 = (a + b\sqrt{82})^2$ u cijelim brojevima a i b. Ovo je očito nemoguće: implicira da je $\sqrt{2}$ u $\mathbb{Z}[\sqrt{82}]$, što je netočno. Dakle, $\mathfrak{p}_2$ nije glavni ideal.

Primjer 5.4.22

Neka je $K = \mathbb{Q}(\sqrt{-30})$. Pokažimo da je grupa klasa produkt dvije cikličke grupe reda 2.

Rješenje: Ovdje je $n = 2$, $r_2 = 1$ i $\text{disc}(K) = -120$. Minkowskijeva ograda je ≈ 6.97, pa je grupa klasa generirana prostim idealima koji dijele 2, 3 i 5.

Sljedeća tablica prikazuje kako se ti prosti brojevi faktoriziraju u proste ideale.

p	$T^2 + 30 \bmod p$	(p)
2	T^2	$\mathfrak{p}_2^2$
3	T^2	$\mathfrak{p}_3^2$
5	T^2	$\mathfrak{p}_5^2$

Za $a, b \in \mathbb{Z}$, $N_{K/\mathbb{Q}}(a+b\sqrt{-30}) = a^2+30b^2$ nikada nije 2, 3 ili 5. Stoga $\mathfrak{p}_2$, $\mathfrak{p}_3$ i $\mathfrak{p}_5$ nisu glavni, pa njihove klase ideala imaju red 2 u grupi klasa od K. Štoviše, budući da je $N_{K/\mathbb{Q}}(\sqrt{-30}) = 30 = 2 \cdot 3 \cdot 5$, slijedi da je $(\sqrt{-30}) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$. Stoga je $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5 \sim 1$ u grupi klasa, pa $[\mathfrak{p}_2]$ i $[\mathfrak{p}_3]$ generiraju grupu klasa.

Relacija $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5 \sim 1$ u grupi klasa može se zapisati kao

$$[\mathfrak{p}_2][\mathfrak{p}_3] = [\mathfrak{p}_5]^{-1} = [\mathfrak{p}_5].$$

Budući da $\mathfrak{p}_5$ nije glavni ideal i $[\mathfrak{p}_2]$ i $[\mathfrak{p}_3]$ imaju red 2 u grupi klasa, $[\mathfrak{p}_2] \neq [\mathfrak{p}_3]$. Stoga je grupa klasa od K $\langle [\mathfrak{p}_2], [\mathfrak{p}_3] \rangle \cong \langle [\mathfrak{p}_2] \rangle \times \langle [\mathfrak{p}_3] \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Primjer 5.4.23

Neka je $K = \mathbb{Q}(\sqrt[3]{2})$. Pokazat ćemo da je grupa klasa ideala trivijalna.

Rješenje: Budući da je $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$ i $r_2 = 1$, Minkowskijeva ograda je

$$(6/27)(4/\pi)\sqrt{108} \approx 2.94,$$

stoga trebamo faktorizirati (2) u proste ideale u $\mathcal{O}_K$. Imamo $(2) = (\sqrt[3]{2})^3$, što znači da je $(\sqrt[3]{2})$ prost ideal norme 2, tako da je jedini prosti ideal norme manje od 2.94 glavni, pa je $h(K) = 1$.

Primjer 5.4.24

Neka je $K = \mathbb{Q}(\sqrt[3]{3})$. Pokazat ćemo da je grupa klasa ideala trivijalna.

Rješenje: Budući da je $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{3}]$ i $r_2 = 1$, Minkowskijeva ograda je

$$(6/27)(4/\pi)\sqrt{243} \approx 4.41,$$

stoga trebamo faktorizirati ideale (2) i (3) u proste ideale u $\mathcal{O}_K$.

p	$T^3 - 3 \bmod p$	(p)
2	$(T+1)(T^2+T+1)$	$\mathfrak{p}_2\mathfrak{p}_2$
3	T^3	$\mathfrak{p}_3^3$

Prema tablici, postoji jedan prosti ideal norme 2 i jedan norme 3. To su ideali $(-1+\sqrt[3]{3})$ i $(\sqrt[3]{3})$ budući da $-1+\sqrt[3]{3}$ ima minimalni polinom $(T+1)^3-3 = T^3+3T^2+3T-2$ s konstantnim članom -2, a $\sqrt[3]{3}$ ima minimalni polinom T^3-3 s konstantnim članom -3 (sjetimo se, konstantni član minimalnog polinoma jednak je normi). Kako je $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ gdje je $\mathfrak{p}_2$ glavni ideal, $\mathfrak{p}_2'$ je također glavni. (Eksplicitno, $\mathfrak{p}_2' = (1+\sqrt[3]{3}+\sqrt[3]{9})$.) Stoga su svi prosti ideali norme manje od 4.41 glavni, pa je $h(K)=1$.

Pokažimo sada kako možemo iskoristiti grupe klasa ideal za rješavanje Diofantskih jednadžbi:

Primjer 5.4.25

Nađimo sva rješenja od

$$x^2+19=y^3, \quad x,y\in\mathbb{Z}.$$

Rješenje: Zapišimo

$$(x+\sqrt{-19})(x-\sqrt{-19})=y^3$$

Neka je $K=\mathbb{Q}(\sqrt{-19})$, tada je $\mathcal{O}_K=\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ i $|\Delta_K|=19$. Računamo Minkowskijevu ogradu:

$$\mu_K=\left(\frac{4}{\pi}\right)\cdot\frac{2!}{2^2}\cdot\sqrt{19}=\frac{2}{\pi}\cdot\sqrt{19}<5$$

Polinom $f=x^2+x+5$ je minimalni polinom od $\frac{1+\sqrt{-19}}{2}$.

$$(x^2+x+1) \quad \text{je ireducibilan modulo } 2 \Rightarrow 2\mathcal{O}_K \text{ prost},$$

$$(x^2+x+2) \quad \text{je ireducibilan modulo } 3 \Rightarrow 3\mathcal{O}_K \text{ prost}.$$

Dakle $h_K=1$.

Dokažimo da su elementi $(x+\sqrt{-19})$ i $(x-\sqrt{-19})$ relativno prosti. Pretpostavimo da $\pi \mid x+\sqrt{-19}$ i $\pi \mid x-\sqrt{-19}$.

$$\pi \mid 2x, \quad \pi \mid 2\sqrt{-19}$$

Ako je x neparan (a time y paran) $\Rightarrow x^2\equiv 1 \pmod 8$

$$\Rightarrow x^2+19\equiv 1+3\equiv 4\equiv 4 \pmod 8.$$

S druge strane $y^3\equiv 0 \pmod 8$, pa smo došli do kontradikcije.

Dakle x je paran, $x=2t$, $t\in\mathbb{Z}$. Kada bi $\sqrt{-19}\mid x$ u $\mathcal{O}_K \Rightarrow 19\mid x$.

$$x^2+19\equiv 19 \pmod{19^2} \Rightarrow y^3\equiv 19 \pmod{19^2},$$

što je kontradikcija. Zaključujemo da $\pi \nmid \sqrt{-19}$.

Pretpostavimo da $\pi|2$. Pošto je $2\mathcal{O}_K$ prost, slijedi da je $\pi = 2$. Međutim, pošto $2 \nmid \sqrt{-19}$, te $2|x$, očito slijedi da $2 \nmid (x \pm \sqrt{-19})$.

Dakle

$$(x + \sqrt{-19}, x - \sqrt{-19}) = 1 \Rightarrow (x + \sqrt{-19}) = \mathfrak{a}^3$$

$$\Rightarrow x + \sqrt{-19} = u\left(c + d\left(\frac{1 + \sqrt{-19}}{2}\right)\right)^3, \quad u \in \mathcal{O}_K^\times, \quad a, b \in \mathbb{Z}$$

Zapišimo zbog jednostavnosti

$$\left(c + d\left(\frac{1 + \sqrt{-19}}{2}\right)\right) = \left(\frac{a + b\sqrt{-19}}{2}\right),$$

gdje a, b moraju biti iste parnosti. Imamo

$$\left(\frac{a + b\sqrt{-19}}{2}\right)^3 = \frac{1}{8}(a^3 + 3a^2b\sqrt{-19} - 57ab^2 - 19b^3\sqrt{-19}).$$

$$\Rightarrow a^3 - 57ab^2 = 8x, \quad 3a^2b - 19b^3 = 8.$$

Primijetimo da vrijedi

$$b\left(3a^2 - 19b^2\right) = 8 \Rightarrow b = \pm 1, 2, 4, 8,$$

te da je $3a^2 - 19b^2$ djeljivo s 4, pošto su a i b iste parnosti, dakle $b = \pm 1, \pm 2$ su jedine mogućnosti Za $b = \pm 1$ dobijemo

$$3a^2 - 19 = \pm 8,$$

Ovo nam daje rješenje $a = \pm 3, b = 1$. Uvrštavanjem u drugu jednadžbu dobivamo

$$a^3 - 57ab^2 = \pm 27 \mp 171 = \pm 144 = 8x.$$

Dakle, dobivamo rješenje $x = \pm 18$. Računamo

$$18^2 + 19 = 324 + 19 = 343 = 7^3,$$

pa je $x = \pm 18$, $y = 7$ zaista rješenje.

Za $b = \pm 2$ dobijemo

$$3a^2 - 19 \cdot 16 = \pm 4,$$

Ovo nam daje rješenje $a = \pm 10, b = -2$. Uvrštavanjem u drugu jednadžbu dobivamo

$$a^3 - 57ab^2 = \pm 1000 \mp 2280 = \pm 1280 = 8x.$$

Dakle dobivamo rješenje $x = \pm 160$. Međutim

$$160^2 + 19 = 25619$$

nije kub, tako da tu ne dobivamo rješenja.

Primjer 5.4.26

Nađimo sva rješenja u $\mathbb{Z}$ jednadžbe $x^3 = y^2 + 5$.

Rješenje:

Započnimo s provjerom parnosti. Ako je x paran, tada je $y^2 \equiv -5 \equiv 3 \pmod 8$, ali 3 modulo 8 nije kvadrat. Stoga je x neparan, pa je y paran.

Primijetimo da su x, y relativno prosti, jer bi inače njihov najveći zajednički djelitelj morao dijeliti $x^3 - y^2 = 5$. Kad bi najveći zajednički djelitelj bio 5, dolazimo do kontradikcije modulo 125, tj. dobili bismo $-25t^2 \equiv 5 \pmod{125}$, što je očito nemoguće.

Zapišimo jednadžbu kao

$$x^3 = y^2 + 5 = (y + \sqrt{-5})(y - \sqrt{-5}). \tag{5.4}$$

Neka je $K = \mathbb{Q}(\sqrt{-5})$. Kada bi bilo da je $h_K = 1$, mogli bismo provjeriti da su $y + \sqrt{-5}$ i $y - \sqrt{-5}$ relativno prosti i njihov produkt je kub, pa su oni oboje kubovi (jedinice u $\mathbb{Z}[\sqrt{-5}]$ su ± 1, koje su oboje kubovi). Međutim, imamo $h_K = 2$, tako da ne možemo to napraviti. Međutim, možemo promotriti faktorizaciju ideala

$$(x)^3 = (y + \sqrt{-5})(y - \sqrt{-5}).$$

Dokažimo prvo da su ideali $(y + \sqrt{-5})$ i $(y - \sqrt{-5})$ relativno prosti. Pretpostavimo da $\wp \subseteq \mathcal{O}_K$ dijeli $(y + \sqrt{-5})$ i $(y - \sqrt{-5})$. To znači da su

$$y + \sqrt{-5} \in \mathfrak{p}, \quad y - \sqrt{-5} \in \mathfrak{p}.$$

Slijedi da su $2y$ i $y^2 + 5 = x^3$ također u $\mathfrak{p}$. Neka je p prost broj takav da $p\mathbb{Z}$ leži ispod $\mathfrak{p}$. Tada su $2y, x^3 \in p\mathbb{Z}$, što smo vidjeli da je nemoguće,

Zaključujemo da je

$$(y + \sqrt{-5}) = I^3$$

za neki ideal I u $\mathcal{O}_K$. Primijetimo da je $[I^3] = [I]$, pošto je $h_K = 2$ (pa je $[I^2] = [\mathcal{O}_K]$ za svaki ideal I). Pošto je I^3 glavni, slijedi da je i I glavni.

Dakle

$$y + \sqrt{-5} = (m + n\sqrt{-5})^3 \tag{5.5}$$

za neke cijele brojeve m i n, pa je

$$y = m^3 - 15mn^2 = m(m^2 - 15n^2), \quad 1 = 3m^2n - 5n^3 = n(3m^2 - 5n^2). \tag{5.6}$$

Iz druge jednadžbe, $n = \pm 1$. Ako je $n = 1$, tada $1 = 3m^2 - 5$, pa $3m^2 = 6$, što nema cjelobrojnih rješenja. Ako je $n = -1$, tada $1 = -(3m^2 - 5)$, pa $3m^2 = 4$, što također nema cjelobrojnih rješenja. Došli smo do zaključka da $y^2 = x^3 - 5$ nema cjelobrojnih rješenja.

Napomenimo ovdje bitnu činjenicu koju smo koristili: ako imamo izraz $X^m = Y \cdot Z$ u $\mathcal{O}_K$, gdje su ideali (Y) i (Z) relativno prosti, te je $(h_K, m) = 1$, tada su Y i Z zapravo m-te potencije u $\mathcal{O}_K$.

Poglavlje 6

Fermatov posljednji teorem za regularne proste brojeve

6.1 Teorem

Neka je p neparan prost broj i $K = \mathbb{Q}(\zeta_p)$. Pisat ćemo ζ umjesto ζ_p za ovo poglavlje.

Početkom 19. stoljeća primijećeno je da je ovo polje usko povezano s Fermatovim posljednjim teoremom. Specifično, ako postoji rješenje jednadžbe

$$x^p + y^p = z^p \tag{6.1}$$

gdje su $x, y, z \in \mathbb{Z}$, može se koristiti faktorizacija

$$x^p + y^p = (x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{p-1}y)$$

kako bi se zaključilo da je

$$(x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{p-1}y) = z^p.$$

Odavde se pokazuje (uz odgovarajuće uvjete za x, y, z) da su faktori s lijeve strane međusobno relativno prosti. Ako je $\mathcal{O}_K$ DJF, slijedi da je svaki $x + \zeta^i y$ p-ta potencija u $\mathcal{O}_K$, budući da im je umnožak takav. Odavde se može lako dobiti kontradikcija koja pokazuje da Fermatova jednadžba nema netrivijalno rješenje u ovom slučaju.

Ovaj dokaz je prvi uspješno proveo Kummer sredinom 19. stoljeća. Shvatio je da njegov dokaz vrijedi ne samo za one p kod kojih je $\mathbb{Z}[\zeta_p]$ DJF, već i za puno veću klasu prostih brojeva. Ključno svojstvo se pokazalo da p ne dijeli broj klasa $h_{\mathbb{Q}(\zeta_p)}$. Kummer je takve proste brojeve nazvao regularni; ako prost broj nije regularan, onda se kaže da je iregularan.

Dokazati ćemo Kummer-ov teorem s dodatnom pojednostavljujućom pretpostavkom da p ne dijeli xyz; ovo se klasično naziva Slučaj I. Slučaj I sadrži većinu zanimljivog sadržaja općeg slučaja i ima prednost da je tehnički puno jednostavniji.

Teorem 6.1.1: (Kummer)

Neka je $p \geq 5$ regularan prost broj. Tada jednadžba

$$x^p + y^p = z^p$$

nema rješenja s $x, y, z \in \mathbb{Z}$ i p koji ne dijeli xyz.

Dokaz. Za početak, lako vidimo da možemo bez smanjenja općenitosti pretpostaviti da x i y nisu kongruentni modulo p. Naime, prvo primijetimo da možemo pretpostaviti da su x, y, z u parovima relativno prosti, inače ih sve podijelimo s najvećim zajedničkim djeliteljem, pa dobijemo u parovima relativno prosta rješenja iste jednadžbe. Dakle, ne mogu i x i y biti kongruentni 0 modulo p. Pretpostavimo sada da je $0 \neq x \equiv y \pmod{p}$. Tada je $z \equiv 2x \pmod{p}$ i $z \not\equiv -x \pmod{p}$ (jer bi inače bilo $y \equiv 0 \pmod{p}$). Sada uz zamjenu varijabli $y' = -z$ i $z' = -y$ imamo jednadžbu

$$x^p + (y')^p = (z')^p$$

takvu da je $x \not\equiv y' \pmod{p}$.

Neka je sada $K = \mathbb{Q}(\zeta_p)$. Pretpostavimo da postoji rješenje $x^p + y^p = z^p$. Kao i prije, pišemo

$$(x+y)(x+\zeta y)\cdots(x+\zeta^{p-1}y) = z^p.$$

Najprije ćemo pokazati da glavni ideali $\left(x+\zeta^i y\right)$ i $\left(x+\zeta^j y\right)$ nemaju zajedničkih faktora za $i \neq j$. □

Lema 6.1.2

Pretpostavimo $x^p + y^p = z^p$ i p ne dijeli xyz. Tada su ideali $\left(x+\zeta^i y\right)$ međusobno relativno prosti za $i = 0, \ldots, p-1$.

Dokaz. Neka su i i j različiti cijeli brojevi između 0 i $p-1$ i pretpostavimo da postoji neki prost ideal $\mathfrak{q}$ od $\mathcal{O}_K$ koji dijeli i $\left(x+\zeta^i y\right)$ i $\left(x+\zeta^j y\right)$. Tada q također dijeli glavne ideale:

$$\left(\left(x+\zeta^i y\right) - \left(x+\zeta^j y\right)\right) = \left(\left(\zeta^i - \zeta^j\right) y\right)$$

i

$$\left(\left(x+\zeta^i y\right) - \zeta^{i-j}\left(x+\zeta^j y\right)\right) = \left(\left(1-\zeta^{i-j}\right) x\right).$$

Napomena: $\zeta^{i-j}\left(x+\zeta^j y\right)$ generira isti ideal kao $x+\zeta^j y$ budući da je ζ^{i-j} jedinica.

Sjetimo se da, budući da $i \neq j$, $\zeta^i - \zeta^j = \zeta^i\left(1-\zeta^{j-i}\right)$ i $1-\zeta^{i-j}$ su oboje asocirani (generiraju isti ideal) broju $1-\zeta$. Zaključujemo da $\mathfrak{q}$ dijeli ideale $(1-\zeta)(x)$ i $(1-\zeta)(y)$.

Međutim, budući da su x i y relativno prosti u $\mathbb{Z}$, slijedi da ne može postojati prost ideal u $\mathcal{O}_K$ koji ih oboje dijeli; stoga je jedina mogućnost $\mathfrak{q} = (1-\zeta)$.

Pretpostavimo dakle da $(1-\zeta)$ dijeli $\left(x+\zeta^i y\right)$ i $\left(x+\zeta^j y\right)$ kao ideale. Ovo odmah implicira da $1-\zeta$ dijeli $x+\zeta^i y$ i $x+\zeta^j y$ kao elemente od $\mathcal{O}_K$. Dakle:

$$x+\zeta^i y \equiv 0 \pmod{1-\zeta}.$$

Također vrijedi $\zeta^i \equiv 1 \pmod{1-\zeta}$, tako da zaključujemo:

$$x+y \equiv 0 \pmod{1-\zeta}.$$

Međutim, $x+y$ je racionalni cijeli broj, tako da ako je djeljiv s $1-\zeta$, onda mora biti djeljiv s p, pošto je $(1-\zeta)\cap\mathbb{Z} = p\mathbb{Z}$.

Sada imamo da p dijeli $x+y$ u $\mathbb{Z}$. Budući da

$$x^p + y^p \equiv x+y \pmod{p},$$

slijedi da p dijeli x^p+y^p, i stoga da p dijeli z. Ovo je kontradikcija našoj pretpostavci da p ne dijeli xyz (ili našoj pretpostavci da su x i y relativno prosti), pa zaključujemo da su $\left(x+\zeta^i\right)$ i $\left(x+\zeta^j y\right)$ relativno prosti ideali, kao što smo i tvrdili. □

Neka je $(z) = \mathfrak{q}_1^{n_1}\cdots\mathfrak{q}_r^{n_r}$ faktorizacija ideala (z) u $\mathcal{O}_K$. Jednakost ideala

$$(x+y)(x+\zeta y)\cdots(x+\zeta^{p-1}y) = (z)^p$$

pokazuje da $(x+y)(x+\zeta y)\cdots(x+\zeta^{p-1}y) = \mathfrak{q}_1^{pn_1}\cdots\mathfrak{q}_r^{pn_r}$.

Budući da su ideali $(x+\zeta^i y)$ u parovima relativno prosti, svaki $\mathfrak{q}_i$ mora se pojaviti u faktorizaciji točno jednog od njih. Kako se svaki $\mathfrak{q}_i$ pojavljuje s eksponentom djeljivim s p, slijedi da se svaki prosti faktor od $(x+\zeta^i y)$ pojavljuje s eksponentom djeljivim s p. Drukčije rečeno, svaki $(x+\zeta^i y)$ je p-ta potencija nekog ideala $\mathfrak{a}_i$ od $\mathcal{O}_K$: $(x+\zeta^i y) = \mathfrak{a}_i^p$.

Sada koristimo hipotezu da je p regularan kako bismo zaključili da su svi $\mathfrak{a}_i$ glavni. Konkretno, primijetimo da je $\mathfrak{a}_i^p$ trivijalan u C_K jer je to glavni ideal $(x+\zeta^i y)$. Budući da p ne dijeli red od C_K, to implicira da $\mathfrak{a}_i$ sam mora biti trivijalan u C_K (jer ako bi C_K imao element reda p, onda bi njegov red bio djeljiv s p), pa je stoga glavni. Dakle, možemo pisati $\mathfrak{a}_i = (\alpha_i)$ za neki $\alpha_i \in \mathcal{O}_K$, i imamo jednakost glavnih ideala

$$(x+\zeta^i y) = (\alpha_i)^p.$$

Ovo implicira da

$$x+\zeta^i y = u\alpha_i^p$$

za neki $u \in \mathcal{O}_K^*$. Sljedeći korak je dobiti malo više informacija o jedinici u.

Lema 6.1.3

Neka je K polje algebarskih brojeva s kompleksnim ulaganjima $\sigma_1, \ldots \sigma_n$. Neka je $\alpha \in K$ cijeli algebarski broj takav da $|\sigma_i(\alpha)| = 1$ za sve $i = 1, \ldots, n$. Tada je α korijen iz jedinice.

Dokaz. Definirajmo S kao skup svih $\alpha \in \mathcal{O}_K$ takvih da $\sigma_i(\alpha)$ ima apsolutnu vrijednost 1 za svaki i. Prvo primijetimo da je S zapravo grupa s obzirom na množenje; to je zato što, ako su $\alpha, \beta \in S$, tada je

$$|\sigma_i(\alpha\beta)| = |\sigma_i(\alpha)| \cdot |\sigma_i(\beta)| = 1,$$

pa je $\alpha\beta \in S$. Zatvorenost S s obzirom na inverz dokazuje se na isti način. Pokazat ćemo da je S konačan; to će implicirati da svi elementi u S imaju konačan red, i stoga su korijeni jedinice.

Neka je $f(x) \in \mathbb{Z}[x]$ karakteristični polinom bilo kojeg $\beta \in S$. ($f(x)$ ima cjelobrojne koeficijente jer je β algebarski cijeli broj.) Imamo

$$f(x) = (x - \sigma_1(\beta)) \cdots (x - \sigma_n(\beta)).$$

Razmotrimo koeficijent a_{n-1} uz x^{n-1} u $f(x)$. To je cijeli broj, jer je $f(x) \in \mathbb{Z}[x]$. Također ima izraz

$$a_{n-1} = -(\sigma_1(\beta) + \cdots + \sigma_n(\beta)).$$

Budući da svaki $\sigma_i(\beta)$ ima apsolutnu vrijednost 1, to implicira da

$$|a_{n-1}| \leq n.$$

Na isti način, pokazuje se da za bilo koji k,

$$|a_k| \leq \binom{n}{k}.$$

Dakle, postoji samo konačno mnogo mogućnosti za svaki a_k, jer je svaki cijeli broj u ograničenom rasponu.

Posebno, to znači da postoji samo konačno mnogo mogućih izbora za $f(x)$, jer postoji samo konačno mnogo izbora za svaki koeficijent od $f(x)$. (Primijetimo također da je stupanj od $f(x)$ fiksan na n.) Svaki takav $f(x)$ ima najviše n korijena, pa sve zajedno može postojati samo konačan broj korijena polinoma koji bi mogli biti karakteristični polinomi elemenata iz S. Posebno, sam S mora biti konačan, kao što smo i tvrdili. □

Lema 6.1.4

Neka je $u \in \mathcal{O}_K^\times$. Tada je $u/\bar{u} = \zeta^b$ za neki b, gdje je $\bar{u}$ kompleksno-konjugirana vrijednost od u.

Dokaz. Neka su $\sigma_1, \ldots, \sigma_{p-1}$ kompleksna ulaganja od $\mathbb{Q}(\zeta)$, poredana na uobičajeni način. Primijetimo da za svaki $\alpha \in \mathbb{Q}(\zeta)$ vrijedi

$$\sigma_i(\overline{\alpha}) = \sigma_i(\sigma_{-1}(\alpha)) = \sigma_{-1}(\sigma_i(\alpha)) = \overline{\sigma_i(\alpha)},$$

zbog $\sigma_{-1}(\alpha) = \overline{\alpha}$ i komutativnosti Galoisove grupe. Posebno, svaki konjugat od $\alpha/\overline{\alpha}$ imat će apsolutnu vrijednost 1, budući da kompleksan broj i njegov kompleksni konjugat imaju istu apsolutnu vrijednost.

Kada je u jedinica, $u/\overline{u}$ je također algebarski cijeli broj, jer je $\overline{u}$ jedinica. Sada možemo primijeniti Lemu 6.1.3 kako bismo zaključili da je $u/\overline{u}$ korijen jedinice. Dakle

$$\frac{u}{\overline{u}} = \pm\zeta^k \tag{6.2}$$

za neki k. Moramo pokazati da je predznak zapravo $+$. Pretpostavimo da je $u/\overline{u} = -\zeta^k$ za neki k. Napišimo

$$u = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}. \tag{6.3}$$

Tada

$$u \equiv a_0 + a_1 + \cdots + a_{p-2} \pmod{1-\zeta}. \tag{6.4}$$

Slično, budući da su $1-\zeta$ i $1-\overline{\zeta} = 1-\zeta^{p-1}$ asocirani, vrijedi

$$\overline{u} \equiv a_0 + a_1 + \cdots + a_{p-2} \pmod{1-\zeta}. \tag{6.5}$$

Stoga,

$$\overline{u} \equiv u \equiv -\zeta^k\overline{u} \equiv -\overline{u} \pmod{1-\zeta}. \tag{6.6}$$

Zbog toga $2\overline{u} \in (1-\zeta)$; budući da je $(1-\zeta)$ prost ideal i 2 nije u tom idealu, to implicira da $\overline{u} \in (1-\zeta)$. No to je nemoguće, jer je $\overline{u}$ jedinica, a ovo nije jedinični ideal. Time dobivamo željenu kontradikciju.

□

Lema 6.1.5

Neka je u jedinica od $\mathcal{O}_K$. Tada se u može napisati kao $\zeta^a\varepsilon$ gdje je ε jedinica maksimalnog realnog potpolja od K.

Dokaz. Prvo možemo primijeniti Lemu 6.1.3 i zaključiti da je $u/\overline{u}$ korijen jedinice. Prema Lemi 6.1.4 to znači da je

$$\frac{u}{\overline{u}} = \zeta^b$$

za neki b.

Sada odaberimo $a \in \mathbb{Z}$ takav da je $2a \equiv b \pmod{p}$ i neka je $\varepsilon = \zeta^{-a}u$. Tada je $u = \zeta^a\varepsilon$, i

$$\bar{\varepsilon} = \zeta^a\overline{u} = \zeta^a\zeta^{-b}u = \zeta^{-a}u = \varepsilon,$$

tako da je ε realan i stoga leži u maksimalnom realnom potpolju od K. □

Nastavljamo dokaz Kummerovog teorema. Sjetimo se da smo dokazali da je $x+\zeta^i y = u\alpha_i^p$ za neki $u \in \mathcal{O}_K^\times$. Sada uzmimo $i = 1$; prema dokazanom do sada, možemo pisati

$$x + \zeta y = \zeta^a\varepsilon\alpha^p$$

za neki cijeli broj a, neku realnu jedinicu ε i neki $\alpha = \alpha_1 \in \mathcal{O}_K$. Pokažimo da je $\alpha^p \equiv b \pmod{p}$ za neki racionalni cijeli broj b. Neka je

$$\alpha = a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2},$$

za neke $a_i \in \mathbb{Z}$. Tada je

$$\begin{aligned}\alpha^p &\equiv \left(a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2}\right)^p \pmod{p}\\ &\equiv a_0 + a_1\zeta^p + \ldots + a_{p-2}\zeta^{p(p-2)} \pmod{p}\\ &\equiv a_0 + a_1 + \ldots + a_{p-2}, \pmod{p}\end{aligned}$$

kao što smo i tvrdili.

Zaključujemo da

$$x + \zeta y \equiv \zeta^a \varepsilon b \pmod{p}.$$

Budući da su ε, b i p svi realni, uzimanjem kompleksnih konjugata dobivamo

$$x + \zeta^{-1} y \equiv \zeta^{-a} \varepsilon b \pmod{p}.$$

Kombinirajući ove jednadžbe, zaključujemo da

$$\zeta^{-a}(x + \zeta y) \equiv \zeta^a (x + \zeta^{-1} y) \pmod{p}$$

što se pojednostavljuje na

$$x + \zeta y - \zeta^{2a-1} y - \zeta^{2a} x \equiv 0 \pmod{p}.$$

Možemo koristiti ovu kongruenciju da dobijemo našu željenu kontradikciju. Pretpostavimo prvo da su 1, ζ, ζ^{2a-1} i ζ^{2a} svi različiti. Budući da je $p \geq 5$, to implicira da su ovi elementi dio integralne baze za $\mathcal{O}_K$. Sada činjenica da je

$$x + \zeta y - \zeta^{2a-1} y - \zeta^{2a} x$$

djeljivo s p u $\mathcal{O}_K$ implicira da x i y moraju biti djeljivi s p u $\mathbb{Z}$; ovo proturječi našoj pretpostavci da p ne dijeli xyz, što završava ovaj slučaj.

To ostavlja slučajeve gdje su neki od 1, ζ, ζ^{2a-1}, ζ^{2a} jednaki. Mogućnosti su:

(1) $1 = \zeta^{2a-1}$. Tada je $\zeta = \zeta^{2a}$, pa nalazimo da

$$(x - y) + (y - x)\zeta \equiv 0 \pmod{p}.$$

Ovo povlači da p dijeli $(x - y)(1 - \zeta)$. Kako smo pretpostavili da x i y nisu kongruentni modulo p, $x - y$ je relativno prost s p; budući da također p ne dijeli $1 - \zeta$ (oni nisu relativno prosti, ali to nije važno), ovo implicira da p ne može dijeliti $(x - y)(1 - \zeta)$; to je željena kontradikcija.

(2) $1 = \zeta^{2a}$. Tada je $\zeta^{2a-1} = \zeta^{-1}$, pa se kongruencija reducira na

$$\zeta y - \zeta^{-1} y \equiv 0 \pmod{p}.$$

Ovo implicira da p dijeli $y(\zeta - \zeta^{-1}) = -y\zeta^{-1}(1-\zeta^2)$; činjenica da p ne dijeli y sada daje kontradikciju kao u prethodnom slučaju.

(3) $\zeta = \zeta^{2a-1}$. Tada je $\zeta^{2a} = \zeta^2$ i kongruencija se reducira na

$$(1-\zeta^2)x \equiv 0 \pmod{p}.$$

Ovaj put p dijeli $x(1-\zeta^2)$; činjenica da p ne dijeli x sada daje kontradikciju. Ovo završava dokaz. □

Napomenimo da smo mi koristili činjenicu da p ne dijeli xyz na bitan način; Kummer je uspio proširiti teorem na slučaj $p|xyz$.

6.2 Regularni prosti brojevi

Još nismo dali nikakve metode za određivanje je li neki prost broj regularan. U ovom odjeljku ćemo navesti neke Kummerove rezultate koji daju lako izračunljive kriterije za regularnost.

Definiramo Bernoullijeve brojeve $B_n \in \mathbb{R}$ formulom:

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n t^n}{n!}.$$

Može se pokazati da je $B_n = 0$ ako je $n > 1$ neparan. Također, vrijedi formula

$$\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0$$

koja ih čini lagano izračunljivima i također pokazuje da su zapravo u $\mathbb{Q}$.

Kummer-ovi glavni rezultati o regularnim prostim brojevima su sljedeći teoremi. Neka je h_p broj klasa od $\mathbb{Q}(\zeta_p)$ i h_p^+ broj klasa maksimalnog realnog potpolja $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Vrijedi da h_p^+ dijeli h_p, i definirajmo $h_p^- = h_p/h_p^+$.

Teorem 6.2.1: Kummer

Neka je p neparan prost broj. Tada p dijeli h_p^- ako i samo ako p dijeli brojnik nekog Bernoullijevog broja B_j gdje je $j = 2, 4, \ldots, p-3$.

Teorem 6.2.2: Kummer

Ako p dijeli h_p^+, onda p dijeli h_p^-.

Iako postoji beskonačno mnogo prostih brojeva za koje p dijeli h_p^-, ne postoje poznati p za koje p dijeli h_p^+. Vandiver je izrekao slutnju da se ovo nikada ne događa, iako ova slutnja nije univerzalno prihvaćena.

Korolar 6.2.3: Kummer

p dijeli h_p ako i samo ako p dijeli brojnik nekog Bernoullijevog broja B_j gdje je $j = 2, 4, \ldots, p-3$.

Koristeći ove rezultate, nalazimo da je 37 prvi iregularni prost broj; on dijeli numerator od B_{32}. Sljedeći nekoliko iregularnih prostih brojeva su 59, 67, 101, 103, 131, 149 i 157.

Možemo dati heurističku argumentaciju za postotak prostih brojeva koji su iregularni. Definiramo indeks iregularnosti $i(p)$ kao broj Bernoullijevih brojeva B_j gdje je $j = 2, 4, \ldots, p-3$ za koje p dijeli brojnik od B_j; dakle $i(p) = 0$ ako i samo ako je p regularan. Pretpostavljajući da su Bernoullijevi brojevi nasumično distribuirani modulo p (što znači da p dijeli B_j s vjerojatnošću $1/p$), vjerojatnost da je $i(p) = k$ za neki k jest:

$$\binom{\frac{p-3}{2}}{k}\left(1-\frac{1}{p}\right)^{\frac{p-3}{2}-k}\left(\frac{1}{p}\right)^{k}.$$

Kako p raste, ovo se približava Poissonovoj distribuciji:

$$\frac{(1/2)^k e^{-1/2}}{k!}.$$

Uzimajući $k = 0$, nalazimo da bi udio regularnih prostih brojeva trebao biti $e^{-1/2}$, što je približno 60,65%. Ovaj rezultat se jako poklapa s numeričkim izračunima.

Korolar 6.2.4: Kummer

Postoji beskonačno mnogo iregularnih prostih brojeva.

Poglavlje 7

p-adski brojevi

7.1 Inverzni limes

Definicija 7.1.1

Inverzni sistem je niz objekata (npr. skupova/grupa/prstena) (A_n) skupa sa nizom morfizama (npr. funkcija/homomorfizama) (f_n)

$$\cdots \to A_{n+1} \xrightarrow{f_n} A_n \to \cdots \xrightarrow{f_2} A_2 \xrightarrow{f_1} A_1.$$

Definicija 7.1.2

Inverzni limes $A = \varprojlim A_n$ inverznog sistema skupova (A_n), (f_n) definiranog kao gore je skup A čiji elementi su beskonačni nizovi (a_n), gdje je $a_n \in A_n$ za svaki $n \geq 0$, te koji zadovoljavaju $f_n(a_{n+1}) = a_n$ za svaki $n \geq 0$.

Napomena 7.1.3

Ako su A_n grupe i f_n homomorfizmi grupa, tada je inverzni limes također grupa. Ako su A_n prsteni i f_n homomorfizmi prstenova, tada je A_n prsten.

7.2 Prsten cijelih p-adskih brojeva

Definicija 7.2.1

Neka je p fiksan prost broj. *Prsten cijelih p-adskih brojeva* $\mathbb{Z}_p$ je inverzni limes

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

inverznog sistema prstenova $(\mathbb{Z}/p^n\mathbb{Z})$ s homomorfizmima prstenova (f_n), gdje je f_n redukcija modulo p^n.

Napomena 7.2.2

Multiplikativna jedinica u prstenu je $1 = (\overline{1}, \overline{1}, \ldots)$, gdje je n-ta $\overline{1}$ označava $1+p^n\mathbb{Z}$. Preslikavanje koje šalje $x \in \mathbb{Z}$ u $(\overline{x}, \overline{x}, \ldots)$, je homomorfizam prstenova koji očito ima trivijalnu jezgru. Dakle vidimo da se $\mathbb{Z}$ ulaže u $\mathbb{Z}_p$, pa vidimo da $\mathbb{Z}_p$ ima karakteristiku 0, te možemo smatrati $\mathbb{Z}$ potprstenom od $\mathbb{Z}_p$. Međutim, prsten $\mathbb{Z}_p$ je puno veći od $\mathbb{Z}$.

Elemente prstena $\mathbb{Z}_p$ ćemo neformalno pisati kao nizove $(a_1, a_2, \ldots)$, gdje cijeli broj $a_i \in [0, p^i - 1]$ reprezentira $a_i + p^i\mathbb{Z}$.

Primjer 7.2.3

U $\mathbb{Z}_7$ imamo

$$\begin{aligned}
2 &= (2, 2, 2, 2, 2\ldots),\\
2002 &= (0, 42, 287, 2002, 2002, \ldots),\\
-2 &= (5, 47, 341, 23999, 16805, \ldots),\\
\frac{1}{2} &= (4, 25, 172, 1201, 8304, \ldots),\\
\sqrt{2} &= \begin{cases} (3, 10, 108, 2166, 4567, \ldots) \\ (4, 39, 235, 235, 12240, \ldots) \end{cases}\\
\sqrt[5]{2} &= (4, 46, 95, 1124, 15530, \ldots)
\end{aligned}$$

Zadatak 7.2.4

Dokažite da postoji $\sqrt[p]{2}$ u $\mathbb{Z}_7$ za svaki $p > 7$.

Definicija 7.2.5

Sjetimo se da je niz homomorfizama grupa *egzaktan* ako je za svaku grupu u nizu slika ulaznog homomorfizma jednaka jezgri izlaznog homomorfizma. Za *kratki egzaktan niz*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0,$$

to znači da je f injektivan, g surjektivan, te da je $\operatorname{im} f = \ker g$. Po prvom teoremu o izomorfizmu grupa, također vrijedi $B/\operatorname{im} f \simeq C$.

Propozicija 7.2.6

Za svaki cijeli broj m, niz

$$0 \to \mathbb{Z}_p \xrightarrow{[p^m]} \mathbb{Z}_p \xrightarrow{\pi_m} \mathbb{Z}/p^m\mathbb{Z} \to 0$$

je egzaktan, gdje je $[p^m]$ množenje s p^m, te je π_m projekcija na $\mathbb{Z}/p^m\mathbb{Z}$, tj. preslikavanje koje šalje niz (a_n) u a_m.

Dokaz. Dokažimo prvo da je množenje s p u $\mathbb{Z}_p$ injektivno. Pretpostavimo suprotno, tj. da je $a = (a_n)$ u jezgri. Tada je $pa = 0$, pa je $pa_n = 0$ za svaki n. Posebno, $pa_{n+1} = 0$ u $\mathbb{Z}/p^{n+1}\mathbb{Z}$. To sada znači da je $a_{n+1} = p^n y_{n+1}$ u $\mathbb{Z}/p^{n+1}\mathbb{Z}$ za neki $y_{n+1} \in \mathbb{Z}/p^{n+1}\mathbb{Z}$. Sada slijedi da je $a_n = f(a_{n+1}) = p^n f(y_{n+1}) = 0$ u $\mathbb{Z}/p^n\mathbb{Z}$. Kako ovo vrijedi za sve n, slijedi $a = 0$.

Egzaktnost s lijeva: Pošto je množenje s p injektivno, vrijedi da je kompozicija tog preslikavanja sa samim sobom m puta (tj. množenje s p^m) injektivno.

Egzaktnost s desna: Zapišimo $\beta \in \mathbb{Z}/p^m\mathbb{Z}$ kao $b + p^m\mathbb{Z}$. Tada će π_m preslikati element $(b, b, b, b, \ldots)$ u β.

Egzaktnost u sredini: Ako je $a \in \mathbb{Z}_p$, tada je $\pi_m(p^m a) = p^m \pi_m(a) = 0$ u $\mathbb{Z}/p^m\mathbb{Z}$. Dakle slika ulaznog preslikavanja je u jezgri izlaznog preslikavanja. Dokažimo suprotnu inkluziju. Neka je $a = (a_n)$ u jezgri od π_m. Dakle vrijedi da je $a_m = 0$. Dakle za svaki $n \geq m$, imamo $a_n \in p^m\mathbb{Z}/p^n\mathbb{Z}$. Dakle postoji jedinstveni b_{n-m} koji se preslikava u a_n pod djelovanjem izomorfizma

$$\mathbb{Z}/p^{n-m}\mathbb{Z} \xrightarrow{p^m} p^m\mathbb{Z}/p^n\mathbb{Z}.$$

Niz tih b_{n-m}-ova je kompatibilan, pošto su a_n-ovi kompatibilni, te postoji element $b = (b_n)$ takav da je $p^m b = a$, dakle a je u slici od množenja s p^m.

□

Korolar 7.2.7

Za svaki prirodan broj m vrijedi $\mathbb{Z}_p/p^m\mathbb{Z}_p \simeq \mathbb{Z}/p^m\mathbb{Z}$.

Propozicija 7.2.8

Element $x \in \mathbb{Z}_p$ je invertibilan ako i samo ako $x \notin p\mathbb{Z}_p$. Drugim riječima, $\mathbb{Z}_p^\times$ je $\mathbb{Z}_p \backslash p\mathbb{Z}_p$.

Dokaz. Ako je $a = (a_n) \in \mathbb{Z}_p$ djeljiv s p, tada je $a_1 = 0$, pa a očito ne može biti invertibilan. Ako a nije djeljiv s p tada za svaki n vrijedi $a_n \in b_n + p^n\mathbb{Z}$ za neki $b_n \in \mathbb{Z}$, te taj b_n nije djeljiv s p. Slijedi da a_n ima inverz c_n u $\mathbb{Z}/p^n\mathbb{Z}$. Također, niz (c_n) mora biti kompatibilan, te je $c = (c_n)$ inverz od a. □

Propozicija 7.2.9

Svaki element $x \in \mathbb{Z}_p$ se može na jedinstven način zapisati kao $p^n u$, gdje je $u \in \mathbb{Z}_p^\times$.

Dokaz. Postojanje zapisa: Ako je $0 \neq a = (a_n)$, tada postoji najveći n takav da je $a_n = 0$. Za taj n, po Propoziciji 7.2.6 vrijedi $a = p^n u$ za neki $u \in \mathbb{Z}_p$. štoviše, u ne može biti djeljiv s p, pošto bi tada bilo $u_{n+1} = 0$, pa je po prethodnoj propoziciji u invertibilan.

Jedinstvenost zapisa: Pretpostavimo $p^n u_1 = p^m u_2$. Ako je $m = n$, tada zbog injektivnosti množenja s p^m imamo $u_1 = u_2$. U suprotnom možemo bez smanjenja općenitosti pretpostaviti da je $n > m$. Tada je $u_2 = p^{n-m} u_2$ invertibilan, što je kontradikcija s prethodnom propozicijom. □

Korolar 7.2.10

Prsten $\mathbb{Z}_p$ je integralna domena.

Dokaz. Množenjem dva nenul elementa $p^n u_1$ i $p_m u_2$ dobivamo $p^{n+m} u_1 u_2$, čija je $(n + m + 1)$-ta komponenta različita od nule. □

Definicija 7.2.11

Neka je $a = (a_n) \in \mathbb{Z}_p$, gdje je po običaju a_n cijeli broj iz $[0, p^n - 1]$. Niz $(b_0, b_1, \ldots)$ za kojeg vrijedi $b_0 = a_1$ i $b_n = (a_{n+1} - a_n)/p^n$ se zove p-adska ekspanzija od a.

Dakle svaki $a \in \mathbb{Z}_p$ se može zapisati kao formalni red

$$a = \sum_{i=0}^{\infty} b_i p^i.$$

Iz definicije odmah slijedi:

Propozicija 7.2.12

Svaki element u $\mathbb{Z}_p$ ima jedinstvenu p-adsku ekspanziju i svaki niz $(b_0, b_1, \ldots)$, gdje je $b_i \in [0, p-1]$ je p-adska ekspanzija nekog elementa iz $\mathbb{Z}_p$.

Dakle, postoji bijekcija između $\mathbb{Z}_p$ i nizova cijelih brojeva s elementima iz $[0, p-1]$.

Definicija 7.2.13

Za svaki $0 \neq a \in \mathbb{Z}_p$, *$p$-adska valuacija* od a, s oznakom $v_p(a)$ je najveći cijeli broj m za koji je a u $p^m\mathbb{Z}_p$. Ekvivalentno $v_p(a)$ je za $a = \sum_{i=0}^{\infty} b_i p^i$ najmanji prirodan broj m takav da je $b_m \neq 0$. Također, ekvivalentno, ako zapišemo $a = p^m u$, gdje je $u \in \mathbb{Z}_p^\times$ tada je $v_p(a) = m$. Definiramo $v_p(0) = +\infty$.

Propozicija 7.2.14

Svaki ne-nul ideal u $\mathbb{Z}_p$ je oblika (p^m) za neki prirodan broj m.

Dokaz. Neka je I ne-nul ideal u $\mathbb{Z}_p$ i neka je $m = \inf\{v_p(a) : a \in I\}$. Pošto je $I \neq (0)$, tada je $m < \infty$, te za svaki $a \in I$ vrijedi $a \in p^m\mathbb{Z}_p = (p^m)$. S druge strane, postoji $a \in I$ takav da je $a = p^m u$. Slijedi da je $u^{-1}a = p^m \in I$, iz čega slijedi da je $(p^m) \subset I$. □

Korolar 7.2.15

Prsten $\mathbb{Z}_p$ je domena glavnih ideala (a time i prsten jedinstvene faktorizacije) s jedinstvenim prostim idealom (p) (te jednim prostim elementom p).

Propozicija 7.2.16

Uz konvenciju da je $n + \infty = \infty$ za svaki cijeli broj n, p-adska valuacija zadovoljava sljedeća svojstva:

1. $v_p(a) = \infty$ ako i samo ako je $a = 0$.
2. $v_p(ab) = v_p(a) + v_p(b)$.
3. $v_p(a + b) \geq \min(v_p(a), v_p(b))$.

Dokaz. Prvo svojstvo slijedi iz definicije. Drugo i treće svojstvo su očito zadovoljena ako su a ili b jednaki 0. Pretpostavimo $a, b \neq 0$. Neka je $v_p(a) = m$ i $v_p(b) = n$.

Da bismo dokazali drugu tvrdnju zapišimo $a = p^m u_1$ i $b = p^n u_2$, gdje su $u_1, u_2 \in \mathbb{Z}_p^\times$. Tada je $ab = p^{m+n} u_1 u_2$, pa je $v_p(ab) = m + n$.

U trećoj tvrdnji možemo bez smanjenja općenitosti pretpostaviti da je $m \leq n$. Slijedi da je $p^n\mathbb{Z}_p \subseteq p^m\mathbb{Z}_p$, pa su i $a, b \in p^m\mathbb{Z}_p$, iz čega slijedi da je $a + b \in p^m\mathbb{Z}_p$, te je $v_p(a + b) \geq \min(v_p(a), v_p(b))$.

□

p-adska valuacija je primjer *diskretne valuacije*.

Definicija 7.2.17

Neka je R komutativni prsten. *Diskretna valuacija* (na R) je funkcija $v : R \to \mathbb{Z} \cup \{\infty\}$ koja zadovoljava svojstva iz propozicije 7.2.16.

Definicija 7.2.18

Prsten diskretne valuacije je domena glavnih ideala koja sadrži jedinstveni maksimalni ideal, te nije polje.

Možda je ova definicija na prvi pogled neobična, pošto se ne spominje valuacija, međutim za svaki prsten diskretne valuacije se može na analogan način definirati diskretna valuacija.

Prsten diskretne valuacije je "najbliže" što komutativni prsten može biti polje, a bez da je zaista polje.

7.3 Polje p-adskih brojeva

Sjetimo se da se polje razlomaka nekog prstena R definira kao skup uređenih parova $(a, b) \in R^2$, koji se obično zapisuje kao a/b gdje vrijedi da je $a/b \sim c/d$ kad god je $ad = bc$.

Definicija 7.3.1

Polje p-adskih brojeva $\mathbb{Q}_p$ je polje razlomaka od $\mathbb{Z}_p$.

Pošto je $a \in \mathbb{Q}_p$ po definiciji $a = (p^m u_1)/(p^n u_2) = p^{m-n} u_1 u_2^{-1}$, možemo svaki element iz $\mathbb{Q}_p$ zapisati kao up^k za $u \in \mathbb{Z}_p^\times$, $k \in \mathbb{Z}$. Sada možemo proširiti definiciju od v_p na $\mathbb{Q}_p$ tako da za $a = up^k$, $u \in \mathbb{Z}_p^\times$, $k \in \mathbb{Z}$ vrijedi $v_p(up^k) = k$, te je kao i prije $v_p(0) := +\infty$.

Napomena 7.3.2

Primijetimo da sada možemo $\mathbb{Z}_p$ identificirati kao podskup od $\mathbb{Q}_p$ sa elementima ne-negativne valuacije, te $\mathbb{Z}_p^\times$ možemo definirati kao podskup $\mathbb{Q}_p$ elemenata s valuacijom 0.
Vrijedi $\mathbb{Q} \subset \mathbb{Q}_p$, te vrijedi za svaki $x \in \mathbb{Q}_p$ je ili $x \in \mathbb{Z}_p$ ili je $x^{-1} \in \mathbb{Z}_p$.

Ovo je jedan od dva načina definiranja polja $\mathbb{Q}_p$. Promotrimo sada drugi način, preko apsolutnih vrijednosti.

7.4 Apsolutne vrijednosti

Definicija 7.4.1

Neka je k polje. *Apsolutna vrijednost* na k je funkcija $\|\| : k \to \mathbb{R}_{\geq 0}$ sa sljedećim svojstvima:

(1) $\|x\| = 0$ ako i samo ako je $x = 0$,

(2) $\|xy\| = \|x\| \cdot \|y\|$.

(3) $\|x + y\| \leq \|x\| + \|y\|$.

Apsolutne vrijednosti se nekada nazivaju i "norme", ali mi ćemo koristiti izraz norme za nešto drugo, te ćemo koristiti naziv "apsolutna vrijednost" kako bismo izbjegli zabunu.

Neke norme zadovoljavaju jače svojstvo

(3') $\|x + y\| \leq \max\{\|x\|, \|y\|\}$.

se zovu *nearhimedske* apsolutne vrijednosti, a one koje ne zadovoljavaju se zovu *arhimedske*.

Definicija 7.4.2

Definiramo p-adsku apsolutnu vrijednost $|\ |_p$ na $\mathbb{Q}_p$ s

$$|x|_p = p^{-v_p(x)}.$$

Napomena 7.4.3

primijetimo da pošto je $\mathbb{Q} \subset \mathbb{Q}_p$, ovo daje definiciju apsolutne vrijednosti $|\ |_p$ na $\mathbb{Q}$. Spomenuti alternativni način definicije od $\mathbb{Q}_p$ je da definiramo $\mathbb{Q}_p$ kao upotpunjenje od $\mathbb{Q}$ (tj. $\mathbb{Q}$ skupa s svim limesima nizova iz $\mathbb{Q}$) s obzirom na apsolutnu vrijednost $|\ |_p$. Dosta knjiga definira $\mathbb{Q}_p$ upravo na ovaj način. Tada se $\mathbb{Z}_p$ definira kao

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\},$$

ili kao upotpunjenje od $\mathbb{Z}$ s obzirom na $|\ |_p$.

Napomena 7.4.4

Naziv *prsten cijelih brojeva* u $\mathbb{Q}_p$ može biti zbunjujući. Naime, $\mathbb{Z}_p$ *nije* integralno zatvorenje od $\mathbb{Z}$ u $\mathbb{Q}_p$. To možemo vidjeti promatranjem kardinaliteta tih skupova. Integralno zatvorenje od $\mathbb{Z}$ u $\mathbb{Q}_p$ je prebrojiv skup, (pošto postoji prebrojivo mnogo polinoma s cjelobrojnim koeficijentima) dok je $\mathbb{Z}_p$ očito neprebrojiv skup. Međutim, istina je da je $\mathbb{Z}_p$ integralno zatvoren u $\mathbb{Q}_p$, te $\mathbb{Z}_p$ sadrži integralno zatvorenje od $\mathbb{Z}$ u $\mathbb{Q}$.

Definicija 7.4.5

Dvije apsolutne vrijednosti $\|\ \|$ i $\|\ \|'$ na polju k su ekvivalentne ako postoji $\alpha \in \mathbb{R}$ takav da je

$$\|x\|' = \|x\|^\alpha$$

za svaki $x \in k$.

Sljedeći teorem, koji nećemo dokazivati, nam govori koje su sve apsolutne vrijednosti, do na ekvivalenciju, na $\mathbb{Q}$. Označimo s $|\ |_\infty$ uobičajenu apsolutnu vrijednost.

Općenito u p-adskoj apsolutnoj vrijednosti, "mali" su brojevi koji su djeljivi velikim potencijama broja p.

Teorem 7.4.6: Ostrowski

Svaka ne-trivijalna apsolutna vrijednost na $\mathbb{Q}$ je ekvivalentna s $|\ |_p$ za neki prost broj p ili $|\ |_\infty$.

Na $\mathbb{Z}_p$ i $\mathbb{Q}_p$ se može definirati *p-adska topologija* preko apsolutne vrijednosti. U p-adskim brojevima su $a, b \in \mathbb{Q}$, promatrani kao elementi od $\mathbb{Q}_p$ "blizu", ako je u brojniku od $a - b$ velika potencija od p. Na primjer, niz $2, 4, 8, 16, 32, \ldots$ konvergira u 0 u $\mathbb{Z}_2$.

p-adska analiza nam je često vrlo korisna, međutim trebamo biti vrlo pažljivi s intuicijom kada radimo s p-adskim brojevima.

Primjer 7.4.7

Neka su $b, c \in \mathbb{Q}$, te neka je p prost broj. Tada postoji niz racionalnih brojeva a_i koji konvergira u b u standardnoj (realnoj) topologiji, te konvergira u c u p-adskoj topologiji. Dokažimo ovu tvrdnju. Neka je

$$d_n = \frac{p^n}{p^n+1} \quad e_n = \frac{1}{p^n+1}.$$

U standardnoj topologiji d_n konvergira u 1, a e_n konvergira u 0, dok u p-adskoj topologiji d_n konvergira u 0, a $e_n = 1 - \frac{p^n}{p^n+1}$ konvergira u 1. Dakle vidimo da će niz $(a_n) = (bd_n + ce_n)$ konvergirati u b u standardnoj topologiji, te u c u p-adskoj.

Prikažimo sada jednu primjenu p-adskih brojeva i jednostavne p-adske analize.

Primjer 7.4.8

Dokažimo da ako prost p dijeli nazivnik od koeficijenata od $(1+t)^a$, onda p dijeli nazivnik od a.
Na primjer,

$$(1+t)^{\frac{1}{6}} = 1 + \frac{1}{6}t - \frac{5}{2^2 3^2}t^2 + \frac{55}{2^4 3^4}t^3 - \frac{935}{2^7 3^5}t^4 + \dots.$$

Vidimo da se u nazivnicima nalaze samo potencije od 2 i 3, tj. prostih djelitelja od 6. Tvrdimo da, za $a \in \mathbb{Q}$, $k \in \mathbb{N}$, se u nazivniku od

$$\binom{a}{k} = \frac{a(a-1)(a-2)\dots(a-k+1))}{k!}$$

nalaze samo potencije prostih brojeva koje dijele nazivnik od a.
Dokažimo tvrdnju obratom po kontrapoziciji: ako p ne dijeli nazivnik od a, tada p ne dijeli nazivnik od $\binom{a}{k}$. Pošto a nema faktore od p u nazivniku, tada je $a \in \mathbb{Z}_p$. Dakle, zaključujemo da je $a = (a_n)$ limes niza (b_n), gdje je $b_n \in \mathbb{Z}$, npr. uzmimo da je b_i i-ti član p-adske ekspanzije $b_i = \sum_{k=0}^{i} a_k p^k$. Općenitije $\mathbb{Z}_p$ je upotpunjenje od $\mathbb{Z}$ u p-adskoj topologiji, pa ova tvrdnja vrijedi za svaki $r \in \mathbb{Z}_p$.
S druge strane, polinomijalna funkcija $x \mapsto \binom{x}{k} \in \mathbb{Q}[x]$ je neprekidna u p-adskoj topologiji, pa zbog $a = \lim_{i\to\infty} b_i$, imamo

$$\binom{a}{k} = \lim_{i\to\infty} \binom{b_i}{k}.$$

Pošto je $b_i \in \mathbb{Z}$, slijedi da je $\binom{b_i}{k} \in \mathbb{Z}$. Pošto je $\binom{a}{k}$ limes elemenata iz $\mathbb{Z}$, slijedi da je $\binom{a}{k} \in \mathbb{Z}_p$, tj. p ne dijeli nazivnik od $\binom{a}{k}$.

7.5 Rješenja polinomijalnih jednadžbi

Lema 7.5.1

Neka je (S_n) inverzni sistem konačnih nepraznih skupova s kompatibilnim preslikavanjem $f_n : S_{n+1} \to S_n$. Tada je $\varprojlim S_n$ neprazan.

Dokaz. Ako su svi f_n surjektivni, tada lako konstruiramo element (s_n): izaberemo bilo koji $s_1 \in S_1$, te za $n \geq 1$ izaberemo $s_{n+1} \in f_n^{-1}(s_n)$. sada nam je cilj opći slučaj reducirati na ovaj.

Neka je $T_{n,n} = S_n$ i za $m > n$ neka je $T_{m,n}$ slika od S_m u S_n, tj.

$$T_{m,n} = f_n(f_{n+1}(\cdots f_{m-1}(S_m)\cdots)).$$

Tada za svaki n imamo niz inkluzija

$$\cdots, \subseteq T_{m,n} \subseteq T_{m-1,n} \subseteq \cdots T_{n,n} \subseteq S_n.$$

Svaki $T_{m,n}$ je konačan neprazan skup, pa slijedi da je za sve osim konačno mnogo inkluzija, ta inkluzija zapravo jednakost. Dakle za svaki n, je $E_n = \cap_m T_{m,n}$ neprazan podskup od S_n. Restringirajući preslikavanje f_n tako da definira preslikavanje $E_{n+1} \to E_n$ dobivamo inverzni sistem (E_n) nepraznih skupova takvih da su sva preslikavanja surjekcija, kao što smo i htjeli. □

Propozicija 7.5.2

Neka je $f \in \mathbb{Z}_p[x]$. Tada su sljedeće tvrdnje ekvivalentne:

(1) Jednadžba $f(x) = 0$ ima rješenja u $\mathbb{Z}_p$.

(2) Jednadžba $f(x) = 0$ ima rješenja u $\mathbb{Z}/p^n\mathbb{Z}$ za svaki $n \in \mathbb{N}$

Dokaz. Neka je S_n skup rješenja u $\mathbb{Z}/p^n\mathbb{Z}$. Tada je $\varprojlim S_n \subseteq \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$ skup rješenja u $\mathbb{Z}_p$. Sada imamo $\varprojlim S_n \neq \emptyset$ ako i samo ako su svi S_n neprazni po Lemi 7.5.1. □

Henselova lema će nam reći da je nešto što je "blizu" rješenja polinomijalne jednadžbe može "popraviti" do egzaktnog rješenja.

Teorem 7.5.3: Henselova lema

Neka je $f_p \in \mathbb{Z}_p[x]$. Pretpostavimo da je $f(a) \equiv 0 \pmod{p}$ i $f'(a) \not\equiv 0 \pmod{p}$. Tada postoji jedinstveni $b \in \mathbb{Z}_p$, $b \equiv a \pmod{p}$ takav da je $f(b) = 0$.

Dokaz. Neka $a_1 = a$ i definiramo za $n \geq 1$

$$a_{n+1} = a_n - f(a_n)/f'(a_n).$$

Dokazujemo indukcijom da za svaki $n \geq 1$ vrijedi

$$f'(a_n) \not\equiv 0 \pmod{p}, \tag{7.1}$$

$$f(a_n) \equiv 0 \pmod{p^n}. \tag{7.2}$$

Primijetimo da (7.1) osigurava da je $f'(a_n) \in \mathbb{Z}_p^\times$, pa je a_{n+1} dobro definiran element iz $\mathbb{Z}_p$. Definicija od a_{n+1} skupa s (7.1) i (7.2) osiguravaju da je $a_{n+1} \equiv a_n \pmod{p^n}$, što znači da niz $(a_n \mod p^n)$ definira element $b \in \mathbb{Z}_p$ za koji vrijedi $f(b) = 0$ i $b \equiv a_1 \equiv a \pmod{p}$.

Za $n = 1$ tvrdnja očito vrijedi, pa pretpostavimo da (7.1) i (7.2) vrijede za a_n. Tada $a_{n+1} \equiv a_n \pmod{p^n}$, pa je $f'(a_{n+1}) \equiv f'(a_n) \not\equiv 0 \pmod{p}$. Dakle (7.1) je zadovoljen za sve $n \in \mathbb{N}$. Da bi pokazali (7.2), napravimo Taylorov razvoj od f oko a_n:

$$f(x) = f(a_n) + f'(a_n)(x - a_n) + (x - a_n)^2 g(x),$$

za neki $g(x) \in \mathbb{Z}_p[x]$. Uvrštavajući $x = a_{n+1}$, dobivamo

$$f(a_{n+1}) = f(a_n) + f'(a_n)(a_{n+1} - a_n) + (a_{n+1} - a_n)^2 g(a_n + 1).$$

Iz definicije a_{n+1} imamo $f'(a_n)(a_{n+1} - a_n) = -f(a_n)$, pa je

$$f(a_{n+1}) = (a_{n+1} - a_n)^2 g(a_{n+1}).$$

Pošto je $a_{n+1} \equiv a_n \pmod{p^n}$, slijedi da je $f(a_{n+1}) \equiv 0 \pmod{p^{n+1}}$, pa (7.2) vrijedi za a_{n+1}.

Pošto $f(x) = 0$ ima jedinstveno rješenje u $\mathbb{Z}/p^n\mathbb{Z}$ kongruentno s a modulo p (jer (7.1) povlači da je $f'(a_n) \not\equiv 0 \pmod{p^n}$, pa je a_n jednostruka nultočka od $f \pmod{p^n}$), slijedi da niz (a_n) definira jedinstveno rješenje u $\mathbb{Z}_p$. □

7.6 Struktura od $\mathbb{Z}_p^\times$

Restrikcija projekcije $\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ na $\mathbb{Z}_p^\times$ definira surjektivni homomorfizam

$$\mathbb{Z}_p^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

Jezgra ovog preslikavanja je $U_n := 1 + p^n\mathbb{Z}_p$. Dakle, vrijedi

$$\mathbb{Z}_p^\times / U_n \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times,$$

pa je

$$\mathbb{Z}_p^\times \simeq \varprojlim(\mathbb{Z}_p^\times / U_n) \simeq \varprojlim(\mathbb{Z}/p^n\mathbb{Z})^\times.$$

primijetimo da je (U_n) padajući niz podgrupa od $\mathbb{Z}_p^\times$:

$$\cdots \subset U_3 \subset U_2 \subset U_1 \subset \mathbb{Z}_p^\times.$$

Lema 7.6.1

Vrijedi:

(1) $\mathbb{Z}_p^\times / U_1 \simeq (\mathbb{Z}/p\mathbb{Z})^\times$.

(2) $U_n / U_{n+1} \simeq \mathbb{Z}/p\mathbb{Z}$.

Dokaz. Prvu tvrdnju smo već dokazali. Za drugu, promotrimo preslikavanje

$$U_n \to \mathbb{Z}/p\mathbb{Z},$$
$$1 + p^n z \mapsto (z \bmod p).$$

To preslikavanje je surjekcija, te je jezgra U_{n+1}. □

Korolar 7.6.2

Grupa U_1/U_n ima p^{n-1} elemenata.

Propozicija 7.6.3

Neka je μ_{p-1} skup rješenja jednadžbe $x^{p-1} = 1$ u $\mathbb{Z}_p^\times$. Tada je μ_{p-1} s operacijom množenja grupa izomorfna s $(\mathbb{Z}/p\mathbb{Z})^\times$, te je $\mathbb{Z}_p^\times = U_1 \times \mu_{p-1}$.

Dokaz. Skup μ_{p-1} je jezgra homomorfizma potenciranja na $(p-1)$-vu potenciju sa $\mathbb{Z}_p^\times$ u $\mathbb{Z}_p^\times$, pa je grupa. Neka je $f(x) = x^{p-1} - 1$. Po Malom Fermatovom teoremu, svaki element $\neq 0$ iz $\mathbb{Z}/p\mathbb{Z}$ je korijen ovog polinoma, te vrijedi $f'(x) \not\equiv 0 \pmod p$ za sve $x \in \{1, 2, \ldots, p-1\}$. Sada po Henselovoj lemi, za svaki $x \in \{1, 2, \ldots, p-1\}$ postoji jedinstveni $a \in \mathbb{Z}_p$ takav da je $f(a) = 0$. Također, ne postoji element iz μ_{p-1} koji je kongruentan 0 modulo p. Slijedi da je redukcija modulo p izomorfizam $\mu_{p-1} \to (\mathbb{Z}/p\mathbb{Z})^\times$.

Primijetimo sada da je $U_1 \cap \mu_{p-1} = \{1\}$, pošto je 1 očito rješenje, a po Henselovoj lemi, rješenje kongruentno 1 mod p je jedinstveno. Također, vrijedi da je $U_1 \cdot \mu_{p-1} = \mathbb{Z}_p^\times$, pošto se bilo koji element $a \in \mathbb{Z}_p^\times$ može podijeliti s elementom iz μ_{p-1} koji je kongruentan s a modulo p da bi dobio element iz U_1. Slijedi da je direktan produkt $U_1 \times \mu_{p-1}$ izomorfan $\mathbb{Z}_p^\times$. □

Lema 7.6.4

Neka je p prost broj. Ako je $p \neq 2$, neka je $n \geq 1$, a ako je $p = 2$, neka je $n \geq 2$. Ako je $x \in U_n \backslash U_{n+1}$, tada je $x^p = U_{n+1} \backslash U_{n+2}$.

Dokaz. Neka je $x \in U_n \backslash U_{n+1}$, dakle $x = 1 + p^n k$, za neki k koji nije djeljiv s p. Tada je

$$x^p = 1 + \binom{p}{1} k p^n + \binom{p}{2} k^2 p^{2n} + \cdots k^p p^{np} \equiv 1 + k p^{n+1} \pmod{p^{n+2}}.$$

Slijedi da je $x^p \in U_{n+1} \setminus U_{n+2}$. □

Propozicija 7.6.5

Ako je $p \neq 2$, tada je $U_1 \simeq \mathbb{Z}_p$. Ako je $p = 2$, tada je $U_1 = \{\pm 1\} \times U_2$, te je $U_2 \simeq \mathbb{Z}_2$.

Dokaz. Neka je prvo $p \neq 2$, te neka je $\alpha = 1 + p \in U_1 \setminus U_2$. Koristeći prethodnu lemu, zaključujemo da je $\alpha^{p^i} \in U_{i+1} \setminus U_{i+2}$. Neka je α_n slika od α u U_1/U_n. Tada je $\alpha_n^{p^{n-2}} \neq 1$, ali je $\alpha_n^{p^{n-1}} = 1$, pa onda α ima red točno p^{n-1}. Dakle U_1/U_n je ciklička grupa generirana s α. Slijedi da imamo izomorfizam inverznih sistema

$$\begin{array}{ccccccc} \cdots & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^{n-1}\mathbb{Z} & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & U_1/U_{n+1} & \longrightarrow & U_1/U_n & \longrightarrow & \cdots \end{array}$$

Nakon što primijetimo da je $\varprojlim(U_1/U_n) = U_1$, slijedi da je $U_1 \simeq \mathbb{Z}_p$.

Za $p = 2$, isti argument s izborom $\alpha = 1 + 4$ dokazuje da je $U_2 \simeq \mathbb{Z}_2$. Koristeći da $\{\pm 1\}$ i U_2 imaju trivijalan presjek (tj. $-1 \notin U_2$, te pošto njihov produkt generira U_1 (jer je $[U_1 : U_2] = 2$), slijedi da je $\{\pm 1\} \times U_2$. □

Teorem 7.6.6

Vrijedi:

(1) Grupa $\mathbb{Z}_p^\times$ je izomorfna s $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ za $p \neq 2$, te s $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ za $p = 2$.

(2) Grupa $\mathbb{Q}_p^\times$ je izomorfna s $\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ ako je $p \neq 2$, te s $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ ako je $p = 2$.

Dokaz. Tvrdnja (1) slijedi iz Propozicije 7.6.3 i 7.6.5.
Da bismo dokazali (2), promotrimo preslikavanje

$$\begin{aligned} \mathbb{Z} \times \mathbb{Z}_p^\times &\to \mathbb{Q}_p^\times \\ (n, u) &\mapsto p^n u, \end{aligned}$$

te primijetimo da je to izomorfizam grupa. Korištenjem (1), tvrdnja slijedi. □

Propozicija 7.6.7

Za $p \neq 2$ i prirodan broj m postoji primitivni m-ti korijen iz jedinice u $\mathbb{Q}_p^\times$ (tj. element reda m) ako i samo ako $m | p-1$, te su u $\mathbb{Q}_2^\times$ elementi -1 i 1 jedini korijeni iz jedinice.

Dokaz. Neka je prvo $p \neq 2$. Da postoje m-ti korijeni iz jedinice kada $m|p-1$ smo vidjeli u Korolaru 7.6.3. S druge strane, kada bi za $m \not| p-1$ postojao m-ti korijen iz jedinice ζ_m, tada bi $\mu_m = \{1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{n-1}q\}$ činili podgrupu reda m od $\mathbb{Z}_p^\times$, što je u kontradikciji s Teoremom 7.6.6, (2).

U $\mathbb{Z}_2$ je očito da su ± 1 korijeni iz jedinice. Iz strukture od $\mathbb{Z}_2^\times$ opisane u Teoremom 7.6.6, vidimo da su to jedini elementi konačnog reda u $\mathbb{Q}_2^\times$.

□

Korolar 7.6.8

Neka su p i q različiti prosti brojevi. Tada polja $\mathbb{Q}_p$ i $\mathbb{Q}_q$ nisu izomorfna.

Dokaz. Tvrdnja direktno slijedi iz prošle propozicije, pošto polja imaju korijene jedinice različitog reda. □

Napomena 7.6.9

Neka je p neparan. Tada će se element -1 nalaziti u podgrupi μ_{p-1}, koja je ciklička reda $p-1$, te je -1 reda 2. Element -1 će dakle biti kvadrat u $\mathbb{Q}_p^\times$ ako i samo ako u μ_{p-1} postoji element reda 4, tj. kada je $p \equiv 1 \pmod 4$.