

UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Hana Ibrahimpašić

Algebraična številska polja z majhnim številom razredov

Osnutek dela diplomskega seminarja

Mentor: prof. dr. Primož Moravec

Ljubljana, 2022

1. UVOD

Enolična faktorizacija celih števil je glavni rezultat teorije števil. Za katera številska polja lahko predstavimo analogen rezultat? Ali lahko tudi določimo, do kakšne mere enolična faktorizacija ne drži v danem številskem polju? Vprašanja bomo usmerili na primerno konstruiran podkolobar in teorijo idealov. Tudi če v tem kolobarju enolične faktorizacije elementov ne bo, enolična faktorizacija idealov bo zagotovljena. Konstruirali bomo končno grupo, katere moč bo ključna. Videli bomo, zakaj nas poleg številskih polj z enolično faktorizacijo zanimajo tudi polja, ki niso daleč od tega. Kot naslov dela napoveduje, opažanja bomo primerno opisali v jeziku konstrukcij, ki jih spoznamo.

2. ALGEBRAIČNO ŠTEVILSKO POLJE IN CELOŠTEVILSKI KOLOBAR

Razširitev polja pogosto obravnavamo kot vektorski prostor nad danim poljem. Tako lahko govorimo o dimenziji tega vektorskega prostora. V algebraični teoriji števil glavno vlogo imajo tiste razširitve polja racionalnih števil, ki jih gledamo kot končno razsežne vektorske prostore.

Definicija 2.1. *Algebraično številsko polje K je končna razširitev polja $\mathbb{Q}$.*

Vsaka končna razširitev polja $\mathbb{Q}$ je enostavna. Tako so $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\zeta_n)$ in $\mathbb{Q}(\sqrt{-5})$ primeri algebraičnih številskih polj. Algebraično številsko polje K je kot končna razširitev tudi algebraična. Vsak $\alpha \in K$ tako zadošča $\alpha^n + a_1\alpha^{n-1} + \dots + a_n = 0$ za neki $n \in \mathbb{N}$ in neke $a_1, \dots, a_n \in \mathbb{Q}$. V naši obravnavi bodo pomembni vsi tisti $\alpha \in K$, pri katerih velja $a_1, \dots, a_n \in \mathbb{Z}$.

Definicija 2.2. Pravimo, da je $\alpha \in \mathbb{C}$ *algebraično celo število*, če je ničla kakega eničnega polinoma s celoštevilskimi koeficienti.

Opomba 2.1. V zgornji definiciji ne zahtevamo, da je polinom nerazcepen. Se pa izkaže, da ima eničen nerazcepen polinom nad $\mathbb{Q}$, katerega ničla je algebraično celo število α , celoštevilске koeficiente.

Zgled 2.1. V $\mathbb{Q}(\sqrt{-5})$ je $1 - \sqrt{-5}$ algebraično celo število, saj je ničla polinoma $x^2 - 2x + 6$. Sedaj probamo poiskati vsa algebraična cela števila v $\mathbb{Q}(\sqrt{-5})$. Vsak $\alpha \in \mathbb{Q}(\sqrt{-5})$ je oblike $p + q\sqrt{-5}$ za $q \neq 0$ ter $p, q \in \mathbb{Q}$. Ta element je ničla polinoma $x^2 - 2px + p^2 + 5q^2$, ki je nerazcepen nad $\mathbb{Q}$. Po opombi 2.1 je α algebraično celo število natanko takrat, ko $2p \in \mathbb{Z}$ in $p^2 + 5q^2 \in \mathbb{Z}$. Slednje je izpolnjeno natanko takrat, ko $p, q \in \mathbb{Z}$. Tako je množica algebraičnih celih števil polja $\mathbb{Q}(\sqrt{-5})$ enaka kolobarju $\mathbb{Z}[\sqrt{-5}]$.

Ali tudi v splošnem algebraična cela števila tvorijo kolobar? Pri odgovoru na to vprašanje nam pomaga naslednja trditev. Dokaz lahko bralec najde v [4].

Trditev 2.1. *Naj bo $\alpha \in \mathbb{C}$. Naslednje trditve so ekvivalentne:*

- (1) α je algebraično celo število;
- (2) aditivna grupa kolobarja $\mathbb{Z}[\alpha]$ je končno generirana;
- (3) α je element podkolobarja $\mathbb{C}$, ki ima končno generirano aditivno grupo.

Vzemimo poljubni algebraični celi števili $\alpha, \beta \in K$. Kolobar $\mathbb{Z}[\alpha, \beta]$ ima končno generirano aditivno grupo, saj jo po trditvi 2.1 imata tudi $\mathbb{Z}[\alpha]$ in $\mathbb{Z}[\beta]$. Potem sta $\alpha + \beta$ in $\alpha\beta$ algebraični celi števili, ker sta elementa kolobarja $\mathbb{Z}[\alpha, \beta]$. Tako vidimo, da algebraična cela števila polja K tvorijo kolobar, ki mu pravimo *celoštevilski kolobar* in ga označimo z $\mathcal{O}_K$.

3. FAKTORIZACIJA IDEALOV CELOŠTEVILSKEGA KOLOBARJA

Izkaže se, da lahko vsak element kolobarja $\mathcal{O}_K$ zapišemo kot produkt nerazcepnih elementov, vendar enoličnost zapisa v splošnem ni zagotovljena. Na primer, v $\mathbb{Z}[\sqrt{-5}]$ velja $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$. Kljub temu imamo v algebraičnih številskih poljih znano posebnost.

Definicija 3.1. *Dedekindova domena* R je cel kolobar, ki je integralno zaprt v svojem polju ulomkov, vsak njegov ideal je končno generiran in vsak njegov neničeln praideal je maksimalen ideal.

Kolobar $\mathcal{O}_K$ je Dedekindova domena. Dokaz tega dejstva si bralec lahko ogleda v [4]. Naslednja trditev tako zagotavlja enolično faktorizacijo idealov v $\mathcal{O}_K$.

Izrek 3.1 (Osnovni izrek teorije idealov). *Naj bo R Dedekindova domena. Vsak neničeln, pravi ideal I kolobarja R lahko zapišemo kot produkt neničelnih praidealov. Ta zapis je enoličen do vrstnega reda faktorjev natančno.*

Zgled 3.1. V $\mathbb{Z}[\sqrt{-5}]$ je $(21) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})(7, 3 + \sqrt{-5})(7, 3 - \sqrt{-5})$.

Pomembno je razumeti, zakaj nam enolična faktorizacija idealov pomaga pri obravnavi enolične faktorizacije elementov. Iz $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$ v $\mathbb{Z}[\sqrt{-5}]$ vidimo, da 3 deli produkt na desni strani, vendar ne deli nobenega izmed faktorjev tega produkta v $\mathbb{Z}[\sqrt{-5}]$. Račun pokaže, da je

$$1 + 2\sqrt{-5} = \sqrt{\kappa}\sqrt{-\gamma}, \quad 1 - 2\sqrt{-5} = \sqrt{\kappa}\sqrt{-\gamma}, \quad 3 = \sqrt{\kappa}\sqrt{\kappa}, \quad 7 = \sqrt{\gamma}\sqrt{\gamma},$$

kjer smo označili $\kappa = 2 + \sqrt{-5}$ in $\gamma = 2 + 3\sqrt{-5}$. Vidimo, da 21 lahko enolično faktoriziramo kot

$$21 = \sqrt{\kappa}\sqrt{\kappa}\sqrt{-\gamma}\sqrt{-\gamma},$$

vendar ne v $\mathbb{Z}[\sqrt{-5}]$. Zgornji faktorji namreč niso elementi $\mathbb{Z}[\sqrt{-5}]$. Tu se pojavi ideja, da takšne faktorje dodamo v algebraično številsko polje K . Izkaže se, da za dani faktor množico vseh algebraičnih celih števil iz K , ki so deljiva s tem faktorjem, identificiramo z idealom kolobarja $\mathcal{O}_K$. Zanima nas, koliko teh faktorjev bi bilo treba dodati, da dobimo enolično faktorizacijo v algebraičnem številskega polju K . Konstruirali bomo grupo, ki nam bo pri tem pomagala.

4. GRUPA RAZREDOV

Definicija 4.1. *Ulomljeni ideal* Dedekindove domene R je neničeln R -podmodul I polja ulomkov domene R za katerega velja, da je $rI \subset R$ za nek neničeln $r \in R$.

Za algebraično številsko polje K označimo množico vseh ulomljenih idealov z $\mathcal{I}_K$. Na $\mathcal{I}_K$ definiramo ekvivalenčno relacijo $\sim$ na naslednji način:

$$I \sim J \Leftrightarrow \text{obstaja neničeln } \alpha \in \mathcal{O}_K, \text{ da velja } I = (\alpha)J.$$

Množica ekvivalenčnih razredov $\mathcal{I}_K / \sim$ postane abelova grupa, če definiramo operacijo $[I] + [J] := [IJ]$. Enota za dano operacijo je razred glavnih idealov $\mathcal{P}_K$. Z obstojem inverzov ni težav. Za Dedekindove domene se namreč izkaže, da za poljuben ideal I obstaja tak ideal J , da je ideal IJ glavní.

Definicija 4.2. Abelovo grupo $\mathcal{I}_K / \sim$ imenujemo *grupa razredov algebraičnega številskega polja K* . Označimo jo s Cl_K .

S pomočjo grupe razredov algebraičnega številskega polja K bomo določili, do kakšne mere enolična faktorizacija ne drži v K .

Trditev 4.1. *Grupa Cl_K je končna.*

Dokaz lahko bralec najde v [3]. Red te grupe, ki ga označimo s h_K , se imenuje *število razredov algebraičnega številskega polja K* . V delu obravnavamo algebraična številska polja K , za katera je h_K enak 1 ali 2. V nadaljevanju si ogledamo, kaj majhno število razredov h_K pove o faktorizaciji elementov polja K .

5. O ENOLIČNI FAKTORIZACIJI IN MAJHNEM ŠTEVILU RAZREDOV

Omenili smo že, da z obstojem faktorizacije v K ni težav. S pomočjo izreka 3.1 dobimo pomemben rezultat o enoličnosti. O tem si bralec lahko več prebere v [3].

Izrek 5.1. *V algebraičnem številskega polju K je faktorizacija enolična (do vrstnega reda in asociiranosti faktorjev natančno) natanko takrat, ko so vsi ideali $\mathcal{O}_K$ glavni.*

Opazimo, da ima grupa razredov algebraičnega številskega polja K le en element natanko takrat, ko so vsi ideali kolobarja $\mathcal{O}_K$ glavni.

Posledica 5.1. *V algebraičnem številskega polju K je faktorizacija elementov enolična natanko takrat, ko je $h_K = 1$.*

Opomba 5.1. Za algebraično številskega polje $\mathbb{Q}$ je pripadajoči celoštevilski kolobar $\mathbb{Z}$. Vemo, da so vsi ideali kolobarja $\mathbb{Z}$ glavni. Posledica tega je enoličnost faktorizacije celih števil.

Še nekateri primeri algebraičnih številskega polj, katerih število razredov je enako 1, so $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{-3})$ in $\mathbb{Q}(\sqrt{5})$. Videli smo, da v $\mathbb{Q}(\sqrt{-5})$ enolične faktorizacije ni. Primer ideala, ki ni glavni, je $(2, 1 + \sqrt{-5})$. Izkaže se, da $\mathbb{Q}(\sqrt{-5})$ ni daleč od enolične faktorizacije. Število razredov tega polja je namreč enako 2. Lahko se vprašamo, če obstaja kakšna značilnost za polja s številom razredov, ki je enako 2. V ta namen predstavimo naslednji primer:

Zgled 5.1. Ogledamo si vse različne faktorizacije števila 21 v $\mathbb{Q}(\sqrt{-5})$. Označimo

$$\mathfrak{p}_1 = (3, 1 + \sqrt{-5}), \quad \mathfrak{p}_2 = (3, 1 - \sqrt{-5}), \quad \mathfrak{p}_3 = (7, 3 + \sqrt{-5}), \quad \mathfrak{p}_4 = (7, 3 - \sqrt{-5}).$$

Vemo, da je $(21) = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3 \cdot \mathfrak{p}_4$. Produkt poljubnih dveh idealov iz tega zapisa je glavni ideal. Z različnimi kombinacijami množenja dobimo

$$(21) = (\mathfrak{p}_1 \cdot \mathfrak{p}_2)(\mathfrak{p}_3 \cdot \mathfrak{p}_4) = (\mathfrak{p}_1 \cdot \mathfrak{p}_3)(\mathfrak{p}_2 \cdot \mathfrak{p}_4) = (\mathfrak{p}_1 \cdot \mathfrak{p}_4)(\mathfrak{p}_2 \cdot \mathfrak{p}_3).$$

Tako dobimo tri različne faktorizacije, od katerih je vsaka dolžine 2:

$$21 = 3 \cdot 7 = (1 - 2\sqrt{-5})(1 + 2\sqrt{-5}) = (4 + \sqrt{-5})(4 - \sqrt{-5}).$$

V tem primeru smo videli, da je bila dolžina poljubne faktorizacije za konkreten element fiksno število. Ameriški matematik Leonard Carlitz (1907–1999) je pokazal, da je to značilnost algebraičnih številskega polj z majhnim številom razredov.

6. CARLITZOV IZREK

Sedaj predstavimo karakterizacijo nerazcepnih elementov kolobarja $\mathcal{O}_K$ s pomočjo grupe razredov Cl_K . Dokaz lahko bralec najde v [2].

Lema 6.1. *Naj za neničeln $\alpha \in \mathcal{O}_K$, ki ni obrnljiv, velja $(\alpha) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ za $n \geq 1$, kjer so $\mathfrak{p}_i$ ne nujno različni praideali kolobarja $\mathcal{O}_K$. Velja, da je α nerazcepen element kolobarja $\mathcal{O}_K$ natanko takrat, ko je $\sum_{i=1}^n [\mathfrak{p}_i]$ in je vsaka prava podvota te vsote neničelna.*

V nadaljevanju si ogledamo, kaj nam slednji rezultat pove za algebraično številsko polje K s številom razredov $h_K = 2$.

Posledica 6.1. *Naj za algebraično številsko polje K velja $h_K = 2$. Za poljuben nerazcepen element $\alpha \in \mathcal{O}_K$ velja ena izmed treh možnosti:*

- (1) $(\alpha) = \mathfrak{p}$, kjer je $\mathfrak{p}$ praideal kolobarja $\mathcal{O}_K$, ki je glavni;
- (2) $(\alpha) = \mathfrak{p}^2$, kjer je $\mathfrak{p}$ praideal kolobarja $\mathcal{O}_K$, ki ni glavni;
- (3) $(\alpha) = \mathfrak{p}\mathfrak{q}$, kjer sta $\mathfrak{p}$ in $\mathfrak{q}$ različna praidealna kolobarja $\mathcal{O}_K$, ki nista glavna.

Opomba 6.1. Slednje izhaja iz dejstva, da za praideal $\mathfrak{p}$ kolobarja $\mathcal{O}_K$, ki ni glavni, velja $\mathfrak{p}^n = (\alpha)$, kjer je n moč razreda $[\mathfrak{p}]$ v Cl_K in $\alpha \in \mathcal{O}_K$ nerazcepen. Za poljuben praideal $\mathfrak{q}$ iz razreda $-[\mathfrak{p}]$ velja $\mathfrak{p}\mathfrak{q} = (\alpha)$, kjer je $\alpha \in \mathcal{O}_K$ nerazcepen element.

Tako smo prišli do napovedane karakterizacije številskih polj z majhnim številom razredov, ki je bila predstavljena leta 1959.

Izrek 6.1 (Carlitzov izrek). *Naj bo $\alpha \in \mathcal{O}_K$ neničeln. Število razredov h_K je največ 2 natanko takrat, ko je število nerazcepnih elementov v poljubni faktorizaciji elementa α odvisno le od α .*

Opomba 6.2. Natančneje, za poljubne $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m \in \mathcal{O}_K$, ki zadoščajo $\alpha_1 \dots \alpha_n = \beta_1 \dots \beta_m$, velja $n = m$.

Dokaz. ($\Rightarrow$) Za primer $h_K = 1$ je očitno. Naj bo $h_K = 2$. Pokažimo, da je dolžina poljubne faktorizacije elementa α odvisna le od α . Ideal (α) lahko predstavimo kot

$$(\alpha) = \mathfrak{p}_1 \cdots \mathfrak{p}_s \mathfrak{q}_1 \cdots \mathfrak{q}_t,$$

kjer so $\mathfrak{p}_i$ za $i \in \{1, \dots, s\}$ glavni ideali in $\mathfrak{q}_j$ za $j \in \{1, \dots, t\}$ ideali, ki niso glavni. Iz posledice 6.1 sledi, da je $\mathfrak{q}_i \mathfrak{q}_j = (\pi_{i,j})$ za $i, j \in \{1, \dots, t\}$. Zato je t sodo število. Poljubna faktorizacija elementa α je tako oblike

$$\alpha = u \mathfrak{p}_1 \cdots \mathfrak{p}_s (\pi_{1,2}) \cdots (\pi_{t-1,t}),$$

kjer je u obrnljiv element. Dolžina te faktorizacije je $s + \frac{t}{2}$ in je odvisna le od α . ($\Leftarrow$) Denimo, da je $h_K > 2$. Radi bi pokazali, da dolžina faktorizacije konkretnega elementa ni fiksno število. Ločimo dva primera:

Denimo, da Cl_K vsebuje element $[I]$ reda $n > 2$. Po opombi 6.1 za praideal $\mathfrak{p} \in [I]$ velja $\mathfrak{p}^n = (\pi_1)$. Če je $\mathfrak{q}$ praideal iz $-[I]$, potem je $\mathfrak{q}^n = (\pi_2)$. Vemo tudi, da je $\mathfrak{p}\mathfrak{q} = (\pi_3)$. Poudarimo, da so π_i nerazcepni elementi kolobarja $\mathcal{O}_K$. Tako je

$$\pi_1 \pi_2 = u \pi_3^n,$$

kjer je u obrnljiv element. Dolžina faktorizacije na levi strani enakosti je 2, na desni pa $n > 2$.

Denimo, da so v Cl_K vsi elementi (z izjemo enote) reda 2. Vzemimo dva različna elementa $[I]$ in $[J]$, ki imata red 2. Tudi element $[I] + [J] = [IJ]$ ima red 2. Naj bodo $\mathfrak{p}_1 \in [I]$, $\mathfrak{p}_2 \in [J]$, $\mathfrak{p}_3 \in [IJ]$ praideali. Po opombi 6.1 velja

$$\mathfrak{p}_1^2 = (\pi_1), \quad \mathfrak{p}_2^2 = (\pi_2), \quad \mathfrak{p}_3^2 = (\pi_3), \quad \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 = (\pi_4),$$

kjer so π_i nerazcepni elementi kolobarja $\mathcal{O}_K$. Tako je

$$\pi_1 \pi_2 \pi_3 = u \pi_4^2,$$

kjer je u obrnljiv element. Dolžina faktorizacije na levi strani enakosti je 3, na desni strani pa 2. $\square$

Opomba 6.3. V dokazu smo uporabili dejstvo, da vsak element grupe razredov vsebuje neskončno mnogo praidealov.

V delu diplomskega seminarja bomo predstavili še nekatere karakterizacije algebrainih številskih polj z majhnim številom razredov.

7. PRIMER UPORABE

Znameniti Fermatov veliki izrek, ki pravi, da ne obstaja celoštevilsko rešitev enačbe $x^p + y^p = z^p$ za neničelne x, y, z in $n > 2$, je motiviral razvoj algebrainne teorije števil. Znan je kot problem z največjim številom neuspešnih dokazov. Francoski matematik Gabriel Lamé (1795–1870) je leta 1847 trdil, da dokaz sledi iz

$$x^p = z^p - y^p = \prod_{n=0}^{p-1} (z - \zeta^n y),$$

kjer je $\zeta = e^{\frac{2\pi i}{p}}$, vendar ta sklep ni bil pravilen. Tu enolična faktorizacija namreč ni zagotovljena, saj za algebraino številsko polje $\mathbb{Q}(\zeta)$ število razredov v splošnem ni enako 1. Primeri, ko je število razredov enako 1, so omogočili iskanje vrednosti p , za katere Fermatov veliki izrek drži. Kot zanimivost omenimo, da je avtor v [4] komentiral, da dokaza ni poznala nobena oseba, ki je živela v času pisanja njegove knjige. Izkazalo se je, da tudi to ni bilo povsem res. Manj kot 20 let kasneje, Fermatov veliki izrek je končno dobil svoj dokaz.

LITERATURA

- [1] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. 11: 391–392, 1960.
- [2] S. T. Chapman, *So what is class number 2?*, Amer. Math. Monthly **126** (2019), 330–339.
- [3] H. Diamond, H. Pollard, *The Theory of Algebraic Numbers*, Mathematical Association of America, Washington, DC, 1950.
- [4] D. A. Marcus, *Number Fields*, Springer, New York, 1977.