

МАТЕМАТИЧКА ГИМНАЗИЈА

МАТУРСКИ РАД
ИЗ МАТЕМАТИКЕ

Квадратна раширења рационалних бројева

Ученик

Огњен Нишкић, IVд

Ментор

др Стеван Гајовић

Београд, 27. мај 2026.

Садржај

1	Увод	1
2	Квадратна раширења	3
2.1	Неопходни појмови из алгебре	3
2.2	Поље $\mathbb{Q}[\sqrt{D}]$	4
2.3	Прстен целих бројева $\mathcal{O}$	6
2.4	Факторизација елемената у $\mathcal{O}$	8
2.5	Дискриминанта поља	11
2.6	Јединствена факторизација елемената	13
3	Идеали квадратних раширења	15
3.1	Дефиниција и основна својства идеала	15
3.2	Операције над идеалима	18
3.3	Максимални и прости идеали	20
3.4	Стандардна форма и норма идеала	23
4	Класна група идеала	29
4.1	Разломачки идеали	29
4.2	Класна група $\text{Cl}(F)$	31
5	Примена	37
5.1	Задатак $n^2 + n + 41$	37
	Литература	39

1

Увод

Теорија бројева представља једну од најстаријих и најзначајнијих грана математике. Још од античких времена, математичаре је занимала дељивост целих бројева, прости бројеви као и решавање диофантових једначина. Развојем и напретком алгебре, дефинисане су нове структуре и методе које су омогућиле дубље разумевање простих бројева, као и ефикасније решавање диофантових једначина. Између осталих, уведен је и појам алгебарских раширења. Најједноставнији, али и најважнији пример алгебарских раширења су квадратна раширења рационалних бројева.

Под квадратним раширењима рационалних бројева подразумевамо скуп $\mathbb{Q}[\sqrt{D}]$, за неки бесквдратан цео број D , који садржи све бројеве облика $a + b\sqrt{D}$, где су a и b рационални бројеви. Идеја увођења скупа $\mathbb{Q}[\sqrt{D}]$ је општији приступ проблемима којима није адекватно приступити искључиво рационалним бројевима. У другом поглављу овог рада ћемо дефинисати прецизно шта представљају цели и прости бројеви у раширењу, као и смисао дељивости и факторизације његових целобројних елемената.

Једна од примена квадратних раширења се огледа у доприносу при доказивања Велике Фермаове теореме за случај $n = 3$, која тврди да за било који природан број $n > 2$ не постоје цели бројеви x, y, z такви да важи: $x^n + y^n = z^n$.

Током рада на доказивању ове теореме, математичари су приметили да постоји пропуст у приступу. Наиме, претпостављено је да у сваком алгебарском раширењу рационалних бројева важи јединствена факторизација целих елемената на просте, што се касније показало погрешним. Управо ова грешка је мотивисала увођење нових алгебарских појмова у математику, као што су идеали и класне групе, који ће јасније дефинисати овај проблем и отклонити га у одређеној мери, о којима ће бити речи у поглављима 3 и 4.

У последњем поглављу ћемо на конкретном задатку показати примену квадратних раширења рационалних бројева.

Желео бих искрено да се захвалим ментору, др Стевану Гајовићу, на предлогу теме за рад, као и на великом ангажовању и помоћи током израде овог рада. Посебну захвалност дугујем на издвојеном времену, корисним саветима и указаној подршци, упркос одсуству из земље и бројним обавезама.

2

Квадратна раширења

2.1 Неопходни појмови из алгебре

Главна тема овог рада су квадратна раширења као и њихов прстен целих бројева који ћемо дефинисати за свако раширење. Неопходно је пре свега да се упознамо са појмовима прстен и поље, као и са својствима која они испуњавају.

Дефиниција 2.1. Поље је уређена тројка $(F, +, \cdot)$ таква да је:

- (1) F непразан скуп са две бинарне операције $+, \cdot : F \times F \rightarrow F$
- (2) $(F, +)$ је Абелова група (сабирање)
- (3) $(F \setminus \{0\}, \cdot)$ је Абелова група (множење)
- (4) Важи дистрибутивност $\cdot$ према $+$:

$$(\forall x, y, z \in F) (x + y) \cdot z = xz + yz.$$

Услов (2) значи да је задовољено следећих 5 услова:

- (2.1) Затвореност према сабирању: $\forall a, b \in F, a + b \in F$
- (2.2) Асоцијативност: $\forall a, b, c \in F, (a + b) + c = a + (b + c)$
- (2.3) Неутрал за сабирање: $0 \in F, a + 0 = 0 + a = a \quad \forall a \in F$
- (2.4) Инверзни елемент: $\forall a \in F, \exists (-a), a + (-a) = 0$
- (2.5) Комутативност: $\forall a, b \in F, a + b = b + a.$

Услов (3) значи да је задовољено следећих 5 услова:

- (3.1) Затвореност према множењу: $\forall a, b \in F, a \cdot b \in F$
- (3.2) Асоцијативност: $\forall a, b, c \in F, (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(3.3) Неутрал за множење: $1 \in F, a \cdot 1 = 1 \cdot a = a \quad \forall a \in F$

(3.4) Инверзни елемент: $\forall a \in F, \exists a^{-1}, aa^{-1} = 1$

(3.5) Комутативност: $\forall a, b \in F, a \cdot b = b \cdot a.$

Неопходно је напоменути и да мултипликативни неутрал и адитивни неутрал нису исти елемент: $1 \neq 0$.

Дефиниција 2.2. Прстен је уређена тројка $(R, +, \cdot)$ таква да је:

- (1) R непразан скуп са две бинарне операције $+, \cdot : R \times R \rightarrow R$
- (2) $(R, +)$ је Абелова група (сабирање)
- (3) Множење $(\cdot)$ је асоцијативно
- (4) Важи дистрибутивност $\cdot$ према $+$:

$$(\forall x, y, z \in R) (x + y) \cdot z = xz + yz.$$

Услови (1), (2) и (4) су идентични као и код поља, једина разлика је у томе што услов (3) подразумева само прве две ставке, а не свих 5:

(3.1) Затвореност према множењу: $\forall a, b \in R, a \cdot b \in R$

(3.2) Асоцијативност: $\forall a, b, c \in R, (a \cdot b) \cdot c = a \cdot (b \cdot c).$

Дефиниција 2.3. Комутативни прстен са јединицом је прстен који задовољава додатна 2 својства:

(3.3) Неутрал за множење: $1 \in R, a \cdot 1 = a \quad \forall a \in R$

(3.5) Комутативност: $\forall a, b \in R, a \cdot b = b \cdot a.$

Дакле можемо приметити да је једина разлика између комутативног прстена са јединицом и поља што поље задовољава својство (3.4), односно да сваки елемент различит од нуле има мултипликативни инверз, док се у прстену то не захтева.

За даље потребе рада сматраћемо да је сваки прстен који користимо комутативни прстен са јединицом.

2.2 Поље $\mathbb{Q}[\sqrt{D}]$

Дефиниција 2.4. Поље

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

где је $D \in \mathbb{Z}$ и $\sqrt{D} \notin \mathbb{Q}$, називамо **квадратним раширењем рационалних бројева**. Ако је $D > 0$ поље је **реално**, а ако је $D < 0$ поље је **имагинарно**.

Квадратно раширење $\mathbb{Q}[\sqrt{D}]$ заиста јесте увек поље. Затворено је за сабирање:

$$(a + b\sqrt{D}) \pm (c + d\sqrt{D}) = (a \pm c) + (b \pm d)\sqrt{D} \in \mathbb{Q}[\sqrt{D}],$$

као и за множење:

$$(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D} \in \mathbb{Q}[\sqrt{D}],$$

а инверз за множење елемента $\alpha = a + b\sqrt{D} \in \mathbb{Q}[\sqrt{D}] \setminus \{0\}$ је елемент:

$$\begin{aligned} \frac{1}{a + b\sqrt{D}} &= \frac{a - b\sqrt{D}}{(a + b\sqrt{D})(a - b\sqrt{D})} = \frac{a - b\sqrt{D}}{a^2 - b^2D} = \\ &= \frac{a}{a^2 - b^2D} + \frac{b}{a^2 - b^2D}\sqrt{D} \in \mathbb{Q}[\sqrt{D}] \setminus \{0\}. \end{aligned}$$

(Напомена: елемент α је једнак нули ако и само ако је $a = b = 0$. Како то није случај, то ни производ $(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2D$ није нула, па су $\frac{a}{a^2 - b^2D}$ и $\frac{b}{a^2 - b^2D}$ рационални бројеви, те је за сваки ненула елемент раширења његов инверзни елемент такође у раширењу).

Даље, сматраћемо да је D бесквадратан. За елемент кажемо да је **бесквадратан** уколико за сваки прост број $p \mid D$ важи $p^2 \nmid D$. Ову претпоставку узимамо из практичних разлога.

Ако би било $D' = n^2D$ за неки природан број n , тада би

$$\begin{aligned} \mathbb{Q}[\sqrt{D'}] &= \{a + b\sqrt{D'} \mid a, b \in \mathbb{Q}\} = \{a + bn\sqrt{D} \mid a, b \in \mathbb{Q}\} = \\ &= \{a + b_1\sqrt{D} \mid a, b_1 \in \mathbb{Q}\} = \mathbb{Q}[\sqrt{D}], \end{aligned}$$

те смо показали да је заправо $\mathbb{Q}[\sqrt{D'}] = \mathbb{Q}[\sqrt{D}]$.

Дефиниција 2.5. За елемент $\alpha = a + b\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$ дефинишемо његов **конјугат**: $\bar{\alpha} = a - b\sqrt{D}$.

Операција конјуговања пролази кроз сабирање, одузимање, множење и дељење. Такође, када два пута конјугујемо елемент, он остаје исти.

Дефиниција 2.6. **Норма** елемента α је рационалан број $N\alpha$:

$$N\alpha = \alpha \cdot \bar{\alpha} = (a + b\sqrt{D})(a - \sqrt{D}) = a^2 - b^2D.$$

Дефиниција 2.7. **Траг** елемента α је рационалан број $\text{Tr}\alpha$:

$$\text{Tr}\alpha = \alpha + \bar{\alpha} = 2a.$$

2.3 Прстен целих бројева $\mathcal{O}$

У пољу $\mathbb{Q}[\sqrt{D}]$ дефинисаћемо целе бројеве, као што су цели бројеви дефинисани у скупу рационалних бројева $\mathbb{Q} \supset \mathbb{Z}$.

Дефиниција 2.8. У пољу $\mathbb{Q}[\sqrt{D}]$ дефинишемо прстен целих бројева

$$\mathcal{O} = \{ \alpha \in \mathbb{Q}[\sqrt{D}] \mid \alpha^2 - t\alpha + n = 0 \text{ за неке } n, t \in \mathbb{Z} \}.$$

Другим речима, прстен целих бројева је скуп свих елемената из $\mathbb{Q}[\sqrt{D}]$ који су нуле неког моничног полинома другог степена.

Теорема 2.1. За свако $\alpha \in \mathbb{Q}[\sqrt{D}] \setminus \mathbb{Q}$, $p(\alpha) = 0$ је нула моничног полинома другог степена са рационалним коефицијентима $p(x) = (x - \alpha)(x - \bar{\alpha})$.

Доказ. Како је у питању полином другог степена, по основној теорему алгебре постоје тачно две нуле, прва нула је α , другу назовимо β . Полином $p(x)$ онда можемо записати као $p(x) = (x - \alpha)(x - \beta)$ јер знамо да је моничан. Множењем заграда, уз услов да је $\alpha = a + b\sqrt{D}$, $a, b \in \mathbb{Q}$, добијамо:

$$p(x) = (x - \alpha)(x - \beta) = x^2 - x(a + b\sqrt{D} + \beta) + \beta(a + b\sqrt{D})$$

Како коефицијенти полинома морају бити рационални бројеви, из коефицијента уз x добијамо да β мора бити облика $\beta = c - b\sqrt{D}$, за неко $c \in \mathbb{Q}$.

Слободан члан полинома такође мора бити рационалан:

$$\beta(a + b\sqrt{D}) = (c - b\sqrt{D})(a + b\sqrt{D}) = (ac - b^2D) + b\sqrt{D}(c - a) \in \mathbb{Q}$$

одакле добијамо $c = a$. Следи да је $\beta = a - b\sqrt{D} = \bar{\alpha}$. □

Последица 1. Елемент $\alpha \in \mathbb{Q}[\sqrt{D}] \setminus \mathbb{Q}$ је нула моничног полинома

$$p(x) = (x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha} = x^2 - (\text{Tr}\alpha)x + N\alpha.$$

Последица 2. Прстен целих бројева $\mathcal{O}$ можемо представити и у облику:

$$\mathcal{O} = \{ \alpha \in \mathbb{Q}[\sqrt{D}] \mid \text{Tr}\alpha, N\alpha \in \mathbb{Z} \}.$$

Погледајмо сада какав експлицитан облик узима прстен целих бројева $\mathcal{O}$ у пољу $\mathbb{Q}[\sqrt{D}]$:

Теорема 2.2. Прстен целих бројева $\mathcal{O}$ у пољу $\mathbb{Q}[\sqrt{D}]$ може бити искључиво облика $\mathcal{O} = \mathbb{Z}[\delta_0] = \mathbb{Z} + \mathbb{Z}\delta_0$, где је

$$\delta_0 = \begin{cases} \sqrt{D}, & \text{за } D \equiv 2, 3 \pmod{4} \\ \frac{1+\sqrt{D}}{2}, & \text{за } D \equiv 1 \pmod{4}. \end{cases}$$

Доказ. Треба показати:

$$\mathcal{O} \subseteq \mathbb{Z}[\delta_0] \quad \text{и} \quad \mathcal{O} \supseteq \mathbb{Z}[\delta_0].$$

Најпре ћемо показати $\mathcal{O} \supseteq \mathbb{Z}[\delta_0]$:

Раздвајамо два случаја:

1) $\delta_0 = \sqrt{D}$

Нека је $\alpha = a + b\sqrt{D}$, $a, b \in \mathbb{Z}$. Тада

$$\text{Tr}(\alpha) = 2a \in \mathbb{Z}, \quad \text{N}(\alpha) = a^2 - b^2D \in \mathbb{Z},$$

па је $\alpha \in \mathcal{O}$, тј.

$$\mathbb{Z}[\sqrt{D}] \subseteq \mathcal{O}.$$

2) $\delta_0 = \frac{1+\sqrt{D}}{2}$

Нека је $\alpha = a + b\frac{1+\sqrt{D}}{2}$, $a, b \in \mathbb{Z}$. Тада

$$\text{Tr}(\alpha) = 2a + b \in \mathbb{Z}, \quad \text{N}(\alpha) = \left(\frac{2a+b}{2}\right)^2 - \frac{b^2D}{4}.$$

Ако је $2 \mid b$, директно следи $\text{N}(\alpha) \in \mathbb{Z}$.

Ако је $2 \nmid b$, тада $(2a+b)^2 \equiv 1 \pmod{4}$ и $b^2 \equiv 1 \pmod{4}$ па

$$\text{N}(\alpha) \in \mathbb{Z} \iff 4 \mid (2a+b)^2 - b^2D \iff D \equiv 1 \pmod{4},$$

па је $\alpha \in \mathcal{O}$ када $D \equiv 1 \pmod{4}$, тј.

$$\mathbb{Z}[\delta_0] \subseteq \mathcal{O} \text{ када } D \equiv 1 \pmod{4}.$$

Остало је још прокоментарисати да је : $\mathbb{Z}[\sqrt{D}] \subseteq \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ када $D \equiv 1 \pmod{4}$:

$$a + b\sqrt{D} = (a - b) + 2b\frac{1 + \sqrt{D}}{2} \in \mathbb{Z}\left[\frac{1 + \sqrt{D}}{2}\right],$$

те директно добијамо

$$\mathbb{Z}[\sqrt{D}] \subseteq \mathbb{Z}\left[\frac{1 + \sqrt{D}}{2}\right].$$

Сада ћемо показати да је $\mathcal{O} \subseteq \mathbb{Z}[\delta_0]$:

Нека је $\alpha = a + b\sqrt{D} \in \mathcal{O}$, где $a, b \in \mathbb{Q}$. Због $\text{Tr } \alpha = 2a \in \mathbb{Z}$ следи да је $a = \frac{r}{2}$ за неко $r \in \mathbb{Z}$.

Нека је $b = \frac{m}{n}$, $(m, n) = 1 \Rightarrow N\alpha = a^2 - b^2D = \frac{r^2}{4} - \frac{m^2}{n^2}D$. Добијамо:

$$4m^2D = n^2(r^2 - 4N\alpha) \Rightarrow n^2 \mid 4D \text{ јер је } (m, n) = 1,$$

$n^2 \nmid D$ јер је D бесквадратан, највише n може делити D , па n мора делити 4. Ако је $n = 4 \Rightarrow 16 \mid 4D \Rightarrow 4 \mid D$ што је контрадикција.

Дакле $n \in \{1, 2\} \Rightarrow b = \frac{m}{n} = \frac{s}{2}$ за неко $s \in \mathbb{Z}$. Вратимо се сада поново на израз за норму:

$$a^2 - b^2D \in \mathbb{Z} \Rightarrow \frac{r^2}{4} - \frac{s^2}{4}D \in \mathbb{Z} \Rightarrow \frac{1}{4}(r^2 - s^2D) \in \mathbb{Z} \Rightarrow r^2 \equiv s^2D \pmod{4}.$$

1) $D \not\equiv 1 \pmod{4}$

$\Rightarrow r^2 \equiv s^2 \equiv 0 \pmod{4}$ јер $t^2 \in \{0, 1\} \pmod{4} \Rightarrow 2 \mid r, 2 \mid s \Rightarrow a, b \in \mathbb{Z} \Rightarrow a + b\sqrt{D} \in \mathbb{Z}[\delta_0]$, где је $\delta_0 = \sqrt{D}$,

$$\Rightarrow \mathcal{O} \subseteq \mathbb{Z}[\delta_0] \text{ где је } \delta_0 = \sqrt{D}, D \equiv 2, 3 \pmod{4}.$$

2) $D \equiv 1 \pmod{4}$

$\Rightarrow r^2 \equiv s^2 \pmod{4} \Rightarrow r \equiv s \pmod{2}$. Нека је онда $r = s + 2k$, $k \in \mathbb{Z}$

$$\alpha = a + b\sqrt{D} = \frac{r}{2} + \frac{s}{2}\sqrt{D} = \frac{s + 2k}{2} + \frac{s}{2}\sqrt{D} = k + s\frac{1 + \sqrt{D}}{2}, k, s \in \mathbb{Z},$$

$$\Rightarrow \mathcal{O} \subseteq \mathbb{Z}[\delta_0] \text{ где је } \delta_0 = \frac{1 + \sqrt{D}}{2}, D \equiv 1 \pmod{4}.$$

□

Сада када смо дефинисали структуру прстена целих бројева, природно је и да дефинишемо неку врсту факторизације његових елемената.

2.4 Факторизација елемената у $\mathcal{O}$

Када причамо о факторизацији елемената у $\mathcal{O}$, важну улогу нам игра норма еленента, као и појмови које ћемо дефинисати у наставку овог дела.

Теорема 2.3. Норма од производа два елемента једнака је производу норми елемената: $N(\alpha\beta) = (N\alpha)(N\beta)$.

Доказ. $N(\alpha\beta) = (\alpha\beta)(\overline{\alpha\beta}) = \alpha\bar{\alpha}\beta\bar{\beta} = (N\alpha)(N\beta)$.

□

Када смо говорили о пољу $\mathbb{Q}[\sqrt{D}]$ нисмо посебно помињали инвертибилне елементе, јер су у сваком пољу сви ненула елементи инвертибилни. Са друге стране, у прстену целих бројева, инвертибилних елемената је знатно мање и имају веома важну улогу у факторизацији елемената.

Дефиниција 2.9. $\epsilon \in \mathbb{Z}[\delta_0]$ је **инвертибилни елемент** ако и само ако постоји елемент $\epsilon' \in \mathbb{Z}[\delta_0]$ такав да је $\epsilon\epsilon' = 1$. Скуп свих инвертибилних елемената означавамо са $\mathbb{Z}[\delta_0]^\times$.

Пример инвертибилног елемента који се налази у сваком квадратном раширењу је $\epsilon = 1$. Што се тиче осталих инвертибилних елемената, прво ћемо доказати једну веома значајну теорему помоћу које ћемо лакше пронаћи остале инвертибилне елементе у неком одређеном раширењу.

Теорема 2.4. Елемент ϵ је инвертибилни елемент ако и само ако је $N\epsilon = \pm 1$.

Доказ. Ако је ϵ инвертибилни елемент:

$$\epsilon \in \mathbb{Z}[\delta_0]^\times \iff \exists v \in \mathbb{Z}[\delta_0], \epsilon v = 1 \Rightarrow (N\epsilon)(Nv) = N(1) = 1 \iff N\epsilon = \pm 1.$$

Ако је $N\epsilon = \pm 1$:

$$N\epsilon = \pm 1 \Rightarrow N\epsilon = \epsilon \cdot \bar{\epsilon} = \pm 1 \Rightarrow \epsilon \cdot (\pm \bar{\epsilon}) = 1,$$

па је $\pm \bar{\epsilon}$ инверз од ϵ , те је ϵ инвертибилни елемент. □

Показаћемо сада на примеру како се траже јединични елементи квадратног раширења.

Пример 2.1. Наћи ћемо све јединичне елементе у прстену $\mathbb{Z}[i]$. Користећи Теорему 2.4, закључујемо да ако је $\epsilon = a + bi$ мора да важи:

$$N\epsilon = N(a + bi) = a^2 - b^2i^2 = a^2 + b^2 = 1.$$

Одавде имамо четири могућности за $\{a, b\}$: $\{1, 0\}$, $\{-1, 0\}$, $\{0, 1\}$, $\{0, -1\}$. Сходно томе, добијамо да су јединични елементи $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

Раширење $\mathbb{Z}[i]$ се назива скупом **Гаусових целих бројева**.

Приметно је да за имагинарна раширења ($D < 0$) норма елемента увек ненегативна, те ће постојати ограничени број решења једначине $N\alpha = 1$, па самим тим и ограничен број јединичних елемената. Код позитивних раширења ($D > 0$) норма може бити и негативна, па у таквим раширењима можемо имати знатно више јединичних елемената. Испоставиће се заправо да ће у сваком позитивном раширењу бити бесконачно много јединичних елемената.

Пример 2.2. Раширење $\mathbb{Z}[\sqrt{319}]$ је реално и нека је $\epsilon = a + b\sqrt{319}$ његов јединични елемент. Знамо да мора да важи

$$N\epsilon = a^2 - 319b^2 = \pm 1.$$

Ово је Пелова једначина и има бесконачно много решења. Основни јединични елемент овог поља (елемент са најмањим $a > 1$) је

$$\epsilon = 12901780 + 722361\sqrt{319}.$$

Како је $N\epsilon = \pm 1$, то ће и $N\epsilon^n = \pm 1$ за свако $n \in \mathbb{N}$, те у овом раширењу има бесконачно много јединичних елемената.

У одељку 2.4 ћмо показати да у већини имагинарних раширења постоји строго ограничење који све елементи могу бити јединични.

Дефиниција 2.10. Елементи $\pi, \theta \in \mathcal{O}$, $\pi \neq \theta$ су **еквивалентни** (означавамо са $\pi \sim \theta$) ако и само ако постоји елемент $\epsilon \in \mathcal{O}^\times$ такав да је $\pi = \epsilon\theta$.

Дефиниција 2.11. Елемент $\pi \in \mathcal{O}$ је **нередукујући** ако и само ако задовољава следећу импликацију:

$$\pi = \alpha\beta, \alpha, \beta \in \mathcal{O} \Rightarrow \alpha \in \mathcal{O}^\times \text{ или } \beta \in \mathcal{O}^\times$$

Нередукујући елемент ће нам бити основа факторизације елемената у $\mathcal{O}$, као што су прости бројеви основа факторизације целих бројева. Постоје и прости елементи, али они нису исто што и нередукујући елементи, о томе ће бити речи мало касије. Сада наводимо важно тврђење везано за нередукујуће елементе.

Теорема 2.5. Сваки елемент $\pi \in \mathcal{O}$ је могуће представити као производ нередукујућих елемената прстена $\mathcal{O}$.

Доказ. Претпоставимо супротно, тј да постоји скуп S (коначан или бесконачан) свих елемената из $\mathcal{O}$ који се не могу представити као производ нередукујућих елемената. Тај скуп има елемент са најмањом нормом по апсолутној вредности, назовимо га σ .

Како σ није нередукујући елемент, можемо га представити као производ барем два нејединична елемента $\sigma = \alpha\beta$, $\alpha, \beta \in \mathcal{O}$. Узимајући норму обе стране, добијамо да је $N\sigma = (N\alpha)(N\beta)$. Како α и β нису јединични, имамо да је $|N(\alpha)| > 1$ и $|N(\beta)| > 1$ (норма је цео број), па је $|N(\alpha)| < |N(\sigma)|$ и $|N(\beta)| < |N(\sigma)|$. По претпоставци, α и β не могу бити у S , те се могу представити у облику производа нередукујућих елемената, $\alpha = \pi_1\pi_2 \dots \pi_k$, $\beta = \lambda_1\lambda_2 \dots \lambda_l$. Закључујемо да је $\sigma = \alpha\beta = \pi_1\pi_2 \dots \pi_k \cdot \lambda_1\lambda_2 \dots \lambda_l$, што је контрадикција. $\square$

Закључујемо да постији факторизација сваког елемента у $\mathcal{O}$. Даље се поставља питање када је та факторизација јединствена, које услове мора да задовољава прстен $\mathcal{O}$. Када уведемо идеале, добићемо и одговарајуће услове за јединствену факторизацију.

Дефиниција 2.12. За две факторизације на нередукујуће елементе $\alpha = \pi_1 \pi_2 \dots \pi_k = \pi'_1 \pi'_2 \dots \pi'_l$ кажемо да су **еквивалентне** ако и само ако важи:

- (1) $k = l$;
- (2) постоји пермутација $\sigma : \{1, 2, \dots, k\} \rightarrow \{1, 2, \dots, k\}$ таква да за свако $i \in \{1, 2, \dots, k\}$ важи: $\pi_i = \epsilon_i \pi'_{\sigma(i)}$, где $\epsilon_i \in \mathcal{O}^\times$.

Дефиниција 2.13. Елемент $p \in \mathcal{O}$ је **прост** ако и само ако за свако $a, b \in \mathcal{O}$ важи импликација:

$$p \mid ab \Rightarrow p \mid a \text{ или } p \mid b$$

Теорема 2.6. Сваки прост елемент је нередукујући.

Доказ. Претпоставимо супротно, тј да постоји прост елемент $p = ab$, $a, b \in \mathcal{O} \setminus \mathcal{O}^\times$. Јасно је тада да импликација $ab \mid ab \Rightarrow ab \mid a$ или $ab \mid b$ није тачна, што је контрадикција. $\square$

2.5 Дискриминанта поља

Остала је још једна битна карактеристика квадратних раширења коју треба дефинисати, дискриминанта поља $F = \mathbb{Q}[\sqrt{D}]$, али да бисмо дошли до ње, прво морамо да дефинишемо:

Дефиниција 2.14. Дискриминанта елемента $\alpha \in \mathcal{O}$ је:

$$\text{disc } \alpha = (\text{Tr } \alpha)^2 - 4N\alpha.$$

Конкретно за поље $\mathbb{Q}[\sqrt{D}]$, где је $D \equiv 2, 3 \pmod{4}$, дискриминанта елемента $\alpha = a + b\sqrt{D}$ износи: $\text{disc } \alpha = 4a^2 - 4(a^2 - b^2D) = 4b^2D$.

Код поља $\mathbb{Q}[\sqrt{D}]$ код ког је $D \equiv 1 \pmod{4}$, израз је нешто компликованији:

$$\text{disc } \alpha = 4a^2 - 4 \left(\left(a + \frac{b}{2} \right)^2 - \frac{b^2}{4}D \right) = -4ab + b^2(D - 1).$$

Теорема 2.7. За $\alpha \in \mathcal{O}$ и $\beta \in \mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha \subseteq \mathcal{O}$ важи $\text{disc } \beta = c^2 \cdot \text{disc } \alpha$ за неки природан број c .

Доказ. У доказу ћемо користити следећа два својства трага и норме елемента:

$$\mathrm{Tr}(a + b\alpha) = 2a + (\mathrm{Tr}\alpha)b \quad ; \quad \mathrm{N}(a + b\alpha) = a^2 + (\mathrm{Tr}\alpha)ab + (\mathrm{N}\alpha)b^2$$

Доказ оба својства је једноставан (преставити α у облику $\alpha = k + n\delta_0$ и искористити дефиницију трага и норме), али подужи, те га зато не наводимо овде.

Нека је $\beta = a + b\alpha$ за неке $a, b \in \mathbb{Z}$:

$$\mathrm{disc} \beta = \mathrm{disc}(a + b\alpha) = (\mathrm{Tr}(a + b\alpha))^2 - 4\mathrm{N}(a + b\alpha).$$

Применом горе наведених својстава добијамо:

$$\begin{aligned} \mathrm{disc} \beta &= (2a + (\mathrm{Tr}\alpha)b)^2 - 4(a^2 + (\mathrm{Tr}\alpha)ab + (\mathrm{N}\alpha)b^2) \\ \mathrm{disc} \beta &= 4a^2 + 4(\mathrm{Tr}\alpha)ab + (\mathrm{Tr}\alpha)^2b^2 - 4a^2 - 4(\mathrm{Tr}\alpha)ab - 4(\mathrm{N}\alpha)b^2 \\ \mathrm{disc} \beta &= (\mathrm{Tr}\alpha)^2b^2 - 4(\mathrm{N}\alpha)b^2 = \mathrm{disc} \alpha \cdot b^2. \end{aligned}$$

□

Приметимо да је дискриминанта елемента β већа од дискриминанте елемента α чијем раширењу припада. Закључујемо:

Последица 3. За елементе $\alpha, \beta \in \mathcal{O}$ важи:

- (1) Ако $\mathbb{Z}[\beta] \subseteq \mathbb{Z}[\alpha] \Rightarrow \mathrm{disc} \alpha \mid \mathrm{disc} \beta$
- (2) Ако $\mathbb{Z}[\beta] = \mathbb{Z}[\alpha] \Rightarrow \mathrm{disc} \alpha = \mathrm{disc} \beta$.

Приметно такође и да, што се више „приближавамо” прстену $\mathcal{O}$, дискриминанта постаје све мања, па је интуитивно дефинисати:

Дефиниција 2.15. Дискриминанта поља $F = \mathbb{Q}[\sqrt{D}]$ је

$$D_F = \mathrm{disc} \mathcal{O} = \mathrm{disc} \delta_0$$

С обзиром на то да знамо које вредности узима δ_0 , лако је показати да дискриминанта поља може имати само две вредности:

$$D_F = \begin{cases} 4D, & D \equiv 2, 3 \pmod{4} \\ D, & D \equiv 1 \pmod{4} \end{cases}$$

и увек важи $F = \mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D_F}]$.

Доказаћмо сада већ најављивану теорему везану за јединичне елементе великог броја имагинарних раширења.

Теорема 2.8. Ако за дискриминанту поља важи $D_F < -4$, у том пољу је скуп свих јединичних елемената $\mathcal{O}^\times = \{\pm 1\}$.

Доказ. Нека је $\epsilon = a + b\delta$ јединични елемент $\mathcal{O} = \mathbb{Z}[\delta]$. Тада важи

$$N(\epsilon) = N(a + b\delta) = a^2 + tab + nb^2 = \pm 1,$$

где је $t = \text{Tr } \delta$ и $n = N\delta$.

Ако је $b = 0$, имамо 2 тривијална решења, $a = 1$ и $a = -1$, односно $\epsilon = 1$ и $\epsilon = -1$. Размотримо сада случај када b није нула. Дељењем обе стране једначине са b^2 добијамо:

$$\left(\frac{a}{b}\right)^2 + t\frac{a}{b} + n = \pm \frac{1}{b^2}.$$

Лева страна се може представити у облику:

$$\left(\frac{a}{b}\right)^2 + t\frac{a}{b} + \frac{t^2}{4} - \frac{t^2}{4} + n = \left(\frac{a}{b} + \frac{1}{2}t\right)^2 - \frac{1}{4}(t^2 - 4n).$$

Квадрат је увек ненегативан, па важи

$$\pm \frac{1}{b^2} \geq -\frac{1}{4}(t^2 - 4n) = -\frac{1}{4}D_F. \quad (2.1)$$

Како је $\pm \frac{1}{b^2} \leq \frac{1}{b^2} \leq 1$ јер је b цео број, видимо да ако је $D_F < -4$, неједначина (2.1) неће имати решење, па су у таквим пољима једини јединични елементи 1 и -1. □

2.6 Јединствена факторизација елемената

Из Теореме 2.5 знамо да се сваки елемент може представити у облику производа напредукујућих елемената. То нам само по себи на жалост није довољно за доказивање неких озбиљнијих тврђења везаних за факторизацију бројева, већ желимо да та факторизација увек буде и јединствена за сваки елемент.

У Примеру 2.1 смо поменули Гаусове целе бројеве, код њих важи јединствена факторизација и у прстену $\mathcal{O} = \mathbb{Z}[i]$ заиста можемо да третирамо елементе као целе бројеве. Код већине поља наилазимо на проблеме при факторизацији.

Пример 2.3. Посматрајмо поље $\mathbb{Q}[\sqrt{-13}]$ и његов прстен целих бројева $\mathcal{O} = \mathbb{Z}[\sqrt{-13}]$. Елемент 14 има две факторизације:

$$14 = 2 \cdot 7 = (1 - \sqrt{-13})(1 + \sqrt{-13})$$

Показаћмо да ове две факторизације заиста нису еквивалентне, јер су $\{2, 7, 1 - \sqrt{-13}, 1 + \sqrt{-13}\}$ нередукујући елементи у прстену $\mathbb{Z}[\sqrt{-13}]$. Како проверавамо да ли је елемент нередукујући?

Претпоставимо да елемент α није нередукујући, односно да се може записати као $\alpha = \pi \cdot \theta$ за неке $\pi, \theta \in \mathbb{Z}[\delta_0] \setminus \mathbb{Z}[\delta_0]^\times$. Узимајући норму обе стране добијамо да је:

$$N\alpha = N(\pi\theta) = (N\pi)(N\theta)$$

(следи да је $N\pi, N\theta < N\alpha$ јер је $N\pi \neq \pm 1 \neq N\theta$, (норма је цео број)).

Закључујемо да уколико елемент није нередукујући мора да постоји елемент са мањом нормом по апсолутној вредности (различитом од 1 и -1) који га дели.

У овом примеру имамо да је:

$$N(2) = 4; \quad N(7) = 49; \quad N(1 - \sqrt{-13}) = N(1 + \sqrt{-13}) = 14.$$

Довољно је да проверимо да не постоји елемент са нормом која дели норму неког од ових елемената, а да је различита од плус минус 1 и плус минус норме тог елемента, односно треба показати да услов:

$$N\pi \in \{2, 7\}$$

није испуњен ни за једно $\pi = a + b\sqrt{-13} \in \mathbb{Z}[\sqrt{-13}]$. Погледајмо шта је $N\pi$:

$$N\pi = N(a + b\sqrt{-13}) = a^2 + 13b^2.$$

1. случај:

$$a^2 + 13b^2 = 2 \quad \Rightarrow \quad b = 0 \quad \Rightarrow \quad a^2 = 2,$$

а ово нема решење за целобројно a .

2. случај:

$$a^2 + 13b^2 = 7 \quad \Rightarrow \quad b = 0 \quad \Rightarrow \quad a^2 = 7.$$

Ни ово нема решење за целобројно a .

Дошли смо до закључка да не постоји тражени елемент π , те смо доказали да су елементи $\{2, 7, 1 - \sqrt{-13}, 1 + \sqrt{-13}\}$ нередукујући у прстену $\mathbb{Z}[\sqrt{-13}]$.

Проблем на који смо наишли, да се неки елементи могу раставити на више нееквивалентних начина нас мотивише да нађемо други приступ факторизацији у $\mathcal{O}$, као и услов који ће нам јасно рећи у којим пољима овај проблем неће постојати. Фокус наредна два поглавља ће бити управо на овоме.

3

Идеали квадратних раширења

3.1 Дефиниција и основна својства идеала

Дефиниција 3.1. Идеал I прстена R је подгрупа прстена R која задовољава следеће три ставке:

- (1) $I \subseteq R$
- (2) $\forall a, b \in I \Rightarrow a + b \in I, a - b \in I$
- (3) $\forall x \in I, \forall a \in R \Rightarrow ax \in I$.

Другим речима, идеал I је адитивна подгрупа прстена R која апсорбује множење из прстена.

Једноставан пример идеала у скупу целих бројева би били парни бројеви. Збир, односно разлика свака два парна броја је паран број, а паран број помножен било којим целим бројем је идаље паран број.

Увешћемо сада појам еквиваленције елемената у односу на идеал I :

Дефиниција 3.2. Елементи a и b су **еквивалентни** (припадају истој **класи еквиваленције**) у односу на идеал I ако и само ако је њихова разлика у идеалу.

$$a \sim b \iff a - b \in I.$$

Пример 3.1. Посматрајмо идеал $I = 5\mathbb{Z} = \{\dots, -5, 0, 5, 10, \dots\}$ који представља скуп свих целих бројева дељивих са 5. Приметимо да су елементи a и b у истој класи акко је њихова разлика дељива са 5, ондосно акко $a \equiv b \pmod{5}$. Јасно је да ће класе еквиваленције заправо бити остаци по модулу 5.

Класа еквиваленције елемента $a \in R$ ће бити скуп $a + I = \{a + x \mid x \in I\}$. Наведимо нека својства класа еквиваленције:

Тврђење 3.1. Нека је I идеал у R . За класе еквиваленције важе следећа два својства:

- (1) $(a + I) + (b + I) = (a + b) + I$
- (2) $(a + I)(b + I) = ab + I$.

Дефиниција 3.3. Количнички прстен је скуп свих класа еквиваленције идеала I прстена R и означава се са R/I .

Пример 3.2. Посматрајмо прстен $R = \mathbb{Z}[\sqrt{-5}]$ и његов идеал $I = 7\mathbb{Z} + \mathbb{Z}(4 - \sqrt{-5}) = \{7a + (4 - \sqrt{-5})b \mid a, b \in \mathbb{Z}\}$. Прво ћемо показати да I заиста јесте идеал прстена R :

- (1) I јесте подскуп R ;
- (2) за $\alpha, \beta \in I$ имамо $\alpha = 7a + (4 - \sqrt{-5})b$ и $\beta = 7c + (4 - \sqrt{-5})d$. $\alpha \pm \beta = (7a + (4 - \sqrt{-5})b) \pm (7c + (4 - \sqrt{-5})d) = 7(a \pm c) + (4 - \sqrt{-5})(b \pm d) \in I$;
- (3) за $\alpha = 7a + (4 - \sqrt{-5})b \in I$ и $x = k + m\sqrt{-5}$, $a, b, k, m \in \mathbb{Z}$ мора да важи $\alpha x = (7a + (4 - \sqrt{-5})b)(k + m\sqrt{-5}) \in I$

$$\alpha x = (7ak + (4 - \sqrt{-5})bk) + am \cdot 7\sqrt{-5} + bm(4 - \sqrt{-5})\sqrt{-5}.$$

Први члан је у идеалу, те је потребан и довољан услов да, с обзиром на то да су am и bm цели бројеви, $7\sqrt{-5}$ и $(4 - \sqrt{-5})\sqrt{-5}$ припадају идеалу ($\gamma_1 = 7$ и $\gamma_2 = (4 - \sqrt{-5})$ се називају генераторма идеала I , довољно је показати да δ_0 пута генератор припада идеалу за сваки генератор γ да би важио услов (3))

$$7\sqrt{-5} = 28 + (-28 + 7\sqrt{-5}) = 4 \cdot 7 + (-7)(4 - \sqrt{-5}) \in I.$$

$$(4 - \sqrt{-5})\sqrt{-5} = 4\sqrt{-5} + 5 = (-16 + 4\sqrt{-5}) + 16 + 5 = 3 \cdot 7 + (-4)(4 - \sqrt{-5}) \in I.$$

Закључак је да I јесте идеал R .

Покушајмо сада да одредимо класе еквиваленције и количнички прстен. За елемент $a = k + l\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ тражимо одговарајућу класу еквиваленције $a + I$. Ту класу можемо записати и као $a + x + I$, где је $x = 7m + (4 - \sqrt{-5})n$, $m, n \in \mathbb{Z}$, произвољан елемент идеала. Одабраћемо x такво да је израз $a + x$ што једноставнији:

$$a + x = k + l\sqrt{-5} + 7m + (4 - \sqrt{-5})n = (k + 7m + 4n) + \sqrt{-5}(l - n).$$

Одабиром $n = l$ ћемо елиминисати комплексан члан из израза, те нам остаје:

$$a + x = (k + 4l) + 7m.$$

Приметимо да за свако $a = k + l\sqrt{-5}$ увек можемо одабрати x тако да $a + x \in \{0, 1, 2, \dots, 6\}$, што нам интуитивно даје да су класе еквиваленције заправо остаци по модулу 7, односно $R/I = \mathbb{Z}/7\mathbb{Z}$. Напомињемо да је ово само интуитивно, строги доказ ове тврдње се изводи преко хомоморфизама.

Дефиниција 3.4. Идеал I прстена R је **главни** ако и само ако је за неко $\alpha \in R$:

$$I = R\alpha = \{r\alpha, r \in R\} = \langle \alpha \rangle$$

Елемент α називамо **генератором** идеала I , $\langle \alpha \rangle$ је нотација коју ћемо користити да обележимо идеал I генерисан елементом α .

Напомена: у раду користимо две нотације за генератор пута прстен, $\alpha R = R\alpha$. Пошто подразумевамо да је множење у прстенима комутативно, ове две нотације су идентичне.

Погледајмо сада нека тривијална али значајна тврђења која важе за главне идеале:

Тврђење 3.2. За сваки главни идеал I прстена R знамо да:

- (1) $Ra = R \iff a \in R^\times$
- (2) $a \mid b \iff b \in Ra \iff Rb \subseteq Ra$.

Пример 3.3. Нека је $I = \mathbb{Z} \cdot 3 + \mathbb{Z}(1 - \delta)$ идеал $R = \mathbb{Z}[\delta] = \mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$. Његови генератори су 3 и $1 - \delta$. Проверимо да се овај идеал не може редукovati у форму $\mathbb{Z} \cdot \alpha$ за неко $\alpha \in R$, односно да није главни.

Претпоставимо да јесте главни, тј $I = R\alpha$. Знамо да елементи 3 и $1 - \delta$ припадају идеалу, те постоје цели бројеви из прстена m, n такви да је $m\alpha = 3$ и $n\alpha = 1 - \delta$. Узимајући норму обе стране, имајући у виду да је норма цео број, добијамо да мора да важи:

$$N\alpha \mid N(3) = 9 \quad N\alpha \mid N(1 - \delta) = N\left(\frac{1 - \sqrt{-23}}{2}\right) = 6,$$

па закључујемо да $N\alpha \mid \text{nzd}(9, 6) = 3$, односно $N\alpha = \pm 3$ или $N\alpha = \pm 1$

- 1. случај: $N\alpha = \pm 3$. То значи да $N\alpha = N(a + b\delta) = 3$ за неке $a, b \in \mathbb{Z}$

$$N(a + b\delta) = N\left(a + \frac{b}{2} + \frac{b\sqrt{-23}}{2}\right) = \left(a + \frac{b}{2}\right)^2 - \left(\frac{b\sqrt{-23}}{2}\right)^2 = \left(a + \frac{b}{2}\right)^2 + \frac{23}{4}b^2 = 3$$

Како су a, b цели бројеви, јасно је да b мора бити нула, па добијамо да је $a^2 = 3$, што нема решења у $\mathbb{Z}$.

- 2. случај: $N\alpha = \pm 1$, па је $\alpha \in R^\times$, односно $I = \alpha R = R$. Ово очигледно није тачно јер, на пример:

$$2 \in R, \quad 3a + b(1 - \delta) = 2 \Rightarrow b = 0 \text{ и } a = \frac{2}{3} \Rightarrow 2 \notin I.$$

Дошли смо до контрадикције, па је закључак да идеал I није главни.

Дефиниција 3.5. Прстен D је **интегрални домен** ако не садржи делиоце нуле, тј важи импликација $ab = 0 \Rightarrow a = 0 \vee b = 0, \forall a, b \in D$.

$\mathbb{Z}/7\mathbb{Z}$ би био пример интегралног домена, док на пример $\mathbb{Z}/6\mathbb{Z}$ није интегрални домен јер је $2 \cdot 3 = 0$. Термин интегралног домена нам је важан јер у њему можемо да скраћујемо елементе, ондосно директно из $ab = ac, a \neq 0$ можемо да закључимо да је $b = c$.

Сваки интегрални домен D има својство: $Da = Db \iff a = b\epsilon, \epsilon \in D^\times$

Дефиниција 3.6. **Главноеидеалски домен (ГИД)** је интегрални домен у ком су сви идеали главни.

Видећемо да је заправо неопходан услов за јединствену факторизацију у $\mathcal{O}$ управо да је $\mathcal{O}$ главноеидеалски домен.

3.2 Операције над идеалима

Имајући у виду да покушавамо да уопшtimo факторизацију елемената идеалима, морамо дефинисати шта представља дељивост у скупу идеала.

Дефиниција 3.7. Нека су I и J идеали. Идеал I **дели** идеал J ако и само ако је J подскуп I : $I \mid J \iff J \subseteq I$.

Ова дефиниција на прву лопту делује помало контраинтуитивно, зашто „већи” идеал дели мањи а не обрнуто? Када погледамо пример, видећемо да је овакво дефинисање дељивости заправо логично. Нека је $I = \langle 2 \rangle$, а $J = \langle 6 \rangle$. С обзиром на то да $2 \in \langle 2 \rangle$ и $6 \in \langle 6 \rangle$, као и да $2 \mid 6$, закључујемо да је правилна дефиниција да I дели J . Са друге стране, знамо да $J = \langle 6 \rangle = \{6r, r \in R\} \subseteq \{2r, r \in R\} = \langle 2 \rangle = I$, дакле $J \subseteq I$ (Ова инклузија важи јер ако је елемент $2r$ у идеалу I , онда због затворености према сабирању и $2r + 2r + 2r = 6r$ такође мора бити у I).

За дељивост идеала тривијално важи транзитивност: ако $I \mid J$ и $J \mid K$ следи да $I \mid K$ (из $I \supseteq J$ и $J \supseteq K$ следи да је $I \supseteq K$).

За два идеала I и J , **најмањи идеал који их дели** је:

$$I + J = \{x + y \mid x \in I, y \in J\} = \text{nzid}(I, J)$$

Како можемо да буде сигурни да је он заиста најмањи? Сваки идеал који дели I мора да садржи све елементе из I , аналогно и за J , а како би био испуњен услов затворености према сабирању, за $\forall x \in I, \forall y \in J; x, y \in \text{nzid}(I, J) \Rightarrow x + y \in \text{nzid}(I, J)$. Затвореност у односу на множење свим елементима из прстена се лако проверава: $(x + y)r = xr + yr; xr \in I, yr \in J \Rightarrow xr + yr \in I + J (\forall r \in R)$.

Дефиниција 3.8. За идеале I и J кажемо да су **узајамно прости** ако и само ако је $I + J = R$.

Теорема 3.1. За идеале I и J прстена R важи $I + J = R$ ако и само ако постоје $x \in I$ и $y \in J$ такви да је $x + y = 1$.

Доказ. 1) ако је $I + J = R$, знамо да R садржи јединицу $\Rightarrow$ постоје $x \in I$ и $y \in J$ такви да је $x + y = 1$.

2) ако постоје $x \in I$ и $y \in J$ такви да је $x + y = 1$, $\Rightarrow 1 \in (I + J) \Rightarrow 1 \cdot r \in (I + J), \forall r \in R \Rightarrow R \subseteq I + J$, али како је $I + J$ идеал $R \Rightarrow I + J = R$. $\square$

Сад када смо дефинисали дељивост идеала, неопходно је да дефинишемо и шта преставља производ два идеала. Како је збир два идеала дефинисан као скуп свих збирова елемената та два идеала, интуитиван предлог би био да је и производ дефинисан као скуп свих производа елемената из оба идеала:

$$IJ = \{xy \mid x \in I, y \in J\}$$

Ова дефиниција на жалост не би била погодна. Приметимо да при оваквом дефинисању IJ није идеал, за неке $x_1, x_2 \in I$, $y_1, y_2 \in J$, x_1y_1 , x_1y_2 , x_2y_1 , и x_2y_2 били у IJ , док њихови зборови $x_1y_1 + x_2y_2$, $x_1y_2 + x_2y_1$ не би морали нужно да буду у IJ . Како бисмо избегли овај проблем, дефинисаћемо производ IJ као скуп свих ових сума са произвољно много чланова, односно:

$$IJ = \left\{ \sum_{i=1}^m x_i y_i \mid x_i \in I, y_i \in J, m \in \mathbb{N} \right\}$$

Овако дефинисано, IJ заиста јесте идеал. Навешћемо сада својства која задовољавају операције сабирања и множења идеала.

Тврђење 3.3. За све идеале I, J, K прстена R знамо да важи:

- (1) $I + J = J + I$; $IJ = JI$ (комутативност)
- (2) $(I + J) + K = I + (J + K)$; $(IJ)K = I(JK)$ (асоцијативност)
- (3) $(I + J)K = IK + JK$ (дистрибутивност)
- (4) $IR = RI = R$
- (5) $I \subseteq J \Rightarrow IK \subseteq JK$
- (6) Ако $IJ = R$, онда је $I = J = R$, односно R је једини идеал са инверзом за операцију множења идеала.

Теорема 3.2. Нека су I, J, K идеали R такви да су I и J узајамно прости и да $I \mid K$ и $J \mid K$. Тада важи да $IJ \mid K$.

Доказ. Пребачено на језик подскупова, имамо да $K \subseteq I$ и $K \subseteq J$. Треба показати да $K \subseteq IJ$:

Посматрајмо поризвољан елемент $k \in K$. Такође из услова да су I и J узајамно прости имамо да постоје $x \in I$ и $y \in J$ такви да је $x + y = 1$. Запишимо елемент k на следећи начин: $k = k \cdot 1 = k \cdot (x + y) = kx + ky = xk + ky$. Даље имамо:

$$\left. \begin{array}{l} x, k \in I \\ k, y \in J \end{array} \right\} \Rightarrow xk + ky \in IJ \Rightarrow k \in IJ.$$

С обзиром на то да ово важи за свако $k \in K$, следи да је $K \subseteq IJ$, што је и требало доказати. □

Лема 3.1. Производ два главна идеала је главни идеал.

Доказ. Нека су $I = \langle \alpha \rangle$ и $J = \langle \beta \rangle$ главни идеали прстена R . Њихов производ је:

$$\begin{aligned} IJ = \langle \alpha \rangle \langle \beta \rangle &= \left\{ \sum \alpha r_1 \cdot \beta r_2 \mid r_1, r_2 \in R \right\} = \left\{ \alpha \beta \sum r_1 r_2 \mid r_1, r_2 \in R \right\} = \\ &= \left\{ \alpha \beta \sum r \mid r \in R \right\} = \langle \alpha \beta \rangle, \end{aligned}$$

те закључујемо да је $IJ = \langle \alpha \beta \rangle$. □

3.3 Максимални и прости идеали

Дефиниција 3.9. Идеал M прстена R је **максималан** акко:

- (1) $M \neq R$
- (2) из $M \subseteq I \subseteq R$ следи $I = M$ или $I = R$ за сваки идеал I прстена R

Максимални идеал у суштини представља „први следећи” идеал после самог R . Било који елемент $t \in R \setminus M$ да додамо у M , како бисмо задржали својство затворености према сабирању и својство апсорпције множења из прстена, односно како би M поново био идеал, морали бисмо му додати и све остале елементе из $R \setminus M$, па би онда био идентички једнак самом прстену. Максималан идеал не мора да буде јединствен, чак напротив, веома често их има бесконачно много.

Пример 3.4. Посматрајмо идеал $M = p\mathbb{Z}$ прстена $\mathbb{Z}$, за било који прост број p . Претпоставимо сада да постоји идеал $\mathbb{Z}a$ за неки цео број a тд. $\mathbb{Z}p \subsetneq \mathbb{Z}a$

(сви идеали у $\mathbb{Z}$ су облика $\mathbb{Z}k$). На основу Тврђења 3.2 (2) следи да $a \mid p$. Како $\mathbb{Z}p \neq \mathbb{Z}a$, мора бити $a \neq \pm p$, па је $a = \pm 1$. То онда имамо да је $\mathbb{Z}a = \mathbb{Z}$, чиме смо показали да је идеал $M = \mathbb{Z}p$ максималан за било које просто p .

Погледајмо сада како налазимо и препознајемо максималне идеале прстена:

Теорема 3.3. Идеал $M \subsetneq R$ је максималан акко је R/M поље.

Доказ. Показаћемо да важи смер с лева на десно.

Одаберимо елемент $a + M \in R/M$ који није нула ($a \notin M$) $\Rightarrow M \subsetneq M + Ra$. Како је M максималан идеал, $M + Ra = R$, па постоје $m \in M, r \in R$ такви да је $m + ab = 1$. Даље имамо да је:

$$(a + M)(b + M) = ab + M = (1 - m) + M = 1 + M.$$

Одавде закључујемо да је $(b + M)$ мултипликативни инверз елемента $(a + M)$ прстена R/M . Како ово важи за сваки ненула елемент прстена, следи да је прстен R/M заправо поље. Аналогним поступком, само уназад, се доказује друга страна еквиваленције. $\square$

Дефиниција 3.10. Идеал P прстена R је **прост** акко:

- (1) $P \neq R$;
- (2) $\forall a, b \in R$ важи импликација $ab \in P \Rightarrow a \in P \vee b \in P$.

Приметимо да су прости идеали дефинисани аналогно простим елементима (Дефиниција 2.13.). Следећа теорема нам говори како препознајемо просте идеале.

Теорема 3.4. Идеал $P \subsetneq R$ је прост акко је R/P интегрални домен.

Доказ. R/P је интегрални домен ако и само ако за сваке $a, b \in R$ важи да:

$$\text{из } (a + P)(b + P) = 0 + P \text{ следи } a + P = 0 \vee b + P = 0.$$

Десна страна је еквивалентна са $a \in P \vee b \in P$, док се услов на левој страни може написати као:

$$(a + P)(b + P) = ab + P = 0 + P,$$

што је еквивалентно са $ab \in P$. Дакле услов да је R/P интегралан домен је еквивалентан са условом да за сваке $a, b \in R$ важи $ab \in P \Rightarrow a \in P \vee b \in P$, што је еквивалентно са тим да је P прост. $\square$

Последица 4. Сваки максимални идеал је прост.

Доказ. Праћењем импликација претходних пар теорема: M је максимални идеал $\Rightarrow R/M$ је поље $\Rightarrow R/M$ је интегрални домен $\Rightarrow M$ је прост идеал, долазимо до доказа. $\square$

С обзиром на то да је сваки максималан идеал прост, поставља се питање када је прост идеал максималан? Следећа два тврђења наводимо без доказа:

Тврђење 3.4. Нека је P прост идеал R . P је максималан идеал R ако прстен R/P има коначно много елемената.

Тврђење 3.5. Нека је R ГИД. Сваки прост идеал R је и максималан.

За дељивост идеала је остало да покажемо још једну, изузетно значајну теорему, која ће нам даље бити основа јединствене факторизације идеала.

Теорема 3.5. (Еуклидова лема за идеале) Нека ју P, I, J идеали R . Важи следећа еквиваленција:

$$P \text{ је прост} \iff (P \mid IJ \iff P \mid I \vee P \mid J, \forall I, J).$$

Доказ. Приметимо да $P \mid I \vee P \mid J \Rightarrow P \mid IJ$ тривијално важи, па нас заправо интересује да докажемо:

$$P \text{ је прост} \iff (P \mid IJ \Rightarrow P \mid I \vee P \mid J, \forall I, J). \quad (3.1)$$

Смер $\Rightarrow$:

P је прост идеал, па за свако $a, b \in R$ важи $ab \in P \Rightarrow a \in P \vee b \in P$.

Претпоставимо супротно, тј $P \nmid I$ и $P \nmid J$ а да важи $P \mid IJ$. То значи да $\exists x \in I, \exists y \in J$ такви да $x \notin P$ и $y \notin P$, али како $P \mid IJ \ni xy$, из услова да је P прост добијамо: $xy \in P \Rightarrow (x \in P \vee y \in P)$, што је контрадикција.

Смер $\Leftarrow$:

$P \mid IJ \Rightarrow P \mid I \vee P \mid J$. Посматрајући главне идеале $I = \langle \alpha \rangle$ и $J = \langle \beta \rangle$ за неке $\alpha, \beta \in R$, имамо да је $IJ = \langle \alpha \rangle \langle \beta \rangle = \langle \alpha\beta \rangle \subseteq P$ (Лема 3.1), што нам заправо говори да $\alpha\beta \in P$. По претпоставци следи да $P \mid \langle \alpha \rangle$ па самим тим и $P \ni \alpha$, или $P \mid \langle \beta \rangle$ па самим тим и $P \ni \beta$, те долазимо до импликације:

$$\alpha\beta \in P \Rightarrow \alpha \in P \vee \beta \in P.$$

Како ово важи за свака два идеала $I = \langle \alpha \rangle$ и $J = \langle \beta \rangle$, импликација ће важити за свака два елемента $\alpha, \beta \in R$, што је и требало доказати. $\square$

Иако постоје квадратна раширења у којима не важи јединствена факторизација елемената, **јединствена факторизација идеала увек важи у свим квадратним раширењима рационалних бројева.** Факторизација

је јединствена искључиво до на пермутацију елемената, када радимо са идеалима немамо никакву еквиваленцију до на множење инвертибилним елементима, јер је инвертибилни елемент пута било који идеал једнак целом прстену. Услов да су две факторизације истог идеала на просте идеале идентичне се изводи управо из Екулидове леме за идеале.

3.4 Стандардна форма и норма идеала

У делу 2.2 смо показали каквог облика мора бити прстен целих бројева $\mathcal{O}$. Сада ћемо навести каквог облика морају бити идеали прстена $\mathcal{O}$, следећу терему наводимо без доказа:

Теорема 3.6. За сваки идеал I прстена $\mathcal{O}$ постоје цели бројеви $a, b, d \in \mathbb{Z}$ за које важи $a > b \geq 0$ и $d > 0$ такви да је:

$$(a) \quad I = d(\mathbb{Z}a + \mathbb{Z}(-b + \delta))$$

(б) $b^2 - tb + n \equiv 0 \pmod{a}$, односно $a \mid N(-b + \delta)$ (ова два услова су еквивалентна) ($t = \text{Tr } \delta$, $n = N\delta$).

Свако $I \subseteq \mathcal{O}$ које задовољава услове (а) и (б) је идеал прстена $\mathcal{O}$. Израз из дела под (а) се назива **стандардна форма идеала**.

Дефиниција 3.11. Норма идеала $I \neq 0$ прстена $\mathcal{O}$ је природан број:

$$NI = |\mathcal{O}/I|.$$

Норма нам овде игра исту улогу као и када смо дефинисали норму елемента, одређује нам поредак у прстену. Наведимо нека својства норме:

Тврђење 3.6. За идеале I и J прстена $\mathcal{O}$ важи:

- (1) $I \mid J \Rightarrow NI \mid NJ$
- (2) $N(I + J) \mid \text{nzd}(NI, NJ)$
- (3) $N\mathcal{O} = 1$, $\mathcal{O}$ је једини идеал норме 1.

Дефиниција 3.12. Конјугат идеала I са стандардном формом $I = d(\mathbb{Z}a + \mathbb{Z}(-b + \delta))$ је идеал $\bar{I} = d(\mathbb{Z}a + \mathbb{Z}(-b + t - \delta))$.

Теорема 3.7. Нека је I ненула идеал $\mathcal{O}$. Тада важи $I\bar{I} = \mathcal{O} \cdot NI$.

Ову терему нећемо доказивати, већ ћемо навести важне последице које добијамо из ње.

Последица 5. Ако су I, J и K идеали $\mathcal{O}$, важи:

$$N(IJ) = (IJ)(\bar{I}\bar{J}) = (I\bar{I})(J\bar{J}) = NI \cdot NJ. \quad (3.1)$$

$$IJ = IK, I \neq 0 \Rightarrow (\bar{I}I)J = (\bar{I}I)K \Rightarrow NI \cdot J = NI \cdot K \Rightarrow J = K. \quad (3.2)$$

Решетке

Сваки прстен целих бројева $\mathcal{O}[\delta] = \mathbb{Z} + \mathbb{Z}\delta$ можемо да видимо као скуп целобројних тачака у декартовом координатном систему, где се на x -оси налазе целобројне тачке, а на y -оси целобројни умношци δ . На овај начин правимо бијекцију између елемента $\alpha = a + b\delta \in \mathcal{O}$ и тачке са целобројним координатама (a, b) :

$$\alpha = a + b\delta \in \mathbb{Z} + \mathbb{Z}\delta \leftrightarrow \begin{bmatrix} a \\ b \end{bmatrix}.$$

Приметимо да скуп $\mathcal{O}[\delta] = \mathbb{Z} + \mathbb{Z}\delta$ покрива све чворове координатног система, као и да свака тачка са целобројним координатама координатног система „живи” у $\mathcal{O}$, те ово заиста јесте бијекција.

Координатни систем можемо да третирамо као векторски простор над $\mathbb{Z}$ димензије 2, чији су јединични вектори:

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightarrow v_1 = 1 \text{ (} x\text{-оса)} \quad ; \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \rightarrow v_1 = \delta \text{ (} y\text{-оса)},$$

и они формирају базичну, квадратну јединичну решетку која одговара прстену $\mathcal{O}[\delta] = \mathbb{Z} + \mathbb{Z}\delta$:

$$\Lambda_0 = \mathbb{Z} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \mathbb{Z} \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

(Прави векторски простор захтева да радимо са пољима, док овде баратамо само целобројним тачкама на обе осе, односно целобројним умножцима вектора $(1,0)$ и $(0,1)$. Интуитивно видимо решетку као векторски простор над $\mathbb{Z}$, иако то формално не постоји).

Ако посматрамо произвољан идеал прстена $\mathcal{O}$ генерисан са два линеарно независна елемента у односу на $\mathbb{Z}$, $I = \mathbb{Z}\alpha + \mathbb{Z}\beta = \mathbb{Z}(a + b\delta) + \mathbb{Z}(c + d\delta)$ (линеарно независни генератори у односу на $\mathbb{Z}$ значи да ниједан генератор није целобројни умножак другог генератора), приметимо да он формира подрешетку решетки Λ_0 , чији су јединични вектори:

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightarrow v_1 = \alpha \text{ (} x\text{-оса)} \quad ; \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \rightarrow v_1 = \beta \text{ (} y\text{-оса)},$$

па је матрични запис решетки која одговара идеалу I у прстену $\mathcal{O}[\delta] = \mathbb{Z} + \mathbb{Z}\delta$:

$$\Lambda = \mathbb{Z}v_1 + \mathbb{Z}v_2 = \mathbb{Z} \begin{bmatrix} a \\ b \end{bmatrix} + \mathbb{Z} \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \left(\mathbb{Z} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \mathbb{Z} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \Lambda_0 \subseteq \Lambda_0.$$

Наведимо сада дозвољене манипулације које можемо примењивати на решетке:

Операција	Ознака
Додај $a \cdot$ пута колону i колони j	$C_j + aC_i$
Замени колоне i и j	$C_i \leftrightarrow C_j$
Помножи колону i са (-1)	$-C_i$

Пример 3.5. Посматрајмо идеал $I = \mathbb{Z}(2 + i) + \mathbb{Z}(-1 + 2i)$ прстена $\mathcal{O} = \mathbb{Z}[i]$. Приметно је да овај нема тако леп запис (није у стандардној форми), те ћемо га средити користећи решетке.

Датом идеалу одговара решетка Λ :

$$\Lambda = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}.$$

Примењивањем дозвољених операција, долазимо до сређеног облика решетке:

$$\Lambda = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix} \xrightarrow{C_2 - 2C_1} \begin{bmatrix} 2 & -5 \\ 1 & 0 \end{bmatrix} \xrightarrow{C_1 \leftrightarrow C_2} \begin{bmatrix} -5 & 2 \\ 0 & 1 \end{bmatrix} \xrightarrow{-C_1} \begin{bmatrix} 5 & 2 \\ 0 & 1 \end{bmatrix},$$

што нас доводи до израза за идеал I у стандардној форми (Теорема 3.6):

$$I = \mathbb{Z} \cdot 5 + \mathbb{Z}(2 + i) = \mathbb{Z} \cdot 5 + \mathbb{Z}(-3 + i).$$

Идеја је увек да сведемо дату решетку на облик где су сви елементи осим последња два елемента у горњем реду (a и b) и последњег елемента у доњем реду (d) нуле. Како би добијени идеал задовољавао услов стандардне форме, неопходно је и да важи $a > b \geq 0$ и $d > 0$, као и да $a \mid N(-b + \delta)$.

Пример 3.6. Нека су $I = \mathbb{Z} \cdot 2 + \mathbb{Z}(1 + \sqrt{-13})$ и $J = \mathbb{Z} \cdot 11 + \mathbb{Z}(3 - \sqrt{-13})$ два идеала прстена $\mathcal{O}[\sqrt{-13}]$. Погледајмо како се одређује збир $I + J$:

$I + J$ мора да садржи све генераторе, ондосно $2, (1 + \sqrt{-13}), 11, (3 - \sqrt{-13}) \in I + J$. Од ова четири генератора формирамо решетку, тако да свака колона представља један елемент (као и до сада, горњи елемент иде уз јединицу, док доњи елемент иде уз δ , у овом случају уз $\sqrt{-13}$):

$$\Lambda = \begin{bmatrix} 2 & 1 & 11 & 3 \\ 0 & 1 & 0 & -1 \end{bmatrix}.$$

Извођењем манипулација над решетком, долазимо до стандардне форме:

$$\Lambda = \begin{bmatrix} 2 & 1 & 11 & 3 \\ 0 & 1 & 0 & -1 \end{bmatrix} \xrightarrow{C_4+C_2} \begin{bmatrix} 2 & 1 & 11 & 4 \\ 0 & 1 & 0 & 0 \end{bmatrix} \xrightarrow{C_4-2C_1} \begin{bmatrix} 2 & 1 & 11 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \xrightarrow{C_3-5C_1} \begin{bmatrix} 2 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \xrightarrow{C_1-2C_3} \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \xrightarrow{C_2-C_3} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \xrightarrow{C_2 \leftrightarrow C_4} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

па је $I + J = \mathbb{Z} + \mathbb{Z}\sqrt{-13} = \mathcal{O}$, одакле добијамо и да су I и J узајамно прости идеали.

Сличан поступак се примењује и при одређивању производа два идеала:

Пример 3.7. Дати су поново исти идеали $I = \mathbb{Z} \cdot 2 + \mathbb{Z}(1 - \sqrt{-13})$ и $J = \mathbb{Z} \cdot 11 + \mathbb{Z}(3 - \sqrt{-13})$ прстена $\mathcal{O} = \mathbb{Z}[\sqrt{-13}]$. Показаћемо како се одређује њихов производ IJ :

Овај пут узимамо производе свака два генератора за елементе у решетки:

$$2 \cdot 11, 2(3 - \sqrt{-13}), (1 - \sqrt{-13}) \cdot 11, (1 - \sqrt{-13})(3 - \sqrt{-13}) :$$

$$\Lambda = \begin{bmatrix} 22 & 6 & 11 & -10 \\ 0 & -2 & -11 & -4 \end{bmatrix}.$$

Операцијама над решетком долазимо до сређеног облика:

$$\begin{aligned} \Lambda &= \begin{bmatrix} 22 & 6 & 11 & -10 \\ 0 & -2 & -11 & -4 \end{bmatrix} \xrightarrow{C_4-2C_2} \begin{bmatrix} 22 & 6 & 11 & -22 \\ 0 & -2 & -11 & 0 \end{bmatrix} \xrightarrow{C_1+C_4} \begin{bmatrix} 0 & 6 & 11 & -22 \\ 0 & -2 & -11 & 0 \end{bmatrix} \\ &\xrightarrow{C_3-5C_2} \begin{bmatrix} 0 & 6 & -19 & -22 \\ 0 & -2 & -1 & 0 \end{bmatrix} \xrightarrow{C_2-2C_3} \begin{bmatrix} 0 & 44 & -19 & -22 \\ 0 & 0 & -1 & 0 \end{bmatrix} \xrightarrow{C_2+2C_4} \begin{bmatrix} 0 & 0 & -19 & -22 \\ 0 & 0 & -1 & 0 \end{bmatrix} \\ &\xrightarrow{C_3 \leftrightarrow C_4} \begin{bmatrix} 0 & 0 & -22 & -19 \\ 0 & 0 & 0 & -1 \end{bmatrix} \xrightarrow{-C_3; -C_4} \begin{bmatrix} 0 & 0 & 22 & 19 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \end{aligned}$$

Дакле добијамо да је $I = \mathbb{Z} \cdot 22 + \mathbb{Z}(19 + \sqrt{-13}) = \mathbb{Z} \cdot 22 + \mathbb{Z}(-3 + \sqrt{-13})$.

Остало је још да покажемо како се рачуна норма идеала помоћу решетки.

Тврђење 3.7. Норма идеала I са генераторима $\alpha = a + b\delta$ и $\beta = c + d\delta$ који су линеарно независни у односу на $\mathbb{Z}$, коме одговара решетка

$$\Lambda = \begin{bmatrix} a & c \\ b & d \end{bmatrix},$$

се рачуна на следећи начин:

$$NI = |\mathcal{O}/I| = \left| \Lambda_0 / \left(\begin{bmatrix} a & c \\ b & d \end{bmatrix} \Lambda_0 \right) \right| = \left| \det \begin{bmatrix} a & c \\ b & d \end{bmatrix} \right| = |ad - bc|.$$

Теорема 3.8. Норма идеала I са стандардном формом је $NI = ad^2$

Доказ. Идеал са стандардном формом има облик:

$$I = d(\mathbb{Z}a + \mathbb{Z}(-b + \delta)) = (\mathbb{Z}ad + \mathbb{Z}(-bd + d\delta)),$$

за неке целе бројеве a, b, d . На основу Тврђења 3.7. имамо:

$$NI = |\mathcal{O}/I| = \left| \Lambda_0 / \left(\begin{bmatrix} ad & -bd \\ 0 & d \end{bmatrix} \Lambda_0 \right) \right| = \det \begin{bmatrix} ad & -bd \\ 0 & d \end{bmatrix} = ad^2.$$

□

Теорема 3.9. Норма идеала $I = \mathcal{O}\alpha$, $\alpha \in \mathcal{O}$ је $|\mathcal{O}/\mathcal{O}\alpha| = |N\alpha|$.

Доказ. Запишимо α као $\alpha = x + y\delta$, за неке $x, y \in \mathcal{O}$. Погледајмо шта је I :

$$I = \mathcal{O}\alpha = (x + y\delta)(\mathbb{Z} + \mathbb{Z}\delta) = \mathbb{Z}(x + y\delta) + \mathbb{Z}(x\delta + y\delta^2).$$

Овде разликујемо два случаја, када је $\delta = \sqrt{D}$ и када је $\delta = \frac{1+\sqrt{D}}{2}$:

(1) $\delta = \sqrt{D}$: тада је $I = \mathbb{Z}(x + y\sqrt{D}) + \mathbb{Z}(x\sqrt{D} + yD)$, окдакле добијамо одговарајућу решетку за I :

$$\Lambda = \begin{bmatrix} x & yD \\ y & x \end{bmatrix},$$

чија је апсолутна вредност детерминанте $|\det \Lambda| = |x \cdot x - yD \cdot y| = |x^2 - y^2D| = |N\alpha|$.

(2) $\delta = \frac{1+\sqrt{D}}{2}$: тада је:

$$\begin{aligned} I &= \mathbb{Z} \left(x + \frac{1+\sqrt{D}}{2}y \right) + \mathbb{Z} \left(\frac{1+\sqrt{D}}{2}x + \left(\frac{1+\sqrt{D}}{2} \right)^2 y \right), \\ I &= \mathbb{Z} \left(x + \frac{1+\sqrt{D}}{2}y \right) + \mathbb{Z} \left(\frac{1+\sqrt{D}}{2}x + \frac{1+D+2\sqrt{D}}{4}y \right), \\ I &= \mathbb{Z} \left(x + \frac{1+\sqrt{D}}{2}y \right) + \mathbb{Z} \left(\frac{1+\sqrt{D}}{2}x + \frac{1+\sqrt{D}}{2}y + \frac{D-1}{4}y \right), \\ I &= \mathbb{Z}(x + y\delta) + \mathbb{Z} \left(\frac{D-1}{4}y + (x+y)\delta \right). \end{aligned}$$

Идеалу I придружујемо решетку Λ :

$$\Lambda = \begin{bmatrix} x & \frac{D-1}{4}y \\ y & x+y \end{bmatrix},$$

чија је апсолутна вредност детерминанте једнака: $|\det \Lambda| = \left| x(x+y) - \frac{D-1}{4}y^2 \right|$.

Са друге стране, норма елемента α једнака је:

$$\begin{aligned} N\alpha &= \alpha \cdot \bar{\alpha} = (x + y\delta)(\overline{x + y\delta}) = \left(x + \frac{1}{2}y + \frac{\sqrt{D}}{2}y \right) \left(x + \frac{1}{2}y - \frac{\sqrt{D}}{2}y \right), \\ |N\alpha| &= \left| \left(x^2 + xy + \frac{1}{4}y^2 \right) - \frac{D}{4}y^2 \right| = \left| x^2 + xy - \frac{D-1}{4}y^2 \right| = \det \Lambda. \end{aligned}$$

У оба случаја смо добили да је $|N\alpha| = |\det \Lambda| = |\mathcal{O}/\mathcal{O}\alpha|$, што је и требало показати. $\square$

4

Класна група идеала

4.1 Разломачки идеали

Увођење коњулата за идеале (Дефиниција 3.12.) нам је омогућило да лакше скраћујемо идеале, односно да из $IJ = IK$ можемо да закључимо да важи $J = K$ ако I није нула идеал. Ипак, адекватније би било да за сваки идеал дефинишемо његов инверзни елемент. Ако се сетимо формуле из Теореме 3.7:

$$I\bar{I} = \mathcal{O} \cdot NI,$$

интуитивно је да за дефиницију инверза за идеал I узмемо:

$$I^{-1} = \frac{1}{NI} \cdot \bar{I}.$$

Иако оваква дефиниција задржава услов затворености према сабирању, као и услов апсорпције множења из прстена $\mathcal{O}$, инверз I^{-1} не мора да буде подскуп $\mathcal{O}$, те он није увек идеал. Стога дефинишемо разломачке идеале који ће управо задовољавати ова својства која желимо да инверзни идеал задовољава.

Дефиниција 4.1. Разломачки идеал $\mathcal{J}$ поља F је подргрупа која задовољава следеће три ставке:

- (1) $\forall a, b \in \mathcal{J} \Rightarrow a + b \in \mathcal{J}, a - b \in \mathcal{J}$
- (2) $\forall \delta \in \mathcal{O}, \delta \mathcal{J} \subseteq \mathcal{J}$
- (3) $\mathcal{J} = \alpha\mathbb{Z} + \beta\mathbb{Z}$, где су $\alpha, \beta \in F$ линеарно независни у односу на $\mathbb{Z}$.

Разломачки идеали не морају бити ни идеали $\mathcal{O}$, ни идеали F . Оне разломачке идеале који су идеали у $\mathcal{O}$ ћемо звати и **интегрални идеали**.

Дефиниција 4.2. Разломачки идеал $\mathcal{J}$ је **главни** ако и само ако има форму:

$$\mathcal{J} = \alpha\mathcal{O} = \{\alpha\beta \mid \beta \in \mathcal{O}\} = \alpha\mathbb{Z} + \alpha\delta\mathbb{Z},$$

за неки елемент $\alpha \in F \setminus \{0\}$.

Наводимо сада експлицитну везу између обичних и разломачких идеала:

Теорема 4.1. Скуп $\mathcal{J} \subseteq F$ је разломачки идеал ако и само ако постоји цео број $e \in \mathbb{Z}$ такав да је $e\mathcal{J}$ идеал прстена $\mathcal{O}$.

Доказ. Нека је $\mathcal{J} \subseteq F$ разломачки идеал. На основу дефиниције 4.1, можемо га записати као:

$$\mathcal{J} = \alpha\mathbb{Z} + \beta\mathbb{Z} = (p_1 + q_1\sqrt{D})\mathbb{Z} + (p_2 + q_2\sqrt{D})\mathbb{Z},$$

за неке рационалне бројеве $p_1 = \frac{a}{k}$, $q_1 = \frac{b}{l}$, $p_2 = \frac{c}{m}$, $q_2 = \frac{d}{n}$,
 $a, b, c, d, k, l, m, n \in \mathbb{Z}$, $\text{nzd}(a, k) = \text{nzd}(b, l) = \text{nzd}(c, m) = \text{nzd}(d, n) = 1$.

Множењем обе стране са $e = \text{nzs}(k, l, m, n)$, добијамо да је:

$$e\mathcal{J} = (a_1 + b_1\sqrt{D})\mathbb{Z} + (c_1 + d_1\sqrt{D})\mathbb{Z},$$

где $a_1, b_1, c_1, d_1 \in \mathbb{Z}$. Одавде је јасно да је $e\mathcal{J} \subseteq \mathcal{O}$, као и да је $e\mathcal{J}$ затворен за сабирање. Остало је још да покажемо да важи:

$$\forall x \in e\mathcal{J}, \forall r \in \mathcal{O} \Rightarrow xr \in e\mathcal{J}.$$

Знамо да је:

$$r(e\mathcal{J}) = re\mathcal{J} = e(r\mathcal{J}) \subseteq r\mathcal{J}, \forall r \in \mathcal{O} \Rightarrow r(e\mathcal{J}) \subseteq e\mathcal{J}, \forall r \in \mathcal{O},$$

одакле добијамо да $rx \in e\mathcal{J}$ за свако $x \in e\mathcal{J}$ и $r \in \mathcal{O}$.

Други смер следи директно из дефиниције разломчаког идеала. $\square$

Цео број e ћмо звати **имениоцем** разломачког идеала $\mathcal{J}$.

Последица 6. За сваки разломачки идеал $\mathcal{J}$ у пољу F постоје цели бројеви a и b за које важи $a > b \geq 0$, као и рационалан број $q \in \mathbb{Q} \setminus \{0\}$, тако да важи:

$$(a) \mathcal{J} = q(a\mathbb{Z} + (-b + \delta)\mathbb{Z})$$

$$(b) b^2 - tb + n \equiv 0 \pmod{a}.$$

Свако $\mathcal{J} \subseteq F$ које задовољава услове (a) и (b) је разломачки идеал у пољу F .

Стандардна ознака за скуп свих идеала прстена $\mathcal{O}$ је $\mathbb{I}_{\mathbb{F}}^+$, док је ознака за скуп свих разломачких идеала у пољу F без плуса, $\mathbb{I}_F$.

Из Последице 6 је јасно да ако је q цео број, имамо скуп интегралних идеала, па је $\mathbb{I}_F^+ \subseteq \mathbb{I}_F$.

4.2 Класна група $\text{Cl}(F)$

Дефиниција 4.3. Нека је $\mathbb{P}_F$ подскуп $\mathbb{I}_F$ који садржи све главне разломачке идеале. Дефинишемо **класну групу** као количничку групу:

$$\text{Cl}(F) = \mathbb{I}_F / \mathbb{P}_F.$$

Приметимо да, уколико је прстен целих бројева $\mathcal{O}$ поља F главноидеалски домен, скуп свих главних разломачких идеала ће бити управо скуп свих разломачких идеала, па ће класна група за такво поље бити тривијална (ако су сви идеали прстена $\mathcal{O}$ главни, тада ће и сви разломачки идеали облика $\frac{1}{e}I$ бити главни разломачки идеали. Како сваком разломачком идеалу одговара неки интегрални идеал, то ће сви разломачки идеали бити главни).

Са друге стране, ако $\mathcal{O}$ није ГИД, класна група нам мери колико је $\mathcal{O}$ „далеко” да буде ГИД. Ради лакше квантификације, дефинишемо:

Дефиниција 4.4. Класни број поља F је број $h(F)$ такав да је:

$$h(F) = |\text{Cl}(F)|.$$

Закључак је да је $\mathcal{O}$ ГИД ако и само ако је $h(F) = 1$.

Количничка група има слична својства као и количнички прстен, те и у њој постоји нека врста класа еквиваленције. Сваки елемент $\text{Cl}(F)$ је облика $[\mathcal{I}] = \mathbb{P}_F \mathcal{I}$. Овај елемент називамо **класом** разломачког идеала $\mathcal{I}$ у пољу F . Приметимо да ако два разломачка идеала $\mathcal{I}$ и $\mathcal{J}$ припадају истој класи, односно $[\mathcal{I}] = [\mathcal{J}]$, то значи, по дефиницији, да се мултипликативно разликују за неки главни разломачки идеал, односно:

$$[\mathcal{I}] = [\mathcal{J}] \iff \mathcal{I} = (\alpha \mathcal{O}) \mathcal{J}, \quad (4.1)$$

за неко $\alpha \in F \setminus \{0\}$.

Знамо да сваком разломачком идеалу $\mathcal{I}$ одговара интегрални идеал $e\mathcal{I}$, за неки цео број e . Последица ове чињенице је да можемо да говоримо о класама разломачких идеала користећи искључиво њихове репрезентативне примере из прстена $\mathcal{O}$:

$$[\mathcal{I}] = [e\mathcal{I}] = [I].$$

Чињеница (4.1) се онда може записати на следећи начин:

$$[I] = [J] \iff \beta I = \gamma J,$$

за неке $\beta, \gamma \in \mathcal{O}$.

Кључна теорема везана за класне групе је **Теорема Минковског**. Њена формулација је геометријска, те је нећемо наводити у том облику, већ ћемо искористити једну, нама кључну последицу везану за идеале која из ње произилази. Следеће тврђење ће нам омогућити да проверимо да ли је одређени прстен целих бројева поља ГИД:

Теорема 4.2. Свака класа у класној групи $\text{Cl}(F)$ садржи идеал који има норму не већу од **границе Минковског** $\mathfrak{M}_F$. Граница Минковског износи:

$$\mathfrak{M}_F = \sqrt{D_F} \cdot \begin{cases} \frac{2}{\pi}, & D_F < 0 \\ \frac{1}{2}, & D_F > 0 \end{cases}.$$

Пример 4.1. Вратимо се још једном на Гаусове целе бројеве $\mathcal{O} = \mathbb{Z}[i]$. Сада можемо формално да покажемо да је $\mathbb{Z}[i]$ ГИД.

Поље $\mathbb{Q}[i]$ је имагинарно, чија је дискриминанта $D_F = 4D = -4$ (видети област 2.5), па имамо да је граница Минковског:

$$\mathfrak{M}_F = \sqrt{|-4|} \cdot \frac{2}{\pi} = \frac{4}{\pi} \approx 1.27324.$$

Како је норма цео број, на основу Теореме 4.2 закључујемо да свака класа садржи идеал чија је норма 1. Тврђење 3.6 (3) нам каже да је једини идеал норме 1 сâм прстен $\mathcal{O}$, па закључујемо да свака класа садржи $\mathcal{O}$. То значи да заправо имамо само једну класу, чији је представник $\mathcal{O}$, па је $\text{Cl}(F) = \{[\mathcal{O}]\}$, односно класни број поља $F = \mathbb{Z}[i]$ је $h(F) = 1$, па закључујемо да је $\mathbb{Q}[i]$ ГИД.

Пример 4.2. Погледајмо још пример из дела 2.6, поље $\mathbb{Q}[\sqrt{-13}]$ и његов прстен целих бројева $\mathcal{O}[\sqrt{-13}]$. Показаћемо да није ГИД и помоћу границе Минковског ћемо одредити његов класни број.

Дискриминанта поља $\mathbb{Q}[\sqrt{-13}]$ је $D_F = -52$, па је граница Минковског за ово поље:

$$\mathfrak{M}_F = \sqrt{52} \cdot \frac{2}{\pi} \approx 4,59.$$

То значи да свака класа садржи идеал чија је норма не већа од 4. Стандардна форма идеала је $I = d(\mathbb{Z} \cdot a + \mathbb{Z}(-b + \delta))$ (уз важан услов да је $b < a$), па је на основу Теореме 3.8 његова норма $NI = ad^2$. Дакле тражимо све идеале прстена $\mathcal{O}[\sqrt{-13}]$ за које важи:

$$NI = ad^2 \in \{1, 2, 3, 4\}.$$

1) $ad^2 = 1$: Следи да је $a = d = 1$, па је $I = \mathbb{Z} + \mathbb{Z}[\sqrt{-13}] = \mathcal{O}$.

2) $ad^2 = 2$: Следи да је $d = 1$ и $a = 2$, па имамо две могућности за I :

$$I = \mathbb{Z} \cdot 2 + \mathbb{Z}\sqrt{-13} \quad \text{и} \quad I = \mathbb{Z} \cdot 2 + \mathbb{Z}(-1 + \sqrt{-13}).$$

3) $ad^2 = 3$: Следи да је $d = 1$ и $a = 3$, па имамо три могућности за I :

$$I = \mathbb{Z} \cdot 3 + \mathbb{Z}\sqrt{-13} \quad , \quad I = \mathbb{Z} \cdot 3 + \mathbb{Z}(-1 + \sqrt{-13}) \quad \text{и} \quad I = \mathbb{Z} \cdot 3 + \mathbb{Z}(-2 + \sqrt{-13}).$$

4) $ad^2 = 4$: Овде сада имамо две могућности за a и d . Прва је да је $d = 2$ и $a = 1$, па је $I = 2 \cdot \mathcal{O}$, а друга је да је $d = 1$ и $a = 4$, па имамо још четири могућности за I :

$$\begin{aligned} I &= \mathbb{Z} \cdot 4 + \mathbb{Z}\sqrt{-13} \quad , \quad I = \mathbb{Z} \cdot 4 + \mathbb{Z}(-1 + \sqrt{-13}), \\ I &= \mathbb{Z} \cdot 4 + \mathbb{Z}(-2 + \sqrt{-13}) \quad \text{и} \quad I = \mathbb{Z} \cdot 4 + \mathbb{Z}(-3 + \sqrt{-13}). \end{aligned}$$

Ово су сви кандидати за идеале са нормом не већом од 4. Сада треба проверити који од њих заиста јесу идеали.

Као у Примеру 3.2, довољно је да проверимо да ли $\alpha\delta$ и $\beta\delta$ припадају идеалу, где су α и β његови генератори. скупови $I = \mathcal{O}$ и $I = 2 \cdot \mathcal{O}$ очигледно јесу идеали $\mathcal{O}$, проверавамо за остале:

i) $I = \mathbb{Z} \cdot 2 + \mathbb{Z}(-b + \sqrt{-13})$, $b \in \{0, 1\}$:

$$\begin{aligned} 2\sqrt{-13} &= 2b - 2b + 2\sqrt{-13} = 2b + 2(-b + \sqrt{-13}) \in I \\ (-b + \sqrt{-13})\sqrt{-13} &= -b\sqrt{-13} - 13 = -13 - b^2 - b(-b + \sqrt{-13}) \in I \iff 2 \mid (13 + b^2), \end{aligned}$$

па имамо да је $b = 1$, односно $I = \mathbb{Z} \cdot 2 + \mathbb{Z}(-1 + \sqrt{-13})$.

ii) $I = \mathbb{Z} \cdot 3 + \mathbb{Z}(-b + \sqrt{-13})$, $b \in \{0, 1, 2\}$:

$$\begin{aligned} 3\sqrt{-13} &= 3b - 3b + 3\sqrt{-13} = 3b + 3(-b + \sqrt{-13}) \in I \\ (-b + \sqrt{-13})\sqrt{-13} &= -b\sqrt{-13} - 13 = -13 - b^2 - b(-b + \sqrt{-13}) \in I \iff 3 \mid (13 + b^2). \end{aligned}$$

Овде видимо да немамо решење. Прелазимо на следећи случај..

iii) $I = \mathbb{Z} \cdot 4 + \mathbb{Z}(-b + \sqrt{-13})$, $b \in \{0, 1, 2, 3\}$:

Потпуно аналогно као и у претходна два случаја, долазимо до услова:

$$4 \mid (13 + b^2),$$

што такође није испуњено ни за једно b .

Приметимо да се у свим могућностима захтева да $a \mid (13 + b^2)$ како би наведени скуп који задовољава стандардну форму идеала заиста био идеал. Ово није случајно, тај услов је управо услов (2) Теореме 3.6 о стандардној форми идеала, $a \mid N(-b + \delta)$, што је у овом конкретном случају: $a \mid N(-b + \sqrt{-13}) = b^2 - (-13) = b^2 + 13$. Како услов (2) наведене теореме нисмо доказали, ово је добар пример на ком видимо како се заправо долази до тог услова.

Дакле у пољу $\mathbb{Q}[\sqrt{-13}]$ постоје само три идеала норме не веће од 4:

$$I_1 = \mathcal{O} \quad , \quad I_2 = 2 \cdot \mathcal{O} \quad \text{и} \quad I_3 = \mathbb{Z} \cdot 2 + \mathbb{Z}(-1 + \sqrt{-13}).$$

Идеали I_1 и I_2 су главни, односно $I_1, I_2 \in [\mathcal{O}]$. Докажимо да I_3 није главни идеал:

Претпоставимо супротно, односно да I_3 јесте главни идеал облика $I_3 = \alpha \mathcal{O}$ за неко $\alpha \in \mathcal{O}$. То значи да постоје цели бројеви из прстена $\mathcal{O}$ такви да је:

$$\alpha\beta = 2 \quad , \quad \alpha\gamma = -1 + \sqrt{-13} \quad , \quad \beta, \gamma \in \mathcal{O}.$$

Узимајући норму обе стране, добијамо да мора да важи:

$$N\alpha \mid N(2) = 4 \quad , \quad N\alpha \mid N(-1 + \sqrt{-13}) = 14,$$

односно да $N\alpha \mid \text{nzd}(4, 14) = 2$.

1. случај: $N\alpha = 2$: Нека је $\alpha = a + b\sqrt{-13}$ за неке целе бројеве a и b :

$$N\alpha = N(a + b\sqrt{-13}) = a^2 + 13b^2 = 2 \quad \Rightarrow \quad b = 0 \quad \Rightarrow \quad a^2 = 2,$$

а ово нема решења за целобројно a .

2. случај: $N\alpha = 1$: Следи да $\alpha \in \mathcal{O}^\times$, па је $I = \alpha \mathcal{O} = \mathcal{O}$. Ово тривијално не важи јер, на пример, $1 \in \mathcal{O}[\sqrt{-13}]$, али $1 \notin I$. Дошли смо до контрадикције.

Доказали смо да идеал I_3 није главни, па самим тим и $\mathcal{O}[\sqrt{-13}]$ не може бити главноидеалски домен. Такође, закључујемо да важи $I_3 \notin [\mathcal{O}]$, па постоји сигурно још једна класа осим тривијалне. Како је ово једини идеал који има норму не већу од 4, а да не припада класи од $\mathcal{O}$, имамо да је:

$$\text{Cl}(F) = \{ [\mathcal{O}], [I_3] \},$$

па је класни број овог поља $h(F) = 2$.

Приметимо још једну важну ствар, шта се догоди када дигнемо I_3 на степен једнак класном броју, у овом случају када квадрирамо I_3 ? Погледајмо:

$$I_3^2 = I_3 \cdot I_3 = (\mathbb{Z} \cdot 2 + \mathbb{Z}(-1 + \sqrt{-13})) \cdot (\mathbb{Z} \cdot 2 + \mathbb{Z}(-1 + \sqrt{-13})).$$

Идеал I_3^2 садржи производе свака два генератора: $\{2 \cdot 2, 2(-1 + \sqrt{-13}), (-1 + \sqrt{-13})^2\}$ (производ $2(-1 + \sqrt{-13})$ се појављује двапут, довољно га је представити једном у матрици). Дозвољеним операцијама над одговарајућом решетком Λ добијамо:

$$\Lambda = \begin{bmatrix} 4 & -2 & -12 \\ 0 & 2 & -2 \end{bmatrix} \xrightarrow{C_3+3C_1} \begin{bmatrix} 4 & -2 & 0 \\ 0 & 2 & -2 \end{bmatrix} \xrightarrow{C_2+C_3} \begin{bmatrix} 4 & -2 & 0 \\ 0 & 0 & -2 \end{bmatrix} \\ \xrightarrow{C_2+C_3} \begin{bmatrix} 4 & -2 & 0 \\ 0 & 0 & -2 \end{bmatrix} \xrightarrow{C_1+2C_2} \begin{bmatrix} 0 & -2 & 0 \\ 0 & 0 & -2 \end{bmatrix} \xrightarrow{-C_1, -C_2} \begin{bmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix},$$

па је $I_3^2 = \mathbb{Z} \cdot 2 + \mathbb{Z} \cdot 2\sqrt{-13} = 2 \cdot \mathcal{O}$.

Одавде видимо да је $[I_3^2] = [2 \cdot \mathcal{O}] = [\mathcal{O}]$, па је класна група заправо генерисана једним елементом:

$$\text{Cl}(F) = \{ [I_3], [I_3^2] \}.$$

Вратимо се још једном на пример из дела 2.6. Он показује две нееквивалентне факторизације истог елемента у прстену $\mathbb{Q}[\sqrt{-13}]$:

$$14 = 2 \cdot 7 = (1 - \sqrt{-13})(1 + \sqrt{-13}) \quad (4.2)$$

Преведено на језик идеала, ова једнакост постаје:

$$\langle 14 \rangle = \langle 2 \rangle \cdot \langle 7 \rangle = \langle 1 - \sqrt{-13} \rangle \cdot \langle 1 + \sqrt{-13} \rangle. \quad (4.3)$$

Може се проверити да се идеал $\langle 7 \rangle$ може раставити као:

$$\begin{aligned} \langle 7 \rangle &= (\mathbb{Z} \cdot 7 + \mathbb{Z}(-1 + \sqrt{-13})) \cdot (\mathbb{Z} \cdot 7 + \mathbb{Z}(-6 + \sqrt{-13})) \\ &= (\mathbb{Z} \cdot 7 + \mathbb{Z}(-1 + \sqrt{-13})) \cdot (\mathbb{Z} \cdot 7 + \mathbb{Z}(1 + \sqrt{-13})) = I_7 \cdot \bar{I}_7, \end{aligned}$$

где су I_7 и $\bar{I}_7$ прости идеали.

Погледајмо чему је једнак производ $I_3 \cdot I_7$:

$$I_3 \cdot I_7 \ni \{14, 2(-1 + \sqrt{-13}), 7(-1 + \sqrt{-13}), (-1 + \sqrt{-13})^2\},$$

па је одговарајућа решетка:

$$\Lambda = \begin{bmatrix} 14 & -2 & -7 & -12 \\ 0 & 2 & 7 & -2 \end{bmatrix} \xrightarrow{C_4+C_1} \begin{bmatrix} 14 & -2 & -7 & 2 \\ 0 & 2 & 7 & -2 \end{bmatrix} \xrightarrow{C_2+C_4} \begin{bmatrix} 14 & 0 & -7 & 2 \\ 0 & 0 & 7 & -2 \end{bmatrix} \\ \xrightarrow{C_3+4C_4} \begin{bmatrix} 14 & 0 & 1 & 2 \\ 0 & 0 & -1 & -2 \end{bmatrix} \xrightarrow{C_4-2C_3} \begin{bmatrix} 14 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 \end{bmatrix} \xrightarrow{C_3 \leftrightarrow C_4; C_1 \leftrightarrow C_3} \begin{bmatrix} 0 & 0 & 14 & 1 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

Погледајмо затим која решетка одговара идеалу $\langle 1 - \sqrt{-13} \rangle$:

$$\begin{aligned} \langle 1 - \sqrt{-13} \rangle &= (1 - \sqrt{-13}) \cdot \mathcal{O} = (1 - \sqrt{-13})(\mathbb{Z} + \mathbb{Z}\sqrt{-13}) \\ &= (\mathbb{Z} - \mathbb{Z}\sqrt{-13}) + (\mathbb{Z}\sqrt{-13} + 13 \cdot \mathbb{Z}), \end{aligned}$$

па је решетка Λ' :

$$\Lambda' = \begin{bmatrix} 1 & 13 \\ -1 & 1 \end{bmatrix} \xrightarrow{C_1 \leftrightarrow C_2} \begin{bmatrix} 13 & 1 \\ 1 & -1 \end{bmatrix} \xrightarrow{C_1 + C_2} \begin{bmatrix} 14 & 1 \\ 0 & -1 \end{bmatrix} = \Lambda.$$

Тиме смо показали да је $I_3 \cdot I_7 = \langle 1 - \sqrt{-13} \rangle$. Аналогно се доказује да је $I_3 \cdot \bar{I}_7 = \langle 1 + \sqrt{-13} \rangle$. Једначина (4.3) онда поприма облик:

$$\langle 14 \rangle = I_3^2 \cdot I_7 \bar{I}_7 = I_3 I_7 \cdot I_3 \bar{I}_7 = I_3^2 I_7 \bar{I}_7, \quad (4.4)$$

где су $I_3, I_7, \bar{I}_7$ прости идеали.

На практичном примеру смо видели да јединствена факторизација идеала важи чак и у пољу у ком не важи јединствена факторизација елемената, зато је приступ факторизацији преко идеала генералнији него преко елемената.

Ова два приступа постају еквивалентна искључиво када је класни број поља једнак јединици, односно када се ради о принципијално идеалском домену. Тада имамо пуну слободу да третирамо елементе, односно главне идеале (зависи за који приступ се одлучимо) као да су обични цели бројеви.

Помоћу класних група и класних бројева се може показати да постоји тачно 9 имагинарних поља чији је прстен целих бројева главноидеалски домен:

$$D \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Идеју да постоји веома мали број имагинарних поља која чији је прстен целих бројева ГИД је предложио Гаус, а доказано је тек средином двадесетог века да за поља $\mathbb{Q}[\sqrt{D}]$ код којих је $D < -163$ је класни број увек већи или једнак 2. Ово је озбиљан резултат у математици и у његовом доказу се користе напредније аналитичке методе које далеко превазилазе ниво овог рада.

Ових 9 бројева се још и називају Хигнерови бројеви, по немачком математичару Курту Хигнеру који је дао највећи допринос при доказивању ове теореме (Старк-Хигнерова теорема).

У следећем поглављу ћемо показати примену квадратних раширења на једном, конкретном задатку.

5

Примена

5.1 Задатак $n^2 + n + 41$

Пре него што почнемо са задатком, доказаћемо једно помоћно тврђење које ће нам бити неопходно за задатак.

Лема 5.1. Прстен целих бројева $\mathcal{O}[\delta]$ поља $\mathbb{Q}[\sqrt{D}]$ је ГИД. Елемент $\alpha \in \mathcal{O}[\delta]$ је нередукујући ако и само ако је норма елемента α прост број.

Доказ. Смер $\Leftarrow$:

Норма елемента α је прост број. Претпоставимо да α није нередукујући, односно $\alpha = \beta\gamma$, за неке $\beta, \gamma \in \mathcal{O} \setminus \mathcal{O}^\times$. Узимајући норму обе стране, имамо да је $N\alpha = N(\beta\gamma) = (N\beta)(N\gamma)$. Како је $N\alpha$ прост број, следи да нека он норми елемената β, γ мора бити или 1 или -1, па је тај елемент инвертибилан, што је контрадикција. За овај смер нам није неопходан услов да је прстен ГИД.

Смер $\Rightarrow$:

Елемент α је нередукујући. Претпоставимо да норма елемента α није прост број, односно да је $N\alpha = b \cdot c$, за неке узајамно просте целе бројеве b и c различите од ± 1 . Даље имамо да је:

$$\alpha\bar{\alpha} = N\alpha = b \cdot c. \quad (5.1)$$

У пољима која имају јединствену факторизацију целих бројева, нередукујући елементи и прости елементи су иста свтар, те због тога имамо да важи:

$$\alpha \mid bc \quad \Rightarrow \quad \alpha \mid b \quad \vee \quad \alpha \mid c.$$

Без умањења општости, узећемо да $\alpha \mid b$, ондосно $b = \alpha \cdot \theta$, где $\theta \in \mathcal{O}[\delta]$. Конјугујући обе стране видимо да је $b = \bar{b} = \overline{\alpha\theta} = \bar{\alpha} \cdot \bar{\theta}$, јер је b цео број, па видимо да $\bar{\alpha} \mid b$. Дакле имамо да $\alpha \mid b$ и $\bar{\alpha} \mid b$, па следи да $\alpha\bar{\alpha} \mid b$, односно $N\alpha \mid b$. Како и $b \mid N\alpha$, следи да је $b = \pm N\alpha$, односно да је $c = \pm 1$, што је контрадикција. $\square$

Задатак 1. Доказати да је вредност полинома $P(n) = n^2 + n + 41$ прост број за све природне бројеве n мање од 40.

Решење 1. Провером пешке за све бројеве $n \in \{1, 2, 3, \dots, 39\}$ видећемо да дат полином заиста јесте увек прост. За $n = 40$, вредност полинома ће бити $P(40) = 40^2 + 40 + 41 = 40(40 + 1) + 41 = 41^2$, што је јасно дељиво са 41.

Поента овог задатка је да га урадимо елегантно, користећи квадратна раширења, без провере за све бројеве мање од 40. Такође, видећемо уопштење овог задатка, то јесте за које све бројеве c се може истом методом показати да полином $Q(n) = n^2 + n + c$ генерише просте бројеве за свако $n < c - 1$.

За почетак, решимо једначину $P(x) = x^2 + x + 41 = 0$:

$$x^2 + x + 41 = 0 \Rightarrow x_{1,2} = \frac{-1 \pm \sqrt{1^2 - 4 \cdot 41}}{2} = \frac{1 \pm \sqrt{-163}}{2}.$$

Полином P можемо да запишемо као $P(x) = k(x - x_1)(x - x_2)$. Како је полином моничан, знамо да је $k = 1$, па добијамо да је:

$$P(x) = \left(x + \frac{1 + \sqrt{-163}}{2}\right) \left(x + \frac{1 - \sqrt{-163}}{2}\right) \quad (5.2)$$

Улазимо у квадратно раширење $\mathbb{Q}[\sqrt{-163}]$:

Како је $-163 \equiv 1 \pmod{4}$, имамо да је $\mathcal{O} = \mathbb{Z}[\delta]$, где је $\delta = \frac{1 + \sqrt{-163}}{2}$. Имајући у виду да разматрамо целе бројеве n , за њих важи $\bar{n} = n$, па наш полином P постаје:

$$P(n) = (n + \delta)(\bar{n} + \bar{\delta}) = (n + \delta)(n + \delta) = N(n + \delta), \quad \text{за } n \in \mathbb{Z}.$$

Свели смо задатак на то да желимо да докажемо да је норма елемента $(n + \delta)$ у овом раширењу прост број за $n < 40$.

Претпоставимо да $n + \delta$ није нередукујући елемент, односно да је $n + \delta = \alpha\beta$, за неке $\alpha, \beta \in \mathcal{O} \setminus \mathcal{O}^\times$. Узимајући норму обе стране, добијамо да је:

$$N(n + \delta) = N(\alpha\beta) = (N\alpha)(N\beta).$$

Погледајмо сад шта знамо о норми елемента $\alpha = a + b\delta$, $a, b \in \mathbb{Z}$ (аналогно је и за β):

$$\begin{aligned} N\alpha &= N(a + b\delta) = N\left(a + \frac{1}{2}b + \frac{\sqrt{-163}}{2}b\right) = \left(a + \frac{1}{2}b\right)^2 - \left(\frac{\sqrt{-163}}{2}b\right)^2 \\ &= a^2 + ab + \frac{1}{4}b^2 + \frac{163}{4}b^2 = a^2 + ab + 41b^2. \end{aligned}$$

Најбоље је да се задржимо на облику:

$$N\alpha = \left(a + \frac{1}{2}b\right)^2 - \left(\frac{\sqrt{-163}}{2}b\right)^2 = \left(a + \frac{1}{2}b\right)^2 + \frac{163}{4}b^2,$$

јер одавде видимо да је $N\alpha \geq \frac{163}{4}b^2$, па закључујемо да је за сваки елемент $\alpha \in \mathbb{Z}[\delta] \setminus \mathbb{Z}$, норма тог елемента:

$$N\alpha \geq \frac{163}{4} \Rightarrow N\alpha \geq 41,$$

јер је норма цео број. Остало је још прокоментарисати зашто ни α ни β не могу бити цели бројеви.

Претпоставимо супротно, да је без умањења општости $\beta = k \in \mathbb{Z} \setminus \{1\}$ (сетимо се да β није инвертибилни елемент). Одатле следи:

$$n + \delta = \alpha\beta = k(a + b\delta) = ka + kb\delta.$$

Коефицијенти уз δ на левој и десној страни морају бити једнаки, па одатле добијамо услов да је: $kb = 1$. Како $k \neq 1$ и с обзиром на то да је и b цео број, знамо да ова једначина нема решења, те смо дошли до контрадикције. Закључујемо да ни α ни β не могу бити цели бројеви.

Дакле уколико $n + \delta$ није нередукујући, мора да важи:

$$N(n + \delta) = (N\alpha)(N\beta) \geq 41 \cdot 41 = 41^2,$$

те закључујемо да је за све n такве да је $N(n + \delta) < 41^2$, елемент $n + \delta$ нередукујући. Услов $N(n + \delta) < 41^2$ је еквивалентан:

$$N(n + \delta) = n^2 + n + 41 < 41^2 \iff n(n + 1) < 40 \cdot 41 \iff n < 40.$$

Дакле, за свако $n < 40$, елемент $n + \delta$ је нередукујући. На основу смера с лево на десно Леме 5.1, закључујемо да за свако $n < 40$ важи да је $N(n + \delta)$ прост, односно да је $P(n)$ прост, што је и требало доказати.

Посматрајмо произвољан полином $Q(x) = x^2 + x + c$. Његове нуле су:

$$x_{1,2} = \frac{-1 \pm \sqrt{1 - 4c}}{2}.$$

Ако се сетимо која сва имагинарна раширења су ГИД, видимо да за $1 - 4c \in \{-3, -7, -11, -19, -43, -67\}$ имамо аналогни задатак као за $1 - 4c = -163$, па видимо да се овакав задатак може поставити и за $c \in \{1, 2, 3, 5, 11, 17\}$. Важно је напоменути да задатак доказујемо за природне бројеве $n < c - 1$, па за $c \in \{1, 2\}$, задатак практично нема смисао.

Литература

- [1] M. Trifković, *Algebraic Theory of Quadratic Numbers*, Springer Universitext, Викторија, Британска Колумбија, Канада, 2013.
- [2] M. R. Murty and J. Esmonde, *Problems in Algebraic Number Theory*, Springer Universitext, Кингстон, Онтарио, Канада, 2004.
- [3] K. Conrad, *Factoring in quadratic fields*, <https://kconrad.math.uconn.edu/blurbs/gradnumthy/quadraticgrad.pdf>