Jaguvus

Ülesannete näisilahendusi

6. aprill 2026. a.

(Kui pole öeldud teisiti, siis R on nullitegureita kommutatiivne ring.)

Ülesanne 1 Tõestada, et mistahes $a, b, c \in R$ korral

a) $a \mid b \wedge b \mid c \Rightarrow a \mid c$; b) $a \mid b \wedge a \mid c \Rightarrow a \mid b \pm c$; c) $a \mid b \Rightarrow a \mid bc$.

Lahendus. a) Kui $a \mid b$ ja $b \mid c$, siis jaguvuse definitsiooni põhjal leiduvad elemendid $e, f \in R$ nii, et $ae = b$ ja $bf = c$. Seega

$$c = bf = (ae)f = a(ef),$$

mis tähendab seda, et $a \mid c$. Väited b) ja c) saab tõestada sarnasel viisil.

Ülesanne 2 Leida arvude 975 ja 645 suurim ühistegur ja vähim ühiskordne a) ringis $\mathbb{Z}$, b) ringis $\mathbb{Q}$.

Lahendus. a) Kasutame suurima ühisteguri leidmiseks Eukleidese algoritmi:

$$\begin{aligned} 975 &= 645 \cdot 1 + 330 \\ 645 &= 330 \cdot 1 + 315 \\ 330 &= 315 \cdot 1 + 15 \\ 315 &= 15 \cdot 21\,. \end{aligned}$$

Näeme, et viimane nullist erinev jääk on 15, seega $\text{SÜT}(975, 645) = 15$. Järelikult

$$\text{VÜK}(975, 645) = \frac{975 \cdot 645}{15} = 975 \cdot 43 = 41\,925\,.$$

b) Ring $\mathbb{Q}$ on korpus, seega mistahes nullist erinevate elementide suurim ühistegur on 1 ja nende vähim ühiskordne on korrutis.

Ülesanne 3 Olgu R Eukleidese ring ja $a, b, u \in R$. Tõestada, et kui u on pööratav, siis $\text{SÜT}(au, b) = \text{SÜT}(a, b)$.

Lahendus 1. Teame, et Eukleidese ringis on mistahes kahel elemendil suurim ühistegur olemas. Tähistame $d = \text{SÜT}(a, b)$ ja $e = \text{SÜT}(au, b)$.

Kuna $d \mid a$, siis ka $d \mid au$. Et d on au ja b ühine tegur ja $e = \text{SÜT}(au, b)$, siis $d \mid e$.

Kuna $e \mid au$, siis $ef = au$ mingi $f \in R$ korral. Järelikult $efu^{-1} = a$, kust $e \mid a$. Et e on a ja b ühine tegur ja $d = \text{SÜT}(a, b)$, siis $e \mid d$.

Oleme näidanud, et $d \mid e$ ja $e \mid d$, mis tähendab, et elemendid e ja d on assotsieeritud. Kuna teame, et SÜT on määratud üheselt assotsieerituse täpsuseni, siis olemegi saanud selle, mida soovisime.

Lahendus 2. Olgu $d = \text{SÜT}(a, b)$. Näitame, et element d rahuldab elementide au ja b suurima ühisteguri definitsiooni kahte tingimust.

1. On selge, et $d \mid au$ ja $d \mid b$.

2. Oletame, et $c \mid au$ ja $c \mid b$. Siis leidub selline $f \in R$, et $cf = au$. Järelikult $cfu^{-1} = a$ ehk $c \mid a$. Kuna c on a ja b ühine tegur, siis $c \mid d$, mida oligi vaja.

Vaatleme kompleksarvude korpuse alamringi $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Defineerime kujutuse $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N} \cup \{0\}$ võrdusega

$$N(a + b\sqrt{-5}) := a^2 + 5b^2 = \left|a + b\sqrt{5}i\right|^2.$$

Nimetame seda kujutust *normiks*. Seega $\mathbb{Z}[\sqrt{-5}]$ elemendi norm on tema mooduli ruut. Kasutades seda, et kompleksarvude korrutise moodul on tegurite moodulite korrutis, saame, et norm säilitab korrutamist:

$$N(z_1 z_2) = |z_1 z_2|^2 = |z_1|^2 |z_1|^2 = N(z_1)N(z_2) \tag{1}$$

iga $z_1, z_2 \in \mathbb{Z}[\sqrt{-5}]$ korral.

Lisaks sellele on norm kooskõlas ka jaguvusseosega, s.t. mistahes arvude $z_1, z_2 \in \mathbb{Z}[\sqrt{-5}]$ korral

$$z_1 \mid z_2 \text{ ringis } \mathbb{Z}[\sqrt{-5}] \implies N(z_1) \mid N(z_2) \text{ ringis } \mathbb{Z}.$$

Tõepoolest, kui $z_1 \mid z_2$ ringis $\mathbb{Z}[\sqrt{-5}]$, siis leidub selline $w \in \mathbb{Z}[\sqrt{-5}]$, et $z_1 w = z_2$. Võrduse (1) põhjal $N(z_1)N(w) = N(z_1 w) = N(z_2)$, millest aga järeldub, et $N(z_1) \mid N(z_2)$ ringis $\mathbb{Z}$.

Paneme veel tähele, et

$$U(\mathbb{Z}[\sqrt{-5}]) = \{1, -1\}.$$

Sisalduvus $\{1, -1\} \subseteq U(\mathbb{Z}[\sqrt{-5}])$ on ilmne. Oletame, et z on pööratav. Siis $z \mid 1$ ringis $\mathbb{Z}[\sqrt{-5}]$ ning järelikult $N(z) \mid N(1) = 1$ ringis $\mathbb{Z}$. Ainus mittenegatiivne naturaalarv, mis jagab arvu 1 täisarvude ringis, on 1 ise. Seega $N(z) = 1$. Lihtne on näha, et ringis $\mathbb{Z}[\sqrt{-5}]$,

$$N(z) = 1 \iff z = 1 \text{ või } z = -1.$$

Seega $z \in \{1, -1\}$ ja $U(\mathbb{Z}[\sqrt{-5}]) \subseteq \{1, -1\}$.

Ülesanne 4 Tõestada, et ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ ei ole faktoriaalne.

Lahendus. Vaatleme arvu 9 kahte teguriteks lahutust ringis $\mathbb{Z}[\sqrt{-5}]$:

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

On selge, et elemendid 3 ja $2 \pm \sqrt{-5}$ ei ole assotsieeritud, sest kui nad oleksid assotsieeritud, siis nad peaksid olema kas võrdsed või erinema märgi poolest.

Näitame veel, et kõik need elemendid on taandumatud. Paneme tähele, et kui $z \in \{3, 2 + \sqrt{-5}, 2 - \sqrt{-5}\}$, siis $N(z) = 9$. Oletame, et $z \in \{3, 2 + \sqrt{-5}, 2 - \sqrt{-5}\}$ ja $z = z_1 z_2$, kus $z_1, z_2 \in \mathbb{Z}[\sqrt{-5}]$. Siis

$$9 = N(z) = N(z_1)N(z_2). \tag{2}$$

Kuna ei leidu selliseid arve $a, b \in \mathbb{N} \cup \{0\}$, et $a^2+5b^2 = 3$, siis ei saa ühegi $\mathbb{Z}[\sqrt{-5}]$ elemendi norm olla 3. Seega võrdusest (2) järeldub, et kas $N(z_1) = 1$ ja $N(z_2) = 9$ või $N(z_1) = 9$ ja $N(z_2) = 1$. Esimesel juhul on z_1 pööratav ja teisel juhul on z_2 pööratav. Sellega oleme tõestanud, et z on taandumatu.

Ülesanne 5 Teha kindlaks, kas elementidel a, b ringist $\mathbb{Z}[\sqrt{-5}]$ on olemas suurim ühistegur ja vähim ühiskordne, kui

a) $a = 3, b = 1 + \sqrt{-5}$;

b) $a = 6, b = 3 + 3\sqrt{-5}$.

Lahendus.

a) Näitame, et $\text{SÜT}(3, 1 + \sqrt{-5}) = 1$. Selleks kontrollime definitsiooni kahte tingimust.

1. Ilmselt $1 \mid 3$ ja $1 \mid 1 + \sqrt{-5}$.
2. Oletame, et $c \mid 3$ ja $c \mid 1 + \sqrt{-5}$, kus $c \in \mathbb{Z}[\sqrt{-5}]$. Siis $N(c) \mid N(3) = 9$ ja $N(c) \mid N(1 + \sqrt{-5}) = 6$ ringis $\mathbb{Z}$. Kuna täisarvude ringis on kõik suurimad ühistegurid olemas, siis suurima ühisteguri definitsiooni põhjal $N(c) \mid \text{SÜT}(9, 6) = 3$. Et arvu 3 ainsad naturaalarvulised jagajad on 1 ja 3, siis saame, et $N(c) = 1$ või $N(c) = 3$. Nagu eespool nägime, on teine võimalus välistatud. Seega $N(c) = 1$, mis tähendab, et $c \in \{1, -1\}$, ning seega $c \mid 1$ ringis $\mathbb{Z}[\sqrt{-5}]$, nagu nõutud.

Näitame nüüd, et ei leidu nende arvude vähimat ühiskordset. Oletame vastuväiteliselt, et $m = \text{VÜK}(3, 1 + \sqrt{-5})$. Kuna $3 \mid m$ ja $1 + \sqrt{-5} \mid m$, siis $9 \mid N(m)$ ja $6 \mid N(m)$. Järelikult $18 = \text{VÜK}(9, 6) \mid N(m)$ ringis $\mathbb{Z}$.

Teisest küljest,

$$3 \mid 3 + 3\sqrt{-5} \wedge 1 + \sqrt{-5} \mid 3 + 3\sqrt{-5} \implies m \mid 3 + 3\sqrt{-5} \implies N(m) \mid N(3 + 3\sqrt{-5}) = 54,$$
$$3 \mid 6 \wedge 1 + \sqrt{-5} \mid 6 \implies m \mid 6 \implies N(m) \mid N(6) = 36.$$

Kuna $N(m)$ on arvude 54 ja 36 ühine tegur, siis $N(m) \mid \text{SÜT}(54, 36) = 18$.

Kuna $18 \mid N(m)$ ja $N(m) \mid 18$ ringis $\mathbb{Z}$, siis $N(m) = 18$. Kui nüüd $m = a + b\sqrt{-5}$, kus $a, b \in \mathbb{Z}$, siis $a^2 + 5b^2 = 18$. Vaatleme erinevaid võimalusi b jaoks.

1. $b = 0$. Siis $a^2 = 18$, mis on vastuolus sellega, et 18 ei ole ühegi täidarvu ruut.
2. $b = 1$. Siis $a^2 = 13$, vastuolu.
3. $b \geq 2$. Siis $a^2 = 18 - 5b^2 \leq -2$, jällegi vastuolu.

Tekkinud vastuolu näitab, et elementidel 3 ja $1+\sqrt{-5}$ ei saa leiduda ühtegi vähimat ühiskordset.

b) Tõestame, et ei leidu elementide 6 ja $3+3\sqrt{-5}$ suurimat ühistegurit. Kuna vähima ühiskordse leidumisest järeldub suurima ühiseguri leidumine, siis ei saa neil elementidel ka vähimat ühiskordset leiduda.

Oletame vastuväiteliselt, et leidub $d = \text{SÜT}(6, 3+3\sqrt{-5})$. Siis $N(d) \mid N(6) = 36$ ja $N(d) \mid N(3+3\sqrt{-5}) = 54$ ringis $\mathbb{Z}$. Järelikult $N(d) \mid \text{SÜT}(36, 54) = 18$.

Teisest küljest, kuna $3 \mid 6$ ja $3 \mid 3+3\sqrt{-5}$, siis $3 \mid d$ ja $9 \mid N(d)$. Et $1+\sqrt{-5} \mid 6$ ja $1+\sqrt{-5} \mid 3+3\sqrt{-5}$, siis $1+\sqrt{-5} \mid d$ ja $6 \mid N(d)$. Kuna $N(d)$ on 6 ja 9 ühine kordne ringis $\mathbb{Z}$, siis $18 = \text{VÜK}(6, 9) \mid N(d)$. Kokkuvõttes $N(d) = 18$. Eespool nägime, et see annab vastuolu. Sellega on ülesanne lahendatud.

Ringi R nimetatakse *Eukleidese ringiks*, kui leidub kujutus $\delta : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ nii, et iga $a \in R$ ja iga $0 \neq b \in R$ korral leiduvad sellised elemendid $q, r \in R$, et $a = bq + r$ ning kas $r = 0$ või $\delta(r) < \delta(b)$.

Definitsioon 1 Nullitegureita kommutatiivset ringi R nimetatakse **Eukleidese ringiks**, kui leidub kujutus

$$\delta : R \setminus \{0\} \to \mathbb{N} \cup \{0\},$$

mis rahuldab tingimusi:

ER1. iga $a, b \in R \setminus \{0\}$ korral $\delta(ab) \geq \delta(a)$,

ER2. iga $a \in R$ ja iga $b \in R \setminus \{0\}$ korral leiduvad sellised $q, r \in R$, et

$$a = bq + r, \quad \text{kusjuures} \quad r = 0 \quad \text{või} \quad \delta(r) < \delta(b).$$

Ülesanne 6 Tõestada, et *Gaussi täisarvude ring*

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

on Eukleidese ring.

Lahendus. Vaatleme kujutust

$$N : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N} \cup \{0\}, \;\; a + bi \mapsto a^2 + b^2 = |a + bi|^2 .$$

Nii nagu eespool saame veenduda, et N säilitab korrutamist. On selge, et N rahuldab, tingimust **ER1.** Näitame, et kehtib ka **ER2.** Võtame ringist $\mathbb{Z}[i]$ elemendid $z = a + bi$ ja $w = c + di \neq 0$. Siis kompleksarvude korpuses

$$\frac{z}{w} = zw^{-1} = e + fi,$$

kus $e, f \in \mathbb{R}$ (tegelikult isegi $e, f \in \mathbb{Q}$). Valime täisarvud k, l nii, et $|e - k| \leq \frac{1}{2}$ ja $|f - l| \leq \frac{1}{2}$. Tähistame

$$q := k + li \in \mathbb{Z}[i], \;\; x := e - k \in \mathbb{R}, \;\; y := f - l \in \mathbb{R} \quad \text{ja} \quad r := w(x + yi).$$

Siis

$$z = w(e + fi) = w((x + k) + (y + l)i) = w(k + li) + w(x + yi) = wq + r,$$

kus $r = z - wq \in \mathbb{Z}[i]$ (sest $z, w, q \in \mathbb{Z}[i]$) ja, juhul kui $r \neq 0$,

$$N(r) = N(w)N(x + yi) = N(w)(x^2 + y^2) \leq N(w)\left(\frac{1}{4} + \frac{1}{4}\right) = N(w) \cdot \frac{1}{2} < N(w).$$