Algebra I
Esimeste kahe praktikumi ülesannete lahendusi.

1. praktikumi ülesanded

Järgnevas kasutame algebraliste struktuuride omaduste tähiseid (G1, G2, KOMM, R3 jne.) näiteülesannete failist.

Ülesanne 2. Uurida järgmiste naturaalarvude hulgal $\mathbb{N}$ defineeritud tehete $*$ omadusi, st teha kindlaks, kas $(N, *)$ on rühmoid, poolrühm, kas seal leidub ühikelement, millistel elementidel on pöördelemendid.

e) $a * b = 4a$; f) $a * b = a + b - ab$.

Lahendus:

e) Kui $a, b \in \mathbb{N}$, siis ka $a * b = 4a \in \mathbb{N}$. Seega $*$ on algebraline tehe naturaalarvude hulgal.

G1: Olgu $a, b, c \in \mathbb{N}$. Siis $(a * b) * c = 4(a * b) = 4a = a * (b * c)$.

G2: Kuna $2 * x = 8 \neq 2$ mistahes $x \in \mathbb{N}$ korral, siis ühikelementi ei leidu.

G3: Ilma ühikelemendita ei saa pöördelemente leida.

KOMM: Kuna $2 * 1 = 8 \neq 4 = 1 * 2$, ei ole tegu kommutatiivse tehtega.

Vastus: $(\mathbb{N}, *)$ on mittekommutatiivne poolrühm.

f) Kuna näiteks $5, 10 \in \mathbb{N}$, aga $5 * 10 = 5 + 10 - 5 \cdot 10 = -35 \notin \mathbb{N}$, ei ole tegu algebralise tehtega.

Vastus: $(\mathbb{N}, *)$ ei ole rühmoid.

Ülesanne 5. Näidata, et (mitteassotsiatiivses) ühikuga rühmoidis võib elemendil olla rohkem kui üks pöördelement. Konstrueerida minimaalne näide. Konstrueerida näide iga võimaliku lõpliku hulga jaoks.

Lahendus: Olgu $A_n = \{1, a_1, \ldots, a_{n-1}\}$. Kui $x, y \in A$, siis defineerime $x * y = 1$, kui $x \neq 1$ ja $y \neq 1$, ning vastavalt ühikelemendi definitsioonile muul juhul. Selle struktuuri Cayley tabel näeb välja järgmine:

$*$	1	a_1	a_2	$\ldots$	a_{n-1}
1	1	a_1	a_2	$\ldots$	a_{n-1}
a_1	a_1	1	1	$\ldots$	1
a_2	a_2	1	1	$\ldots$	1
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
a_{n-1}	a_{n-1}	1	1	$\ldots$	1

Kõik ühikelemendist erinevad elemendid on üksteise pöördelemendid. Ühikelemendi ainus pöördelement on ta ise.

Vastus: Minimaalne näide on A_3. Näide n-elemendilise hulga jaoks on A_n.

Ülesanne 6. Positiivsete reaalarvude hulgal $\mathbb{R}^+$ on defineeritud kahekohaline tehe $*$ alljärgnevalt. Uurida seda tehet analoogiliselt ülesandega 2.

b) $a * b = \sqrt{ab}$; d) $a * b = 1$.

Lahendus: b) Kuna positiivsete reaalarvude ruutjuured ja korrutised on samuti positiivsed reaalarvud, on tegu algebralise tehtega.

G1: Kuna $2 * (4 * 4) = \sqrt{2 \cdot \sqrt{4 \cdot 4}} = \sqrt{8} \neq \sqrt{8 \cdot \sqrt{2}} = \sqrt{\sqrt{2 \cdot 4} \cdot 4} = (2 * 4) * 4$, siis $*$ ei ole assotsiatiivne.

G2: Oletame, et meil on ühikelement $e \in \mathbb{R}^+$. Siis $e * 4 = 2\sqrt{e} = 4$, kust $e = 4$. Samas ka $e * 1 = \sqrt{e} = 1$, kust $e = 1$, mis on eelnevaga vastuolus. Seega ühikelementi ei leidu.

G3: Ilma ühikelemendita ei saa pöördelemente leida.

KOMM: Olgu $a, b \in \mathbb{R}^+$. Siis $a * b = \sqrt{ab} = \sqrt{ba} = b * a$, sest reaalarvude korrutamine on kommutatiivne.

Vastus: $(\mathbb{R}^+, *)$ on kommutatiivne rühmoid.

d) üks on positiivne reaalarv, seetõttu on $*$ algebraline tehe.

G1: Olgu $a, b, c \in \mathbb{R}^+$. Siis $(a * b) * c = 1 * c = 1 = a * 1 = a * (b * c)$.

G2: Kuna $4 * x = 1$ mistahes $x \in \mathbb{R}^+$ korral, ei sobi ükski arv x ühikelemendiks.

G3: Ilma ühikelemendita ei saa pöördelemente leida.

KOMM: Kuna $a * b = 1 = b * a$ iga $a, b \in \mathbb{R}$ korral, on $*$ kommutatiivne.

Vastus: $(\mathbb{R}^+, *)$ on kommutatiivne poolrühm.

Ülesanne 9. Tõestada, et lõpliku poolrühma iga elemendi mingi aste on idempotent.

Lahendus: Olgu $a \in A$. Kuna A on lõplik hulk, siis leiduvad arvud $m, n \in \mathbb{N}$, $m > n$ selliselt, et $a^m = a^n$ (vastasel juhul oleks hulgas vähemalt loenduv arv elemente $a, a^2, a^3, \ldots$). Paneme muuseas tähele, et elemendi a astmed on korrektselt defineeritud, sest tehe on assotsiatiivne.

Siis iga $x > n$ korral $a^{x+m-n} = a^{x-n} \cdot a^m = a^{x-n} \cdot a^n = a^{x+n-n} = a^x$, sest astmed on defineeritud vaid positiivsete naturaalarvuliste astendajate korral. Seega, kuna $m(m-n) \geq m \cdot 1 > n$, siis

$$\begin{aligned} & [a^{m(m-n)}]^2 = a^{m(m-n)+m(m-n)} = a^{m(m-n)+(m-1)(m-n)} \\ = \; & a^{m(m-n)+(m-2)(m-n)} = \ldots = a^{m(m-n)}. \end{aligned}$$

Järelikult $a^{m(m-n)}$ on nõutud idempotent.

Ülesanne 13. Uurida, millised järgmistest hulga $\mathbb{R}$ teisenduste hulkadest on (Abeli) rühmad teisenduste kompositsiooni suhtes:

a) $\{f : \mathbb{R} \to \mathbb{R} | f(x) = ax + b, a, b \in \mathbb{R}, a < 0\}$.

Lahendus: Kuna vaid samasusteisendus $1_\mathbb{R}$ sobib teisenduste komponeerimisel ühikelemendiks, siis ei ole tegu monoidiga, sest: kui $1_\mathbb{R}(1) = a \cdot 1 + b = 1$, siis $a + b = 1$; aga samas $1_\mathbb{R}(0) = a \cdot 0 + b = 0$, seega $b = 0$ ja $a = 1 > 0$.

Vastus: See hulk ei ole rühm teisenduste korrutamise suhtes.

Ülesanne 14. Uurida, millised järgmistest maatriksite hulkadest on (Abeli) rühmad maatriksite korrutamise suhtes:

d) selliste maatriksite $S \in \mathrm{Mat}_n(\mathbb{R})$ hulk, mille korral $S^T A S = A$, kus A on fikseeritud regulaarne sümmeetriline (kaldsümmeetriline) maatriks;

Lahendus: Me teame, et maatriksite korrutamine on assotsiatiivne (G1), selle ühikelemendiks on ühikmaatriks ja pöördelemendiks pöördmaatriks. Olgu $S, T \in \mathrm{Mat}_n(\mathbb{R})$ ja $S^TAS = A$, $T^TAT = A$. Siis ka

$$(ST)^TA(ST) = T^T(S^TAS)T = T^TAT = A.$$

Seega on tegu algebralise tehtega.

G2: Ilmselt $E^TAE = EA = A$, ja ühikmaatriks kuulub sellesse hulka.

G3: Olgu $S \in \mathrm{Mat}_n(\mathbb{R})$ ja $S^TAS = A$. Siis $0 \neq |A| = |S^TAS| = |S^T| \cdot |A| \cdot |S|$, mistõttu $|S| \neq 0$ ja maatriksil S leidub pöördmaatriks S^{-1}.

Kuna $S^TAS = A$, siis

$$(S^{-1})^TAS^{-1} = (S^{-1})^T(S^TAS)S^{-1} = (SS^{-1})^TA(SS^{-1}) = EAE = A$$

ja ka A^{-1} kuulub sellesse hulka. Seega on antud juhul tegu rühmaga.

KOMM: Olgu $A = E \in \mathrm{Mat}_3(\mathbb{R})$, $B = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{Mat}_3(\mathbb{R})$ ja $C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \in \mathrm{Mat}_3(\mathbb{R})$. Siis $B^TAB = B^TB = E = A$, $C^TAC = E = A$, aga

$$BC = \begin{pmatrix} \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & -\frac{1}{4} & -\frac{1}{4} \\ 0 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \text{ ja } CB = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{4} & -\frac{1}{4} & \frac{1}{2} \\ \frac{1}{4} & -\frac{1}{4} & -\frac{1}{2} \end{pmatrix}.$$

Järelikult üldjuhul maatriksite korrutamine sellisel hulgal kommutatiivne ei ole (aga 2×2 maatriksite ja $A = E$ korral näiteks ikkagi on).

Vastus: Selline hulk on mittekommutatiivne rühm maatriksite korrutamise suhtes.

Ülesanne 16. Olgu antud rühmoid $A = \{a, b, c, d\}$ oma Cayley tabeliga

*	a	b	c	d
a	a	c	d	d
b	a	a	b	b
c	d	a	c	d
d	d	c	d	c

Teha kindlaks, millised alamhulkadest $\{a\}$, $\{c, d\}$, $\{a, c, d\}$ on rühmoidi A alamrühmoidid. Kas sellel rühmoidil on veel alamrühmoide?

Lahendus: Leiame iga elemendi poolt moodustatud alamrühmoidi: kuna $a * a = a$, siis $< a >= \{a\}$. Samas $b * b = a$, $a * b = c$, $a * c = d$ ja seega $< b >= A$. Veel on $d * d = c = c * c$, $d * c = c * d = d$, kust $< d >= \{c, d\}$. Lõpuks on $< c >= \{c\}$, sest $c * c = c$.

Eelneva põhjal on $\{a\}$, $\{c,d\}$ alamrühmoidid. Kuna $a*c = a*d = d*a = c*a = d$, on ka $\{a,c,d\}$ alamrühmoid. Iga elementi b sisaldav alamrühmoid on alati A ise, ja kuna $a*c = d$, on $< a,c >= \{a,c,d\}$. Lisaks nägime juba, et ka $\{c\}$ on alamrühmoid.

Meil on veel võimalik, et alamrühmoidi moodustaksid elemendid a ja d (eelnevast nähtuvalt see nii ei ole). Sellega on elementi b mitte sisaldavad alamhulgad ammendatud.

Vastus: Kõik kolm on alamrühmoidid, lisaks on ka $\{c\}$ ja A alamrühmoidid. Mõnikord loetakse ka tühi hulk alamrühmoidiks.

Ülesanne 19. Tõestada, et igal lõpmatul rühmal on lõpmatu palju alamrühmi.

Lahendus: Rühma G elemendi x järguks nimetatakse vähimat naturaalarvu n, mille korral $x^n = 1$. Kui sellist arvu ei leidu, siis öeldakse, et element x on lõpmatut järku.

Lõpmatus rühmas G kas kõik elemendid on lõplikku järku, või leidub vähemalt üks lõpmatut järku element x. Esimesel juhul valime vabalt ühe elemendi a_1 rühmast G. Siis selle elemendi poolt moodustatud alamrühm $< a_1 >$ on lõplik, seega $G \setminus < a_1 > \neq \emptyset$ ja on tegelikult samuti lõpmatu. Valime sealt elemendi $a_2 \in G \setminus < a_1 >$, moodustame $< a_2 >$, ja jälle on $(G \setminus < a_1 >) \setminus < a_2 >$ lõpmatu. Selliselt jätkates saame loenduva arvu alamrühmi $< a_1 >, < a_2 >, \ldots$, mis valikuprotsessi tõttu on kõik erinevad.

Teisel juhul on meil lõpmatut järku element a, s.t. $a^m \neq a^n$ mistahes $m, n \in \mathbb{N}$, $m \neq n$ korral. Aga siis on meil alamrühmad $G_n = \{a^{nk} | k \in \mathbb{Z}\}$. Seejuures suvalised kaks neist on erinevad, sest kui näiteks $n > m$, siis ilmselt $a^m \notin G_n$, sest vastasel korral ka $a^m = 1$, või $a^m = a^{kn}$ ($|k|>0$, millest $kn - m \neq 0$) ja $a^{kn-m} = 1$. See on aga vastuolus sellega, et a on lõpmatut järku. Seega on meil loenduv arv alamrühmi G_n.

2. praktikumi ülesanded

Ülesanne 1. Millised järgmistest hulkadest on ringid tavalise arvude liitmise ja korrutamise suhtes? Kas nende hulgas on korpusi?

a) $n\mathbb{Z} = \{na | a \in \mathbb{Z}\}, n \in \mathbb{N}$; c) $\{\frac{a}{b} \in \mathbb{Q} | a, b \in \mathbb{Z}, \text{SÜT}(a, b) = 1, 12 \vdots b\}$;

b) $\{a + b\sqrt[3]{2} | a, b \in \mathbb{Q}\}$; d) $\{\frac{a}{b} \in \mathbb{Q} | a, b \in \mathbb{Z}, \text{SÜT}(a, b) = 1, b \not\vdots 5\}$.

Lahendus: a) Fikseerime naturaalarvu n.

$R1$: Olgu $na, nb \in n\mathbb{Z}$, st $a, b \in \mathbb{Z}$. Siis $na + nb = n(a + b) \in n\mathbb{Z}$, sest $a + b \in \mathbb{Z}$. Seega on $(n\mathbb{Z}, +)$ rühmoid.

$AG1$: Igasuguste reaalarvude liitmine on assotsiatiivne.

$AG2$: Kuna $0 = 0z$, siis on nullelement alati olemas.

$AG3$: Ilmselt $-(nz) = (-n)z$ iga $z \in \mathbb{Z}$ korral, sest $(-n)z + nz = (n - n)z = 0z = 0$.

$AG4$: Igasuguste reaalarvude liitmine on kommutatiivne.

$R2$: Olgu $na, nb \in n\mathbb{Z}$, st $a, b \in \mathbb{Z}$. Siis $na \cdot nb = n[nab] \in n\mathbb{Z}$, sest $nab \in \mathbb{Z}$. Seega on $(n\mathbb{Z}, \cdot)$ rühmoid.

$G1$: Igasuguste reaalarvude korrutamine on assotsiatiivne.

$G2$: Vaid juhul $1\mathbb{Z}$ on $1 = 1 \cdot 1 \in 1\mathbb{Z}$. Kui $n \neq 1$, siis on $|nz| = 0$ või $|nz| > 1$ iga $z \in \mathbb{Z}$ korral. Seega ei ole võimalik, et $1 = nz$ mingi $n \neq 1$ ja $z \in \mathbb{Z}$ korral. Järelikult on $n\mathbb{Z}$ monoid vaid siis, kui $n = 1$.

$R3$: Reaalarvude liitmine on korrutamise suhtes distributiivne.

Seega on $n\mathbb{Z}$ ring. Isegi kommutatiivne ring.

Kahe pöördarv $\frac{1}{2}$ ei ole täisarv ja ei kuulu hulka $1\mathbb{Z} \setminus \{0\}$, mis ei ole seega rühm. Kui $n \neq 1$, ei ole hulgas $n\mathbb{Z}$ isegi ühikelementi. Järelikult ei ole $n\mathbb{Z}$ korpus.

Vastus: $(n\mathbb{Z}, \cdot)$ on ring, mis ei ole korpus.

b) Kuna $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$, ja ei ole võimalik (mille näitamine läheb Algebra I kursusest väga kaugele) avaldada $\sqrt[3]{4} = a + b\sqrt[3]{2}$ mingite $a, b \in \mathbb{Q}$ korral, siis ei ole antud hulk korrutamise suhtes kinnine ja tegu ei ole ringiga. Kontrolltöösse selliseid ülesandeid ei tule, ja kui kogemata juhtubki tulema, siis mistahes vähegi detailsem katse seda lahendada annab täispunktid.

Vastus: See hulk ei ole ring.

c) $R1$: Olgu $a, b, c, d \in \mathbb{Z}$, $\text{SÜT}(a, b) = \text{SÜT}(c, d) = 1$, $12 \vdots b$, $12 \vdots d$. Siis $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. Taandame saadud murru. Siis: kui $b = c$, on taandatud murru nimetaja 1, ja $12 \vdots 1$. Kui $b = 12$ või $d = 12$, saame lugejat ja nimetajat jagada vähemalt arvuga d või c, mistõttu on taandatud murru nimetaja absoluutväärtus ülimalt 12 ja 12 jagaja. Kui $\max(b, d) = 6$, $b \neq d$, siis $\min(b, d) \in \{1, 2, 3, 4\}$. Esimesel kahel juhul on taandatud murru nimetaja absoluutväärtus ülimalt 12 ja 12 jagaja, kolmandal ja neljandal juhul saame murru lugejat ja nimetajat jagada vähemalt arvuga 3 või 2. Tulemuse nimetaja absoluutväärtus on jälle ülimalt 12 ja 12 jagaja. Ülejäänud juhtudel on $|bd| \leq 12$. Seega on tegu rühmoidiga liitmise suhtes.

$AG1$: Igasuguste reaalarvude liitmine on assotsiatiivne.

$AG2$: Loeme antud juhul nulli sellese hulka sisse. Siis on meil nullelement olemas. Muidu ei ole rangelt võttes $\SÜT(0, x)$ defineritud v.a. kui $x = 0$ ja meil ei ole ringi.

$AG3$: Ilmselt $-\frac{a}{b} = \frac{-a}{b}$.

$AG4$: Igasuguste reaalarvude liitmine on kommutatiivne.

$R2$: Olgu $a, b, c, d \in \mathbb{Z}$, $\SÜT(a, b) = \SÜT(c, d) = 1$, $12 \vdots b$, $12 \vdots d$. Siis $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. Osas $R1$ tehtud aruteluga analoogiliselt arutledes saame, et ka $\frac{ac}{bd}$ taandatud kuju korral on nimetajaks 12 jagaja. Seega on tegu korrutamise suhtes rühmoidiga.

$G1$: Igasuguste reaalarvude korrutamine on assotsiatiivne.

$G2$: Kuna $1 = \frac{1}{1}$, ja $12 \vdots 1$, on meil monoid.

Seega on antud hulk ring arvude liitmise ja korrutamise suhtes.

$R3$: Reaalarvude liitmine on korrutamise suhtes distributiivne.

Samas $\frac{5}{3}$ kuulub sellesse hulka, aga $\frac{3}{5}$ ei kuulu, sest $12 \not\vdots 5$. Järelikult ei ole $\{\frac{a}{b} \in \mathbb{Q} | a, b \in \mathbb{Z}, \SÜT(a, b) = 1, 12 \vdots b\} \setminus \{0\}$ rühm ja tegu ei ole korpusega.

Vastus: See hulk moodustab ringi, aga mitte korpuse.

d) Analoogiliselt ülesandega c) saab näidata, et kehtivad $R1, AG1-AG4, R2, G1, G2$ ja $R3$. Seega tegu on ringiga. Ja samamoodi $\frac{5}{3}$ kuulub sellesse hulka, aga $\frac{3}{5}$ ei kuulu, mistõttu ei ole tegu korpusega.

Vastus: See hulk moodustab ringi, aga mitte korpuse.

Ülesanne 5. Tõestada, et maatriksid

$$O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, T = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

üle $\mathbb{Z}_2$ moodustavad maatriksite liitmise ja korrutamise suhtes korpuse. Koostada selle korpuse liitmise ja korrutamise Cayley tabelid.

Lahendus: Ei ole raske neid maatrikseid omavahel liita ja korrutada ning saada järgmised Cayley tabelid:

$+$	O	E	S	T
O	O	E	S	T
E	E	O	T	S
S	S	T	O	E
T	T	S	E	O

$\cdot$	O	E	S	T
O	O	O	O	O
E	O	E	S	T
S	O	S	T	E
T	O	T	E	S

Kuna maatriksite liitmine on maatriksite korrutamise suhtes distributiivne ja mõlemad tehted on assotsiatiivsed, ja eelnevatest Cayley tabelitest on näha ühikelemendi (E), nullelemendi (O), vastaselementide ja pöördelementide (v.a. O oma) olemasolu ning mõlema tehte kommutatiivsus, on tegu isegi kommutatiivse korpusega.

Ülesanne 6. Teha kindlaks, millised järgmistest hulkadest on ringid või korpused. Iga ühikelemendiga ringi korral, mis ei ole korpus, leida selle ringi pööratavate elementide hulk. Ülesannetes a)-f) on teheteks arvude tavaline liitmine ja korrutamine.

c) $\{a + b\sqrt{3} | a, b \in 2\mathbb{Z}\}$; e) $\{a + b\sqrt{2}i | a, b \in \mathbb{Q}\}$.

Lahendus: c) $R1$: Olgu $a, b, c, d \in 2\mathbb{Z}$. Siis

$$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3}.$$

Jřelikult on liitmine siin algebraline tehe.

$AG1$: Reaalarvude liitmine on assotsiatiivne.

$AG2$: Ilmselt $0 = 0 + 0\sqrt{3}$, sest $0 \in 2\mathbb{Z}$.

$AG3$: Samamoodi $-(a + b\sqrt{3}) = (-a) + (-b)\sqrt{3}$, kuna paarisarvude vastandarvud on paarisarvud.

$AG4$: Reaalarvude liitmine on kommutatiivne.

$R2$: Olgu $a, b, c, d \in 2\mathbb{Z}$. Siis

$$(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}.$$

Kuna paarisarvude summad ja korrutised on paarisarvud, siis jřelikult on korrutamine samuti algebraline tehe.

$G1$: Reaalarvude korrutamine on assotsiatiivne.

$G2$: Kui $1 = a + b\sqrt{3}$, siis $\sqrt{3} = \frac{1-a}{b} \in \mathbb{Q}$, kui $b \neq 0$. Järelikult $b = 0$, ja $a = 1$. Kuid samas $1 \notin 2\mathbb{Z}$. Seega ühikelement siia hulka ei kuulu.

$R3$: Reaalarvude liitmine on korrutamise suhtes distributiivne.

$G3$: Ühikelementi ei ole, seega ei saa pöördelemente defineeridagi.

$G4$: Reaalarvude korrutamine on kommutatiivne.

Reaalarvude seas nullitegureid ei saa olla, sest kui $ab = 0$, siis $a = 0$ või $b = 0$, kui $a, b \in \mathbb{R}$.

Vastus: Tegu on kommutatiivse ringiga, mis ei ole korpus ja milles ei ole nullitegureid.

e) $R1$: Olgu $a, b, c, d \in \mathbb{Q}$. Siis

$$(a + b\sqrt{2}i) + (c + d\sqrt{2}i) = (a + c) + (b + d)\sqrt{2}i.$$

Jřelikult on liitmine siin algebraline tehe.

$AG1$: Kompleksarvude liitmine on assotsiatiivne.

$AG2$: Ilmselt $0 = 0 + 0\sqrt{2}i$, sest $0 \in \mathbb{Q}$.

$AG3$: Samamoodi $-(a + b\sqrt{2}i) = (-a) + (-b)\sqrt{2}i$, kuna ratsionaalarvude vastandarvud on ratsionaalarvud.

$AG4$: Kompleksarvude liitmine on kommutatiivne.

$R2$: Olgu $a, b, c, d \in \mathbb{Q}$. Siis

$$(a + b\sqrt{2}i)(c + d\sqrt{2}i) = (ac - 2bd) + (ad + bc)\sqrt{2}i.$$

Kuna ratsionaalarvude summad ja korrutised on ratsionaalarvud, siis järelikult on korrutamine samuti algebraline tehe.

$G1$: Kompleksarvude korrutamine on assotsiatiivne.
$G2$: Ilmselt $1 = 1 + 0\sqrt{2}i$.
$R3$: Kompleksarvude liitmine on korrutamise suhtes distributiivne.
$G3$: Olgu $a, b \in \mathbb{Q}$ ja $a + b\sqrt{2}i \neq 0$, st kas $a \neq 0$ või $b \neq 0$. Siis

$$\frac{1}{a + b\sqrt{2}i} = \frac{a - b\sqrt{2}i}{a^2 - (b\sqrt{2}i)^2} = \frac{a}{a^2 + 2b^2} + \frac{-b}{a^2 + 2b^2}\sqrt{2}i.$$

On selge, et $\frac{a}{a^2+2b^2}, \frac{-b}{a^2+2b^2} \in \mathbb{Q}$, ja murru lugeja on positiivne. Järelikult on tegu korpusega. [Kontroll:

$$\begin{aligned} & (a + b\sqrt{2}i)(\frac{a}{a^2 + 2b^2} + \frac{-b}{a^2 + 2b^2}\sqrt{2}i) \\ = \quad & \frac{a^2 - b^2\sqrt{2}^2 i^2}{a^2 + 2b^2} + \frac{(-ab + ba)\sqrt{2}i}{a^2 + b^2} = 1 + 0 = 1. \ ] \end{aligned}$$

$G4$: Kompleksarvude korrutamine on kommutatiivne.
Vastus: Tegu on kommutatiivse korpusega.

Ülesanne 7. Tõestada, et järgmised maatriksite hulgad on ringid maatriksite liitmise ja korrutamise suhtes. Teha kindlaks, millised neist on kommutatiivsed ja millised on korpused. Leida kõik pööratavad elemendid neis ringides, mis ei ole korpused. Leida kõik nullitegurid nulliteguritega ringides.
b) $M = \left\{ \begin{pmatrix} a & 3b \\ b & a \end{pmatrix} | a, b \in 2\mathbb{Z} \right\}$.
Lahendus: $R1$: Olgu $c, d, e, f \in 2\mathbb{Z}$. Siis

$$\begin{pmatrix} c & 3d \\ d & c \end{pmatrix} + \begin{pmatrix} e & 3f \\ f & e \end{pmatrix} = \begin{pmatrix} c + e & 3(d + f) \\ d + f & c + e \end{pmatrix}.$$

Kuna paarisarvude summa on paarisarv, siis kuulub summamaatriks hulka M.
$AG1$: Maatriksite liitmine on assotsiatiivne.
$AG2$: Kuna $0 \in 2\mathbb{Z}$, siis nullmaatriks kuulub hulka M, võttes $a = b = 0$.
$AG3$: Ilmselt $-\begin{pmatrix} a & 3b \\ b & a \end{pmatrix} = \begin{pmatrix} -a & -3b \\ -b & -a \end{pmatrix}$ kuulub hulka M.
$AG4$: Maatriksite liitmine on kommutatiivne.
$R2$: Olgu $c, d, e, f \in 2\mathbb{Z}$. Siis

$$\begin{pmatrix} c & 3d \\ d & c \end{pmatrix} \begin{pmatrix} e & 3f \\ f & e \end{pmatrix} = \begin{pmatrix} ce + 3df & 3cf + 3de \\ cf + de & ce + 3df \end{pmatrix}.$$

Kuna paarisarvude korrutised ja summad on alati paarisarvud, siis kuulub saadud maatriks hulka M (kus $a = ce + 3df$, $b = cd + de$), ja tegu on rühmoidiga.
$G1$: Maatriksite korrutamine on assotsiatiivne.
$G2$: Kuna $a \in 2\mathbb{Z}$, ei saa ühikmaatriksit sellisel kujul esitada, ja ühikmaatriks on ainus maatriks, mis maatriksite korrutamisel ühikelemendiks sobib. Seega monoidi meil ei ole.

$R3$: Maatriksite liitmine on maatriksite korrutamise suhtes distributiivne.

$G3$: Kuna $\det\begin{pmatrix} a & 3b \\ b & a \end{pmatrix} = a^2 - 3b^2$, ja $|a^2 - 3b^2| > 1$ (sest kui $a^2 = 3b^2$, siis $\sqrt{3} = \frac{a}{b}$, aga $\sqrt{3}$ on irratsionaalarv, ja $a^2 - 3b^2 \neq \pm 1$, sest vasakul pool võrdusmärki on on paarisarv), ei saa ühelgi maatriksil olla pöördmaatriksit hulgas M, sest maatriksi ja tema pöördmaatriksi determinandid on pöördarvud. Kui üks neist on ühest suurem, peab teine olema väiksem. Järelikult pööratavaid elemente siin ei leidu, isegi kui ühikmaatriks sellesse hulka kuuluks.

$G4$: Kuna analoogiliselt $R2$-ga on $c, d, e, f \in 2\mathbb{Z}$ korral

$$\begin{pmatrix} e & 3f \\ f & e \end{pmatrix}\begin{pmatrix} c & 3d \\ d & c \end{pmatrix} = \begin{pmatrix} ce + 3df & 3cf + 3de \\ cf + de & ce + 3df \end{pmatrix},$$

siis on antud juhul tegu kommutatiivse ringiga.

Olgu $A = \begin{pmatrix} c & 3d \\ d & c \end{pmatrix} \neq 0 \neq \begin{pmatrix} e & 3f \\ f & e \end{pmatrix} = B$, st $a, b, c, d \in 2\mathbb{Z}$ ja kas $c \neq 0$ või $d \neq 0$ ja $e \neq 0$ või $f \neq 0$. Ilmselt $\det(A) = c^2 - 3d^2 \neq 0 \neq e^2 - 3f^2 = \det(B)$, sest muidu oleks nt. $c^2 - 3d^2 = 0$, kust juhul $d \neq 0$ on $\sqrt{3} = \frac{c}{d} \in \mathbb{Q}$, vastuolu. Kui $d = 0$, siis ka $d = 0$, samuti vastuolu. Ja teise determinandi korral saab samamoodi arutleda. Järelikult $\det(AB) = \det(A) \cdot \det B \neq 0$, mistõttu $AB \neq 0$. Nullitegureid selles ringis seega olla ei saa.

Vastus: See hulk moodustab kommutatiivse nulliteguriteta ringi, mis ei ole korpus.

Märkus: tegelikult on näha, et struktuurid ülesannetes 6. c) ja 7. b) on isomorfsed, ehk tegu on sama struktuuriga, antud juhul kommutatiivse nulliteguriteta ringiga, mis ei ole korpus. Esitatud detailsed tõestused kinnitavad seda asjaolu.

Ülesanne 8. Tõestada, et järgmised funktsioonide hulgad $\mathbb{R} \to \mathbb{R}$ on kommutatiivsed ühikelemendiga ringid funktsioonide punktiviisilise liitmise ja korrutamise suhtes. Leida nende ringide pööratavad elemendid. Millistes neist ringidest leidub nullitegureid?

c) lõigul $[0, 1]$ diferentseeruvate funktsioonide hulk;

Lahendus: $R1$: Kahe diferenseeruva funktsiooni summa on diferentseeruv $((f + g)' = f' + g')$.

$AG1$: Kuna iga $x \in \mathbb{R}$ ja diferentseeruvate funktsioonide f, g, h korral $(f+(g+h))(x) = f(x)+(g(x)+h(x)) = (f(x)+g(x))+h(x) = ((f+g)+h)(x)$, siis $f + (g + h) = (f + g) + h$.

$AG2$: Nullfunktsioon on diferentseeruv.

$AG3$: Kui funktsioon f on diferenseeruv, siis on seda ka funktsioon $-f$, kus $(-f)(x) = -f(x)$ iga $x \in \mathfrak{V}$ korral.

$AG4$: Analoogiliselt $AG1$-ga $f + g = g + f$ suvaliste diferentseeruvate funktsioonide f, g korral.

$R2$: Kahe diferentseeruva funktsiooni korrutis on diferentseeruv $((f \cdot g)' = f'g + fg')$.

$G1$: Analoogiliselt $AG1$-ga $f(gh) = (fg)h$ suvaliste diferentseeruvate funktsioonide f, g, h korral.

$G2$: Konstantne funktsioon 1, st $1(x) = 1$ iga $x \in \mathbb{R}$ korral, on diferentseeruv.

$R3$: Kuna iga $x \in \mathbb{R}$ ja diferentseeruvate f, g, h korral

$$\begin{aligned}[(f+g)\cdot h](x) &= (f+g)(x)\cdot h(x) = (f(x)+g(x))\cdot h(x)\\ &= f(x)\cdot h(x) + g(x)\cdot h(x) = [(f\cdot h)+(g\cdot h)](x),\end{aligned}$$

on meil $(f+g)\cdot h = f\cdot h + g\cdot h$. Analoogiliselt saab näidata, et $f\cdot(g+h) = f\cdot g + f\cdot h$.

$G3$: Funktsiooni $f : \mathbb{R} \to \mathbb{R}$ pöördfunktsiooniks peaks ilmselt olema $\frac{1}{f} : \mathbb{R} \to \mathbb{R}$, kus $\frac{1}{f}(x) = \frac{1}{f(x)}$. Selline funktsioon leidub parajasti siis, kui $f(x) \neq 0$ iga $x \in \mathbb{R}$ korral.

$G4$: Analoogiliselt $AG1$-ga $fg = gf$ suvaliste diferentseeruvate funktsioonide f, g korral.

Olgu $f(x) = (x - 0,5)^2$, kui $x \in [0,5; 1]$ ja $f(x) = 0$, kui $x \in [0; 0,5]$, ning $g(x) = 0$, kui $x \in [0,5; 1]$ ja $g(x) = (x - 0,5)^2$, kui $x \in [0; 0,5]$. Siis $f \neq 0$, $g \neq 0$, aga $fg = 0$ ja mõlemad funktsioonid on diferentseeruvad (ainus küsitav koht on punktis $0,5$, kus mõlema funktsiooni tuletised kummalgi poollõigul annavad 0).

Vastus: Pööratavad elemendid on diferentseeruvad funktsioonid, mille väärtuseks ei ole 0 mitte üheski punktis lõigul $[0, 1]$. Nullitegureid leidub.

Ülesanne 10. Leida ringide $\mathbb{Z}_7, \mathbb{Z}_{10}, \mathbb{Z}_{12}$ kõik pööratavad elemendid.

Lahendus: Vt ülesannet 9. b). Selle põhjal on $\mathbb{Z}_7$ pööratavad elemendid $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$ ja $\overline{6}$, st kõik nullist erinevad elemendid. Ringi $\mathbb{Z}_{10}$ pööratavad elemendid on järelikult $\overline{1}, \overline{3}, \overline{7}$ ja $\overline{9}$. Ja ringi $\mathbb{Z}_{12}$ pööratavad elemendid on $\overline{1}, \overline{5}, \overline{7}$ ja $\overline{11}$.

Ülesanne 18. Leida ringide $\mathbb{Z}_7, \mathbb{Z}_{10}$ ja $\mathbb{Z}_{12}$ kõik alamringid.

Lahendus: Olgu $R \leq \mathbb{Z}_7$ alamring. Siis kas $R = \{\overline{0}\}$ või leidub $\overline{a} \in R$, $a \neq 0$.

Kui $a = 1$, siis $\overline{1} + \overline{1} = \overline{2} \in R$, $\overline{1} + \overline{2} = \overline{3} \in R$ jne. Seega $R = \mathbb{Z}_7$.

Kui $a = 2$, siis $\overline{2} + \overline{2} + \overline{2} + \overline{2} = \overline{1} \in R$ ja eelmise arutelu põhjal ikkagi $R = \mathbb{Z}_7$.

Kui $a = 3$, siis $\overline{3} + \overline{3} + \overline{3} + \overline{3} + \overline{3} = \overline{1} \in R$ ja ikkagi $R = \mathbb{Z}_7$.

Kui $a = 4$, siis $\overline{4} + \overline{4} = \overline{1} \in R$ ja $R = \mathbb{Z}_7$.

Kui $a = 5$, siis $\overline{5} + \overline{5} + \overline{5} = \overline{1} \in R$ ja $R = \mathbb{Z}_7$.

Kui $a = 6$, siis $\overline{6} + \overline{6} + \overline{6} + \overline{6} + \overline{6} + \overline{6} = \overline{1} \in R$ ja $R = \mathbb{Z}_7$.

Seega on ainsateks võimalikeks alamringideks $\{\overline{0}\}$ ja R. Ilmselt on need hulgad ka kinnised liitmise ja korrutamise suhtes.

Olgu $R \leq \mathbb{Z}_{10}$ alamring. Jälle kas $R = \{\overline{0}\}$ või leidub $\overline{a} \in R$, $a \neq 0$.

Kui $a = 1$, siis saame jällegi, et $R = \mathbb{Z}_{10}$.

Kui $a = 2$, siis $\overline{2} + \overline{2} = 4$, $\overline{2} + \overline{4} = \overline{6}$, $\overline{2} + \overline{6} = \overline{8}$, $\overline{4} + \overline{6} = 0$ ja ei ole raske näha, et paarisarve (ja nulli) liites ja korrutades ning kümnega jagades on jäägiks paarisarv või null. Seega on üks alamring $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$.

Kui $a = 3$, siis $\overline{3} + \overline{3} + \overline{3} + \overline{3} + \overline{3} + \overline{3} + \overline{3} = \overline{1}$ ja $R = \mathbb{Z}_{10}$.

Samamoodi on $a = 7$ või $a = 9$ korral $3 \cdot \overline{7} = \overline{1} = 9 \cdot \overline{9}$ ja $R = \mathbb{Z}_{10}$.

Kui $a = 4, a = 6$ või $a = 8$, siis $3 \cdot \overline{4} = 2$, $2 \cdot \overline{6} = \overline{2}$ või $4 \cdot \overline{8} = \overline{2}$ ja eelneva põhjal $R = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$.

Kui $a = 5$, siis $\overline{5} + \overline{5} = \overline{0}$, $\overline{5} \cdot \overline{5} = \overline{5}$, $\overline{5} + \overline{0} = \overline{5}$, $\overline{0} + \overline{0} = \overline{0}$ ja $\overline{0} \cdot \overline{0} = \overline{0} \cdot \overline{5} = \overline{0}$. Seega on $R = \{\overline{0}, \overline{5}\}$.

Vastus: $\mathbb{Z}_{10}$ alamringid on $\{\overline{0}\}$, $\{\overline{0}, \overline{5}\}$, $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$, $\mathbb{Z}_{10}$.