1 Algebralised struktuurid

Meenutame põhiliste algebraliste struktuuride definitsioone.

Definitsioon 1 Olgu A mittetühi hulk. Kujutust $\omega : A^n \to A$ nimetatakse *n-kohaliseks algebraliseks tehteks* hulgal A.

Definitsioon 2 *Rühmaks* nimetatakse hulka A, millel on defineeritud üks kahekohaline tehe $*$ (tähistame $*((a,b)) = a * b$), nii et

G1. $(\forall a, b, c \in A)((a * b) * c = a * (b * c))$ (assotsiatiivsus);

G2. $(\exists e \in A)(\forall a \in A)(a * e = e * a = a)$ (leidub *ühikelement*);

G3. $(\forall a \in A)(\exists a^{-1} \in A)(a * a^{-1} = a^{-1} * a = e)$ (igal elemendil leidub *pöördelement*).

Öeldakse, et hulk A on rühm tehte $*$ suhtes ja kirjutatakse $(A, *)$.

Kui hulgal A on defineeritud kahekohaline algebraline tehe, siis A on rühmoid. Assotsiatiivset rühmoidi nimetatakse *poolrühmaks*. Kui poolrühmas leidub ühikelement, siis teda nimetatakse *monoidiks*.

Kahekohaline tehe $*$ hulgal A on *kommutatiivne*, kui kehtib samasus

KOMM. $(\forall a, b \in A)(a * b = b * a)$.

Rühma, mille tehe on kommutatiivne, nimetatakse *kommutatiivseks* ehk *Abeli rühmaks*.

Tihti tähistatakse Abeli rühma tehet märgiga "+" ja nimetatakse liitmiseks. Sellisel juhul võtavad Abeli rühma aksioomid järgmise kuju:

AG1. $(\forall a, b, c \in A)((a + b) + c = a + (b + c))$ (assotsiatiivsus);

AG2. $(\exists 0 \in A)(\forall a \in A)(a + 0 = a)$ (leidub *nullelement*);

AG3. $(\forall a \in A)(\exists -a \in A)(a + (-a) = 0)$ (igal elemendil leidub *vastandelement*);

AG4. $(\forall a, b \in A)(a + b = b + a)$ (kommutatiivsus).

Definitsioon 3 *Ringiks* nimetatakse hulka R, millel on defineeritud kaks kahekohalist tehet, $+$ (liitmine) ja $\cdot$ (korrutamine), nii et

R1. $(R, +)$ on Abeli rühm;

R2. $(R, \cdot)$ on monoid;

R3. $(\forall a, b, c \in R)(a \cdot (b + c) = a \cdot b + a \cdot c$ ja $(a + b) \cdot c = a \cdot c + b \cdot c)$ (distributiivsus).

Märkus 1 Tihti defineeritakse ringid ilma nõudeta R2. Sellisel juhul kutsutakse meie poolt vaadeldavaid ringe assotsiatiivseteks ühikelemendiga ringideks.

Märkus 2 Kui mingis algebralises struktuuris kõneldakse korrutamistehtest $\cdot$, siis enamasti jäetakse tehtemärk ära ning kirjutatakse $a \cdot b$ asemel lihtsalt ab.

Definitsioon 4 Ringi $(R, +, \cdot)$ nimetatakse *korpuseks*, kui igal nullist erineval elemendil on olemas pöördelement. Sel juhul $(R \setminus \{0\}, \cdot)$ on rühm.

Ringi (korpust) nimetatakse *kommutatiivseks*, kui tema korrutamine on kommutatiivne.

Ringi R nullist erinevat elementi a nimetatakse *nulliteguriks*, kui leidub selline nullist erinev element $b \in R$, et $ab = 0$.

Lause 1 *Korpuses ei ole nullitegureid.*

Ülesanne 1 *Mitu a) ühekohalist, b) kahekohalist, c) kolmekohalist algebralist tehet saab defineerida kaheelemendilisel hulgal?*

Vaatleme kaheelemendilist hulka A. Saab tõestada, et kui B on m-elemendiline hulk, siis leidub 2^m kujutust $B \to A$. Kuna ühekohaline tehe hulgal A on lihtsalt teisendus $A \to A$, siis ühekohalisi tehteid on $2^2 = 4$. Kahekohalisi tehteid, s.t. kujutusi $A^2 \to A$, on $2^{(2^2)} = 16$ ja kolmekohalisi tehteid on $2^{(2^3)} = 256$.

Ülesanne 2 *Iga allpooldefineeritud tehte $*$ korral tooge näiteid arvuhulkadest millel see tehe on algebraline tehe ja millel mitte.*

a) $a * b = a + b$;

b) $a * b = ab$;

c) $a * b = \text{SÜT}(a, b)$;

d) $a * b = a^b$;

e) $a * b = a - b$;

f) $a * b = a^2 + b^2$;

Järgneva tabeli teises veerus on näited hulkadest, millel antud tehe on algebraline, ja kolmandas veerus näited hulkadest, millel ei ole.

Tehe	On algebrline tehe	Ei ole algebraline tehe
a) $a + b$	$\{0\}$, $\{2^k \mid k \in \mathbb{N}\}$	$\{1, 2, 4\}$, algarvude hulk
b) ab	$\{-1, 0, 1\}$, $\{2^k \mid k \in \mathbb{Z}\}$	$\mathbb{Z}^-$, irratsionaalarvude hulk
c) $\text{SÜT}(a, b)$	$\{1, 2, 3\}$, $\{2^k \mid k \in \mathbb{N} \cup \{0\}\}$	$\{2, 3\}$, algarvude hulk
d) a^b	$\{0, 1\}$, $\mathbb{N}$	$\{2\}$, $\mathbb{Z}$
e) $a - b$	$\{0\}$, $\mathbb{Z}$	$\{1\}$, $\mathbb{N}$
f) $a^2 + b^2$	$\{0\}$, $\mathbb{N}$	$\{1\}$, $\mathbb{Z}^-$

Ülesanne 3 *Uurige iga allpool naturaalarvude hulgal defineeritud tehte $*$ korral tema omadusi, s.t tehke kindlaks, kas see tehe on algebraline tehe hulgal $\mathbb{N}$, kas ta on assotsiatiivne, kommutatiivne, kas leidub ühikelement, millistel elementidel on pöördelemendid.*

a) $a * b = \max\{a, b\}$;

b) $a * b = \min\{a, b\}$;

c) $a * b = \text{SÜT}(a, b)$;

d) $a * b = \text{VÜK}(a, b)$;

e) $a * b = a + b + 3$;

f) $a * b = a$.

a) Kuna mistahes naturaalarvude korral $a * b = \max\{a, b\} \in \mathbb{N}$, siis $*$ on algebraline tehe ja $(\mathbb{N}, *)$ rühmoid. Uurime tingimusi G1-G3 ja KOMM.

G1. Tehe $*$ on assotsiatiivne, sest iga $a, b, c \in \mathbb{N}$ korral

$$(a*b)*c = \max\{a, b\}*c = \max\{\max\{a, b\}, c\} = \max\{a, \max\{b, c\}\} = a*\max\{b, c\} = a*(b*c).$$

G2. Kuna $a * 1 = \max\{a, 1\} = a = \max\{1, a\} = 1 * a$ iga $a \in \mathbb{N}$ korral, siis naturaalarv 1 on ühikelement tehte $*$ suhtes.

G3. Ühikelement on alati pööratav. Kui aga $a \in \mathbb{N}$ ja $a \geq 2$, siis elemendil a ei leidu pöördelementi tehte $*$ suhtes, sest $a * b = \max\{a, b\} \geq a \geq 2$ ja seega $a * b \neq 1$ ühegi $a \in \mathbb{N}$ korral. Seega ühikelement on ainus pööratav element ja tegemist ei ole rühmaga.

KOMM. Tehe $*$ on kommutatiivne, sest $a * b = \max\{a, b\} = \max\{b, a\} = b * a$ iga $a, b \in \mathbb{N}$ korral.

Vastus: $(\mathbb{N}, *)$ on kommutatiivne monoid.

Ülesanne 4 *Millised järgmistest hulkadest on ringid tavalise arvude liitmise ja korrutamise suhtes? Kas nende hulgas on korpusi?*

a) $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}, n \in \mathbb{N}$;

b) $\left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$;

c) $\left\{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\right\}$;

d) $\left\{\frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z}, \text{SÜT}(a, b) = 1, 12 \vdots b\right\}$;

e) $\left\{\frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z}, \text{SÜT}(a, b) = 1, b \not\vdots 5\right\}$.

b) Tähistame $R := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. On selge, et $R \subseteq \mathbb{R}$. Veendume, et reaalarvude liitmine ja korrutamine on algebralised tehted hulgal R. Mistahes $a, b, c, d \in \mathbb{Q}$ korral

$$\begin{aligned}(a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a + c) + (b + d)\sqrt{2} \in R,\\ (a + b\sqrt{2})(c + d\sqrt{2}) &= (ac + 2bd) + (ad + bc)\sqrt{2} \in R,\end{aligned}$$

sest $a + c, b + d, ac + 2bd, ad + bc \in \mathbb{Q}$. Seega on $+$ ja $\cdot$ tõesti algebralised tehted.

Kuna kõik R elemendid on ühtlasi ka reaalarvud ja reaalarvude liitmine ja korrutamine on assotsiatiivne ja kommutatiivne, siis ka hulga R elementide liitmine ja korrutamine on assotsiatiivne ja kommutatiivne. Täpselt samal põhjusel kehtivad hulga R elementide jaoks distributiivsuse säädused. Kuna $0 = 0 + 0 \cdot \sqrt{2} \in R$ ja iga $r \in R$ korral $r + 0 = r$, siis 0 on nullelement. Elemendi $a + b\sqrt{2} \in R$ vastandelemendiks on element $(-a) + (-b)\sqrt{2} \in R$, sest $(a + b\sqrt{2}) + ((-a) + (-b)\sqrt{2}) = 0$. Seega $(R, +)$ on Abeli rühm. Kuna $1 = 1 + 0 \cdot \sqrt{2} \in R$ ja $r \cdot 1 = r$ iga $r \in R$ korral ning nägime, et korrutamine on assotsiatiivne, siis $(R, \cdot)$ on monoid. Seega kokkuvõttes $(R, +, \cdot)$ on ring.

Näitame veel, et R on korpus. Selleks peame veenduma, et igal elemendil $a + b\sqrt{2} \neq 0$, $a, b \in \mathbb{Q}$, on olemas pöördelement. Kindlasti on sellel elemendil olemas pöördelement korpuses $\mathbb{R}$, selleks on pöördarv $\frac{1}{a+b\sqrt{2}} \in \mathbb{R}$. Paneme tähele, et kui $a + b\sqrt{2} \neq 0$, siis kas $a \neq 0$ või $b \neq 0$. Kui me oletaksime, et $a - b\sqrt{2} = 0$, siis võrdusest $a = b\sqrt{2}$ saaksime, et tegelikult $a \neq 0$ ja $b \neq 0$ ja seega $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$, mis aga ei ole võimalik. Seega $a - b\sqrt{2} \neq 0$ ja

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in R,$$

sest $\frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in \mathbb{Q}$. Sellega oleme näidanud, et $\frac{1}{a+b\sqrt{2}}$ on elemendi $a+b\sqrt{2}$ pöördelement ja seega R on korpus.

Ülesanne 5 *Olgu X mittetühi hulk ja $\mathcal{P}(X)$ tema kõigi alamhulkade hulk. Mistahes alamhulkade $A, B \subseteq X$ korral defineerime nende sümmeetrilise vahe võrdusega $A\triangle B = (A \setminus B) \cup (B \setminus A)$. Tehke kindlaks, kas a) $(\mathcal{P}(X), \triangle, \cup)$, b) $(\mathcal{P}(X), \triangle, \cap)$ on ring.*

On selge, et kui $A, B \subseteq X$, siis ka $A\triangle B \subseteq X$ ja seega sümmeetriline vahe (mida vaatleme liitmise osas) on algebraline tehe hulgal $\mathcal{P}(X)$, nagu ka ühend ja ühisosa (mida vaatleme korrutamise osas).

AG1. Standardsel viisil on võimalik kontrollida, et $(A\triangle B)\triangle C = A\triangle(B\triangle C)$.

AG4. Tänu ühendi kommutatiivsusele kehtib $A\triangle B = (A \setminus B) \cup (B \setminus A) = (B \setminus A) \cup (A \setminus B) = B\triangle A$ iga $A, B \subseteq X$ korral, s.t. tehe $\triangle$ on kommutatiivne.

AG2. Kuna $\varnothing \in \mathcal{P}(X)$ ja iga $A \in \mathcal{P}(X)$ korral

$$A\triangle\varnothing = (A \setminus \varnothing) \cup (\varnothing \setminus A) = A \cup \varnothing = A,$$

siis $\varnothing$ sobib nullelemendiks.

AG3. Elemendi $A \in \mathcal{P}(X)$ vastandelemendiks $-A$ on A ise, sest

$$A\triangle A = (A \setminus A) \cup (A \setminus A) = \varnothing \cup \varnothing = \varnothing.$$

Sellega oleme näidanud, et $(\mathcal{P}(X), \triangle)$ on Abeli rühm.

R2. Ilmselt on ka tehted $\cup$ ja $\cap$ assotsiatiivsed. Ühikelemendiks ühendi suhtes on tühi hulk ja ühisosa suhtes hulk X. Järelikult on $(\mathcal{P}(X), \cup)$ ja $(\mathcal{P}(X), \cap)$ monoidid.

R3. Kontrollime distributiivsuse säädusi. Kuna tehted $\cup$ ja $\cap$ on kommutatiivsed, siis piisab tegelikult vaid ühe sääduse kontrollimisest, sest kommutatiivsuse tõttu järeldub teine esimesest.

Osutub, et võrdus $A \cup (B\triangle C) = (A \cup B)\triangle(A \cup C)$ ei kehti kõigi $A, B, C \in \mathcal{P}(X)$ korral. Kuna $X \neq \varnothing$, siis leidub $a \in X$. Võttes $A := B := \{a\}$ ja $C := \varnothing$ saame, et $A \cup (B\triangle C) = A \cup (B\triangle\varnothing) = A \cup B = \{a\}$ ja $(A \cup B)\triangle(A \cup C) = (A \cup A)\triangle(A \cup \varnothing) = A\triangle A = \varnothing$, mis on erinevad hulgad. Seega $(\mathcal{P}(X), \triangle, \cup)$ ei ole ring.

Veendume, et

$$A \cap (B\triangle C) = (A \cap B)\triangle(A \cap C).$$

Selleks peame esiteks näitama, et $A \cap (B\triangle C) \subseteq (A \cap B)\triangle(A \cap C)$.Võtame elemendi $a \in A \cap (B\triangle C)$. Siis $a \in A$ ja $a \in B\triangle C$. Sümmeetrilise vahe definitsiooni põhjal on kaks võimalust: kas $a \in B$ ja $a \notin C$ või $a \in C$ ja $a \notin B$. Esimesel juhul $a \in A \cap B$ ja $a \notin A \cap C$, järelikult $a \in (A \cap B)\triangle(A \cap C)$. Teisel juhul $a \in A \cap C$ ja $a \notin A \cap B$, seega jällegi $a \in (A \cap B)\triangle(A \cap C)$. Sellega on ühtepidi sisalduvus tõestatud. Teistpidi sisalduvuse tõestamiseks oletame, et $a \in (A \cap B)\triangle(A \cap C)$. Siis on kaks võimalust: kas $a \in A \cap B$ ja $a \notin A \cap C$ või $a \in A \cap C$ ja $a \notin A \cap B$. Mõlemal juhul $a \in A$. Kuna esimesel juhul $a \notin A \cap C$, siis $a \notin C$, seega $a \in B \setminus C$ ja $a \in B\triangle C = (B \setminus C) \cup (C \setminus B)$. Teisel juhul, kuna $a \notin A \cap B$, siis $a \notin B$, seega $a \in C \setminus B$ ning jälle $a \in B\triangle C = (B \setminus C) \cup (C \setminus B)$. Mõlemal juhul saime, et $a \in A \cap (B\triangle C)$, millega oleme tõestanud, et $A \cap (B\triangle C) \supseteq (A \cap B)\triangle(A \cap C)$.

Vastus: a) $(\mathcal{P}(X), \triangle, \cup)$ ei ole ring,b) $(\mathcal{P}(X), \triangle, \cap)$ on ring.

Ülesanne 6 *Olgu R lõplik ring. Tõestage, et iga element, millel on olemas parempoolne pöördelement, on pööratav.*

Oletame, et elemendil $a \in R$ on olemas parempoolne pöördelement $b \in R$, s.t. $ab = 1$, kus 1 on ringi R ühikelement. Vaatleme teisendust $f_a : R \to R$, mis on defineeritud võrdusega

$$f_a(x) = xa.$$

Kui $xa = ya$, siis $x = x(ab) = (xa)b = (ya)b = y(ab) = y$ iga $x, y \in R$ korral. Seega f_a on üksühene. Kuna R on lõplik ring, siis järeldub sellest, et f_a on ka päälekujutus. Järelikult leidub selline element $c \in R$, et $1 = f_a(c) = ca$. Siis $c = c(ab) = (ca)b = b$, s.t. b on elemendi a pöördelement.

Ülesanne 7 *Olgu $n \in \mathbb{N}, n \geq 2$. Öeldakse, et täisavud a ja b on kongruentsed mooduli n järgi, kui arv $a - b$ jagub arvuga n. Tähistatakse $a \equiv b \pmod{n}$. Saab tõestada, et $a \equiv b \pmod{n}$ parajasti siis, kui a ja b annavad arvuga n jagamisel sama jääägi. Hulka $\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}$ nimetatakse arvu a jäägiklassiks mooduli n järgi. Tähistame $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ ja defineerime sellel hulgal liitmise ja korrutamise võrdustega*

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b}, \\ \overline{a}\,\overline{b} &= \overline{ab}. \end{aligned}$$

Tõestage, et $\mathbb{Z}_n$ on ring nende tehete suhtes. Seda ringi nimetatakse jäägiklassiringiks mooduli n järgi.

Kõigepäält, on võimalik näidata, et need definitsioonid on korrektsed, s.t. et nad ei sõltu jäägiklasside esindajate valikust. Tõepoolest, kui $\overline{a_1} = \overline{a_2}$ ja $\overline{b_1} = \overline{b_2}$, s.t. $n \mid a_1 - a_2$ ja $n \mid b_1 - b_2$ (nii tähistame seda, et $a_1 - a_2$ jagub arvuga n; ütleme: n jagab arvu $a_1 - a_2$), siis

$$\begin{aligned} &n \mid (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2), \\ &n \mid a_1 b_1 - a_2 b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2, \end{aligned}$$

seega $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ ja $\overline{a_1 b_1} = \overline{a_2 b_2}$.

Definitsioonist on kohe näha, et liitmine ja korrutamine on algebralised tehted.

Kasutades liitmise definitsiooni ja seda, et täisarvude liitmine on assotsiatiivne, näeme, et

$$(\overline{a} + \overline{b}) + \overline{b} = \overline{a+b} + \overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} + \overline{b+c} = \overline{a} + (\overline{b} + \overline{c}).$$

Täpselt samamoodi saab veenduda, et liitmine on kommutatiivne, korrutamine on assotsiatiivne ja kommutatiivne ning kehtivad distributiivsuse säädused. Nullelemendiks on $\overline{0}$, sest iga $\overline{a} \in \mathbb{Z}_n$ korral $\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$, ning elemendi $\overline{a}$ vastandelemendiks on element $\overline{-a}$, sest $\overline{a} + \overline{-a} = \overline{0}$. Ühikelemendiks on jäägiklass $\overline{1}$.

Ülesanne 8 *Koostage ringi $\mathbb{Z}_6$ elementide korrutustabel. Leidke selle ringi kõik pööratavad elemendid ja nullitegurid.*

Koostame Cayley tabelid ringi $\mathbb{Z}_6$ liitmis- ja korrutamistehte jaoks:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

,

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

.

Korrutamistabelist on näha, et elemendi $\overline{5}$ pöördelement on $\overline{5}$, $\overline{5} \cdot \overline{5} = \overline{1}$. Seega ringi $\mathbb{Z}_6$ pööratavate elementide rühm $U(\mathbb{Z}_6) = \{\overline{1}, \overline{5}\}$. Kuna elemendid $\overline{2}, \overline{3}, \overline{4}$ ei ole pööratavad, siis $\mathbb{Z}_6$ ei ole korpus. Tabelist on näha, et $\overline{2}, \overline{3}$ ja $\overline{4}$ on nullitegurid, sest $\overline{2} \cdot \overline{3} = \overline{0}$ ja $\overline{4} \cdot \overline{4} = \overline{0}$.

2 Alamstruktuurid

Algebralise struktuuri *alamstruktuuriks* nimetatakse tema mittetühja alamhulka, mis on kinnine kõigi tehete suhtes.

Definitsioon 5 Olgu $(A, \cdot)$ rühmoid (poolrühm). Mittetühja hulka $B \subseteq A$ nimetatakse rühmoidi (poolrühma) A *alamrühmoidiks (alampoolrühmaks)*, kui

AR. $(\forall a, b \in B)(ab \in B)$. (kinnisus korrutamise suhtes)

Definitsioon 6 Olgu $(G, \cdot)$ rühm. Alamhulka $H \subseteq G$ nimetatakse rühma G *alamrühmaks*, kui

ALG1. $(\forall a, b \in H)(ab \in H)$; (kinnisus korrutamise suhtes)

ALG2. $(\forall a \in H)(a^{-1} \in H)$. (kinnisus pöördelemendi võtmise suhtes)

Definitsioon 7 Olgu $(R, +, \cdot)$ ring ühikelemendiga 1. Alamhulka $R' \subseteq R$ nimetatakse ringi R *alamringiks*, kui

AR1. $(\forall a, b \in R')(a + b \in R')$; (kinnisus liitmise suhtes)

AR2. $(\forall a \in R')(-a \in R')$; (kinnisus vastandelemendi võtmise suhtes)

AR3. $(\forall a, b \in R')(ab \in R')$; (kinnisus korrutamise suhtes)

AR4. $1 \in R'$. (kinnisus ühikelemendi suhtes)

Definitsioon 8 Olgu $(K, +, \cdot)$ korpus. Alamhulka $K' \subseteq K$ nimetatakse korpuse K *alamkorpuseks*, kui

AK1. $(\forall a, b \in K')(a + b \in K')$; (kinnisus liitmise suhtes)

AK2. $(\forall a \in K')(-a \in K')$; (kinnisus vastandelemendi võtmise suhtes)

AK3. $(\forall a, b \in K')(ab \in K')$; (kinnisus korrutamise suhtes)

AK4. $(\forall a \in K' \setminus \{0\})(a^{-1} \in K')$. (kinnisus pöördelemendi võtmise suhtes)

Ülesanne 9 *Olgu antud rühmoid $A = \{a, b, c, d\}$ oma Cayley tabeliga*

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

Tehke kindlaks, millised alamhulkadest $\{a\}, \{b, c\}, \{a, b, c\}$ on rühmoidi A alamrühmoidid.

Peame uurima, millised nendest hulkadest on kinnised tehte $*$ suhtes. Mingi hulk $B \subseteq A$ on alamrühmoid, kui hulga B elementidele vastavate ridade ja veergude lõikekohtades on ainult hulga B elemendid. Nagu näha, hulkade $\{a\}$ ja $\{b, c\}$ korral see niimoodi ongi, kuid hulga $\{a, b, c\}$ korral see nii pole ($ac = d \notin \{a, b, c\}$):

$*$	a
a	a

,

$*$	b	c
b	c	b
c	b	c

,

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

.

Vastus: hulgad $\{a\}$ ja $\{b, c\}$ on alamrühmoidid, aga $\{a, b, c\}$ ei ole.

Ülesanne 10 *Leidke rühma $(\mathbb{Z}_n, +)$ kõik alamrühmad.*

Lihtne on näha, et hulgad $\overline{d}\mathbb{Z}_n = \{\overline{ds} \in \mathbb{Z}_n \mid s \in \mathbb{Z}\}$, kus d on arvu n tegur ehk jagaja (seda tähistame $d \mid n$), on alamrühmad. Näitame, et rühma $(\mathbb{Z}_n, +)$ kõik alamrühmad on sellisel kujul. Oletame, et $A \subseteq \mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ on alamrühm. Kindlasti $\overline{0} \in A$, sest iga alamrühm peab sisaldama nullelemendi. Kui $A = \{\overline{0}\}$, siis $A = \overline{0}\mathbb{Z}_n$. Oletame, et $A \neq \{\overline{0}\}$ ja valime sellise $\overline{d} \in A$, et $d \in \{1, 2, \ldots, n-1\}$ ja ühegi $b \in \{1, 2, \ldots, d-1\}$ korral $\overline{b} \notin A$. Kuna A peab olema kinnine liitmise ja vastandelemendi võtmise suhtes, siis $\overline{d}\mathbb{Z}_n \subseteq A$.

Näitame, et ka $A \subseteq \overline{d}\mathbb{Z}_n$. Olgu $\overline{a} \in A$, kusjuures $a \in \{1, 2, \ldots, n-1\}$. Kasutades jäägiga jagamist võime leida sellised $q \in \mathbb{N}$ ja $r \in \{0, 1, \ldots, d-1\}$, et $a = dq + r$. Siis

$$a \underbrace{-d - \ldots - d}_{q \text{ korda}} = r \text{ ja } \overline{r} = \overline{a} \underbrace{-\overline{d} - \ldots - \overline{d}}_{q \text{ korda}} \in A.$$

Tänu d valikule peab $r = 0$, s.t. $a = dq$ ja $\overline{a} = \overline{dq} \in \overline{d}\mathbb{Z}_n$.

Ülesanne 11 *Tõestage, et rühma alamrühmade ühisosa on samuti alamrühm.*

Olgu antud rühm A ja tema alamrühmad A_i, $i \in I$, kus I on mingi indeksite hulk (see võib olla ka lõpmatu).

ALG1. Olgu $a, b \in \bigcap_{i \in I} A_i$. Ühisosa definitsiooni põhjal $a, b \in A_i$ iga $i \in I$ korral. Kuna A_i on alamrühm, siis $ab \in A_i$, iga $i \in I$ korral. Seega $ab \in \bigcap_{i \in I} A_i$.

ALG2. Olgu $a \in \bigcap_{i \in I} G_i$. Siis $a \in G_i$ iga $i \in I$ korral. Kuna G_i on alamrühm, siis $a^{-1} \in G_i$, iga $i \in I$ korral. Seega $a^{-1} \in \bigcap_{i \in I} G_i$.

Ülesanne 12 Olgu X ja Y mittetühjad hulgad, $Y \subseteq X$. Tehke kindlaks, kas hulk $\mathcal{P}(Y)$ on ringi $(\mathcal{P}(X), \triangle, \cap)$ alamring.

AR1. Kui $A, B \in \mathcal{P}(Y)$, s.t. $A, B \subseteq Y$, siis ka $A \triangle B \subseteq Y$ ehk $A \triangle B \in \mathcal{P}(Y)$.

AR2. Kui $A \subseteq Y$ siis tema vastandelement, mis on A ise, on samuti Y alamhulk.

AR3. Kui $A, B \subseteq Y$, siis ka $A \cap B \subseteq Y$.

AR4. Kuna ringi $(\mathcal{P}(X), \triangle, \cap)$ ühikelement on X, siis see ei kuulu hulka $\mathcal{P}(Y)$, kui $X \neq Y$.

Vastus: $\mathcal{P}(Y)$ on ringi $(\mathcal{P}(X), \triangle, \cap)$ alamring ainult siis, kui $X = Y$.

Märkus. Kui lähtuda ringi üldisemast definitsioonist (sellest, kus ei nõuta korrutamise suhtes ühikelemendi olemasolu), siis ei saa ka alamringilt nõuda ühikelemendi sisaldamist ning sellisel juhul oleks iga tingimusi AR1-AR3 rahuldav alamhulk alamring.

Ülesanne 13 *Leidke ringi $\mathbb{R}$ vähim alamring, mis sisaldab arvu $\sqrt{5}$.*

Olgu otsitav ring R. Tingimuse AR4 põhjal reaalarv $1 \in R$. Tingimuse AR1 tõttu siis $\mathbb{N} \subseteq R$ ja tingimuse AR2 tõttu $\mathbb{Z} \subseteq R$. Tingimusest AR3 järeldub, et iga $b \in \mathbb{Z}$ korral $b\sqrt{5} \in R$. Seega AR1 tõttu ka kõik arvud $a + b\sqrt{5}$, kus $a, b \in \mathbb{Z}$, kuuluvad hulka R. Tähistame selliste arvude hulga $\mathbb{Z}[\sqrt{5}]$. Niisiis $\mathbb{Z}[\sqrt{5}] \subseteq R \subseteq \mathbb{R}$. Tõestame, et $\mathbb{Z}[\sqrt{5}]$ on ringi $\mathbb{R}$ alamring.

AR1. Kui $a + b\sqrt{5}, c + d\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$, siis ka

$$(a + b\sqrt{5}) + (c + d\sqrt{5}) = (a + c) + (b + d)\sqrt{5} \in \mathbb{Z}[\sqrt{5}],$$

sest $a + c, b + d \in \mathbb{Z}$.

AR2. Kui $a + b\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$, siis $-(a + b\sqrt{5}) = (-a) + (-b)\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$.

AR3. Kui $a + b\sqrt{5}, c + d\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$, siis

$$(a + b\sqrt{5})(c + d\sqrt{5}) = (ac + 5bd) + (ad + bc)\sqrt{5} \in \mathbb{Z}[\sqrt{5}].$$

AR4. Loomulikult ka $1 = 1 + 0\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$.

Seega $\mathbb{Z}[\sqrt{5}]$ on ringi $\mathbb{R}$ alamring, mis sisaldab arvu $\sqrt{5}$. Kuna R on vähim sellise omadusega alamring (s.t. ei sisalda enam teisi selle omadusega alamringe), siis $R = \mathbb{Z}[\sqrt{5}]$.

Vastus: ringi $\mathbb{R}$ vähim alamring, mis sisaldab arvu $\sqrt{5}$, on $\mathbb{Z}[\sqrt{5}]$.

3 Isomorfismid

Definitsioon 9 Olgu G_1 ja G_2 rühmad (rühmoidid, poolrühmad). Kujutust $\varphi : G_1 \to G_2$ nimetatakse rühmade (rühmoidide, poolrühmade) *homomorfismiks*, kui

GH. $(\forall a, b \in G_1)(\varphi(ab) = \varphi(a)\varphi(b))$. (korrutamise säilitamine)

Definitsioon 10 Olgu R_1 ja R_2 ringid ühikelementidega 1 ja $1'$, vastavalt. Kujutust $\varphi : R_1 \to R_2$ nimetatakse (ringide) *homomorfismiks*, kui

RH1. $(\forall a, b \in R_1)(\varphi(a + b) = \varphi(a) + \varphi(b))$; (liitmise säilitamine)

RH2. $(\forall a, b \in R_1)(\varphi(ab) = \varphi(a)\varphi(b))$; (korrutamise säilitamine)

RH3. $\varphi(1) = 1'$. (ühikelemendi säilitamine)

Algebraliste struktuuride *isomorfismiks* nimetatakse nende bijektiivset homomorfismi. Kui leidub isomorfism ühest algebralisest struktuurist teise, siis neid struktuure nimetatakse *isomorfseteks*. Korpusi loetakse isomorfseteks, kui nad on isomorfsed kui ringid.

Ülesanne 14 *Tõestage, et poolrühmad* $(\mathcal{P}(X), \cap)$ *ja* $(\mathcal{P}(X), \cup)$ *on isomorfsed.*

Selleks peame defineerima ühe kujutuse $f : \mathcal{P}(X) \to \mathcal{P}(X)$, mis oleks bijektiivne ja säilitaks tehte (rahuldaks tingimust GH).

Olgu $A \subseteq X$. Defneerime

$$f(A) := X \setminus A.$$

Injektiivsus. Oletame, et $A, B \subseteq X$ ja $X \setminus A = X \setminus B$. Siis $A = X \setminus (X \setminus A) = X \setminus (X \setminus B) = B$ (vt. [1], Lause 1.1.12(i)), s.t. f on injektiivne.

Sürjektiivsus. Võtame $A \subseteq X$. Siis $f(X \setminus B) = X \setminus (X \setminus B) = B$, s.t. $X \setminus B$ on elemendi B originaal f suhtes. Seega f on sürjektiivne.

GH. Kui $A, B \subseteq X$, siis $f(A \cap B) = X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B) = f(A) \cup f(B)$.

Sellega oleme tõestanud, et poolrühmad $(\mathcal{P}(X), \cap)$ ja $(\mathcal{P}(X), \cup)$ on isomorfsed.

Ülesanne 15 *Tehke kindlaks, kas rühmad* $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ *ja* $(\mathbb{Z}_4, +)$ *on isomorfsed.*

Liitmine rühmal $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$ käib komponenthaaval, s.o. $(\overline{a_1}, \overline{b_1}) + (\overline{a_2}, \overline{b_2}) = (\overline{a_1 + a_2}, \overline{b_1 + b_2})$. Paneme tähele, et iga $(\overline{a}, \overline{b}) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ korral $(\overline{a}, \overline{b}) + (\overline{a}, \overline{b}) = (\overline{0}, \overline{0})$. Oletame, et leidub isomorfism $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$. Siis iga $z \in \mathbb{Z}_2 \times \mathbb{Z}_2$ korral

$$f(z) + f(z) = f(z + z) = f((\overline{0}, \overline{0})) = \overline{0} \in \mathbb{Z}_4.$$

Kuna f on sürjektiivne, siis leidub selline $z \in \mathbb{Z}_2 \times \mathbb{Z}_2$, et $f(z) = \overline{1} \in \mathbb{Z}_4$. Kuid $\overline{1} + \overline{1} = \overline{2} \neq \overline{0}$ ringis $\mathbb{Z}_4$.

Vastus: rühmad $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ ja $(\mathbb{Z}_4, +)$ ei ole isomorfsed.

Ülesanne 16 *Tõestage, et rühmad* $(\mathbb{R}, +)$ *ja* $(\mathbb{R}^+, \cdot)$ *on isomorfsed.*

Defineerime kujutuse $f : \mathbb{R} \to \mathbb{R}^+$ võrdusega

$$f(a) := e^a,$$

kus e on naturaallogaritmi alus. Kuna $\ln : \mathbb{R}^+ \to \mathbb{R}$, $(\ln \circ f)(a) = \ln e^a = a$ iga $a \in \mathbb{R}$ korral ja $(f \circ \ln)(b) = e^{\ln b} = b$ iga $b \in \mathbb{R}^+$ korral, siis $\ln \circ f = 1_{\mathbb{R}}$ ja $f \circ \ln = 1_{\mathbb{R}^+}$, s.t. kujutus f on pööratav ja seega bijektiivne. Kuna $f(a + b) = e^{a+b} = e^a e^b = f(a)f(b)$, siis ta säilitab ka tehte. Seega oleme tõestanud, et rühmad $(\mathbb{R}, +)$ ja $(\mathbb{R}^+, \cdot)$ on isomorfsed.

Ülesanne 17 *Tõestage, et rühmad* $(\mathbb{Q}, +)$ *ja* $(\mathbb{Q}^+, \cdot)$ *ei ole isomorfsed.*

Oletame, et leidub nende rühmade isomorfism $f : \mathbb{Q} \to \mathbb{Q}^+$. Siis leidub selline murd $\frac{a}{b}$, et $f\left(\frac{a}{b}\right) = 2$. Järelikult

$$2 = f\left(\frac{a}{b}\right) = f\left(\frac{a}{2b} + \frac{a}{2b}\right) = f\left(\frac{a}{2b}\right) f\left(\frac{a}{2b}\right) = \left(f\left(\frac{a}{2b}\right)\right)^2,$$

s.t. 2 on mingi ratsionaalarvu ruut, aga see on võimatu. Seega rühmad $(\mathbb{Q}, +)$ ja $(\mathbb{Q}^+, \cdot)$ ei ole isomorfsed.

Viited

[1] Kilp, M., Algebra I, Tartu, 1998.