

# Sissejuhatus algebra struktuuridesse

## 5. praktikum

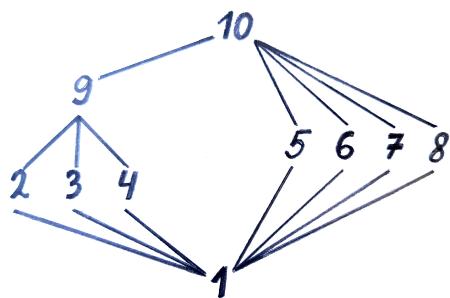
Näidislahendused

### 1. ülesanne (Nikita Leo)

Loetleme  $A_4$  alamrühmad.

- a.  $\{\varepsilon\}$
- b.  $\{\varepsilon, (12)(34)\}$
- c.  $\{\varepsilon, (13)(24)\}$
- d.  $\{\varepsilon, (14)(23)\}$
- e.  $\{\varepsilon, (234), (243)\}$
- f.  $\{\varepsilon, (134), (143)\}$
- g.  $\{\varepsilon, (124), (142)\}$
- h.  $\{\varepsilon, (123), (132)\}$
- i.  $\{\varepsilon, (12)(34), (13)(24), (14)(23)\}$
- j.  $A_4$

Joonistame Hasse diagrammi.



Tegemist on võrega, sest igal kahel elemendil leidub ülemine ja alumine raja. Kahe alamrühma alumiseks rajaks on nende ühisosa, alamrühmade  $H_1$  ja  $H_2$  ülemiseks rajaks on nende korrutis

$$H_1 H_2 = \{xy : x \in H_1, y \in H_2\}.$$

See võre ei ole modulaarne, sest sisaldab alamvõret  $\{1, 4, 5, 9, 10\}$ , mis on isomorfne võrega  $N_5$ . Lemma 8.16 kohaselt iga distributiivne võre on modulaarne. Kuna vaadeldav võre ei ole modulaarne, siis ta ei ole ka distributiivne. Vaadeldav võre on lõplik, seega täielik.

## 2. ülesanne (Lahenduse autor on toimetusele teada)

Tööstame, et täielike võrede mistahes võimsusega otsekorrutis on ise ka täielik võre. Olgu  $V_i$ ,  $i \in I$  täielikud võred; näitame, et

$$V = \prod_{i \in I} V_i$$

on ka täielik võre. Vastavalt algebrate otsekorrutise definitsioonile on tehted  $\wedge$  ja  $\vee$  defineeritud punktiviisiliselt, s.t.

$$\begin{aligned} (a_i)_{i \in I} \vee (b_i)_{i \in I} &= (a_i \vee b_i)_{i \in I}; \\ (a_i)_{i \in I} \wedge (b_i)_{i \in I} &= (a_i \wedge b_i)_{i \in I}. \end{aligned}$$

Vastavalt loengukonspekti konstruktsioonile

$$\begin{aligned} (a_i)_{i \in I} \leqslant (b_i)_{i \in I} &\iff (a_i)_{i \in I} = (a_i)_{i \in I} \wedge (b_i)_{i \in I} \\ &\iff (a_i)_{i \in I} = (a_i \wedge b_i)_{i \in I} \\ &\iff \forall i \in I: a_i = a_i \wedge b_i \\ &\iff \forall i \in I: a_i \leqslant b_i. \end{aligned}$$

Olgu  $U \subset V$ ; näitame, et hulgal  $U$  leidub võres  $V$  alumine raja. Tähistame iga  $i \in I$  korral

$$U_i = \{a_i \mid (a_j)_{j \in I} \in U\}.$$

Siis  $U_i \subset V_i$  ehk tal leidub alumine raja  $u_i$ . Vaatleme elementi  $u = (u_i)_{i \in I}$ . Näitame, et  $u$  on hulga  $U$  alumine raja.

Esiteks veendumme, et  $u$  on hulga  $U$  alumine tõke. Olgu  $(a_i)_{i \in I} \in U$ . Iga  $i$  korral  $a_i \in U_i$ ; et  $u_i$  on alumine tõke, siis  $u_i \leqslant a_i$ . Järelikult  $u = (u_i)_{i \in I} \leqslant (a_i)_{i \in I}$ .

Nüüd näitame, et  $u$  on suurim alumine tõke. Olgu  $v = (v_i)_{i \in I} \in V$  hulga  $U$  mingi alumine tõke. Siis iga  $i \in I$  ja  $a = (a_i)_{i \in I} \in U$  korral  $v_i \leqslant a_i$  ehk  $v_i$  on  $U_i$  alumine tõke. Et  $u_i$  on  $U_i$  suurim alumine tõke, siis  $v_i \leqslant u_i$ . Järelikult  $v \leqslant u$  ehk  $u$  on alumine raja.

Ülemise raja olemasolu töestus on duaalne.

## 3. ülesanne (Lahenduse autor on toimetusele teada)

Tööstame, et täienditega distributiivses võres on täiendid üheselt määratud.

Olgu  $V$  distributiivne võre ja olgu  $a \in V$ . Olgu  $x, y \in V$  mõlemad  $a$  täiendid, näitame, et  $x = y$ .

Kuna  $x, y \in V$  on täiendid, siis  $a \vee x = a \vee y = 1$  ning  $a \wedge x = a \wedge y = 0$ . Täiendi ühesuseks näitame siis, et  $x = y$ .

$$\begin{aligned}
x &= (x \vee a) \wedge x = && \text{(neelduvus)} \\
&= (y \vee a) \wedge x && (x, y \text{ on täiendid ehk } y \vee a = x \vee a = 1 \text{ ja kommutatiivsus}) \\
&= (y \wedge x) \vee (a \wedge x) && \text{(distributiivsus)} \\
&= (y \wedge x) \vee (a \wedge y) && (x, y \text{ on täiendid ehk } a \wedge x = a \wedge y = 0) \\
&= (x \wedge y) \vee (a \wedge y) && \text{(kommutatiivsus)} \\
&= (x \vee a) \wedge y && \text{(distributiivsus)} \\
&= (y \vee a) \wedge y && (x, y \text{ on täiendid ehk } y \vee a = x \vee a = 1 \text{ ja kommutatiivsus}) \\
&= y && \text{(neelduvus)}
\end{aligned}$$

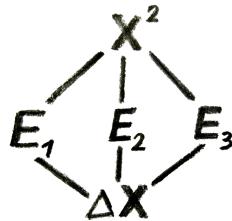
#### 4. ülesanne (Nikita Leo)

Töestame, et võre  $Eq(X)$  on modulaarne parajasti siis, kui  $|X| \leq 3$ . Teoreemist 8.14 teame, et võre on modulaarne parajasti siis, kui see ei sisalda võrega  $N_5$  isomorfset alamvõret. Muuhulgas tähendab see, et võre, milles on vähem kui 5 elementi, on modulaarne. Kõigepealt veendume, et  $|X| = 0, 1, 2, 3$  korral võre  $Eq(X)$  on modulaarne. Järgnevas tähistab  $\Delta X$  hulka  $\{(x, x) : x \in X\}$ .

- Olgu  $X = \emptyset$ , siis  $Eq(X) = \{\emptyset\}$  on modulaarne, sest sisaldab vähem kui 5 elementi.
- Olgu  $|X| = \{1\}$ , siis  $Eq(X) = \{\{(1, 1)\}\}$  on modulaarne, sest sisaldab vähem kui 5 elementi.
- Olgu  $|X| = \{1, 2\}$ , siis  $Eq(X) = \{\Delta X, X^2\}$  on modulaarne, sest sisaldab vähem kui 5 elementi.
- Olgu  $|X| = \{1, 2, 3\}$ , siis  $Eq(X) = \{\Delta X, E_1, E_2, E_3, X^2\}$ , kus

$$\begin{aligned}
E_1 &= \{(1, 1)\} \cup \{2, 3\}^2 \\
E_2 &= \{(2, 2)\} \cup \{1, 3\}^2 \\
E_3 &= \{(3, 3)\} \cup \{1, 2\}^2
\end{aligned}$$

Kui  $Eq(X)$  ei oleks modulaarne, siis see sisaldaks võrega  $N_5$  isomorfset alamvõret. Kuna  $|Eq(X)| = 5$ , siis viimane on võimalik vaid juhul, kui  $Eq(X)$  oleks ise isomorfne  $N_5$ -ga. On lihtne veenduda, et  $Eq(X)$  ei ole isomorfne  $N_5$ -ga, seega  $Eq(X)$  on modulaarne.



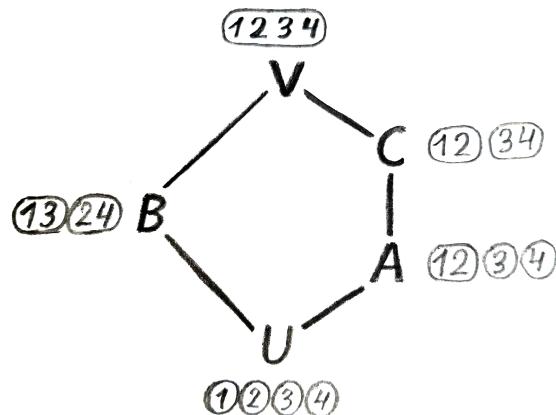
Nüüd veendume, et kui  $X$  sisaldab vähemalt neli elementi, siis  $Eq(X)$  ei ole modulaarne. Olgu  $x_1, x_2, x_3, x_4$  hulga  $X$  neli erinevat elementi. Tähistame

$$M = \{x_1, x_2, x_3, x_4\}.$$

Olgu  $\mathcal{E}$  suvaline ekvivalentsusseos hulgal  $X \setminus M$  (näiteks  $\Delta(X \setminus M)$  või  $(X \setminus M)^2$ ). Vaatleme hulgal  $X$  järgmisi ekvivalentsusseoseid.

$$\begin{aligned} U &= \mathcal{E} \cup \{x_1\}^2 \cup \{x_2\}^2 \cup \{x_3\}^2 \cup \{x_4\}^2 \\ A &= \mathcal{E} \cup \{x_1, x_2\}^2 \cup \{x_3\}^2 \cup \{x_4\}^2 \\ C &= \mathcal{E} \cup \{x_1, x_2\}^2 \cup \{x_3, x_4\}^2 \\ B &= \mathcal{E} \cup \{x_1, x_3\}^2 \cup \{x_2, x_4\}^2 \\ V &= \mathcal{E} \cup \{x_1, x_2, x_3, x_4\}^2 \end{aligned}$$

Hulk  $S = \{U, A, B, C, V\} \subset Eq(X)$  on kinnine ülemise ja alumise raja võtmise suhtes, seega on alamvõre. See võre on isomorfne võrega  $N_5$ . Kuna  $Eq(X)$  sisaldab alamvõret, mis on isomorfne võrega  $N_5$ , siis  $Eq(X)$  ei ole modulaarne.



## 5. ülesanne (Lahenduse autor on toimetusele teada)

Olgu  $\Omega = \Omega_2 = \{\vee, \wedge\}$  võre signatuur ja  $X = \{x, y\}$ . Leiame kõik esimese ja teise astme  $\Omega$ -termid.

Koostame tabeli nullinda, esimese ja teise astme  $(\Omega, X)$ -termidest. Vastavalt definitsioonile on nullinda astme termid  $x$  ja  $y$ . Iga järgmise astme termid saame konstrueerida nii: võtame eelmistest ridadest kaks  $(\Omega, X)$ -termi, kusjuures vähemalt üks nendest eelmisest reast, ja paneme nende vahel sümboli  $\vee$ . Sama kordame sümboliga  $\wedge$ .



## 6. ülesanne (Lahenduse autor on toimetusele teada)

Olgu  $f: \mathbf{A} \rightarrow \mathbf{B}$  ja  $g: \mathbf{A} \rightarrow \mathbf{C}$  universaalalgebrate homomorfismid,  $\text{Ker}(g) \subseteq \text{Ker}(f)$  ja  $g$  surjektiivne. Tõetsame, et leidub homomorfism  $h: \mathbf{C} \rightarrow \mathbf{B}$  nii, et  $f = hg$ .

Defineerime kujutuse  $h: C \rightarrow B$  järgnevalt. Olgu  $x \in C$ ; et  $g$  on surjektiivne, siis leidub  $a \in A$  nii, et  $g(a) = x$ . Defineerime siis  $h(x) = f(a)$ .

Veendume, et  $h$  on korrektsest defineeritud. Olgu  $x \in C$ , kusjuures  $a, b \in A$  on sellised, et  $g(a) = g(b) = x$ . Et  $h$  oleks korrektsest defineeritud peame veenduma, et  $f(a) = f(b)$ . See on vahetu järeldus sellest, et  $\text{Ker}(g) \subseteq \text{Ker}(f)$ . On ilmne, et kehtib  $f = hg$ .

Viimaks näitame, et  $h$  on universaalalgebrate homomorfism. Olgu  $n \in \mathbb{N} \setminus \{0\}$ ,  $\omega \in \Omega_n$  ja  $x_1, \dots, x_n \in C$ . Et  $g$  on surjektiivne, siis leiduvad originaalid  $a_1, \dots, a_n \in A$  nii, et iga  $i$  korral  $g(a_i) = x_i$ . Saame

$$\begin{aligned} h(\omega_C(x_1, \dots, x_n)) &= h(\omega_C(g(a_1), \dots, g(a_n))) \\ &= h(g(\omega_A(a_1, \dots, a_n))) \\ &= f(\omega_A(a_1, \dots, a_n)) \\ &= \omega_B(f(a_1), \dots, f(a_n)) \\ &= \omega_B(h(g(a_1)), \dots, h(g(a_n))) \\ &= \omega_B(h(x_1), \dots, h(x_n)). \end{aligned}$$

Olgu  $\omega \in \Omega_0$ . Näitame, et  $h(0_\omega^C) = 0_\omega^B$ . Et  $g$  on homomorfism, siis  $g(0_\omega^A) = 0_\omega^C$ . Saame

$$h(0_\omega^C) = g(h(0_\omega^A)) = f(0_\omega^A) = 0_\omega^B.$$

## 7. ülesanne (Lahenduse autor on toimetusele teada)

Tõestame, et mistahes universaalalgebra  $\mathbf{A}$  jaoks leidub universaalalgebra  $\mathbf{B}$  nii, et  $\text{Con}(\mathbf{A}) = \text{Sub}(\mathbf{B})$ .

Olgu  $\mathbf{A}$  suvaline universaalalgebra; tähistame tema tüüpi sümboliga  $\Omega$ . Defineerime algebra  $\mathbf{B}$  järgmiselt. Põhihulk on  $B = A \times A$ ; Tüüp on  $\Omega'$ , kus

$$\begin{aligned} \Omega'_0 &= \{1_a \mid a \in A\}; \\ \Omega'_1 &= \Omega_1 \sqcup \{(-)^{-1}\}; \\ \Omega'_2 &= \Omega_2 \sqcup \{\circ\}; \\ \Omega'_n &= \Omega_n \text{ iga } n \geq 3 \text{ korral.} \end{aligned}$$

Tehed on defineeritud järgmiselt:

- Iga  $n \in \mathbb{N} \setminus \{0\}$ ,  $\omega \in \Omega_n$  ja  $(a_1, b_1), \dots, (a_n, b_n) \in B$  korral

$$\omega_B((a_1, b_1), \dots, (a_n, b_n)) = (\omega_A(a_1, \dots, a_n), \omega_A(b_1, \dots, b_n)).$$

- Iga  $1_a$ ,  $a \in A$  korral

$$0_{1_a}^B = (a, a).$$

- Iga  $(a, b) \in B$  korral

$$(a, b)^{-1} = (b, a).$$

- Iga  $(a, b), (c, d) \in B$  korral

$$(a, b) \circ (c, d) = \begin{cases} (a, d), & \text{kui } b = c; \\ (a, b), & \text{muudel juhtudel.} \end{cases}$$

Näitame, et  $\text{Con}(\mathbf{A}) \subseteq \text{Sub}(\mathbf{B})$ . Olgu  $R \in \text{Con}(\mathbf{A})$  kongruents, siis  $R \subset A \times A = B$ . Näitame, et alamhulk  $R$  on  $\mathbf{B}$  tehete suhtes kinnine.

- Olgu  $n \in \mathbb{N} \setminus \{0\}$ ,  $\omega \in \Omega_n$  ja  $(a_1, b_1), \dots, (a_n, b_n) \in R$ ; siis  $a_1 R b_1, \dots, a_n R b_n$ . Et  $R$  on  $\mathbf{A}$  tehetega kooskõlas saame,

$$\omega_A(a_1, \dots, a_n) R \omega_A(b_1, \dots, b_n)$$

ehk

$$\omega_B((a_1, b_1), \dots, (a_n, b_n)) = (\omega_A(a_1, \dots, a_n), \omega_A(b_1, \dots, b_n)) \in R.$$

- Olgu  $a \in A$ , näitame, et  $0_{1_a}^B \in R$ . Tõepoolest, et  $R$  on refleksiivne, siis  $a Ra$  ehk  $0_{1_a}^B = (a, a) \in R$ .
- Olgu  $(a, b) \in R$ ; näitame, et  $(a, b)^{-1} \in R$ . Et  $R$  on sümmeetrisiline, siis  $a R b$  kehtivusest saame  $b R a$ , mis tähendab, et  $(a, b)^{-1} = (b, a) \in R$ .
- Olgu  $(a, b), (c, d) \in R$ . Näitame, et  $(a, b) \circ (c, d) \in R$ . Kui  $b \neq c$ , siis  $(a, b) \circ (c, d) = (a, b) \in R$ . Kui  $b = c$ , siis  $(a, b) \circ (c, d) = (a, d)$ . Et  $(a, b) \in R$  ja  $(b, d) \in R$ , siis  $R$  transitiivsuse tõttu tõepoolest  $(a, d) \in R$ .

Seega  $R \in \text{Sub}(\mathbf{B})$ .

Näitame, et  $\text{Sub}(\mathbf{B}) \subseteq \text{Con}(\mathbf{A})$ . Olgu  $R \in \text{Sub}(\mathbf{B})$  alamalgebra. Näitame, et vaadelduna seosena on ta kongruents.

- *Refleksiivsus*. Olgu  $a \in A$  ja näitame, et  $a Ra$ . Et  $R$  on alamalgebra, siis  $0_{1_a}^B = (a, a) \in R$ .
- *Sümmeetria*. Olgu  $(a, b) \in R$ . Näitame, et  $(b, a) \in R$ . Et  $R$  on alamalgebra, siis  $(a, b)^{-1} = (b, a) \in R$ .
- *Transitiivsus*. Olgu  $(a, b), (b, c) \in R$ . Näitame, et  $(a, c) \in R$ . Et  $R$  on alamalgebra, siis  $(a, b) \circ (b, c) = (a, c) \in R$ .
- *Kooskõla tehetega*. Olgu  $n \in \mathbb{N} \setminus \{0\}$ ,  $\omega \in \Omega_n$  ja  $a_1, \dots, a_n, b_1, \dots, b_n \in A$ , kusjuures  $(a_1, b_1), \dots, (a_n, b_n) \in R$ . Siis et  $R$  on alamalgebra,

$$\omega_B((a_1, b_1), \dots, (a_n, b_n)) = (\omega_A(a_1, \dots, a_n), \omega_A(b_1, \dots, b_n)) \in R.$$

Seega  $R \in \text{Con}(\mathbf{A})$ . Järelikult  $\text{Con}(\mathbf{A}) = \text{Sub}(\mathbf{B})$ .

## 8. ülesanne (Martin Puškin)

Näeme, et  $S$  on kommutatiivne, assotsiaatiivne ja kehtib, et  $x^3 = x^4$  (kust  $x^k = x^3 \forall k \geq 3$ ). Seega on igal muutkonnal, mis sisaldab poolrühma  $S$ , need samasused. Täheldame, et poolrühmas  $S$  ei kehti samasused

$$\begin{aligned} x^2 &= x, \\ x^3 &= x, \\ x^3 &= x^2, \end{aligned}$$

sest valides  $x = 2$  saame igal juhul vastuolu.

Oletame, et poolrühmal  $S$  on veel minge samasus, nt

$$t_1(x_1, x_2, \dots, x_n) \equiv t_2(x_1, x_2, \dots, x_n).$$

Täheldame, et kuna meil on kommutatiivsus ja assotsiatiivsus, on samasus kujul

$$x_1^{k_1} x_2^{k_2} \dots x_m^{k_m} \equiv x_1^{l_1} x_2^{l_2} \dots x_p^{l_p}, \quad (1)$$

kus  $k_i, l_i \in \mathbb{N}$  ning üldistust kitsendamata  $m \leq p \leq n$ .

Täheldame, et poolrühm  $S$  on tegelikult monoid ühikelemendiga 3. Valime nüüd samasuses (1) muutuja  $x_1$  väärtsuseks 2 ja ülejäänud muutujate väärtsuseks 3. Siis saame, et  $2^{k_1} = 2^{l_1}$ , kust järeldamme, et kas  $k_1, l_1 \geq 3$  või  $k_1 = l_1$ . Analoogselt saame iga  $k_i, l_i$  jaoks, kus  $i, j \leq m$ . Seega samasuse  $x^3 = x^4$  tõttu  $x_i^{k_i} = x_i^{l_i}, \forall i \leq m$ .

Olgu nüüd  $p > m$ . Võtame  $x_i = 3, \forall i \leq m$  ja  $x_{m+1} = 0$ . Siis on vasakpoolse termi väärthus 3, kuid parempoolse väärthus 0. Seega samasus ei kehti ja saame, et  $p = m$ . Kokkuvõttes järeldasime, et see samasus on tületatav etteantud samasustest ja järelkult ongi  $S$  poolt tekitatud muutkonnas täpselt sellised poolrühmad, mis täidavad antud samasusi.