Sissejuhatus algebra struktuuridesse. Praktikum 2

Näidislahendused

9. aprill 2020. a.

Ülesanne 1 (Nikita Leo)

Täisarvu a jäägiklassi mooduli $k \in \mathbb{N}$ järgi tähistame $[a]_k$. Kõigepealt veendume kujutuse φ definitsiooni korrektsuses. Olgu täisarvud a ja b sellised, et $[a]_n = [b]_n$. Peame veenduma, et siis $[a]_m = [b]_m$. Kuna $[a]_n = [b]_n$, siis $a \equiv b \pmod{n}$ ehk $n \mid a - b$. Kuna $m \mid n$ ja $n \mid a - b$, siis ka $m \mid a - b$. Seega $a \equiv b \pmod{m}$ ehk $[a]_m = [b]_m$. Nüüd näitame, et φ on homomorfism. Selleks peab veenduma, et kui $x, y \in \mathbb{Z}_n$, siis $\varphi(x + y) = \varphi(x) + \varphi(y)$. Olgu $x, y \in \mathbb{Z}_n$ suvalised. Valime klassidest x ja y vastavalt esindajad a ja b, siis

$$\varphi(x + y) = \varphi([a]_n + [b]_n) = \varphi([a + b]_n) =$$
$$[a + b]_m = [a]_m + [b]_m = \varphi([a]_n) + \varphi([b]_n) = \varphi(x) + \varphi(y).$$

Nüüd näitame, et kujutus φ on sürjektiivne. Olgu $y \in \mathbb{Z}_m$ suvaline. Peame leidma $x \in \mathbb{Z}_n$ nii, et $\varphi(x) = y$. Valime klassist y esindaja a. Siis x rolli sobib $[a]_n$. Seega φ on tõepoolest sürjektiivne. Rühm $\mathrm{Ker}(\varphi)$ on isomorfne rühmaga $\mathbb{Z}_{n/m}$ (märgime, et kuna m ja n on naturaalarvud ning $m \mid n$, siis ka n/m on naturaalarv). Selles vendumiseks vaatleme kujutust $f : \mathbb{Z}_{n/m} \to \mathrm{Ker}(\varphi)$, mis on defineeritud eeskirjaga

$$f([a]_{n/m}) = [am]_n.$$

Kõigepealt veendume definitsiooni korrektsuses. Olgu täisarvud a ja b sellised, et $[a]_{n/m} = [b]_{n/m}$. Näitame, et siis $[am]_n = [bm]_n$. Kuna $[a]_{n/m} = [b]_{n/m}$, siis $a \equiv b \pmod{\frac{n}{m}}$ ehk $\frac{n}{m} \mid a - b$. Korrutades mõlemad pooled arvuga m saame $n \mid am - bm$. Seega $am \equiv bm \pmod{n}$ ehk $[am]_n = [bm]_n$. Veel peab veenduma, et iga $a \in \mathbb{Z}$ korral $[am]_n \in \mathrm{Ker}(\varphi)$. Olgu a suvaline täisarv. Definitsiooni kohaselt $[am]_n \in \mathrm{Ker}(\varphi)$ parajasti siis, kui $\varphi([am]_n) = [0]_m$. Kujutuse φ definitsiooni kohaselt $\varphi([am]_n) = [am]_m$. Kuna $m \mid am$, siis $am \equiv 0 \pmod{m}$ ehk $[am]_m = [0]_m$. Seega $\varphi([am]_n) = [0]_m$ ning $[am]_n \in \mathrm{Ker}(\varphi)$. Näitame, et f on rühmade isomorfism. Kõigepealt veendume, et f on homomorfism. Olgu $x, y \in \mathbb{Z}_{n/m}$ suvalised. Valime klassidest x ja y vastavalt esindajad a ja b, siis

$$f(x + y) = f([a]_{n/m} + [b]_{n/m}) = f([a + b]_{n/m}) =$$
$$[(a + b)m]_n = [am]_n + [bm]_n = f([a]_{n/m}) + f([b]_{n/m}) = f(x) + (y).$$

Nüüd näitame, et f on injektiivne. Olgu $x, y \in \mathbb{Z}_{n/m}$ suvalised. Valime klassidest x ja y vastavalt esindajad a ja b. Näitame, et kui $f(x) = f(y)$, siis $x = y$. Eeldame, et $f(x) = f(y)$. See tähendab, et $[am]_n = [bm]_n$ ehk $am \equiv bm \pmod{n}$. Seega $n \mid am - bm = (a-b)m$. Jagades mõlemad pooled arvuga m saame $\frac{n}{m} \mid a - b$ ehk $a \equiv b \pmod{\frac{n}{m}}$. Seega $x = [a]_{n/m} = [b]_{n/m} = y$. Oleme näidanud, et f on injektiivne. Nüüd veendume, et f on sürjektiivne. Olgu $y \in \mathrm{Ker}(\varphi)$ suvaline. Veendume, et leidub $x \in \mathbb{Z}_{n/m}$ nii, et $f(x) = y$. Valime klassist y esindaja a. Kuna $y \in \mathrm{Ker}(\varphi)$, siis $\varphi(y) = \varphi([a]_n) = [a]_m = [0]_m$. Kuna $[a]_m = [0]_m$, siis $m \mid a$ ja seega leidub täisarv b nii, et $bm = a$. Siis x rolli sobib $[b]_{n/m}$, sest $f([b]_{n/m}) = [bm]_n = [a]_n = y$. Sellega on tõestatud on f on rühmade isomorfism.

Ülesanne 2 (lahenduse autor on toimetusele teada)

Olgu $K_4 = \{\varepsilon, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \subset A_4$. Leiame kõik A_4 kõrvalklassid K_4 järgi.

Esiteks leiame rühma A_4. Esitades rühma S_4 elemente sõltumatute permutatsioonide korrutisena on üldse olemas järgmist liiki elemendid:

1. element ε;
2. üks tsükkel pikkusega 2;
3. kaks sõltumatut tsüklit pikkusega 2;
4. üks tsükkel pikkusega 3;
5. üks tsükkel pikkusega 4.

Rühma A_4 kuuluvad 1., 3. ja 4. liik. Kirjutame välja kõik sellised elemendid ja nende esitused substitutsioonidena (vt. tabel). 4. liiki elemente saame läbi käia järgnevalt. Käime läbi kõik võimalused valida neljast elemendist kolm; iga sellise valiku korral on kaks erinevat võimalikku tsükli "suunda".

Edasi toimime järgmiselt. Eesmärk on jaotada elemendid kõrvalklassideks K_4 järgi. Valime tabelist esimese substitutsiooni σ, mille kõrvalklass ei ole teada ja arvutame tema kõrvalklassi σK_4 ehk arvutame $\sigma\pi$ kõikide $\pi \in K_4$ korral. Saadud permutatsioonid märgime kõrvalklassi σK_4.

Esiteks ei ole teada ε kõrvalklass, aga on selge, et ε kõrvalklass on täpselt alamrühm K_4 ise.

Esimene permutatsioon, mille kõrvalklass nüüd teada ei ole, on $(1,2,3)$. Leiame selle.

$$(1,2,3)\varepsilon = (1,2,3)$$

$$(1,2,3)(1,2)(3,4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1,3,4)$$

$$(1,2,3)(1,3)(2,4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (2,4,3)$$

$$(1,2,3)(1,4)(2,3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = (1,4,2).$$

Esimene permutatsioon, mille kõrvalklassi me ei tea, on $(1,3,2)$. Et igas kõrvalklassis on 4 elementi, siis teame, et kõik alles jäänud elemendid peavad kuuluma kõrvalklassi $(1,3,2)K_4$.

Tsüklitena	Substitutsioonina	Kõrvalklass
ε	$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$	K_4
$(1,2)(3,4)$	$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$	K_4
$(1,3)(2,4)$	$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$	K_4
$(1,4)(2,3)$	$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$	K_4
$(1,2,3)$	$\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$	$(1,2,3)K_4$
$(1,3,2)$	$\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}$	$(1,3,2)K_4$
$(1,2,4)$	$\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$	$(1,3,2)K_4$
$(1,4,2)$	$\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}$	$(1,2,3)K_4$
$(1,3,4)$	$\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}$	$(1,2,3)K_4$
$(1,4,3)$	$\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$	$(1,3,2)K_4$
$(2,3,4)$	$\begin{pmatrix}1&2&3&4\\1&3&4&1\end{pmatrix}$	$(1,3,2)K_4$
$(2,4,3)$	$\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$	$(1,2,3)K_4$

Niisiis on olemas kolm kõrvalklassi $K_4, (1,2,3)K_4$ ja $(1,3,2)K_4$. Seega saame koostada Cayley tabeli

	K_4	$(1,2,3)K_4$	$(1,3,2)K_4$
K_4	K_4	$(1,2,3)K_4$	$(1,3,2)K_4$
$(1,2,3)K_4$	$(1,2,3)K_4$	$(1,3,2)K_4$	K_4
$(1,3,2)K_4$	$(1,3,2)K_4$	K_4	$(1,2,3)K_4$

Näeme, et rühm on isomorfne rühmaga $(\mathbb{Z}_3, +)$.

Ülesanne 3 (lahenduse autor on toimetusele teada)

Leiame rühma $U(\mathbb{Z}_{21})$ kõikide elementide järgud ja lahutame selle p-komponentide sisemiseks otsesummaks. Teatavasti $\mathbb{Z}_{21}$ pööratavad elemendid on need, mis on

ühistegurita arvuga 21; teisisõnu need, mis ei jagu 7 ega 3-ga. Teeme tabeli:

x	x^2	x^3	x^4	x^5	x^6	järk
1						1
2	4	8	16	11	1	6
4	16	1				3
5	4	20	16	17	1	6
8	1					2
10	16	13	4	19	1	6
-10	16	-13	4	-19	1	6
-8	1					2
-5	4	1				3
-4	16	-1	4	-16	1	6
-2	4	-8	16	-11	1	6
-1	1					2

p-komponendid on niisiis $\{1, 8, -8, -1\}$ ja $\{1, 4, -5\}$. Terve rühm esitub nende kahe komponendi sisemise otsesummana.

Ülesanne 4 (Nikita Leo)

Kahe erineva intervalli $[0, 1)$ kuuluva arvu vahe ei saa olla täisarv, seega kahele erinevale ratsionaalarvule sellest intervallist vastavad alati erinevad ekvivalentsiklassid. Kuna ratsionaalarve on intervallis $[0, 1)$ lõpmata palju, siis lõpmata palju on ka erinevaid ekvivalentsiklasse. Niisiis faktorrühmas $\mathbb{Q}/\mathbb{Z}$ on lõpmata palju elemente. Olgu $X \in \mathbb{Q}/\mathbb{Z}$ suvaline. Valime klassist X mingi esindaja x, siis $X = x + \mathbb{Z}$. Näitame, et elemendil X on lõplik järk. Selleks piisab leida selline naturaalarv n, mille puhul $nX = \mathbb{Z}$ ($\mathbb{Z}$ on rühma $\mathbb{Q}/\mathbb{Z}$ ühikelement). Kuna x on ratsionaalarv, siis ta esitub kujul $x = \frac{m}{n}$, kus m on mingi täisarv ja n mingi naturaalarv. Siis

$$nX = n\left(\frac{m}{n} + \mathbb{Z}\right) = n\frac{m}{n} + \mathbb{Z} = m + \mathbb{Z} = \mathbb{Z}.$$

Seega rühma $\mathbb{Q}/\mathbb{Z}$ kõigil elementidel on tõepoolest lõplik järk.

Ülesanne 5 (Karolina Tammemaa)

Selles lahenduses kasutame aditiivset sümboolikat.

" $\Rightarrow$ " Näitame kõigepealt et lihtne Abeli rühm on lõplikut järku, kusjuures tema järk on algarv. Kuna ta on lihtne rühm, siis tal pole normaaljagajaid. Oletades, et ta on lõpmatu, peab iga elemendi järk olema lõpmatu, sest vastasel juhul moodustaks lõpliku järguga element pärisalamrühma, mis oleks normaaljagajaks. Võtame $a \in G \setminus \{0\}$, siis on meil, et $< 2a > \subset < a >$ aga samas ei saa olla $< a > \subset < 2a >$, sest see tähendaks, et $n \cdot 2a = a$, mingi $n \in \mathbb{N}$ korral, mis on vastuolus sellega, et iga elmendi järk on lõpmatu. Nüüd aga moodustab

$< 2a >$ pärisalamhulga, mis on vastuolus serllega, et G on lihtne rühm. Seega on G lõplik rühm. Seega on G perioodiline ja on esitatav oma p-komponentide otsesummana. Kuna iga p-komponent on alamrühm, siis koosneb G ainult ühest p-komponendist. Kuna iga p-komponent sisaldab elementi järguga p ja kuna iga nullist erineva elemendi järk peab olema võrdne rühma järguga, siis $|G| = p$.

" $\Leftarrow$ "Kuna iga alamrühma järk jagab rühma järku, aga antud juhul on rühma järk algarv, siis järelikult pole rühmas ühtegi mittetriviaalset alamrühma ja tegu on lihtsa rühmaga. Kuna tegu on ka lõpliku rühmaga, siis iga $a \in G \setminus \{0\}$ korral $< a >= G$. Kõik lõplikud tsüklilised rühmad on kommutatiivsed, sest iga $l, n \in \mathbb{N}$ korral $la + na = (l + n)a = (n + l)a = na + la$. Seega on tegu lihtsa Abeli rühmaga.

Ülesanne 6 (Karolina Tammemaa)

Olgu meil mittetriviaalne jaguv rühm G. Ning olgu $a \in G \setminus \{0\}$. Olgu p_1 ja p_2 erinevad algarvud. Siis leiduvad sellseid $b_1, b_2 \in G$, et $p_1 b_1 = a = p_2 b_2$. Nüüd aga $p_1 b_1 - p_2 b_2 = 0$. Oletame vastuväiteliselt, et selles rühmas on olemas baas. Kui nüüd b_1 esitada baasielementide lineaarkombinatsioonina, siis olgu e_1 mingi lineaarkombinatsioonis esinev baasielement, mille kordaja ei ole null (see peab leiduma, sest $b_1 \neq 0$).

Kuna baasielemendid on lineaarselt sõltumatud, siis võrdusest $p_1 b_1 - p_2 b_2 = 0$ järeldub, et iga baaasielemendi kordaja on null ehk:

$$p_1 \cdot k_1 \cdot e_1 - p_2 \cdot k_2 \cdot e_1 = (p_1 k_1 - p_2 k_2) e_1 = 0$$

kus $k_1, k_2 \in \mathbb{Z}$ ja $e_1 \in G$. Seega $p_1 k_1 - p_2 k_2 = 0$, kust saame, et $p_1 \mid k_2$ ja $p_2 \mid k_1$. Kuna algarvud olid valitud vabalt, siis saame siit, et iga algarv jagab kordajaid k_1 ja k_2. Mis on aga võimalik ainult juhul kui k_1, k_2 on võrdsed nulliga. See on aga vastuolu, sest me eelnevalt eeldasime, et $k_1 \neq 0$.

Ülesanne 7 (Nikita Leo)

Olgu G rühm ja H tema normaaljagaja ning p algarv. Tõestame, et kui H ja G/H on p-rühmad, siis ka rühm G on p-rühm (p-rühma all mõistame sellist rühma, mille kõigi elementide järk on p aste). Olgu $g \in G$ suvaline. Tähistagu e rühma G ühikelementi. Veendume, et $\mathrm{ord}(g)$ on p aste. Vaatleme rühma G/H elementi gH. Kuna G/H on eelduse kohaselt p-rühm, siis $\mathrm{ord}(gH) = p^k$, kus $k \in \mathbb{N}_0$. Seega $(gH)^{p^k} = g^{p^k} H = H$. Sellest järeldub, et $g^{p^k} \in H$. Kuna H on eelduse kohaselt p-rühm, siis $\mathrm{ord}(g^{p^k}) = p^m$, kus $m \in \mathbb{N}_0$. Niisiis $(g^{p^k})^{p^m} = g^{p^{k+m}} = e$. Sellest tuleneb, et $\mathrm{ord}(g) \mid p^{k+m}$, seega $\mathrm{ord}(g)$ on ise p aste.

Märkus: Lisaeeldusel, et G on lõplik, on tõestus veelgi lihtsam. Teame, et lõplik rühm on p-rühm parajasti siis, kui tema elementide arv on p aste. Kui G on lõplik, siis lõplikud on ka H ja G/H. Kuna H ja G/H on eelduse kohaselt p-rühmad, siis $|H| = p^k$ ning $|G/H| = p^m$, kus $k, m \in \mathbb{N}_0$. Lagrange'i teoreemi

kohaselt $|G| = |H| \cdot |G/H|$. Seega $|G| = p^k \cdot p^m = p^{k+m}$. Kuna G elmentide arv on p aste, siis G on p-rühm.

Ülesanne 8 (Nikita Leo)

Tähistagu e ning $\mathbb{1}$ vastavalt rühmade G ja K^* ühikelemente. Kõigepealt tõestame, et H on rühma G normaaljagaja. Selleks kasutame konspekti lauset 2.12. Olgu $g \in G$ ja $h \in H$ suvalised. Näitame, et $g^{-1}hg \in H$. Märgime, et $\varphi(g^{-1}hgh^{-1}) = \mathbb{1}$. Tõepoolest, kuna φ on homomorfism, siis $\varphi(g^{-1}hgh^{-1}) = \varphi(g)^{-1}\varphi(h)\varphi(g)\varphi(h)^{-1}$, ja kuna rühma K^* tehe on kommutatiivne, siis

$$\varphi(g)^{-1}\varphi(h)\varphi(g)\varphi(h)^{-1} = \varphi(g)^{-1}\varphi(g)\varphi(h)\varphi(h)^{-1} = \mathbb{1}.$$

Seega $g^{-1}hgh^{-1} \in \operatorname{Ker}\varphi$ ning kuna $\operatorname{Ker}\varphi \subset H$, siis ka $g^{-1}hgh^{-1} \in H$. Kuna $g^{-1}hgh^{-1} \in H$ ja $h \in H$, siis ka nende korrutis on rühmas H, st $g^{-1}hgh^{-1}h = g^{-1}hg \in H$. Sellega oleme näidanud, et H on normaaljagaja.

Nüüd veendume, et G/H on tsükliline rühm. Selleks rakendame teist isomorfismiteoreemi. Kuna $\operatorname{Ker}\varphi$ ja H on rühma G normaaljagajad ning $\operatorname{Ker}\varphi \subset H$, siis teine isomorfismiteoreem ütleb meile, et

$$(G/\operatorname{Ker}\varphi)/(H/\operatorname{Ker}\varphi) \cong G/H.$$

Esitame tõestuse skeemi. Esimese sammuna tõestame, et tsüklilise rühma faktorrühm on tsükliline rühm. Teise sammuna näitame, et rühm $G/\operatorname{Ker}\varphi$ on tsükliline. Siis saame järeldada, et ka $(G/\operatorname{Ker}\varphi)/(H/\operatorname{Ker}\varphi)$ on tsükliline, ning kuna G/H on viimasega isomorfne, siis saame järeldada, et ka G/H on tsükliline.

Lause 1. *Olgu G tsükliline rühm ning H tema normaaljagaja, siis G/H on samuti tsükliline rühm.*

Tõestus. Olgu a rühma G genereeriv element. Näitame, et aH on rühma G/H genereeriv element. Selleks veendume, et rühma G/H kõik elemendid esituvad elemendi aH astmetena. Vaatleme rühma G/H suvalist elementi X. Valime temast esindaja g, siis X esitub kujul gH. Kuna a on rühma G genereeriv element, siis leidub $k \in \mathbb{Z}$ nii, et $a^k = g$. Siis $(aH)^k = a^kH = gH = X$. Seega X tõepoolest esitub elemendi aH astmena. Niisiis on G/H tsükliline rühm.

□

Nüüd veendume, et rühm $G/\operatorname{Ker}\varphi$ on tsükliline. Kõigepealt moodustame funktsioonist φ uue funktsiooni $\varphi' : G \to \operatorname{Im}\varphi$, kitsendades funktsiooni φ sihthulka hulgani $\operatorname{Im}\varphi$ (st $\varphi'(g) = \varphi(g)$ iga $g \in G$ korral, ainult sihthulgad on erinevad). Märgime, et φ' on sürjektiivne homomorfism. Vastavalt loengukonspekti järelduse 2.21 saame, et $G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$ (märgime, et $\operatorname{Ker}\varphi' = \operatorname{Ker}\varphi$). Teame, et tsüklilise rühma iga alamrühm on ka tsükliline. Kuna $\operatorname{Im}\varphi$ on rühma K^* alamrühm ning K^* on tsükliline, siis ka $\operatorname{Im}\varphi$ on tsükliline. Lõpuks, kuna $\operatorname{Im}\varphi$ ja $G/\operatorname{Ker}\varphi$ on isomorfsed ning $\operatorname{Im}\varphi$ on tsükliline, siis tsükliline on ka $G/\operatorname{Ker}\varphi$. Kuna tsüklilise rühma faktorrühm on ka tsükliline, siis tsükliline on ka rühm $(G/\operatorname{Ker}\varphi)/(H/\operatorname{Ker}\varphi)$ ja seega isomorfsuse tõttu ka G/H.