Sissejuhatus algebra struktuuridesse.
Praktikum 3

Näidislahendused

14.04.2020

Ülesanne 1 (Karolina Tammemaa)

Tähistame $R := Mat_n(\mathbb{Z}_7)$. On selge, et $I, 0 \in Z(R)$. Näitame, et ka $\lambda I \in Z(r)$, kus $\lambda \in \mathbb{Z}_7$. Kuna iga $r \in R$ korral $(\lambda I)r = \lambda r = \lambda r I = r(\lambda I)$, siis $\lambda I \in Z(R)$. Olgu $z \in Z(R)$. Ta saab maatrikskujul välja kirjutada kui

$$\begin{pmatrix} z_{11} & ... & z_{1n} \\ ... & ... & ... \\ z_{n1} & ... & z_{nn} \end{pmatrix}$$

Vaatame maatriksit r, kus kohal $(1,1)$ on 1 ja igal pool mujal on nullid. Siis

$$\begin{pmatrix} z_{11} & ... & z_{1n} \\ ... & ... & ... \\ z_{n1} & ... & z_{nn} \end{pmatrix} \cdot r = \begin{pmatrix} z_{11} & 0 & ... & 0 \\ ... & ... & ... & ... \\ z_{1n} & 0 & ... & 0 \end{pmatrix}$$

ja samas

$$r \cdot \begin{pmatrix} z_{11} & ... & z_{1n} \\ ... & ... & ... \\ z_{n1} & ... & z_{nn} \end{pmatrix} = \begin{pmatrix} z_{11} & ... & z_{1n} \\ 0 & ... & 0 \\ ... & ... & ... \\ 0 & ... & 0 \end{pmatrix}$$

Seega $z_{12} = z_{13} = ... = z_{1n} = 0$ ja $z_{21} = z_{31} = ... = z_{n1} = 0$. Korrutades z-i erinevate maatriksitega, kus täpselt üks diagonaalielement on 1 ja kõik teised maatriksi elemendid on nullid saab näidata, et z peab olema diagonaalkujul. Näitame nüüd, et kui z on diagonaalkujul, siis kõik tema diagonaalielemendid on võrdsed. Oletame et z on kujul

$$z = \begin{pmatrix} a & 0 & ... & 0 \\ 0 & b & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & d \end{pmatrix}$$

ja vaatame maatriksit r mille iga elemendi väärtus on 1. Siis

$$\begin{pmatrix} a & 0 & ... & 0 \\ 0 & b & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & d \end{pmatrix} \cdot r = \begin{pmatrix} a & a & ... & a \\ b & b & ... & b \\ ... & ... & ... & ... \\ d & d & ... & d \end{pmatrix}.$$

Samas

$$r \cdot \begin{pmatrix} a & 0 & ... & 0 \\ 0 & b & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & d \end{pmatrix} = \begin{pmatrix} a & b & ... & d \\ a & b & ... & d \\ ... & ... & ... & ... \\ a & b & ... & d \end{pmatrix}.$$

Näeme, et $z \in Z(R)$ siis ja ainult siis, kui $a = b = ... = d$.

Ülesanne 2 (Nikita Leo)

Definitsioon 1. *Olgu R ja S ringid. Kujutust $f : R \to S$ nimetatakse ühikuta ringide homomorfismiks, kui iga $a \in R$ ja $b \in R$ korral*

H1: $f(a + b) = f(a) + f(b)$;

H2: $f(0) = 0$;

H3: $f(-a) = -f(a)$;

H4: $f(ab) = f(a)f(b)$.

Märgime, et punktid 2 ja 3 järelduvad punktist 1, seega punktid 2 ja 3 võiks ka ära jätta.

On vahetult kontrollitav, et järgmised kolm kujutust on ühikuta ringide homomorfismid.

1. $f_1 : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(m, n) \mapsto m$
2. $f_2 : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(m, n) \mapsto n$
3. $f_3 : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(m, n) \mapsto 0$

Leiame nende tuumad ja kujutised.

1. $\operatorname{Ker} f_1 = \{(0, n) : n \in \mathbb{Z}\}$, $\operatorname{Im} f_1 = \mathbb{Z}$
2. $\operatorname{Ker} f_2 = \{(m, 0) : m \in \mathbb{Z}\}$, $\operatorname{Im} f_2 = \mathbb{Z}$
3. $\operatorname{Ker} f_3 = \mathbb{Z} \times \mathbb{Z}$, $\operatorname{Im} f_3 = \{0\}$

Näitame, et need on ainsad homomorfismid ringide $\mathbb{Z} \times \mathbb{Z}$ ja $\mathbb{Z}$ vahel. Olgu $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ ühikuta ringide homomorfism. Tõestame, et $f = f_1$, $f = f_2$ või $f = f_3$. Tähistame $x = f(1,0)$ ja $y = f(0,1)$. Märgime, et omadustest $H1$, $H2$ ning $H3$ järeldub, et suvaliste $a, b, m \in \mathbb{Z}$ korral

H5: $f(ma, mb) = mf(a, b)$.

Olgu $m, n \in \mathbb{Z}$ suvalised, siis

$$\begin{aligned} f(m,n) &= f(m,0) + f(0,n) && (H1) \\ &= mf(1,0) + nf(0,1) && (H5) \\ &= mx + ny. \end{aligned}$$

Niisiis suvaliste $m \in \mathbb{Z}$ ja $n \in \mathbb{Z}$ korral

$$f(m,n) = mx + ny. \tag{1}$$

Olgu nüüd $m_1, m_2, n_1, n_2 \in \mathbb{Z}$ suvalised, siis vastavalt omadusele $H4$ ning valemile (1) saame

$$\begin{aligned} f(m_1m_2, n_1n_2) &= f(m_1, n_1)f(m_2, n_2) \\ &= (m_1x + n_1y)(m_2x + n_2y) \\ &= m_1m_2x^2 + m_1n_2xy + n_1m_2xy + n_1n_2y^2. \end{aligned}$$

Teiselt poolt vastavalt valemile (1)

$$f(m_1m_2, n_1n_2) = m_1m_2x + n_1n_2y.$$

Niisiis suvaliste $m_1, m_2, n_1, n_2 \in \mathbb{Z}$ korral kehtib

$$m_1m_2x^2 + m_1n_2xy + n_1m_2xy + n_1n_2y^2 = m_1m_2x + n_1n_2y.$$

Valides $m_1 = m_2 = 1$ ning $n_1 = n_2 = 0$, saame $x^2 = x$, seega $x = 0$ või $x = 1$. Analoogiliselt, valides $m_1 = m_2 = 0$ ning $n_1 = n_2 = 1$, saame $y^2 = y$, millest $y = 0$ või $y = 1$. Märgime, et kui x ja y oleksid mõlemad võrdsed ühega, siis valides m_1, m_2, n_1, n_2 kõik võrdseks ühega saaksime vastuolu. Seega jääb üle kolm varianti:

1. $x = 1$ ja $y = 0$, sellisel juhul $f = f_1$;
2. $x = 0$ ja $y = 1$, sellisel juhul $f = f_2$;
3. $x = 0$ ja $y = 0$, sellisel juhul $f = f_3$.

Sellega on tõestatud, et ainsad ühikuta ringide homomorfismid ringide $\mathbb{Z} \times \mathbb{Z}$ ja $\mathbb{Z}$ vahel on f_1, f_2 ja f_3.

Ülesanne 3 (Karolina Tammemaa)

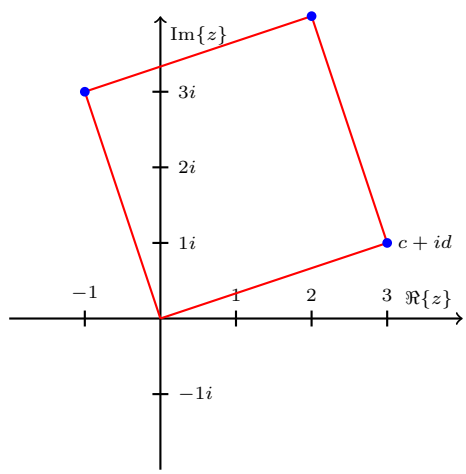
Olgu meil mingi mittetriviaalne ideaal I. Siis seal leidub nullist erineva element $c + id \in I$. Kuna ideaal on iga R elemendiga korrutamise suhtes kinnine, siis ka $ic - d \in I$. Ka on ideaal liitmise suhtes kinnine ja seega

$$(c + id) + (ic - d) = c - d + i(c + d) \in I.$$

Paneme nüüd tähele, et igal faktorringi $\mathbb{Z}[i]/I$ kõrvalklassil on esindaja komplekstasandil paiknevas ruudus tippudega

$$0,\ c + id,\ ic - d,\ c - d + i(c + d).$$

Iga ringi $\mathbb{Z}[i]$ elemendi saab viia sinna ruutu liites või lahutades vajadust mööda elemente $c + id$ ja $-d + ic$. Kuna sellises ruudus on lõplik arv täisarvuliste kordajadatega punkte, siis on ka faktorringi $\mathbb{Z}[i]/I$ järk lõplik.
Idee illustreerimiseks on lisatud joonis, kus $c = 3, d = 1$:



Ülesanne 4 (Nikita Leo)

Olgu R lihtne ühikuga ring. Tähistagu Z ringi R tsentrit. Näitame, et Z on ringi R ühikuga alamring (see kehtib ka siis, kui R ei ole lihtne). On ilmne, et $0 \in Z$ ja $1 \in Z$. Olgu $z_1, z_2 \in Z$ suvalised. Veendume, et $z_1 + z_2 \in Z$ ning $z_1 z_2 \in Z$. Olgu $r \in R$ suvaline, siis

$$(z_1 + z_2)r = z_1 r + z_2 r = r z_1 + r z_2 = r(z_1 + z_2)$$

ning

$$z_1 z_2 r = z_1 r z_2 = r z_1 z_2,$$

järelikult $z_1 + z_2 \in Z$ ja $z_1 z_2 \in Z$. Lõpuks on jäänud veenduda, et kui $z \in Z$, siis ka $-z \in Z$. Olgu $z \in Z$ suvaline, siis iga $r \in R$ korral

$$(-z)r = -(zr) = -(rz) = r(-z),$$

järelikult ka $-z \in Z$.

On ilmne, et ring Z on kommutatiivne. Näitame, et iga nullist erinev element ringis Z on pööratav. Olgu $z \in Z \setminus \{0\}$ suvaline. Vaatleme hulka $I = \{zr : r \in R\}$. Veendume, et I on ringi R ideaal. Ilmselt on I mittetühi. Olgu $i_1 \in I$ ja $i_2 \in I$ suvalised. Veendume, et $i_1 + i_2 \in I$. Kuna $i_1, i_2 \in I$, siis $i_1 = zr_1$ ja $i_2 = zr_2$, kus $r_1, r_2 \in R$. Seega

$$i_1 + i_2 = zr_1 + zr_2 = z(r_1 + r_2) \in I.$$

Olgu nüüd $i \in I$ ja $s \in R$ suvalised. Veendume, et $is \in I$ ja $si \in I$. Kuna $i \in I$, siis $i = zr$, kus $r \in R$. Järelikult $is = zrs \in I$ ning $si = szr = zsr \in I$, kus teise võrdusmärgi juures on kasutatud seda, et $z \in Z$, mistõttu $sz = zs$. Sellega tõestasime, et I on ringi R ideaal. Kuna ring R on lihtne ning I on ideaal ringis R, siis $I = \{0\}$ või $I = R$. Kuna $z \in I$ ja $z \neq 0$, siis $I \neq \{0\}$. Järelikult $I = R$. Seega $1 \in I$. Niisiis leidub selline $r \in R$, et $zr = 1$. Märgime kohe, et kuna $z \in Z$, siis $zr = rz$. Järelikult ka $rz = 1$. Lõpuks on jäänud veel veenduda, et $r \in Z$. Olgu s suvaline. Näitame, et $sr = rs$.

$$\begin{aligned} zs &= sz && \text{(sest } z \in Z\text{)} \\ zsr &= szr \\ zsr &= s && \text{(sest } zr = 1\text{)} \\ rzsr &= rs \\ sr &= rs && \text{(sest } rz = 1\text{)} \end{aligned}$$

Niisiis $r \in Z$, kusjuures $zr = rz = 1$. Seega z on pööratav ringis Z, mida oligi vaja näidata. Niisiis Z on korpus.

Ülesanne 5 (Martin Puškin)

Teame, et maatriksid kujul

$$\begin{pmatrix} a & b & c \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, a, b, c \in \mathbb{R}$$

moodustavad minimaalse parempoolse ideaali. Näitan, et leidub teine mittetriviaalne parempoolne ideaal, mis ei ole minimaalne. Vaatame hulka I, kuhu kuuluvad maatriksid kujul

$$\begin{pmatrix} a & b & c \\ d & e & f \\ 0 & 0 & 0 \end{pmatrix}, a, b, c, d, e, f \in \mathbb{R}$$

On ilmne, et see hulk on liitmise suhtes kinnine. Näitan, et see on parempoolne ideaal.

$$\begin{pmatrix} a & b & c \\ d & e & f \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} g & h & i \\ j & k & l \\ m & n & p \end{pmatrix} = \begin{pmatrix} ag+bj+cm & ah+bk+cn & ai+bl+cp \\ dg+ej+fm & dh+ek+fn & di+el+fp \\ 0 & 0 & 0 \end{pmatrix} \in I$$

Seega ongi I parempoolne mittetriviaalne ideaal, mis pole minimaalne.

Ülesanne 6 (Nikita Leo)

Märgime, et $\operatorname{Ker}\varphi$ on mooduli M alammoodul ning $\operatorname{Im}\varphi$ on mooduli N alammoodul. Kuna moodulid M ja N on lihtsad, siis $\operatorname{Ker}\varphi = \{0_M\}$ või $\operatorname{Ker}\varphi = M$ ning $\operatorname{Im}\varphi = \{0_N\}$ või $\operatorname{Im}\varphi = N$. Kui $\operatorname{Im}\varphi = \{0_N\}$ või $\operatorname{Ker}\varphi = M$, siis φ on nullhomomorfism. Seega on jäänud vaadelda juht, kus $\operatorname{Ker}\varphi = \{0_M\}$ ning $\operatorname{Im}\varphi = N$. Sellisel juhul φ on injektiivne, sest $\operatorname{Ker}\varphi = \{0_M\}$, ning sürjektiivne, sest $\operatorname{Im}\varphi = N$. Järelikult sellisel juhul φ on bijektiivne homomorfism ehk isomorfism.

Ülesanne 7 (Lahenduse autor on toimetusele teada)

Olgu $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ lühike täpne jada, B lihtne moodul. Näitame, et leidub selline homomorfism $h\colon C \to B$, et $gh = 1_C$.

Et B on lihtne moodul, siis, et $\operatorname{Ker} g$ on B alammoodul, kehtib $\operatorname{Im} f = \operatorname{Ker} g = B$ või $\operatorname{Im} f = \operatorname{Ker} g = \{0\}$.

- $\operatorname{Im} f = \operatorname{Ker} g = B$. Et g on sürjektiivne, siis iga $c \in C$ esitub kujul $g(b)$, kus $b \in B$. Et iga $b \in B$ korral $g(b) = 0$, siis järelikult $C = \{0\}$. Defineerime $h\colon C \to B$ seosega $h(0) = 0$, on ilmne, et see on homomorfism. Siis $g(h(0)) = g(0) = 0$. Et 0 on C ainuke element, siis tähendab see, et $gh = 1_C$.

- $\operatorname{Im} f = \operatorname{Ker} g = \{0\}$. Et $\operatorname{Ker} g = \{0\}$, siis g on injektiivne; täpse jada omadus on, et g on sürjektiivne. Järelikult g on moodulite isomorfism. Seega leidub tal pöördfunktsioon $h = g^{-1}$, mis on samuti homomorfism, ehk $hg = g^{-1}g = 1_C$.

Ülesanne 8 (Martin Puškin)

Teame, et moodul P on projektiivne parajasti siis, kui lühike täpne jada $0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0$ tegurdub. Veel teame, et f on monomorfism ja g on epimorfism. On ilmne, et A ja B on ka Abeli rühmad üle $\mathbb{Z}$.

Vaatame lühikest täpset jada $0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} P \to 0$, kus P on lõplik mittetriviaalne Abeli rühm A $\mathbb{Z}$-moodulina. Olgu $a \in A$ ja $ord(a) = n \neq 1$ (selline element leidub, sest A on mittetriviaalne). Siis olgu $b := (n-1)a$.

Oletame vastuväiteliselt, et jada tegurdub, st meil leidub sobiv homomorfism h nii, et $gh = 1_P$. Olgu $h(a) = a'$. Siis

$$na' = a' + (n-1)a' = h(a) + h(b) = h(a+b) = h(na) = h(0) = 0.$$

Siit saame, et $na' \overset{*}{=} 0 \Rightarrow n = 0$, mis on vastuolu.

* *sest* $\mathbb{Z}$ *on väändeta Abeli rühm ja* $a' \neq 0$.