АЛГЕБРА 1

Елементи опште алгебре

Хомоморфизми, директни производи и конгруенције

Зоран Петровић

9. октобар 2012.

Нека су $\mathbb{A}$, $\mathbb{B}$ и $\mathbb{C}$ алгебре исте сигнатуре:

$$\begin{aligned}\mathbb{A} &= (A, \phi_1, \ldots, \phi_r, a_1, \ldots, a_s),\\ \mathbb{B} &= (B, \psi_1, \ldots, \psi_r, b_1, \ldots, b_s),\\ \mathbb{C} &= (C, \theta_1, \ldots, \theta_r, c_1, \ldots, c_s).\end{aligned}$$

Овде су a_i, b_j, c_k изабрани елементи, док су остало операције ненулте дужине. Наравно, $\sharp(\phi_i) = \sharp(\psi_i) = \sharp(\theta_i)(= n_i)$.

Дефиниција 1 Функција $h\colon A \to B$ је хомоморфизам алгебре $\mathbb{A}$ у алгебру $\mathbb{B}$ уколико важи:

- за све $j = \overline{1,s}$: $h(a_j) = b_j$.
- за све $i = \overline{1,r}$ и све $u_1, \ldots, u_{n_i} \in A$:
  $h(\phi_i(u_1, \ldots, u_{n_i})) = \psi_i(h(u_1), \ldots, h(u_{n_i}))$.

Дакле, хомоморфизам је она функција једног скупа носача у други, која изабране елементе слика у одговарајуће изабране елементе, а комутира са свим операцијама. Када желимо да истакнемо да је $h\colon A \to B$ хомоморфизам алгебри, писаћемо: $h\colon \mathbb{A} \to \mathbb{B}$ је хомоморфизам.

Дефиниција 2 Нека је $h\colon \mathbb{A} \to \mathbb{B}$ хомоморфизам.

- Уколико је h „1–1", кажемо да је h мономорфизам.
- Уколико је h „на", кажемо да је h епиморфизам.
- Уколико је h „1–1" и „на", кажемо да је h изоморфизам.
- Уколико је $\mathbb{A} = \mathbb{B}$, кажемо да је h ендоморфизам.
- Уколико је h изоморфизам и ендоморфизам, кажемо да је h аутоморфизам.

Став 3 Нека су $h\colon \mathbb{A} \to \mathbb{B}$ и $g\colon \mathbb{B} \to \mathbb{C}$ хомоморфизми. Тада:

а) $g \circ h$ је хомоморфизам.

б) Ако је су g и h мономорфизми, онда је то и $g \circ h$.

в) Ако је су g и h епиморфизми, онда је то и $g \circ h$.

г) Ако је су g и h изоморфизми, онда је то и $g \circ h$.

д) Ако је h изоморфизам, онда је h^{-1} изоморфизам.

Доказ. Доказаћемо само тврђења а) и д) (јасно је да остали резултати следе из основних чињеница о функцијама).

Доказ за а)

$$\begin{aligned}(g \circ h)(a_i) &= g(h(a_i)) \\ &= g(b_i) \quad \text{(пошто је } h \text{ хомоморфизам)} \\ &= c_i \qquad \text{(пошто је } g \text{ хомоморфизам).}\end{aligned}$$

$$\begin{aligned}(g \circ h)(\phi_i(u_1, \ldots, u_{n_i}) &= g(h(\phi_i(u_1, \ldots, u_{n_i})) \\ &= g(\psi_i(h(u_1), \ldots, h(u_{n_i})) \quad (\ h \text{ је хомоморфизам}) \\ &= \theta_i(g(h(u_1)), \ldots, g(h(u_{n_i}))) \quad (g \text{ је хомоморфизам}) \\ &= \theta_i((g \circ h)(u_1), \ldots, (g \circ h)(u_{n_i})).\end{aligned}$$

Доказ за д) Знамо да h^{-1} постоји и да $h^{-1}\colon B \to A$. Треба показати да је h^{-1} хомоморфизам.

Како је $h(a_i) = b_i$, то је и $h^{-1}(b_i) = a_i$.

Нека су $v_1, \ldots, v_{n_i}$ произвољни елементи из B. Како је h „на", то постоје u_j из A такви да је $h(u_j) = v_j$ за све $j = \overline{1, n_i}$. Добијамо

$$\begin{aligned}h^{-1}(\psi_i(v_1, \ldots, v_{n_i})) &= h^{-1}(\psi_i(h(u_1), \ldots, h(u_{n_i})) \\ &= h^{-1}(h(\phi_i(u_1, \ldots, u_{n_i}))(h \text{ је хомоморфизам}) \\ &= \phi_i(u_1, \ldots, u_{n_i}) \\ &= \phi_i(h^{-1}(v_1), \ldots, h^{-1}(v_{n_i})).\end{aligned}$$

□

Наведимо неке примере.

Пример 4 Са $\mathbf{R}^+$ означимо скуп позитивних реалних бројева. Тада је функција $\ln\colon \mathbf{R}^+ \to \mathbf{R}$ хомоморфизам групе $(\mathbf{R}^+, \cdot, ^{-1}, 1)$ у групу $(\mathbf{R}, +, -, 0)$ (добро нам је познато да је $\ln(x \cdot y) = \ln x + \ln y$, $\ln(x^{-1}) = -\ln x$ и $\ln 1 = 0$). ♣

Пример 5 Конјуговање, тј. функција $g\colon \mathbf{C} \to \mathbf{C}$, задата са $g(z) = \overline{z}$ представља ендоморфизам алгебре $\mathbb{C} = (\mathbf{C}, +, \cdot, 0, 1)$ (са $\mathbf{C}$ је наравно означен скуп свих комплексних бројева). ♣

Пример 6 Ако је $\rho_n\colon Z \to Z_n$ функција која целом броју придружује његов остатак по модулу n (где је $n \geq 2$), онда је тако задат хомоморфизам комутативног прстена са јединицом $\mathbb{Z} = (Z, +, \cdot, -, 0, 1)$ у комутативан прстен са јединицом $\mathbb{Z}_n = (Z_n, +_n, \cdot_n, -_n, 0, 1)$

Покажимо да је ρ_n заиста хомоморфизам. Пре свега, јасно је да је $\rho_n(0) = 0$ и $\rho_n(1) = 1$. Проверимо да важи и

$$\rho_n(s+t) = \rho_n(s) +_n \rho_n(t), \rho_n(s \cdot t) = \rho_n(s) \cdot_n \rho_n(t), \rho_n(-s) = -_n \rho(s).$$

Пре свега,

$$s = q \cdot n + \rho_n(s), \quad t = q' \cdot n + \rho_n(t),$$

за јединствено одређене целе бројеве q и q' (дељење са остатком). Добијамо да је

$$s + t = (q + q') \cdot n + (\rho_n(s) + \rho_n(t)).$$

Подсетимо се операције сабирања по модулу n. Добијамо да је

$$\rho_n(s) + \rho_n(t) = q'' \cdot n + (\rho_n(s) +_n \rho_n(t)),$$

за јединствено одређен цео број q'' (наравно да је тај број у овом случају или 0 или 1). Заменом у претходну једначину добијамо да је

$$s + t = (q + q' + q'') \cdot n + (\rho_n(s) +_n \rho_n(t)).$$

Како је $0 \leq \rho_n(s) +_n \rho_n(t) < n$, то на основу јединствености дељења са остатком можемо да закључимо да је $\rho_n(s) +_n \rho_n(t)$ заиста остатак при дељењу броја $s + t$ са n, тј. да важи

$$\rho_n(s+t) = \rho_n(s) +_n \rho_n(t),$$

а то је и требало доказати. На врло сличан начин се показује да је и

$$\rho_n(s \cdot t) = \rho_n(s) \cdot_n \rho_n(t),$$

Покажимо за крај да је $\rho(-s) = -_n s$ за све целе бројеве s. Пре свега,

$$s = q \cdot n + \rho_n(s),$$

за јединствено одређен цео број q. Тада је

$$-s = (-q) \cdot n + (-\rho_n(s)).$$

Уколико је $\rho_n(s) = 0$, то добијамо да је и $\rho_n(-s) = 0$, те је заиста $\rho_n(-s) = -_n \rho_n(s)$ (поновите дефиницију унарне операције $-_n$). У супротном је $0 < n - \rho_n(s) < n$. Добијамо да је

$$-s = (-q - 1) \cdot n + (n - \rho_n(s)),$$

где је $-q-1$ цео број, а $0 < \ n-\rho_n(s) < n$. Дакле, $n-\rho_n(s)$ је остатак при дељењу $-s$ са n, тј. заиста је $\rho_n(-s) = -_n s$. ♣

Позабавимо се сада нечим другим. Нека за наше алгебре $\mathbb{A}$ и $\mathbb{B}$ важи да је $A \subseteq B$. Природно је тада размотрити инклузију скупа A у скуп B, тј. функцију $i\colon A \to B$ такву да је $i(u) = u$ за све $u \in A$. Поставља се питање: да ли је i хомоморфизам? Анализирајмо мало ту ситуацију. Уколико је i заиста хомоморфизам, онда мора бити $i(a_k) = b_k$ за све $k = \overline{1,s}$ а како је $i(a_k) = a_k$, закључујемо да мора бити $a_k = b_k$ за све $k = \overline{1,s}$. Слично, мора бити испуњено и

$$\phi(u_1, \ldots, u_{n_k}) = i(\phi(u_1, \ldots, u_{n_k})) = \psi(i(u_1), \ldots, i(u_{n_k})) = \psi(u_1, \ldots, u_{n_k}),$$

за све $u_j \in A$. Дакле, операције ϕ и ψ морају давати исти резултат уколико су им аргументи из A. Често се краће каже да је операција ϕ рестрикција операције ψ.

Дефиниција 7 Нека су $\mathbb{A}$ и $\mathbb{B}$ алгебре за које важи: $A = B$. Тада је $\mathbb{A}$ подалгебра алгебре $\mathbb{B}$ уколико је за све $k = \overline{1,s}$ испуњено $a_k = b_k$ и уколико за све $i = \overline{1,r}$ и све $u_1, \ldots, u_{n_i} \in A$ важи: $\phi_i(u_1, \ldots, u_{n_i}) = \psi_i(u_1, \ldots, u_{n_i})$

Уколико је $\mathbb{A}$ подалгебра од $\mathbb{B}$, то ћемо краће записивати са:

$$\mathbb{A} \leq \mathbb{B}.$$

Приметимо да из претходне дискусије следи да је $\mathbb{A} \leq \mathbb{B}$ ако и само ако је инклузија $i\colon A \to B$ хомоморфизам.

Примере није тешко наћи:

$$\mathbb{Z}(= (Z, +, \cdot, 0, 1)) \leq \mathbb{Q}(= (Q, +, \cdot, 0, 1)) \leq \mathbb{R}(= (R, +, \cdot, 0, 1)) \leq \mathbb{C}(= (C, +, \cdot, 0, 1)),$$

но приметимо да

$$\mathbb{Z}_n \not\leq \mathbb{Z},$$

јер се операције не поклапају на мањем скупу.

Један важан пример подалгебре појављује се на следећи начин. Нека је $h\colon \mathbb{A} \to \mathbb{B}$ хомоморфизам алгебри. Посматрајмо слику функције h:

$$\mathrm{Im}(h) = h[A] = \{h(u) : u \in A\}.$$

Како је $h(a_i) = b_i$ (подсетите се конвенције са почетка ове лекције), то сви изабрани елементи $b_1, \ldots, b_s$ припадају $\mathrm{Im}(h)$. Осим тога, нека су $v_1, \ldots, v_{n_i}$ произвољни елементи из $\mathrm{Im}(h)$. Тада постоје $u_1, \ldots, u_{n_i}$ за такви да је $h(u_1) = v_1, \ldots, h(u_{n_i}) = v_{n_i}$. Стога добијамо:

$$\psi_i(v_1, \ldots, v_{n_i}) = \psi_i(h(u_1), \ldots, h(u_{n_i})) = h(\phi_i(v_1, \ldots, v_{n_i})) \in \mathrm{Im}(h).$$

Дакле, рестрикције операција $\psi_1, \ldots, \psi_r$ задају операције на $\mathrm{Im}(h)$, а како и $b_1, \ldots, b_s \in \mathrm{Im}(h)$, то је природно задата структура алгебре на $\mathrm{Im}(h)$, која је чини подалгебром алгебре $\mathbb{B}$. Користимо ознаку $h[\mathbb{A}]$ да означимо ту подалгебру.

Пређимо сада на појам директног производа алгебри.

Дефиниција 8 Нека су

$$\mathbb{A} = (A, \phi_1, \ldots, \phi_r, a_1, \ldots, a_s)$$

и

$$\mathbb{B} = (B, \psi_1, \ldots, \psi_r, b_1, \ldots, b_s)$$

две алгебре исте сигнатуре. Директан производ ових алгебри је алгебра

$$\mathbb{P} = (P, \zeta_1, \ldots, \zeta_r, p_1, \ldots, p_s),$$

где је $P = A \times B$, $p_j = (a_j, b_j)$, а операције ζ_i задате са:

$$\zeta_i((u_1, v_1), \ldots, (u_{n_i}, v_{n_i})) := (\phi_i(u_1, \ldots, u_{n_i}), \psi(v_1, \ldots, v_{n_i})).$$

Дакле, операције ζ_i су задате „по координатама".

Јасно је да је сигнатура алгебре $\mathbb{P}$ једнака сигнатури алгебра $\mathbb{A}$ и $\mathbb{B}$. Ми ћемо се касније бавити производима конкретних алгебарских структура, на пример, производима група, Абелових група, комутативних прстена са јединицом, и тада ћемо се детаљније бавити овим појмом. Урадимо за сада само један једноставан пример.

Пример 9 Посматрајмо производ Абелових група $\mathbb{Z}_3$ и $\mathbb{Z}_4$. Скуп носач P је скуп

$$Z_3 \times Z_4 = \{0, 1, 2\} \times \{0, 1, 2, 3\}.$$

Операција на P је задата са:

$$(m_1, n_1) + (m_2, n_2) = (m_1 +_3 m_2, n_1 +_4 n_2),$$

где $m_i \in Z_3$, а $n_j \in Z_4$. На пример,

$$(2, 3) + (1, 2) = (0, 1).$$

Касније ћемо видети да постоји изоморфизам овог производа и групе $\mathbb{Z}_{12}$. ♣

Може се дефинисати и производ алгебри $\mathbb{A}_1, \ldots, \mathbb{A}_n$ (за ма које n):

$$\mathbb{A}_1 \times \cdots \times \mathbb{A}_n.$$

где се операције изводе „по координатама", но алтернативно се тај производ може добити и поновљеним производима две алгебре (тј. тако ће се добити изоморфне алгебре). Нпр. алгебра $\mathbb{A}_1 \times \mathbb{A}_2 \times \mathbb{A}_3$ изоморфна је алгебри $(\mathbb{A}_1 \times \mathbb{A}_2) \times \mathbb{A}_3$ (а такође и алгебри $\mathbb{A}_1 \times (\mathbb{A}_2 \times \mathbb{A}_3)$), но више о томе ће бити речи касније, за конкретне алгебарске структуре. Произвољан директан производ (можда и бесконачно много алгебри)

$$\prod_{i \in I} \mathbb{A}_i,$$

такође није тешко дефинисати, али га ми нећемо разматрати.

У случају директног производа алгебри $\mathbb{A} \times \mathbb{B}$, природно се појављују два епиморфизма, пројекције на прву, односно другу координату:

$$\pi_A : \mathbb{A} \times \mathbb{B} \to \mathbb{A}, \quad \pi_A(u, v) = u,$$
$$\pi_B : \mathbb{A} \times \mathbb{B} \to \mathbb{B}, \quad \pi_A(u, v) = v.$$

Није тешко проверити да су то заиста хомоморфизми одговарајућих алгебри који су очигледно „на". Оно што је занимљиво у вези ових хомоморфизама је следећа чињеница. За сваку алгебру $\mathbb{C}$ исте сигнатуре, као и $\mathbb{A}$ и $\mathbb{B}$ и све хомоморфизме $h\colon \mathbb{C} \to \mathbb{A}$ и $g\colon \mathbb{C} \to \mathbb{B}$ постоји јединствено одређени хомоморфизам $f\colon \mathbb{C} \to \mathbb{A} \times \mathbb{B}$ за који важи:

$$\pi_A \circ f = g, \text{ и } \pi_B \circ f = h.$$

Наравно да се хомоморфизам f задаје са: $f(w) = (g(w), h(w))$ за $w \in C$. Није тешко проверити да се тако заиста добија један хомоморфизам. Суштина овог резултата је у томе да је задавање хомоморфизма у производ еквивалентно задавању хомоморфизма у сваку компоненту. Видећемо касније како то изгледа на конкретним примерима група и хомоморфизама.

Дефиниција 10 Нека је $\mathfrak{M}$ нека класа алгебри. Та класа је

а) затворена у односу на подалгебре уколико важи:

ако $\mathbb{A} \in \mathfrak{M}$ и $\mathbb{B} \leq A$ онда и $\mathbb{B} \in \mathfrak{M}$;

б) затворена у односу на хомоморфне слике уколико важи:

ако је $h\colon \mathbb{A} \to \mathbb{B}$ хомоморфизам и $\mathbb{A} \in \mathfrak{M}$ онда и $h[\mathbb{A}] \in \mathfrak{M}$;

в) затворена у односу на директне производе уколико важи:

ако за све $i \in I$ $A_i \in \mathfrak{M}$ онда и $\prod_{i \in I} \mathbb{A}_i \in \mathfrak{M}$,

Наведимо сада једну теорему, коју нећемо доказивати, а која карактерише једнакосне класе алгебри (варијетете).

Теорема 11 Нека је $\mathfrak{M}$ нека класа алгебри. Та класа је варијетет ако и само ако је затворена у односу на подалгебре, хомоморфне слике и директне производе.

Пажљив читалац није пропустио да примети да у примеру варијетета нисмо навели класу свих поља. То наравно није случајно, јер класа свих поља не чини варијетет — директан производ два поља није поље. Наиме, ако су E и F, ма која поља онда у производу $E \times F$ важи:

$$(1_E, 0_F) \cdot (0_E, 1_F) = (0_E, 0_F),$$

те у том производу постоје прави делитељи нуле, а њих нема у пољима. Вратићемо се на ово касније када будемо проучавали прстене и поља.

Пређимо сада на појам *конгруенције*.

Дефиниција 12 Нека је

$$\mathbb{A} = (A, \phi_1, \ldots, \phi_r, a_1, \ldots, a_s)$$

нека алгебра и $\sim$ релација еквиваленције на скупу носачу A. Та релација је конгруенција уколико за све $i = \overline{1,r}$ и све $u_j, v_k \in A$:

ако је $u_1 \sim v_1, \ldots, u_{n_i}, \sim v_{n_i}$ онда је и $\phi_i(u_1, \ldots, u_{n_i}) \sim \phi_i(v_1, \ldots, v_{n_i})$.

Другим речима, ако при ма којој операцији аргументе заменимо еквивалентним елементима, добијамо резултат еквивалентан почетном. Наведимо неке примере.

Пример 13 Основни пример конгруенције је пример конгруенције по модулу неког природног броја n ($n \geq 2$):

$$a \equiv b \pmod{n} \text{ ако и само ако } n \mid (a - b).$$

Конгруенцију по модулу n често ћемо означавати и са $\equiv_n$, због краткоће записа.

Није тешко проверити да је $\equiv_n$ заиста конгруенција (у горе наведеном смислу) алгебре $\mathbb{Z} = (\mathbf{Z}, +, \cdot)$. Наиме, лако се провери да је то релација еквиваленције. Проверимо да се „слаже са операцијама".

Уколико је $a \equiv_n b$ и $a_1 \equiv_n b_1$, онда $n \mid (a - b)$ и $n \mid (a_1 - b_1)$, тј.

$$a - b = nq \quad \text{и} \quad a_1 - b_1 = nq_1,$$

за неке целе бројеве q, q_1. Тада је

$$(a + a_1) - (b + b_1) = (a - b) + (a_1 - b_1) = nq + nq_1 = n(q + q_1),$$

па је заиста $(a + a_1) \equiv_n (b + b_1)$.

Такође,

$$aa_1 - bb_1 = aa_1 - ba_1 + ba_1 - bb_1 = (a-b)a_1 + b(a_1 - b_1) = nqa_1 + bnq_1 = n(qa_1 + bq_1),$$

те је $ab \equiv_n a_1 b_1$. ♣

Пример 14 Дефинишимо релацију $\sim$ на скупу свих природних бројева са: $a \sim b$ ако и само ако се цифре на месту десетица у декадном запису ових бројева подударају.

На пример, $134 \sim 1235$, јер је 3 на месту десетица и код једног и код другог броја, док $3 \not\sim 13$ пошто у првом броју имамо 0 на месту десетица (која се наравно на пише у случају једноцифрених бројева), а у другом 3. Но, $100 \sim 3$, пошто оба броја имају 0 на месту десетица. Јасно је да је ово једна релација еквиваленције. Но, она није конгруенција структуре $(\mathbf{N}, +, \cdot)$. На пример, $13 \sim 411$ и $258 \sim 52$, али $13 + 258 = 271$, а $411 + 52 = 463$, па $(13 + 258) \not\sim (411 + 52)$. ♣

Као што нам функције које сликају скуп носач једне структуре у скуп носач друге структуре нису посебно интересантне уколико нису и хомоморфизми (јер не поштују структуру), тако нам и произвољне релације еквиваленције на скупу носачу неке алгебре нису нарочито интересантне (јер не поштују структуру). Није неочекивано да постоји важна веза између хомоморфизама и конгруенција. Ево једног веома важног примера конгруенције.

Пример 15 Нека су

$$\mathbb{A} = (A, \phi_1, \ldots, \phi_r, a_1, \ldots, a_s) \quad \text{и} \quad \mathbb{B} = (B, \psi_1, \ldots, \psi_r, b_1, \ldots, b_s)$$

две алгебре и $h\colon \mathbb{A} \to \mathbb{B}$ хомоморфизам. Језгро овог хомоморфизма, у ознаци $\mathrm{Ker}(h)$ је конгруенција алгебре $\mathbb{A}$, која се дефинише на следећи начин:

$$(u, v) \in \mathrm{Ker}(h) \overset{\text{def}}{\iff} h(u) = h(v).$$

Ако се присетимо се да се бинарна релација дефинише као скуп уређених парова, онда нам ова дефиниција неће изгледати необично (не би било баш лепо писати $u\,\mathrm{Ker}(h)\,v$, зар не?). Није тешко проверити да је ово заиста конгруенција. Проверу да је ово релација еквиваленције могу читаоци сами лако да изведу (а пошто је лако, а и могу, онда и треба!), ми ћемо овде проверити слагање са операцијама.

Дакле, нека су $u_j, v_k \in A$ за које важи

$$(u_1, v_1) \in \mathrm{Ker}(h), \ldots, (u_{n_i}, v_{n_i}) \in \mathrm{Ker}(h).$$

Треба показати да

$$(\phi_i(u_1, \ldots, u_{n_i}), \phi_i(v_1, \ldots, v_{n_i})) \in \mathrm{Ker}(h),$$

тј. да је

$$h(\phi_i(u_1, \ldots, u_{n_i})) = h(\phi_i(v_1, \ldots, v_{n_i})).$$

Проверимо то:

$$\begin{aligned} h(\phi_i(u_1, \ldots, u_{n_i})) &= \psi_i(h(u_1), \ldots, h(u_{n_i})) \text{ (јер је } h \text{ хомоморфизам)} \\ &= \psi_i(h(v_1), \ldots, h(u_{v_i})) \text{ (јер } (u_j, v_j) \in \mathrm{Ker}(h) \text{ за све } j) \\ &= h(\phi_i(v_1, \ldots, v_{n_i})) \text{ (јер је } h \text{ хомоморфизам).} \quad ♣ \end{aligned}$$

Свака конгруенција на датој алгебри омогућава конструкцију количничке алгебре. Размотримо ту важну конструкцију.

Дефиниција 16 Нека је

$$\mathbb{A} = (A, \phi_1, \ldots, \phi_r, a_1, \ldots, a_s),$$

дата алгебра и $\sim$ конгруенција те алгебре. Ако са $A/_\sim$ означимо скуп свих класа еквиваленције, а са $[u]$ класу класу еквиваленције елемента $u \in A$, онда количничку алгебру ове алгебре по конгруенцији $\sim$, у ознаци $\mathbb{A}/_\sim$, задајемо са:

$$\mathbb{A}/_\sim = (A/_\sim, \Phi_1, \ldots, \Phi_r, [a_1], \ldots, [a_s]),$$

где су операције Φ_i дефинисане са:

$$\Phi_i([u_1], \ldots, [u_{n_i}]) := [\phi_i(u_1, \ldots, u_{n_i})].$$

Морамо проверити добру дефинисаност ових операција. Наиме, морамо проверити следеће:

ако је $[u_1] = [v_1], \ldots, [u_{n_i}] = [v_{n_i}]$, онда је $[\phi_i(u_1, \ldots, u_{n_i})] = [\phi_i(v_1, \ldots, v_{n_i})]$.

То није тешко проверити и у провери се користи чињеница да је $\sim$ конгруенција. Наиме, ако је

$$[u_1] = [v_1], \ldots, [u_{n_i}] = [v_{n_i}],$$

то заправо значи да је

$$u_1 \sim v_1, \ldots, u_{n_i} \sim v_{n_i}.$$

Како је $\sim$ конгруенција, следи да мора бити

$$\phi_i(u_1, \ldots, u_{n_i}) \sim \phi_i(v_1, \ldots, v_{n_i}),$$

а то управо значи да је

$$[\phi_i(u_1, \ldots, u_{n_i})] = [\phi_i(v_1, \ldots, v_{n_i})].$$

Пример 17 На алгебарској структури $\mathbb{Z} = (Z, +, \cdot, 0, 1)$, задата је конгруенција $\equiv_n$, где је $n \geq 2$ природан број. Добијамо количничку структуру $\mathbb{Z}/_{\equiv_n} = (Z/_{\equiv_n}, +, \cdot, [0], [1])$. Овде смо користили исте ознаке за операције на количничкој структури као и на почетној алгебри (а то ћемо често, због једноставности записа, радити и касније). Операције на количничкој структури задате су са:

$$[a] + [b] := [a + b], \quad [a] \cdot [b] := [a \cdot b].$$

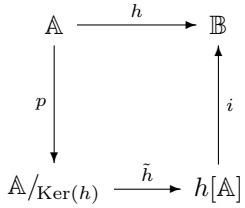
Приметимо да постоји тачно n различитих класа еквиваленције. Наиме, сваки цео број m конгруентан је по модулу n тачно једном од бројева из скупа $\{0, 1, \ldots, n-1\}$. То је јасно из чињенице да се он може записати у облику $m = qn + r$, где су бројеви q и r јединствено задати под условом да је $0 \leq r < n$. Дакле, $\mathbb{Z}/_{\equiv_n} = \{[0], [1], \ldots, [n-1]\}$. Како се сабирају и множе ове класе? Јасно је о чему се ради. Уколико су

$[s], [t] \in \{[0], [1], \ldots, [n-1]\}$, онда је $[s] + [t]$ она класа из тог скупа, која је једнака класи $[s + t]$. Јасно је да то мора бити класа $[s +_n t]$, јер се збир $s +_n t$ и дефинише као остатак при дељењу $s + t$ са n. Слично је и $[s] \cdot [t] = [s \cdot_n t]$. Видимо да заправо функција $h: Z_n \to \mathbb{Z}/_{\equiv_n}$ задата са: $h(s) := [s]$ остварује изоморфизам структура $\mathbb{Z}_n$ и $\mathbb{Z}/_{\equiv_n}$. Тако смо установили да се све алгебарске структуре $\mathbb{Z}_n$ могу добити (до на изоморфизам) као количничке структуре (при различитим конгруенцијама) алгебарске структуре $\mathbb{Z}$. ♣

Ако је $\mathbb{A}$ нека алгебра и $\sim$ конгруенција те алгебре, на природан начин се дефинише хомоморфизам $p: \mathbb{A} \to \mathbb{A}/_\sim$ са: $p(u) := [u]$, где је $u \in A$. Читаоцу остављамо да провери да је p заиста хомоморфизам. С обзиром да је p и „на", зовемо га и канонским епиморфизмом алгебре $\mathbb{A}$ на своју количничку алгебру $\mathbb{A}/_\sim$.

За крај ове лекције наводимо теорему о разлагању (декомпозицији) хомоморфизма.

Теорема 18 Нека су $\mathbb{A}$ и $\mathbb{B}$ алгебре и $h: \mathbb{A} \to \mathbb{B}$ хомоморфизам алгебри. Тада се хомоморфизам h може разложити у облику следеће композиције: $h = i \circ \tilde{h} \circ p$, где је i инклузија подалгебре $h[\mathbb{A}]$ у алгебру $\mathbb{B}$, p канонски епиморфизам алгебре $\mathbb{A}$ на своју количничку алгебру $\mathbb{A}/_{\mathrm{Ker}(h)}$, а $\tilde{h}$ изоморфизам $\tilde{h}: \mathbb{A}/_{\mathrm{Ker}(h)} \to h[\mathbb{A}]$ задат са: $\tilde{h}([u]) := h(u)$. Дакле, следећи дијаграм комутира.



Доказ. Морамо проверити да ли је $\tilde{h}$ добро дефинисан и да ли је изоморфизам. Пре свега, нека је $[u] = [v]$. Треба проверити да је $\tilde{h}([u]) = \tilde{h}([v])$, тј. да је $h(u) = h(v)$, но чињеница да је $[u] = [v]$ нам управо даје да $(u, v) \in \mathrm{Ker}(h)$, тј. $h(u) = h(v)$, што се заправо и тражило. Дакле, $\tilde{h}$ јесте добро дефинисана функција. Јасно је да је $\tilde{h}$ „на". Проверимо да је и „1-1". Претпоставимо да је $\tilde{h}([u]) = \tilde{h}([v])$. То значи да је $h(u) = h(v)$, те $(u, v) \in \mathrm{Ker}(h)$, па је заиста $[u] = [v]$. Остаје да проверимо да је $\tilde{h}$ хомоморфизам.

$$\begin{aligned}
\tilde{h}(\Phi_i([u_1], \ldots, [u_{n_i}])) &= \tilde{h}([\phi_i(u_1, \ldots, u_{n_i})]) \text{ по дефиницији операције } \Phi_i \\
&= h(\phi_i(u_1, \ldots, u_{n_i})) \text{ по дефиницији функције } \tilde{h} \\
&= \psi_i(h(u_1), \ldots, h(u_{n_i})) \text{ јер је } h \text{ хомоморфизам} \\
&= \psi_i(\tilde{h}([u_1]), \ldots, \tilde{h}([u_{n_i}])) \text{ по дефиницији } \tilde{h}.
\end{aligned}$$

Дакле, $\tilde{h}$ је заиста изоморфизам. Покажимо још да дијаграм комутира.

$$(i \circ \tilde{h} \circ p)(u) = i(\tilde{h}(p(u)))$$

$$
\begin{aligned}
&= i(\tilde{h}([u])\\
&= i(h(u))\\
&= h(u).
\end{aligned}
$$

Овде смо наравно користили да је $p(u) = [u]$ и да је $i(v) = v$ за све $v \in h[\mathbb{A}]$, пошто је i инклузија. Овим је доказ завршен. □

Пример 19 Уочимо хомоморфизам $\rho_n\colon \mathbb{Z} \to \mathbb{Z}_n$, где је $\rho_n(m)$ остатак при дељењу m са n. Применити на њега теорему о разлагању хомоморфизма.

Јасно је да је хомоморфизам „на". Из теореме о разлагању хомоморфизма следи да је $\mathbb{Z}/_{\mathrm{Ker}(\rho_n)} \cong \mathbb{Z}_n$. Одредимо $\mathrm{Ker}(\rho_n)$. На основу дефиниције језгра хомоморфизма добијамо да је $(r, s) \in \mathrm{Ker}(\rho_n)$ ако и само ако је $\rho_n(r) = \rho_n(s)$. Другим речима, $(r, s) \in \mathrm{Ker}(\rho_n)$ ако и само ако r и s имају исти остатак при дељењу са n. Покажимо да је то еквивалентно са $r \equiv_n s$.

Пре свега, ако је $r = qn + \rho_n(r)$ и $s = q'n + \rho_n(s)$ и ако је $\rho_n(r) = \rho_n(s)$, онда је $r - s = n(q - q')$ и заиста је $r \equiv_n s$. Обратно, нека је $r \equiv_n s$. Како је јасно да је $r \equiv_n \rho_n(r)$ (зашто?), добијамо, с обзиром да је $\equiv_n$ релација еквиваленције, да је $\rho_n(r) \equiv_n \rho_n(s)$. Но и $\rho_n(r)$ и $\rho_n(s)$ су бројеви из скупа $\{0, \ldots, n-1\}$. Уколико претпоставимо да је нпр. $\rho_n(r) \leq \rho_n(s)$ добићемо да је $0 \leq \rho_n(s) - \rho_n(r) < n$ и да $n \mid (\rho_n(s) - \rho_n(r))$. То је могуће једино ако је $\rho_n(r) = \rho_n(s)$. Дакле, заиста се конгруенција $\mathrm{Ker}(\rho_n)$ поклапа са $\equiv_n$ и из теореме о разлагању хомоморфизма следи да је $\mathbb{Z}/_{\equiv_n} \cong \mathbb{Z}_n$, као што смо већ раније показали. ♣