АЛГЕБРА

Групе

Хомоморфизми и теореме о изоморфизмима

Зоран Петровић

21. март 2011.

Већ смо упознати са појмом изоморфизма група. Општији појам је појам хомоморфизма.

Дефиниција 1 Нека су $(G,\cdot)$ и $(H,*)$ групе. Функција $f\colon G\to H$ је хомоморфизам уколико за све $x,y\in G$ важи:

$$f(x\cdot y)=f(x)*f(y).$$

Дакле, изоморфизам је онај хомоморфизам који је и бијекција. Приметимо да се лако показује, на исти начин као и у случају изоморфизма, да се при сваком хомоморфизму неутрал групе G слика у неутрал групе H, а инверз елемента из групе G у инверз његове слике у групи H (подсетите се тог доказа). Како хомоморфизам не мора бити бијекција, природно је испитати у којој мери дати хомоморфизам „одступа“ од изоморфизма. Важан појам у вези са тим је и појам *језгра* хомоморфизма.

Дефиниција 2 Нека је $f\colon G\to H$ хомоморфизам група. Језгро хомоморфизма f, у ознаци $\mathrm{Ker}(f)$ дефинише се са:

$$\mathrm{Ker}(f):=\{g\in G: f(g)=e_H\},$$

где је са e_H означен неутрал у H.

Став 3 Језгро сваког хоморфизма $f\colon G\to H$ је нормална подгрупа групе G.

Доказ. Како је $f(e_G)=e_H$, то $e_G\in\mathrm{Ker}(f)$, па $\mathrm{Ker}(f)\neq\emptyset$. Претпоставимо да $x,y\in\mathrm{Ker}(f)$. Треба показати да $x^{-1}y\in\mathrm{Ker}(f)$. Но,

$$f(x^{-1}y)=f(x)^{-1}*f(y)=e_H^{-1}*e_H=e_H,$$

те заиста $x^{-1}y\in\mathrm{Ker}(f)$. Дакле, доказали смо да је $\mathrm{Ker}(f)\leq G$.

Да бисмо показали да је језгро нормална подгрупа, посматрајмо произвољне елементе $x\in\mathrm{Ker}(f)$ и $g\in G$. Тада је

$$f(gxg^{-1})=f(g)*f(x)*f(g)^{-1}=f(g)*e_H*f(g)^{-1}=e_H,$$

те закључујемо да је $g\mathrm{Ker}(f)g^{-1} \subseteq \mathrm{Ker}(f)$, за све $g \in G$, те је заиста $\mathrm{Ker}(f) \triangleleft G$. □

Став 4 Хомоморфизам група $f: G \to H$ је „1–1“ ако и само ако је

$$\mathrm{Ker}(f) = \{e_G\}.$$

Доказ.
$\Longrightarrow$: Претпоставимо да је f „1–1“ и нека $x \in \mathrm{Ker}(f)$. То значи да је

$$f(x) = e_H = f(e_G).$$

Како је f „1–1“, мора бити $x = e_G$. Закључујемо да је $\mathrm{Ker}(f) = \{e_G\}$.
$\Longleftarrow$: Нека је $\mathrm{Ker}(f) = \{e_G\}$. Претпоставимо да је $f(x) = f(y)$. То значи да је

$$f(x^{-1}y) = f(x^{-1}) * f(y) = f(x)^{-1} * f(y) = e_H^{-1} * e_H = e_H,$$

па је $x^{-1}y \in \mathrm{Ker}(f) = \{e_G\}$. Добијамо да је $x = y$, те закључујемо да је f „1–1“. □

Уколико је $\mathrm{Ker}(f) = \{e_G\}$, кажемо и да је језгро тривијално. Ако је f „1–1“ хомоморфизам, кажемо и да је f *мономорфизам*.

Дефиниција 5 Слика хомоморфизма $f: G \to H$, у ознаци $\mathrm{Im}(f)$, дефинише се са:

$$\mathrm{Im}(f) := \{y \in H : (\exists x \in G) y = f(x)\}.$$

Дакле, слика хоморфизма је заправо обична слика функције f.

Став 6 Ако је $f: G \to H$ хомоморфизам, онда је $\mathrm{Im}(f) \leq H$.

Доказ. Како је $e_H = f(e_G)$, то $\mathrm{Im}(f) \neq \emptyset$. Претпоставимо да $y_1, y_2 \in \mathrm{Im}(f)$. То значи да постоје x_1, x_2 такви да је $f(x_1) = y_1$ и $f(x_2) = y_2$. Но, тада је

$$y_1^{-1} * y_2 = f(x_1)^{-1} * f(x_2) = f(x_1^{-1}x_2) \in \mathrm{Im}(f).$$

□

Приметимо да слика хомоморфизма не мора бити нормална подгрупа од H. Наиме, ако је $H \leq G$ онда је слика од H при инклузији (која је хомоморфизам) сама подгрупа H и ако она није нормална, то нам даје тражени пример.

Хомоморфизам, који је уједно и „на“, зовемо *епиморфизам*. Основни пример епиморфизма је следећи. Нека је G група и H ма која њена нормална подгрупа. Тада је са $p(a) = aH$ задат један *епиморфизам* $p: G \to G/H$. Наравно, јасно је да је p „на“. Осим тога

$$p(ab) = (ab)H = (aH)(bH) = p(a)p(b),$$

те је p и хомоморфизам.

Наведимо сада прву теорему о изоморфизмима за групе.

Теорема 7 Нека је $f: G \to H$ хомоморфизам група. Тада f индукује изоморфизам $\tilde{f}: G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ дефинисан са: $\tilde{f}(x\,\mathrm{Ker}(f)) := f(x)$.

Доказ. Покажимо најпре да је $\tilde{f}$ добро дефинисана функција. Наиме, нека је $x\,\mathrm{Ker}(f) = y\,\mathrm{Ker}(f)$. То значи да $x^{-1}y \in \mathrm{Ker}(f)$. Дакле, $f(x^{-1}y) = e_H$, па је $f(x) = f(y)$, те је $\tilde{f}(x\,\mathrm{Ker}(f)) = \tilde{f}(y\,\mathrm{Ker}(f))$. Функција $\tilde{f}$ је хомоморфизам:

$$\tilde{f}\left((x\,\mathrm{Ker}(f))(y\,\mathrm{Ker}(f))\right) = \tilde{f}((xy)\,\mathrm{Ker}(f)) = f(xy) = f(x) * f(y) =$$

$$= \tilde{f}(x\,\mathrm{Ker}(f)) * \tilde{f}(y\,\mathrm{Ker}(f)).$$

Из дефиниције хомоморфизма $\tilde{f}$, очигледно је да је $\mathrm{Im}(\tilde{f}) = \mathrm{Im}(f)$.

Остаје да се покаже да је $\tilde{f}$ „1–1“. тј. да је $\mathrm{Ker}(\tilde{f})$ тривијално. Претпоставимо да $x\,\mathrm{Ker}(f) \in \mathrm{Ker}(\tilde{f})$. То значи да је $\tilde{f}(x\,\mathrm{Ker}(f)) = e_H$. Из дефиниције $\tilde{f}$, следи да $x \in \mathrm{Ker}(f)$, те је $x\,\mathrm{Ker}(f) = \mathrm{Ker}(f)$. □

Наведимо неке примере примене ове теореме.

Пример 8 Ако са $\rho(x, n)$ означимо остатак при дељењу целог броја x природним бројем $n \geq 2$, онда је са $f(x) = \rho(x, n)$ дефинисан хомоморфизам група $f: \mathbb{Z} \to \mathbb{Z}_n$, који индукује изоморфизам $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Препоручујемо читаоцима да се сами увере у наведени резултат.

Пример 9 Ако са V означимо подгрупу групе S_4 дату са:

$$V = \{(1), (12)(34), (13)(24), (14)(23)\},$$

онда је $V \triangleleft S_4$ и $S_4/V \cong S_3$.

Већ нам је познато да је V нормална подгрупа (зашто то знамо?). Остаје да се нађе тражени изоморфизам. У ту сврху, ако је $X = \{(12)(34), (13)(24), (14)(23)\}$, дефинишимо хомоморфизам $f : S_4 \to S_X$ са:

$$f(\pi)(x) = \pi x \pi^{-1},$$

за $x \in X$. Како је $V \triangleleft S_4$, јасно је да је $\pi x \pi^{-1} \in V$, за све $x \in X \subset V$. Но, не може бити $\pi x \pi^{-1} = (1)$, јер би тада било $x = (1)$, што није тачно. Дакле, $f(\pi)$ заиста припада S_X. Проверимо да ли је f хомоморфизам:

$$f(\sigma\pi)(x) = (\sigma\pi)x(\sigma\pi)^{-1} = \sigma(\pi x \pi^{-1})\sigma^{-1} = f(\sigma)(\pi x \pi^{-1}) = f(\sigma)(f(\pi)(x)).$$

Добијамо да је $f(\sigma\pi) = f(\sigma) \circ f(\pi)$, те је f заиста хомоморфизам.

Одредимо језгро хомоморфизма f. Пре свега, како је V комутативна, то је $V \subseteq \mathrm{Ker}(f)$ (зашто?). Покажимо да важи и обратно, тј. да је заправо $\mathrm{Ker}(f) = V$. Претпоставимо да $\pi \in \mathrm{Ker}(f)$. То значи да је π пермутација из S_4 за коју важи:

$$\pi(12)(34)\pi^{-1} = (12)(34), \quad (1)$$

$$\pi(13)(24)\pi^{-1} = (13)(24), \quad (2)$$

$$\pi(14)(23)\pi^{-1} = (14)(23). \quad (3)$$

Претпоставимо да је $\pi(1) = 1$. Како је $\pi(12)(34)\pi^{-1} = (\pi(1)\pi(2))(\pi(3)\pi(4))$, из претпоставке да је $\pi(1) = 1$ и једнакости (1), следи да је

$$(1\pi(2))(\pi(3)\pi(4)) = (12)(34).$$

Видимо да мора бити $\pi(2) = 2$ и $\pi(3) \in \{3, 4\}$. Уколико је $\pi(3) = 3$, добијамо да је $\pi = (1) \in V$. Претпоставимо да је $\pi(3) = 4$. То значи да је заправо $\pi = (34)$. Но, то би значило да је

$$\pi(13)(24)\pi^{-1} = (\pi(1)\pi(3))(\pi(2)\pi(4)) = (14)(23),$$

што је у супротности са (2). Дакле, претпоставка да је $\pi(1) = 1$, доводи до закључка да је π идентична пермутација, те да π припада V. На исти начин се показује да, уколико је $\pi(k) = k$ за било које k, мора бити $\pi = (1)$.

Претпоставимо да π нема фиксну тачку . Сада можемо, без губитка општости, претпоставити да је $\pi(1) = 2$. Из (1) добијамо

$$(2\pi(2))(\pi(3)\pi(4)) = (12)(34).$$

Очигледно да мора бити $\pi(2) = 1$ и $\pi(3) \in \{3, 4\}$. Како π нема фиксну тачку, добијамо да је $\pi(3) = 4$ и $\pi(4) = 3$, тј. $\pi = (12)(34) \in V$.

На овај начин смо показали да је $\mathrm{Ker}(f) = V$. Прва теорема о изоморфизмима каже да је тада

$$S_4/\mathrm{Ker}(f) \cong \mathrm{Im}(f),$$

тј. да је количничка група S_4/V изоморфна једној подгрупи од S_X. Но, $|S_4/V| = 24/4 = 6 = |S_X|$. Закључујемо да мора бити $\mathrm{Im}(f) = S_X$ и добијамо изоморфизам $S_4/V \cong S_X \cong S_3$. ♣

Наведимо сада један став, који се доказује помоћу наведене теореме.

Став 10 Ако је H подгрупа групе G таква да је $[G : H] = p$, при чему је p најмањи прост број који дели ред групе G, онда је $H \triangleleft G$.

Доказ. Нека је $X = G/H$ (дакле, X је скуп свих левих косета подгрупе H у групи G). Дефинишимо хомоморфизам $f: G \to S_X$ са:

$$f(g)(aH) = (ga)H,$$

за $a \in G$ (елементи у X су леви косети од H, дакле подскупови од G облика aH за неко $a \in G$). На основу прве теореме о изоморфизмима, $G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$. Приметимо да важи следеће:

$$\mathrm{Ker}(f) \subseteq H.$$

Наиме, ако $g \in \mathrm{Ker}(f)$, онда мора бити и $f(g)(H) = H$ (H је један од косета, а по претпоставци је $f(g) = id_X$), тј. $gH = H$. Но, из $gH = H$,

следи да g припада H. Добили смо да је група $G/\mathrm{Ker}(f)$ изоморфна једној подгрупи групе S_X. С обзиром да је $|X| = p$, добијамо да

$$|G/\mathrm{Ker}(f)| \mid p! \quad . \tag{4}$$

Но, како је $\mathrm{Ker}(f) \subseteq H$, то је

$$|G/\mathrm{Ker}(f)| = [G : \mathrm{Ker}(f)] = [G : H] \cdot [H : \mathrm{Ker}(f)] = p \cdot [H : \mathrm{Ker}(f)]. \tag{5}$$

Из (4) и (5) добијамо

$$[H : \mathrm{Ker}(f)] \mid (p-1)! \quad . \tag{6}$$

Но, како $[H : \mathrm{Ker}(f)]$ дели ред подгрупе H, а ред подгрупе H дели ред групе G, то добијамо да је $[H : \mathrm{Ker}(f)]$ делитељ реда групе G, у којем се, уколико тај делитељ није једнак 1, на основу (6), као прости фактори појављују искључиво прости бројеви мањи од p (ти прости фактори морају делити $(p-1)!$, па самим тим морају бити мањи од p), што није могуће. Закључујемо да је $[H : \mathrm{Ker}(f)] = 1$, те је $H = \mathrm{Ker}(f)$. Како је језгро хомоморфизма увек нормална подгрупа, добијамо да је и подгрупа H нормална. □

Напомена 1: Као и увек, врло је важно да се у тврђење не уноси нешто чега у њему нема! Дакле, уопште се не тврди да *за сваку групу* G уопште постоји подгрупа H индекса као у ставу. Но, *ако постоји*, онда је она нормална.

Напомена 2: У доказу овог става користили смо следећи резултат. Ако је K подгрупа од H коначног индекса $[H : K]$ и H подгрупа од G коначног индекса $[G : H]$, онда је

$$[G : K] = [G : H] \cdot [H : K].$$

Докажимо га.

Пре свега, нека је $[G : H] = m$ и $[H : K] = n$. Показаћемо да је $[G : K] = mn$. Како је $[G : H] = m$, то постоје елементи $g_1, g_2, \ldots, g_m \in G$ такви да је

$$G = g_1 H \sqcup g_2 H \sqcup \ldots \sqcup g_m H. \tag{7}$$

Такође постоје и елементи $h_1, h_2, \ldots, h_n \in H$ за које је

$$H = h_1 K \sqcup h_2 K \sqcup \ldots \sqcup h_n K. \tag{8}$$

Заменом (8) у (7), добијамо

$$G = g_1 h_1 K \cup g_1 h_2 K \cup \ldots \cup g_1 h_n K \cup \ldots \cup g_m h_1 K \cup g_m h_2 K \cup \ldots \cup g_m h_n K. \tag{9}$$

Ако покажемо да су скупови у наведеној унији различити (подсетимо се да су различити косети обавезно дисјунктни), доказ ће бити завршен. Но, заиста је тако. Наиме, претпоставимо да је

$$g_i h_j K = g_k h_l K, \tag{10}$$

за неке индексе i, j, k, l. Тада је и

$$g_i h_j KH = g_k h_l KH,$$

а како је $KH = H$ (зашто?), то мора бити

$$g_i h_j H = g_k h_l H,$$

па је

$$g_i H = g_k H.$$

Но, то је могуће једино ако је $i = k$. Множењем (10) слева са g_i^{-1} добијамо

$$h_j K = h_l K,$$

но то је могуће једино ако је $j = l$.

Пример 11 Свака група реда 15 је циклична.

На основу Кошијеве теореме постоји елемент x реда 3 и елемент y реда 5. Подгрупа $H = \langle y \rangle$ је стога индекса 3 и на основу претходног става она је нормална. Стога је

$$xyx^{-1} = y^r \tag{11}$$

за неко $r \in \{1, 2, 3, 4\}$. Уколико је $r = 1$, онда на стандардан начин добијамо да је $G \cong \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$. Покажимо да остале могућности за r нису могуће. Ако (11) помножимо слева са x и здесна са x^{-1}, добијамо

$$x^2 y x^{-2} = x y^r x^{-1} = (xyx^{-1})^r = (y^r)^r = y^{r^2}. \tag{12}$$

Множењем (12) слева са x и здесна са x^{-1} добијамо

$$x^3 y x^{-3} = y^{r^3}. \tag{13}$$

Но, с обзиром да је $x^3 = e$ из (13) добијамо

$$y = y^{r^3}, \tag{14}$$

тј.

$$y^{r^3 - 1} = e. \tag{15}$$

Дакле, с обзиром да је $\omega(y) = 5$, мора бити $5 \mid r^3 - 1$. Но, лако се може проверити да 5 не дели ниједан од бројева $2^3 - 1$, $3^3 - 1$, $4^3 - 1$. ♣

Друга и трећа теорема о изоморфизмима укључују у своју формулацију две подгрупе дате групе G.

Теорема 12 (Друга теорема о изоморфизмима) Нека је G група, $H \leq G$ и $K \triangleleft G$. Тада је $HK \leq G$, $H \cap K \triangleleft H$ и

$$HK/K \cong H/H \cap K.$$

Доказ. Пре свега, треба показати да је $HK \leq G$. Како $e \in H \cap K$, то је $e = ee \in HK$, па $HK \neq \emptyset$. Претпоставимо да су x и y елементи из HK. Дакле, постоје елементи $h, h' \in H$ и $k, k' \in K$ такви да је $x = hk$, $y = h'k'$. Тада је

$$x^{-1}y = k^{-1}h^{-1}h'k' = k^{-1}((h')^{-1}h)^{-1}k' =$$

$$= \overbrace{((h')^{-1}h)^{-1}}^{\in H} \underbrace{\overbrace{\left(\underbrace{((h')^{-1}h)}_{\in H}\underbrace{k^{-1}}_{\in K}((h')^{-1}h)^{-1}\right)}^{\in K} k'}_{\in K} \in HK.$$

С обзиром да је $K \triangleleft G$, то је и $K \triangleleft HK$. Дефинишимо функцију $f\colon H \to HK/K$ са: $f(h) = hK$. С обзиром да је

$$f(hh') = (hh')K = (hK)(h'K) = f(h)f(h'),$$

f је хомоморфизам.

Докажимо да је f „на“. Нека је xK произвољан елемент из HK/K. Дакле, за неко $h \in H$ и $k \in K$, $x = hk$. Тада је

$$xK = (hk)K = h(kK) = hK = f(h),$$

па је f заиста „на“.

Одредимо језгро хомоморфизма f. Узмимо произвољни елемент $h \in H$. Тада $h \in \mathrm{Ker}(f)$ ако и само ако је $f(h) = K$ (K је неутрал у HK/K). С обзиром да је $f(h) = hK$, добијамо да је $h \in \mathrm{Ker}(f)$ ако и само ако $h \in K$, тј. $\mathrm{Ker}(f) = H \cap K$. Прва теорема о изоморфизмима даје: $H/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$, тј. $H/H \cap K \cong HK/K$. Приметимо да $H \cap K \triangleleft H$ следи из чињенице да је $H \cap K$ језгро неког хомоморфизма. □

Пример 13 Нека су $m, n \geq 2$ природни бројеви. Применити другу теорему о изоморфизмима на групе $\mathbb{Z}$, $m\mathbb{Z}$ и $n\mathbb{Z}$.

Друга теорема о изоморфизмима даје

$$(m\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z} \cong m\mathbb{Z}/(m\mathbb{Z} \cap n\mathbb{Z}).$$

Нека је $d = \mathrm{NZD}(m, n)$, а $s = \mathrm{NZS}(m, n)$, тада је

$$m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}, \quad m\mathbb{Z} \cap n\mathbb{Z} = s\mathbb{Z}.$$

Дакле,

$$d\mathbb{Z}/n\mathbb{Z} \cong m\mathbb{Z}/s\mathbb{Z}.$$

Група $d\mathbb{Z}$ изоморфна је групи $\mathbb{Z}$ при изоморфизму $f\colon \mathbb{Z} \to d\mathbb{Z}$ датом са $f(x) = dx$. Нека је $n = dn'$. При изоморфизму f, подгрупа $n'\mathbb{Z}$ слика се на подгрупу $n\mathbb{Z}$. Другим речима, имамо изоморфизам

$$d\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n'\mathbb{Z}.$$

Знамо да је $sd = mn$, па је $n' = n/d = s/m$. Заправо је група $m\mathbb{Z}/s\mathbb{Z}$ изоморфна групи $\mathbb{Z}/n'\mathbb{Z}$. ♣

Пример 14 Нека је $H \leq G$, $K \triangleleft G$ и $\mathrm{NZD}(|H|, [G : K]) = 1$. Показати да је $H \subseteq K$.

Нека је $n = |HK/K|$. На основу друге теореме о изоморфизмима, важи изоморфизам $HK/K \cong H/(H \cap K)$. Добијамо да $n \mid |H|$. С друге стране, $HK/K \leq G/K$, те $n \mid |G/K|$. Како је $\mathrm{NZD}(|H|, [G : K]) = 1$, добијамо да је $n = 1$. То значи да је $HK = K$. Како је $H \subseteq HK$ (зашто?), следи да је $H \subseteq K$. ♣

Теорема 15 (Трећа теорема о изоморфизмима) Нека су H и K нормалне подгрупе групе G за које је $H \subseteq K$. Тада је $K/H \triangleleft G/H$ и

$$(G/H)/(K/H) \cong G/K.$$

Доказ. Дефинишимо функцију $f\colon G/H \to G/K$ са $f(gH) = gK$. Ова функција јесте добро дефинисана пошто из претпоставке да је $gH = g'H$ следи да је $g^{-1}g' \in H$, а како је $H \subseteq K$, то из $g^{-1}g' \in H$ следи да $g^{-1}g' \in K$, па је $gK = g'K$. Очигледно је да је f један епиморфизам. Одредимо језгро од f.

$$gH \in \mathrm{Ker}(f) \text{ акко } gK = K \text{ акко } g \in K.$$

Видимо да је $\mathrm{Ker}(f) = K/H$. Резултат се сада добија применом прве теореме о изоморфизмима. □

Пример 16 Нека су природни бројеви $m, n \geq 2$ такви да $m \mid n$. Применити трећу теорему о изоморфизмима на: $\mathbb{Z}$, $m\mathbb{Z}$ и $n\mathbb{Z}$.

Наравно, $n\mathbb{Z}$ је подгрупа од $\mathbb{Z}$ генерисана елементом n. Како $m \mid n$, то је $n\mathbb{Z} \subseteq m\mathbb{Z}$. Дакле, на основу треће теореме о изоморфизмима, добијамо

$$(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}.$$

Као и у раније наведеном примеру,

$$m\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z},$$

где је $d = n/m$. Ми знамо да је свака циклична група реда n изоморфна са $\mathbb{Z}_n$ и $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$. Осим тога, за сваки делилац реда цикличне групе, постоји тачно једна подгрупа те групе тог реда. Уколико је G циклична група реда n и $d \mid n$, онда постоји тачно једна подгрупа H групе G, која је реда d и тада је $G/H \cong \mathbb{Z}_m$, где је $m = n/d$. ♣