АЛГЕБРА 1

Групе

Нормалне подгрупе, количничке групе,

хомоморфизми и теореме о изоморфизмима

Зоран Петровић

Шесто предавање

У случају да је $H \leq G$ разматрали смо скуп G/H, скуп свих левих косета подгрупе H у групи G. Испоставља се да се у неким случајевима на овом скупу може задати структура групе.

Уведимо најпре следећу дефиницију.

Дефиниција 1 Нека је G група и $x, y \in G$. Елемент y је конјугован елементу x уколико постоји $g \in G$ за који је $y = gxg^{-1}$.

Није тешко уверити се да је на овај начин дефинисана једна релација еквиваленције. Наиме, сваки елемент је конјугован сам себи: $x = exe^{-1}$. Ако је y конјугован елементу x, тј. ако је $y = gxg^{-1}$, онда је и $x = (g^{-1})y(g^{-1})^{-1}$, па је x конјугован елементу y. Проверу транзитивности остављамо читаоцима. Класе еквиваленције при овој релацији називају се и класе конјугације.

Дефиниција 2 Подгрупа H групе G је нормална уколико је H унија неких класа конјугације. Ако је H нормална подгрупа од G онда пишемо:

$$H \triangleleft G.$$

Став 3 Нека је $H \leq G$. Следећи услови су еквивалентни:

1. $H \triangleleft G$;
2. за све $g \in G$: $gHg^{-1} \subseteq H$;
3. за све $g \in G$: $gH = Hg$.

Доказ.

$1 \implies 2$. Нека су $g \in G$ и $h \in H$ произвољни. Елемент ghg^{-1} је конјугат елемента $h \in H$. Како је H нормална подгрупа, она је унија класа конјугације, па самим тим мора да садржи целу класу конјугације елемента h. Стога је и $ghg^{-1} \in H$.

$2 \implies 3$. Нека је $g \in G$ произвољан елемент. Докажимо да је $gH \subseteq Hg$. Посматрајмо елемент $h \in H$. На основу 2, $ghg^{-1} \in H$, па је $ghg^{-1} = h'$ за неко $h' \in H$. Но, тада је и $gh = h'g \in Hg$, па закључујемо да је $gH \subseteq Hg$. Обратно, уочимо елемент $hg \in Hg$. Елемент $g^{-1}h(g^{-1})^{-1}$ на основу 2 припада H, па је $g^{-1}h(g^{-1})^{-1} = h_1$ за неко $h_1 \in H$. Стога је $hg = gh_1 \in gH$, те је $Hg \subseteq gH$.

$3 \implies 1$. Претпоставимо да је C нека класа конјугације за коју је $C \cap H \neq \emptyset$. Треба доказати да је $C \subseteq H$. Узмимо елемент $h \in C \cap H$. Тада је сваки елемент из C облика ghg^{-1} за неки $g \in G$. Но, како је по 3, $gH = Hg$, то је $gh = h'g$ за неко $h' \in H$, па је $ghg^{-1} = h'gg^{-1} = h'$. Закључујемо да $ghg^{-1} \in H$. Дакле, заиста је $C \subseteq H$. □

Приметимо да, у случају да је $H \triangleleft G$, важи једнакост $gHg^{-1} = H$.

Став 4 Свака подгрупа индекса 2 је нормална.

Доказ. Нека је $H \leq G$ и $[G : H] = 2$. То значи да је за сваки елемент $a \notin H$ из G испуњено:

$$G = H \sqcup aH.$$

Но, такође је и

$$G = H \sqcup Ha.$$

Како је $aH \cap H = \emptyset$, мора бити $aH \subseteq Ha$. Но, из истих разлога је $Ha \subseteq aH$. Закључујемо да је $aH = Ha$ за све $a \in G \setminus H$. Ако пак $a \in H$, онда је $aH = H$ (H је подгрупа, па је производ ма која два елемента из H у H; осим тога, ако је $h \in H$ произвољан елемент, онда је $h = a(a^{-1}h) \in aH$), а такође је и $Ha = H$. Дакле, и у овом случају важи једнакост $aH = Ha$, па је $H \triangleleft G$. □

Дефиниција 5 Нека је G група. Дефинишемо центар групе G, у ознаци $Z(G)$ са:

$$Z(G) := \{g \in G : (\forall x \in G)(xg = gx)\}.$$

Став 6 $Z(G)$ је подгрупа групе G.

Доказ. Како је $ex = xe$ за све $x \in G$, то $e \in Z(G)$. Претпоставимо да g припада центру. То значи да је $gx = xg$ за све $x \in G$. Но, тада следи да је и $g^{-1}x = xg^{-1}$ за све $x \in G$, те $g^{-1} \in Z(G)$. Коначно, ако $g, h \in Z(G)$ и $x \in G$, онда је

$$(gh)x = g(hx) = g(xh) = (gx)h = (xg)h = x(gh),$$

те $gh \in Z(G)$. $\square$

Пример 7 Важи следеће:

1. за све $n \geq 2$: $A_n \triangleleft \mathbb{S}_n$;
2. за сваку групу G: $\{e\} \triangleleft G$;
3. за сваку групу G: $G \triangleleft G$;
4. за сваку групу G: $Z(G) \triangleleft G$;
5. за све $n \geq 3$: $\langle \rho \rangle \triangleleft \mathbb{D}_n$.

У случају да су X и Y подскупови од G, дефинишемо $X \cdot Y$ са:

$$X \cdot Y := \{x \cdot y : x \in X, y \in Y\}.$$

Став 8 Скуп свих левих косета нормалне подгрупе H групе G чини једну групу у односу на управо дефинисано множење подскупова од G.

Доказ. Нека су aH и bH произвољни косети. Докажимо да је, при услову да је $H \triangleleft G$,

$$(aH) \cdot (bH) = (ab)H.$$

Ово није тешко доказати. Наиме, приметимо да је $HH = H$. Јасно је да је $HH \subseteq H$ (производ два елемента из H такође је у H пошто је H подгрупа од G). Осим тога, како $e \in H$, добијамо $H = eH \subseteq HH$. Добијамо:

$$(aH) \cdot (bH) = a(Hb)H = a(bH)H = (ab)(HH) = (ab)H.$$

Овде смо користили чињеницу да је $H \triangleleft G$ и асоцијативност множења.

Сада није тешко показати да је $(G/H, \cdot)$ група. Наиме,

$$((aH) \cdot (bH)) \cdot (cH) = ((ab)H) \cdot (cH) =$$

$$= ((ab)c)H = (a(bc))H = (aH) \cdot ((bc)H) = (aH) \cdot ((bH) \cdot (cH)).$$

Јасно је да је $H = eH$ неутрал:

$$(aH) \cdot H = (aH) \cdot (eH) = (ae)H = aH,$$

као и

$$H \cdot (aH) = (eH) \cdot (aH) = (ea)H = aH.$$

Инверз елемента aH је $a^{-1}H$:

$$(aH) \cdot (a^{-1}H) = (aa^{-1})H = eH = H;$$

$$(a^{-1}H) \cdot (aH) = (a^{-1}a)H = eH = H.$$

□

Овако добијена група зове се количничка група групе G по нормалној подгрупи H. Убудуће, када говоримо о групи G/H подразумевамо да је H нормална подгрупа од G и да је множење косета дефинисано на наведени начин. Наравно, често нећемо писати неке непотребне заграде и знак множења.

Дефиниција 9 Група G је проста уколико су њене једине нормалне подгрупе G и $\{e\}$.

Уколико група G није комутативна, то не мора бити ни њена количничка група. Ипак има случајева у којима количничка група јесте комутативна, а сама група то није.

Дефиниција 10 Ако су $x, y \in G$, дефинишемо комутатор елемената x и y, у ознаци $[x, y]$ са:

$$[x, y] := x^{-1}y^{-1}xy.$$

Приметимо да је $xy = yx$ акко $[x, y] = e$. Подгрупу групе G генерисану комутаторима означавамо са $[G, G]$ и зовемо комутаторска подгрупа од G.

Став 11 а) Комутаторска подгрупа је нормална подгрупа.
б) Ако је $H \triangleleft G$, онда је G/H комутативна ако и само ако је $[G, G] \subseteq H$.

Доказ. а) Производ два комутатора не мора бити комутатор, али инверз ма ког комутатора јесте комутатор:

$$[x, y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}(y^{-1})^{-1}(x^{-1})^{-1} = y^{-1}x^{-1}yx = [y, x].$$

У сваком случају, ми посматрамо подгрупу генерисану комутаторима и треба да покажемо да је она нормална. Сваки елемент подгрупе генерисане неким скупом X је скуп свих могућих производа елемената из X и њихових инверза. Како је инверз комутатора и сам комутатор, то је сваки елемент из комутаторске групе производ комутатора. Стога, нека су $g, x_1, y_1, \ldots, x_n, y_n$ произвољни елементи групе G. Тада је

$$g[x_1, y_1][x_2, y_2] \cdots [x_n, y_n]g^{-1} = (g[x_1, y_1]g^{-1})(g[x_2, y_2]g^{-1}) \cdots (g[x_n, y_n]g^{-1})$$

Но,

$$g[x, y]g^{-1} = gx^{-1}y^{-1}xyg^{-1} = (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) =$$

$$= (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) = [gxg^{-1}, gyg^{-1}],$$

те добијамо

$$g[x_1, y_1] \cdots [x_n, y_n] g^{-1} = [gx_1 g^{-1}, gy_1 g^{-1}] \cdots [gx_n g^{-1}, gy_n g^{-1}] \in [G, G].$$

б) $\Rightarrow$: Претпоставимо да је група G/H комутативна. То значи да је за све $x, y \in G$ испуњено:

$$xH \cdot yH = yH \cdot xH.$$

Другим речима,

$$xyH = yxH,$$

па мора бити

$$(yx)^{-1}(yx) \in H,$$

те

$$[x, y] = x^{-1}y^{-1}xy \in H.$$

Дакле, комутатор ма која два елемента је у H, па закључујемо да је $[G, G] \subseteq H$.

$\Leftarrow$: Претпоставимо да је $[G, G] \subseteq H$. Треба показати да је група G/H комутативна. Нека су $x, y \in G$ произвољни елементи. По претпоставци $[x, y] \in H$, тј. $x^{-1}y^{-1}xy \in H$. То значи да је $(yx)^{-1}(xy) \in H$, па мора бити $(yx)H = (xy)H$, тј. $(yH) \cdot (xH) = (xH) \cdot (yH)$. Закључујемо да је G/H комутативна група. □

Група $G/[G, G]$ назива се Абелизација групе G и означава са G^{Ab} (комутативне групе се зову и Абелове групе). Понеки пут је погодно за испитивање да ли су две групе изоморфне прећи на њихове Абелизације, зато што важи следећи став.

Став 12 Ако је $G \cong H$ онда је и $G^{\mathrm{Ab}} \cong H^{\mathrm{Ab}}$.

Нека је $f\colon G \to H$ изоморфизам. Тада је $f([x, y]) = [f(x), f(y)]$, што се лако може установити. Одавде следи да

$$f\left[[G, G]\right] \subseteq [H, H]. \tag{1}$$

Дефинишимо функцију

$$\tilde{f}\colon G^{\mathrm{Ab}} \to H^{\mathrm{Ab}},$$

са:

$$\tilde{f}(x[G, G]) := f(x)[H, H].$$

Показаћемо да је $\tilde{f}$ добро дефинисана функција, која остварује изоморфизам између $G/[G, G]$ и $H/[H, H]$.

Добра дефинисаност: Нека је

$$x[G, G] = y[G, G].$$

Треба показати да је

$$f(x)[H,H] = f(y)[H,H].$$

Но, како је $x[G,G] = y[G,G]$, мора бити $x^{-1}y \in [G,G]$, па на основу (1) следи да $f(x)^{-1}f(y) = f(x^{-1}y) \in [H,H]$. Дакле, заиста је

$$f(x)[H,H] = f(y)[H,H].$$

$\tilde{f}$ је „на": Нека је $z[H,H]$ произвољан елемент из H^{Ab}. Како је f „на", то постоји $x \in G$ за који је $f(x) = z$. Но, тада је $\tilde{f}(x[G,G]) = f(x)[H,H] = z[H,H]$, па је $\tilde{f}$ заиста „на".

$\tilde{f}$ је „1–1": Ако је

$$\tilde{f}(x[G,G]) = \tilde{f}(y[G,G]),$$

то значи да је

$$f(x)[H,H] = f(y)[H,H],$$

па је

$$f(x^{-1}y) \in [H,H].$$

Другим речима, за неке $z_1, u_1, \ldots, z_n, u_n \in H$ је

$$f(x^{-1}y) = [z_1,u_1]\cdots[z_n,u_n].$$

Како је f „на", то постоје $x_1, y_1, \ldots, x_n, y_n \in G$ такви да је

$$f(x_1) = z_1, \ldots, f(x_n) = z_n, \quad f(y_1) = u_1, \ldots, f(y_n) = u_n.$$

То значи да је

$$f(x^{-1}y) = [f(x_1),f(y_1)]\cdots[f(x_n),f(y_n)] = f([x_1,y_1]\cdots[x_n,y_n]).$$

Како је f „1–1", мора бити

$$x^{-1}y = [x_1,y_1]\cdots[x_n,y_n].$$

Следи да $x^{-1}y \in [G,G]$, па је $x[G,G] = y[G,G]$ и закључујемо да је и функција $\tilde{f}$ „1–1".

$\tilde{f}$ се слаже са операцијама:

$$\tilde{f}((x[G,G])\cdot(y[G,G])) = \tilde{f}((xy)[G,G]) = f(xy)[H,H] = (f(x)f(y))[H,H] =$$

$$= (f(x)[H,H])(f(y)[H,H]) = \tilde{f}(x[G,G])\tilde{f}(x[G,G]).$$

Закључујемо да је $\tilde{f}$ заиста изоморфизам. □

Пример 13 За све $n \geq 2$: $\mathbb{S}_n^{\mathrm{Ab}} \cong \mathbb{Z}_2$.

Показаћемо да је $[\mathbb{S}_n, \mathbb{S}_n] = A_n$ за све $n \geq 2$. Јасно је да је $\pi^{-1}\sigma^{-1}\pi\sigma$ парна пермутација за сваке две пермутације π и σ (зашто?). Према томе, $[\mathbb{S}_n, \mathbb{S}_n] \subseteq A_n$.

Случај $n = 2$ је тривијалан. Претпоставимо стога да је $n \geq 3$. Докажимо да сваки цикл дужине 3 припада $[\mathbb{S}_n, \mathbb{S}_n]$. Како ти цикли генеришу A_n, добићемо да је $[\mathbb{S}_n, \mathbb{S}_n] = A_n$. Но,

$$(abc) = (ab)(bc) = (ab)(ac)(ab)(ac) = (ab)^{-1}(ac)^{-1}(ab)(ac) = [(ab), (ac)].$$

Како је $[\mathbb{S}_n : A_n] = 2$, то је група $\mathbb{S}_n/A_n$ реда 2 и као таква је изоморфна групи $\mathbb{Z}_2$. ♣

Пример 14 За све $l \geq 2$:

1. $(\mathbb{D}_{2s})^{\mathrm{Ab}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$;
2. $(\mathbb{D}_{2s-1})^{\mathrm{Ab}} \cong \mathbb{Z}_2$.

Показаћемо најпре да је $[\mathbb{D}_n, \mathbb{D}_n] = \langle \rho^2 \rangle$. Проверимо све случајеве:

1. $[\rho^k, \rho^l] = \varepsilon$;
2. $[\sigma\rho^k, \rho^l] = (\sigma\rho^k)^{-1}(\rho^l)^{-1}(\sigma\rho^k)\rho^l = \sigma\rho^k\rho^{-l}\sigma\rho^k\rho^l = \rho^{-k}\rho^l\rho^{k+l} = \rho^{2l}$;
3. $[\rho^k, \sigma\rho^l] = (\rho^k)^{-1}(\sigma\rho^l)^{-1}\rho^k(\sigma\rho^l) = \rho^{-k}\sigma\rho^l\rho^k\sigma\rho^l = \rho^{-k}\rho^{-l}\rho^{-k}\rho^l = \rho^{-2k}$;
4. $[\sigma\rho^k, \sigma\rho^l] = (\sigma\rho^k)^{-1}(\sigma\rho^l)^{-1}\sigma\rho^k\sigma\rho^l = \sigma\rho^k\sigma\rho^l\sigma\rho^k\sigma\rho^l = \rho^{-k}\rho^l\rho^{-k}\rho^l = \rho^{2l-2k}$.

Видимо да је заиста $[\mathbb{D}_n, \mathbb{D}_n] = \langle \rho^2 \rangle$. Сада се разликују случајеви када је n парно, односно непарно. Наиме, ако је $n = 2s - 1$, ред елемента ρ^2 је n (зашто?), па је $\langle \rho^2 \rangle = \langle \rho \rangle$. Стога је $[\mathbb{D}_{2s-1}, \mathbb{D}_{2s-1}] = \langle \rho \rangle$ и заиста је $(\mathbb{D}_{2s-1})^{\mathrm{Ab}} \cong \mathbb{Z}_2$.

У случају $n = 2s$, ред елемента ρ^2 је s и

$$(\mathbb{D}_{2s})^{\mathrm{Ab}} = \{\langle \rho^2 \rangle, \sigma\langle \rho^2 \rangle, \rho\langle \rho^2 \rangle, \sigma\rho\langle \rho^2 \rangle\}.$$

Ово је група са 4 елемента у којој је сваки елемент реда 2 (проверити ово!), па на основу ранијих резултата (а може и директно), добијамо да је $(\mathbb{D}_{2s})^{\mathrm{Ab}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. ♣

Докажимо на крају још један став, који нам даје карактеризацију група одређеног реда.

Став 15 Ако је p непаран прост број, онда је свака група реда $2p$ или циклична или је изоморфна групи $\mathbb{D}_p$.

Доказ. Нека је G група реда $2p$. На основу Кошијеве теореме, у групи G постоји елемент x реда p и елемент y реда 2. Како ред елемента дели ред групе, то $y \notin \langle x \rangle$. Стога је

$$G = \langle x \rangle \sqcup y\langle x \rangle = \{e, x, \ldots, x^{p-1}, y, yx, \ldots, yx^{p-1}\}.$$

Ред елемента yx може бити 2, p или $2p$ ($yx \neq e$). Уколико је $\omega(yx) = 2p$, група G је циклична.

Покажимо да $\omega(yx) \neq p$. Претпоставимо да је $\omega(yx) = p$. Тада добијамо (рачунамо у групи $G/\langle x\rangle$ — подгрупа $\langle x\rangle$ је нормална пошто је индекса 2):

$$\langle x\rangle = e\langle x\rangle = (yx)^p\langle x\rangle = (yx\langle x\rangle)^p = (y\langle x\rangle)^p = y^p\langle x\rangle.$$

Дакле, $y^p \in \langle x\rangle$. Како је p непаран број, а $\omega(y) = 2$, мора бити $y \in \langle x\rangle$, што није тачно. Добили смо контрадикцију, те можемо закључити да $\omega(yx) \neq p$. Остаје случај $\omega(yx) = 2$. Тада добијамо да је $(yx)^2 = e$, па је $yxyx = e$ из чега следи да је $yx = x^{-1}y$. С обзиром да је $x^p = e$ и $y^2 = e$, видимо да се изоморфизам између G и $\mathbb{D}_p$ може остварити придруживањем $y \mapsto \sigma$, $x \mapsto \rho$. □

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

Дефиниција 16 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 17 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 18 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 19 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 20 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 21 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* $p\colon G \to G/H$. 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 22 Нека је $f\colon G \to H$ хомоморфизам група. Тада f индукује изоморфизам $\tilde{f}\colon G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ 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 23 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 $f\colon \mathbb{Z} \to \mathbb{Z}_n$, који индукује изоморфизам $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Препоручујемо читаоцима да се сами увере у наведени резултат.

Пример 24 Ако са V означимо подгрупу групе S_4 дату са:

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

онда је $V \lhd S_4$ 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:

$$\pi(12)(34)\pi^{-1} = (12)(34), \tag{2}$$
$$\pi(13)(24)\pi^{-1} = (13)(24), \tag{3}$$
$$\pi(14)(23)\pi^{-1} = (14)(23). \tag{4}$$

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 (2), 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 (3). 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 (2) 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 (мада га ми нећемо давати).

Став 25 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 $H \triangleleft G$.

Напомена: 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.

Пример 26 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

$$xyx^{-1} = y^r \tag{5}$$

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 (5) помножимо слева са x и здесна са x^{-1}, добијамо

$$x^2yx^{-2} = xy^rx^{-1} = (xyx^{-1})^r = (y^r)^r = y^{r^2}. \tag{6}$$

Множењем (6) слева са x и здесна са x^{-1} добијамо

$$x^3yx^{-3} = y^{r^3}. \tag{7}$$

Но, с обзиром да је $x^3 = e$ из (7) добијамо

$$y = y^{r^3}, \tag{8}$$

тј.

$$y^{r^3-1} = e. \tag{9}$$

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 27 (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

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

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

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 28 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 $\mathbb{Z}/n'\mathbb{Z}$. ♣

Теорема 29 (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 $f: G/H \to G/K$ 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 30 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 $m = n/d$. ♣