АЛГЕБРА 1

Групе

Аутоморфизми група

Зоран Петровић

7. децембар 2011.

Нека је G група. Са $\mathrm{Aut}(G)$ означавамо скуп свих аутоморфизама групе G:

$$\mathrm{Aut}(G) := \{f : G \to G \mid f \text{ је аутоморфизам}\}.$$

Како је композиција два аутоморфизма такође аутоморфизам, а и инверз аутоморфизма је аутоморфизам то је $(\mathrm{Aut}(G), \circ)$ једна група (идентично пресликавање је наравно аутоморфизам), коју зовемо *група аутоморфизама групе* G.

Нека $g \in G$. Дефинишимо $u_g : G \to G$ са:

$$u_g(x) = gxg^{-1}.$$

Није тешко уверити се да је u_g аутоморфизам групе G. Наиме,

$$u_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = u_g(x)u_g(y).$$

Осим тога,

$$(u_g \circ u_h)(x) = u_g(u_h(x)) = u_g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = u_{gh}(x).$$

Дакле, $u_g \circ u_h = u_{gh}$. Како је, очигледно, $u_e = \mathrm{id}_G$, то добијамо да је, за свако $g \in G$: $u_g \circ u_{g^{-1}} = u_e = \mathrm{id}_G$. Закључујемо да је u_g бијекција и да је, заправо, $u_g^{-1} = u_{g^{-1}}$. На овај начин смо показали не само да је сваки u_g један аутоморфизам, него и да скуп свих аутоморфизама тог облика, чини једну подгрупу групе свих аутоморфизама. Аутоморфизме овог облика зваћемо *унутрашњи аутоморфизми* и користићемо ознаку

$$\mathrm{Inn}(G) := \{u_g \mid g \in G\},$$

за подгрупу свих унутрашњих аутоморфизама групе G.

Знамо да је $(\mathrm{Inn}(G), \circ) \leq (\mathrm{Aut}(G), \circ)$, но поставља се питање да ли је то и нормална подгрупа. Проверимо то. Нека је $\phi \in \mathrm{Aut}(G)$. Треба показати да је

$$\phi \circ \mathrm{Inn}(G) \circ \phi^{-1} \subseteq \mathrm{Inn}(G).$$

Нека $g \in G$. Тада за сваки $x \in G$:

$$\begin{aligned}(\phi \circ u_g \circ \phi^{-1})(x) &= \phi(u_g(\phi^{-1}(x))) \\ &= \phi(g\phi^{-1}(x)g^{-1}) \\ &= \phi(g)\phi(\phi^{-1}(x)\phi(g^{-1}) \\ &= \phi(g)x\phi(g)^{-1} \\ &= u_{\phi(g)}(x).\end{aligned}$$

Дакле, $\phi \circ u_g \circ \phi^{-1} = u_{\phi(g)} \in \mathrm{Inn}(G)$. Закључујемо да је $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$.

Количничку групу $\mathrm{Aut}(G)/\mathrm{Inn}(G)$, означавамо са $\mathrm{Out}(G)$ и зовемо *група спољашњих аутоморфизама групе* G (сваки косет у овој групи, различит од $\mathrm{Inn}(G)$, задат је неким аутоморфизмом који није унутрашњи, тј. који није задат неким конкретним елементом групе G као што је задат унутрашњи аутоморфизам).

Став 1 Придруживање

$$gZ(G) \mapsto u_g$$

представља изоморфизам група $G/Z(G)$ и $\mathrm{Inn}(G)$.

Доказ. Посматрамо функцију $\phi : G/Z(G) \to \mathrm{Inn})G)$ задату са:

$$\psi(gZ(G)) = u_g.$$

Треба доказати да је ψ изоморфизам.

Докажимо најпре да је ψ добро дефинисана. У ту сврху, нека је $gZ(G) = hZ(G)$. Треба показати да је $u_g = u_h$. Из $gZ(G) = hZ(G)$ следи да је $g^{-1}h \in Z(G)$, тј. да за сваки $x \in G$ важи

$$g^{-1}hx = xg^{-1}h.$$

Множењем ове једнакости слева са g, а здесна са h^{-1} добијамо да за сваки $x \in G$:

$$hxh^{-1} = gxg^{-1},$$

тј. да је за свако $x \in G$: $u_h(x) = u_g(x)$. Закључујемо да је заиста $u_g = u_h$.

На сличан начин се проверава да је ψ „1–1“. Нека је $\psi(gZ(G)) = \psi(hZ(G))$. То жачи да је $u_g = u_h$, те је за све $x \in G$: $u_g(x) = u_h(x)$. Дакле, за све $x \in G$ важи:

$$gxg^{-1} = hxh^{-1}.$$

Множењем ове једнакости слева са g^{-1}, а здесна са h добијамо да за свако $x \in G$ важи:

$$g^{-1}hx = xg^{-1}h,$$

што заправо значи да $g^{-1}h \in Z(G)$, те закључујемо да је $gZ(G) = hZ(G)$. Тако смо добили да је ψ „1–1“.

Функција ψ је очигледно „на“ (зашто?), те нам само преостаје да покажемо да се слаже са операцијама, тј. да је за све $g, h \in G$

$$\psi((gZ(G))(hZ(G))) = \psi(gZ(G)) \circ \psi(hZ(G)).$$

(Присетимо се да је операција у $\mathrm{Inn}(G)$ заправо композиција функција.) Но,

$$\begin{aligned} \psi((gZ(G))(hZ(G))) &= \psi((gh)Z(G)) \\ &= u_{gh} \\ &= u_g \circ u_h \\ &= \psi(gZ(G)) \circ \psi(hZ(G)). \end{aligned}$$

□

Поставља се питање да ли група унутрашњих аутоморфизама може бити циклична. Наравно, уколико је група G комутативна, сваки унутрашњи аутоморфизам је идентитет (зашто?), те је тада $\mathrm{Inn}(G) = \{\mathrm{id}_G\}$, но то је тривијална група. Следећи став нам даје одговор на то питање.

Став 2 Група $\mathrm{Inn}(G)$ никада није (нетривијална) циклична група.

Доказ. Претпоставимо да је $\mathrm{Inn}(G)$ циклична група. На основу претходног става добијамо да је и $G/Z(G)$ циклична, тј. да постоји $x \in G$ за који је $G/Z(G) = \langle xZ(G) \rangle$. Показаћемо да одатле следи да је G комутативна група. У ту сврху, нека су y, z произвољни елементи из G. Како ј $xZ(G)$ генератор групе $G/Z(G)$, то постоје $m, n \in \mathbb{Z}$ за које је

$$yZ(G) = (xZ(G))^m \quad \text{и} \quad zZ(G) = (xZ(G))^n.$$

Но, то заправо значи да постоје $c, d \in Z(G)$ такви да је

$$y = x^m c \quad \text{и} \quad z = x^n d.$$

(Зашто?) Но, тада добијамо да је

$$\begin{aligned} yz &= x^m c x^n d \\ &= x^m x^n c d \quad (c \in Z(G)) \\ &= x^n x^m c d \\ &= x^n d x^m c \quad (d \in Z(G)) \\ &= zy. \end{aligned}$$

Дакле, G је комутативна група, па је $G = Z(G)$, те је $G/Z(G)$ тривијална група, те је тривијална и група $\mathrm{Inn}(G)$. □

Одређивање групе аутоморфизама произвољне групе није лак задатак, стога ћемо се ми овде ограничити само на неке једноставније случајеве и примере.

Позабавимо се најпре питањем одређивања групе аутоморфизама цикличне групе.

Свака бесконачна циклична група изоморфна је групи $\mathbb{Z}$. Није тешко уверити се да су једини аутоморфизми ове групе идентитет и $x \mapsto -x$ (проверите ово). Стога је $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

Нека је $n \geq 2$ и $f \in \mathrm{Aut}(\mathbb{Z}_n)$ (како је јасно да из $G \cong H$ следи да је $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$ (уверите се у то!), као и да је свака нетривијална коначна циклична група изоморфна тачно једној групи $\mathbb{Z}_n$, за $n \geq 2$, ми разматрамо тај случај). Елемент 1 је генератор групе $\mathbb{Z}_n$ и аутоморфизам f је потпуно одређен сликом елемента 1. Наиме, нека је $f(1) = r$. Уколико је $x \in \mathbb{Z}_n$, то је

$$x = \underbrace{1 +_n \cdots +_n 1}_{x},$$

те добијамо

$$f(x) = f(\underbrace{1 +_n \cdots +_n 1}_{x}) = \underbrace{f(1) +_n \cdots +_n f(1)}_{x} = \underbrace{r +_n \cdots +_n r}_{x}.$$

Но,

$$\underbrace{r +_n \cdots +_n r}_{x} = r \cdot_n x.$$

Наиме, и лева и десна страна ове једнакости су заправо остатак при дељењу rx са n. Према томе, добијамо да је за свако $x \in \mathbb{Z}_n$:

$$f(x) = r \cdot_n x.$$

Дакле, из чињенице да се f слаже са операцијама видели смо каквог је облика f. Поставља се питање: какво мора бити $r \in \mathbb{Z}_n$ да са $x \mapsto r \cdot_n x$ буде задат аутоморфизам групе $\mathbb{Z}_n$? Пре свега, с обзиром на својства операција $+_n$ и $\cdot_n$, овакво придруживање увек се слаже са операцијом. Како је група $\mathbb{Z}_n$ коначна, то је довољно проверити за које r је овакво придруживање „на“ (зашто?). Но, то није тешко. Довољно је испитати када је 1 слика неког елемента (пошто је 1 генератор групе $\mathbb{Z}_n$). То значи да треба установити за које $r \in \mathbb{Z}_n$ постоји $s \in \mathbb{Z}_n$ тако да је $r \cdot_n s = 1$. Но, добро нам је познато да то важи ако и само ако је r узајамно просто са n. Подсетимо се да смо са $\Phi(n)$ означили све елементе из скупа $\{1, \ldots, n-1\}$ који су узајамно прости са n. Дакле, придруживање $x \mapsto r \cdot_n x$ задаје аутоморфизам групе $\mathbb{Z}_n$ ако и само ако $r \in \Phi(n)$. Но, $(\Phi(n), \cdot_n)$ је група и на основу претходног разматрања, може се очекивати да постоји веза ове групе и групе $\mathrm{Aut}(\mathbb{Z}_n)$. Заправо важи следећи став.

Став 3 Функција $\Psi\colon \mathrm{Aut}(\mathbb{Z}_n) \to \Phi(n)$, задата са:

$$\Psi(f) = f(1)$$

је изоморфизам група $(\mathrm{Aut}(G), \circ)$ и $(\Phi(n), \cdot_n)$.

Доказ. На основу претходног разматрања, Ψ је бијекција (зашто?). Потребно је само проверити слагање са операцијама. Но, то није тешко:

$$\begin{aligned}\Psi(f \circ g) &= (f \circ g)(1) \\ &= f(g(1)) \\ &= f(1) \cdot_n g(1).\end{aligned}$$

(користили смо доказани резултат по коме је $f(x) = f(1) \cdot_n x$ за аутоморфизам f и елемент x). Овим је доказ завршен. □

Погледајмо сада неке примере.

Пример 4 Показати да је $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathbb{S}_3$.

$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$. Сви елементи ове групе (сем неутрала) су реда 2. Означимо са X скуп свих елемената реда 2 у овој групи. Посматрајмо функцију

$$\Psi\colon \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \to S_X,$$

дефинисану са:

$$\Psi(\phi) := \phi|_X.$$

Јасно је да је ово добро дефинисана функција пошто аутоморфизам не мења ред елемента, па је заиста $\phi[X] = X$ за сваки аутоморфизам ϕ (пажљив читалац ће приметити да ово није баш права рестрикција, пошто при рестрикцији "смањујемо" само домен, а не и кодомен, али јасно је шта желимо да урадимо). Сваки аутоморфизам је потпуно одређен вредностима у елементима реда 2, пошто се неутрал обавезно слика у неутрал. Стога је Ψ "1–1". Но, Ψ је и "на" пошто свака пермутација скупа X задаје један аутоморфизам (производ свака два различита елемента из X једнак је трећем елементу). Стога је Ψ и "на". С обзиром да је у обе групе операција $\circ$, то се Ψ слаже и са операцијом, те је заиста један изоморфизам. Како је X скуп од три елемента, то је тврђење доказано. ♣

Пример 5 Одредити групу $\mathrm{Aut}(\mathbb{S}_3)$.

$\mathbb{S}_3 = \{(1),(12),(13),(23),(123),(132)\}$. Нека је $X = \{(12),(13),(23)\}$. Као и у претходном примеру, пошто су у X сви елементи реда 2 у групи $\mathbb{S}_3$, то за сваки $\phi \in \mathrm{Aut}(\mathbb{S}_3)$ важи: $\phi[X] = X$. Осим тога, вредности које аутоморфизам "узима" на елементима скупа X јединствено одредјују тај аутоморфизам (елементи из X генеришу $\mathbb{S}_3$). И не само то – вредности на скупу X могу се узети произвољно и тако добити један аутоморфизам (размислите и проверите на примеру!). Дакле, као и у претходном примеру, "рестрикција" задаје изоморфизам група $\mathrm{Aut}(\mathbb{S}_3)$ и S_X, па је $\mathrm{Aut}(\mathbb{S}_3) \cong \mathbb{S}_3$. ♣

Напомена. Приметимо да групе $\mathbb{Z}_2 \times \mathbb{Z}_2$ и $\mathbb{S}_3$ нису изоморфне, али њихове групе аутоморфизама то јесу.

Нека су G и H произвољне групе. Ако је $\phi \in \mathrm{Aut}(G)$ и $\psi \in \mathrm{Aut}(H)$, онда је лако проверити да је функција $\phi \times \psi$, дефинисана са:

$$\phi \times \psi(g, h) = (\phi(g), \psi(h)),$$

за $g \in G$ и $h \in H$ аутоморфизам групе $G \times H$. Јасно је у опхтем случају не мора сваки аутоморфизам групе $G \times H$ да буде тог облика (једини аутоморфизам групе $\mathbb{Z}_2$ је идентитет, а видели смо да је $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathbb{S}_3$). Следећи став нам даје довољне услове да сваки аутоморфизам буде овог облика.

Став 6 Нека је $|G| = m$, $|H| = n$ и нека су m и n узајамно прости. Тада је $\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

Доказ. Главни део доказа састоји се у томе да се покаже да је при датим условима сваки аутоморфизам $\Theta \in \mathrm{Aut}(G \times H)$ облика $\phi \times \psi$, за неки ϕ из $\mathrm{Aut}(G)$ и неки ψ из $\mathrm{Aut}(H)$. Нека је e неутрал у G и ε неутрал у H. Тврдимо да важи следеће:

$$\Theta(g, \varepsilon) = (\phi(g), \varepsilon),$$

где је ϕ неки аутоморфизам групе G. Претпоставимо да је за неко $g \in G$ испуњено: $\Theta(g, \varepsilon) = (\phi(g), h_0)$, где је h_0 елемент из H различит од неутрала (јасно је да је прва компонента задата *неком* функцијом од g – касније ћемо показати да је задата аутоморфизмом). Како је $m = |G|$, то је $g^m = e$ и добијамо да је $(g, \varepsilon)^m = (e, \varepsilon)$. Стога је

$$(\phi(g), h_0)^m = \Theta(g, \varepsilon)^m = \Theta((g, \varepsilon)^m) = \Theta(e, \varepsilon) = (e, \varepsilon).$$

Дакле, $h_0^m = e$. Стога $\omega(h_0) \mid m$. Како $h_0 \in H$, а $|H| = n$, то важи и $\omega(h_0) \mid n$. По претпоставци је $h_0 \neq \varepsilon$, те је $\omega(h_0) \neq 1$. Добијамо да m и n имају заједнички делилац већи од 1, што противречи претпоставци да су узајамно прости. То показује да је заиста

$$\Theta(g, \varepsilon) = (\phi(g), h_0)$$

за све $g \in G$. Приметимо да ϕ мора бити "1–1", јер је Θ "1–1". Како је G коначна група, следи да је ϕ и "на". Но, ϕ се слаже и са операцијама:

$$(\phi(g_1 g_2), \varepsilon) = \Theta(g_1 g_2, \varepsilon\varepsilon) = \Theta(g_1, \varepsilon)\Theta(g_2, \varepsilon) = (\phi(g_1), \varepsilon)(\phi(g_2), \varepsilon) = (\phi(g_1)\phi(g_2), \varepsilon),$$

па је заиста $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$.

На потпуно исти начин се показује да је

$$\Theta(e, h) = (e, \psi(h)),$$

за неки $\psi \in \mathrm{Aut}(H)$. Коначно добијамо:

$$\Theta(g, h) = \Theta((g, \varepsilon)(e, h)) = \Theta(g, \varepsilon)\Theta(e, h) = (\phi(g), \varepsilon)(e, \psi(h)) = (\phi(g), \psi(h)).$$

Сада је лако проверити да је један изоморфизам

$$F\colon \mathrm{Aut}(G \times H) \to \mathrm{Aut}(G) \times \mathrm{Aut}(H)$$

задат са $F(\phi, \psi) = \phi \times \psi$. Остављамо читаоцима да ово провере. $\square$

Овај резултат, уз раније резултате о аутоморфизмима цикличних група има једну, помало неочекивану последицу.

Последица 7 Нека су m и n узајамно прости природни бројеви. Тада је $\varphi(mn) = \varphi(m)\varphi(n)$.

Доказ. Присетимо се да је $\varphi(n) = |\Phi(n)|$, где је $\Phi(n) = \{k : 1 \leq k < n,\ \mathrm{NZD}(k, n) = 1\}$. Како су m и n узајамно прости, имамо изоморфизам $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. Стога је

$$\Phi(mn) \cong \mathrm{Aut}(\mathbb{Z}_{mn}) \cong \mathrm{Aut}(\mathbb{Z}_m \times \mathbb{Z}_n) \cong \mathrm{Aut}(\mathbb{Z}_m) \times \mathrm{Aut}(\mathbb{Z}_n) \cong \Phi(m) \times \Phi(n).$$

Добијамо $\varphi(mn) = |\Phi(mn)| = |\Phi(m) \times \Phi(n)| = |\Phi(m)||\Phi(n)| = \varphi(m)\varphi(n)$ $\square$

Наравно, овде смо у доказу користили једноставну чињеницу да из $G \cong G_1$ и $H \cong H_1$ следи $G \times H \cong G_1 \times H_1$. Докажите је за вежбу.