АЛГЕБРА

Групе

Конјугација и нормалне подгрупе;

количничке групе

Зоран Петровић

14. март 2011.

Започнимо ову лекцију следећом дефиницијом.

Дефиниција 1 Елемент y је конјугован елементу x (елемент y је конјугат елемента x) у групи G уколико постоји $g \in G$ тако да је

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

Јасно је да је на овај начин дефинисана једна релација еквиваленције на скупу G. Наиме, сваки елемент x је конјугован сам себи пошто је $x = exe^{-1}$. Уколико је y конјугован елементу x, тј. постоји $g \in G$ тако да је $y = gxg^{-1}$, онда је и x конјугован y, јер је $x = g^{-1}y(g^{-1})^{-1}$. Ако је y конјугован елементу x ($y = gxg^{-1}$ за неко $g \in G$), а z конјугован елементу y ($z = hyh^{-1}$), онда је и z конјугован елементу x: $z = (hg)x(hg)^{-1}$.

Класу еквиваленције при овој релацији зовемо класа конјугације (или класа конјугованости).

Пример 2 Одредити класе конјугације у групи $\mathbb{D}_n$.

Разликоваћемо два случаја.

1. $\underline{n = 2l+1}$: Из

$$(\sigma\rho^s)\sigma(\sigma\rho^s)^{-1} = \sigma\rho^s\sigma\sigma\rho^s = \sigma\rho^{2s}$$

и

$$\rho^s\sigma\rho^{-s} = \sigma\rho^{-2s} = \sigma\rho^{2l+1-2s}$$

следи да је једна класа конјугације

$$\{\sigma, \sigma\rho, \sigma\rho^2, \dots, \sigma\rho^{2l}\}.$$

Из
$$(\sigma\rho^s)\rho^k(\sigma\rho^s)^{-1} = \sigma\rho^s\rho^k\sigma\rho^s = \sigma\sigma\rho^{-s}\rho^{-k}\rho^s = \rho^{-k} = \rho^{2l+1-k},$$
као и из чињенице да је $\rho^s\rho^k\rho^{-s} = \rho^k$, следи да су

$$\{\rho, \rho^{2l}\}, \quad \{\rho^2, \rho^{2l-1}\}, \quad \dots \quad, \{\rho^l, \rho^{l+1}\}$$

такође класе конјугације. Осим тога, $\{\varepsilon\}$ је једина преостала класа конјугације.

2. <u>$n = 2l$</u>: Како је

$$(\sigma\rho^s)\sigma(\sigma\rho^s)^{-1} = \sigma\rho^{2s} \quad \text{и} \quad (\sigma\rho^s)\sigma\rho(\sigma\rho^s)^{-1} = \sigma\rho^{2s-1},$$

а
$$\rho^s\sigma\rho^{-s} = \sigma\rho^{-2s} = \sigma\rho^{2l-2s} \quad \text{и} \quad \rho^s\sigma\rho\rho^{-s} = \sigma\rho^{1-2s} = \sigma\rho^{2l+1-2s}$$
то је класа конјугације елемента σ једнака $\{\sigma\rho^{2s} : 0 \leq s \leq l-1\}$, а класа конјугације елемента $\sigma\rho$ је $\{\sigma\rho^{2s+1} : 0 \leq s \leq l-1\}$. Осим тога, како је $\rho^s\rho^k\rho^{-s} = \rho^k$, а

$$(\sigma\rho^s)\rho^k(\sigma\rho^s)^{-1} = \sigma\rho^s\rho^k\sigma\rho^s = \rho^{-k} = \rho^{2l-k},$$

то су двочлане класе конјугације:

$$\{\rho, \rho^{2l-1}\}, \{\rho^2, \rho^{2l-2}\}, \quad \dots \quad, \{\rho^{l-1}, \rho^{l+1}\},$$

док се једине преостале класе конјугације једночлане:

$$\{\varepsilon\}, \quad \{\rho^l\}.$$

Приметимо на крају да у случају да је n непарно у $\mathbb{D}_n$ постоји само једна једночлана класа конјугације, док их у случају да је n парно има две. ♣

Пример 3 Испитајмо како изгледају класе конјугације у групи S_n и одредимо их за групе S_4 и A_4.

Приметимо најпре да су ма која два цикла исте дужине конјугована. Наиме, ако су $(a_1a_2\dots a_k)$ и $(b_1b_2\dots b_k)$ цикли дужине k из S_n и ако је π нека пермутација из S_n за коју је $\pi(a_i) = b_i$ за све $i = \overline{1,k}$, тада је

$$\pi(a_1a_2\dots a_k)\pi^{-1} = (\pi(a_1)\pi(a_2)\dots\pi(a_k)) = (b_1b_2\dots b_k).$$

Општије, важи следеће. Две пермутације σ и ρ из S_n су конјуговане ако и само ако имају исту циклусну структуру, тј. ако у растављању на производ дисјунктних циклуса у пермутацији σ има исти број циклуса дужине $1, 2, 3, \dots$ као и у пермутацији ρ. Ово није тешко доказати, али због уштеде времена, доказ нећемо исписивати. Но, резултат би требало да буде очигледан из претходно наведене једнакости.

Позабавимо се сада класама конјугације у групама S_4 и A_4.

У случају групе S_4, можемо користити наведени резултат. Добијамо да су класе конјугације следеће:

$$\{(1234),(1324),(2134),(2314),(3124),(3214)\};$$
$$\{(123),(132),(124),(142),(134),(143),(234),(243)\};$$
$$\{(12),(13),(14),(23),(24),(34)\};$$
$$\{(12)(34),(13)(24),(14)(23)\};$$
$$\{(1)\}.$$

Видимо да постоји само једна једночлана класа конјугације.

У случају групе A_4 морамо пажљивије радити. Нпр. у A_4 циклуси (123) и (132) нису конјуговани. Наиме, ако је π пермутација за коју је

$$\pi(123)\pi^{-1} = (132),$$

она *није* парна пермутација. Наиме, $\pi(4) = 4$, а осим тога мора бити $(\pi(1)\pi(2)\pi(3)) = (132)$, што оставља следеће могућности за π: $\pi = (23)$, или $\pi = (12)$, или $\pi = (23)$. Ниједна од ових пермутација није парна. Дакле, елементи (123) и (132) нису у истој класи конјугације у A_4. Но, ипак није тешко уверити се да су класе конјугације дате са:

$$\{(123),(124),(134),(234)\};$$
$$\{(132),(142),(143),(243)\};$$
$$\{(12)(34),(13)(24),(14)(23)\};$$
$$\{(1)\}.$$

Видимо да и у овом случају постоји само једна једночлана класа конјугације. □

Уведимо сада један важан појам.

Дефиниција 4 Нека је G група. Центар групе G, у ознаци $Z(G)$ дефинише се као скуп свих елемената из G, који комутирају са свим елементима те групе:

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

Није тешко проверити да је $Z(G)$ једна подгрупа групе G. Наиме, како је $eg = ge$ за све $g \in G$, то $e \in Z(G)$. Ако $x, y \in Z(G)$, онда

$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy),$$

па $xy \in Z(G)$. Осим тога, ако је $x \in Z(G)$, тј. за све $g \in G$ важи $xg = gx$, онда, множећи ову једнакост здесна и слева са x^{-1}, добијамо $gx^{-1} = x^{-1}g$. Закључујемо да и x^{-1} припада центру.

Веза између центра и конјугације дата је следећим ставом чији доказ следи непосредно из дефиниције центра.

Став 5 Центар групе G је унија свих једночланих класа конјугације.

Пример 6 Центар групе $\mathbb{D}_n$ је тривијалан уколико је n непаран број, а једнак је $\{\varepsilon, \rho^{n/2}\}$ уколико је n паран број.

Претпоставимо да је елемент $\sigma\rho^k$ у центру групе $\mathbb{D}_n$. То значи да је

$$(\sigma\rho^k)\rho = \rho(\sigma\rho^k),$$

тј.

$$\sigma\rho^{k+1} = \sigma\rho^{k-1}.$$

Одавде следи да је $\rho^2 = \varepsilon$, што није могуће. Дакле, можемо да закључимо да ниједан елемент облика $\sigma\rho^k$ не може бити у $Z(\mathbb{D}_n)$.

Посматрајмо елементе облика ρ^k за $1 \leq k < n$. Уколико је неки такав елемент у центру, мора бити

$$\rho^k(\sigma\rho) = (\sigma\rho)\rho^k,$$

па је

$$\sigma\rho^{-k}\rho = \sigma\rho^{k+1}.$$

Добијамо да мора бити $\rho^{2k} = \varepsilon$. Како је $n = \omega(\rho)$, добијамо да $n \mid 2k$. Уколико је n непаран, добили бисмо да $n \mid k$, што није могуће ($1 \leq k < n$). Дакле, центар групе $\mathbb{D}_n$ је тривијалан уколико је n непаран број. Уколико је пак n паран, онда $(n/2) \mid k$. Но, с обзиром да је $k < n$, закључујемо да мора бити $k = n/2$. Није тешко проверити (учините то!) да је у овом случају елемент $\rho^{n/2}$ заиста у центру. Дакле, за парне n је $Z(\mathbb{D}_n) = \{\varepsilon, \rho^{n/2}\}$. ♣

Напомена: Центар групе $\mathbb{D}_n$ могли смо да одредимо и из чињенице да знамо класе конјугације (центар је унија једночланих класа конјугације), али је добро то урадити и директно.

Дефиниција 7 Централизатор елемента $g \in G$, у ознаци, $Z(g)$ је скуп свих елемената групе G који комутирају са g:

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

Став 8 Важи следеће: а) $Z(g) \leq G$;

б) број елемената у класи конјугације елемента $g \in G$ једнак је индексу његовог централизатора.

Доказ. Провера чињенице да је $Z(g)$ подгрупа групе G изводи се на потпуно аналоган начин провери да је $Z(G)$ подгрупа.

Означимо са $C(g)$ класу конјугације елемента g. Другим речима,

$$C(g) = \{gxg^{-1} : g \in G\}.$$

Дефинишемо функцију $f: G/Z(g) \to C(g)$, са

$$f(xZ(g)) = xgx^{-1}.$$

Докажимо да је f добро дефинисана. Дакле, нека је $xZ(g) = yZ(g)$. Треба показати да је $xgx^{-1} = ygy^{-1}$. Но, како је $xZ(g) = yZ(g)$, то је $y^{-1}x \in Z(g)$, па је

$$(y^{-1}x)g = g(y^{-1}x).$$

Множењем ове једнакости слева са y, а здесна са x^{-1} и коришћењем асоцијативности множења добијамо тражени резултат (проверите!).

Јасно је да је f „на“. Докажимо да је f „1–1“. Нека је $f(xZ(g)) = f(yZ(g))$, тј. $xgx^{-1} = ygy^{-1}$. Одавде следи да је $(x^{-1}y)g = g(x^{-1}y)$, тј. $x^{-1}y \in Z(g)$, па је $xZ(g) = yZ(g)$. $\square$

Последица 9 Свака коначна група реда p^n, где је p прост број, а $n \geq 2$, има нетривијалан центар.

Доказ. Као и у случају сваке релације еквиваленције, група G је дисјунктна унија различитих класа конјугације. Осим тога, центар групе G је унија свих једночланих класа конјугације. Добијамо да је

$$G = Z(G) \sqcup C_1 \sqcup \ldots \sqcup C_k, \tag{1}$$

при чему класе C_i нису једночлане. Другим речима,

$$|G| = |Z(G)| + |C_1| + \cdots + |C_k|,$$

при чему је $|C_i| > 1$. Како је $|C_i|$ једнако индексу централизатора (било ког) елемента из C_i и како је $|C_i| \neq 1$, мора бити $p \mid |C_i|$. Из (1) следи да $p \mid |Z(G)|$, па центар заиста није тривијалан. $\square$

Последица 10 Ако је p прост број, онда је свака група реда p^2 или циклична или изоморфна групи $\mathbb{Z}_p \times \mathbb{Z}_p$.

Доказ. Уколико у G постоји елемент реда p^2, група G је циклична. Претпоставимо да у G нема елемената реда p^2. Како према претходном $Z(G)$ није тривијална група, закључујемо да постоји елемент $x \in Z(G)$, који је нужно реда p. Нека је $H = \langle x \rangle$. Уколико је y ма који елемент из $G \setminus \langle x \rangle$, онда је y такође реда p и нека је $K = \langle y \rangle$. Како је $H \subseteq Z(G)$, сваки елемент из H комутира са сваким из K. Осим тога, ако је $H \cap K \neq \{e\}$, онда је $|H \cap K| = p$, па је $H = H \cap K = K$, што противречи претпоставци. Дакле, $H \cap K = \{e\}$. Уколико још докажемо да је $H \cdot K = G$, према ставу о разлагању на производ, добијамо да је $G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Јасно је да је

$$H \cdot K = \{x^r y^s : 0 \leq r < p, 0 \leq s < p\}.$$

Показаћемо да међу овим елементима нема једнаких. Како их има $p^2 = |G|$, одатле добијамо да је $G = H \cdot K$. Претпоставимо да је

$$x^r y^s = x^t y^u.$$

Добијамо да је
$$x^{r-t} = y^{u-s}.$$

Тај елемент је и у H и у K. Како је пресек ових подгрупа тривијалан, закључујемо да је $x^{r-t} = e = y^{u-s}$. Но, како су и r и t ненегативни и мањи од $p = \omega(x)$, закључујемо да је $r - t = 0$, тј. $r = t$. На исти начин добијамо да је $s = v$ те међу наведеним елементима заиста нема једнаких. Дакле, заиста је $G = H \cdot K$, те је доказ завршен. $\square$

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

$$H \lhd G.$$

Став 12 Нека је $H \leq G$. Следећи услови су еквивалентни:

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

Доказ.

$1 \Rightarrow 2$: 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 $ghg^{-1} \in H$.

$2 \Rightarrow 3$: 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 $Hg \subseteq gH$.

$3 \Rightarrow 1$: 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 $C \subseteq H$. $\square$

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

Став 13 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 $H \triangleleft G$. □

Пример 14 Важи следеће:

1. за све $n \geq 2$: $A_n \triangleleft S_n$;
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 15 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 $a^{-1}H$:

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

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

$\square$

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 16 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 17 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 18 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

$$g[x_1, y_1] \cdots [x_n, y_n]g^{-1} = [gx_1g^{-1}, gy_1g^{-1}] \cdots [gx_ng^{-1}, gy_ng^{-1}] \in [G, G].$$

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. $\square$

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 19 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

$$f\,[[G, G]] \subseteq [H, H]. \tag{2}$$

Дефинишимо функцију

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

са:

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

Показаћемо даје $\tilde{f}$ 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 (2) 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. $\square$

Пример 20 За све $n \geq 2$: $S_n^{\mathrm{Ab}} \cong \mathbb{Z}_2$.

Показаћемо да је $[S_n, S_n] = A_n$ 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, $[S_n, S_n] \subseteq A_n$.

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

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

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

Пример 21 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 22 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 $y \mapsto \sigma$, $x \mapsto \rho$. $\square$