АЛГЕБРА 2: ГРУПЕ

ЗОРАН ПЕТРОВИЋ

Теореме о изоморфизму и њихове примене

Подсетимо се, на почетку, прве теореме о изоморфизму за групе, која је проучавана у Алгебри 1. Погледајте одговарајуће поглавље у уџбенику *Алгебра за информатичаре*.

Теорема 1. *Нека је $f\colon G \to H$ хомоморфизам група. Тај хомоморфизам производи изоморфизам $\tilde{f}\colon G/\mathrm{Ker}\, f \to \mathrm{Im}\, f$, који је задат са: $\tilde{f}(x\mathrm{Ker}\, f) = f(x)$.*

Доказаћемо сада једну теорему која је последица прве теореме о изоморфизму, а која сама има занимљиве последице.

Теорема 2. ($n!$-теорема) *Ако група G има подгрупу H индекса n, онда она има и нормалну подгрупу $N \subseteq H$ тако да $|G : N| \mid n!$.*

✍ Чињеница да је $|G : H| = n$ каже да је број левих косета подгрупе H у G једнак n, тј. да скуп $\mathscr{L}_H = \{xH : x \in G\}$ има n елемената. Подсетимо се да је са $\mathbb{S}_X$ означена група пермутација скупа X, тј. бијекција скупа X у самог себе. Дефинишемо хомоморфизам $f\colon G \to \mathbb{S}_{\mathscr{L}_H}$ са: $f(g)(xH) = gxH$.

Треба најпре проверити да ли је заиста $f(g)$ бијекција за свако $g \in G$, а потом и да је f хомоморфизам, тј. да је $f(g_1g_2) = f(g_1) \circ f(g_2)$ (подсетимо се да је операција у $\mathbb{S}_{\mathscr{L}_H}$ композиција пресликавања) за све $g_1, g_2 \in G$. Проверимо најпре ово друго. Нека su $g_1, g_2, x \in G$ ма који елементи.. Тада:

$$f(g_1g_2)(xH) = g_1g_2xH = f(g_1)(g_2xH) = f(g_1)(f(g_2)(xH)) = (f(g_1) \circ f(g_2))(xH).$$

Како ово важи за све $x \in G$ имамо да је $f(g_1g_2) = f(g_1) \circ f(g_2)$ за све $g_1, g_2 \in G$.

Из управо доказаног имамо да је $f(g^{-1}) \circ f(g) = f(g^{-1}g) = f(e) = f(g) \circ f(g^{-1})$, а $f(e)(xH) = exH = xH$, па је $f(e) = \mathrm{id}_{\mathscr{L}_H}$ и добијамо да је $f(g)$ бијекција чији је инверз $f(g^{-1})$.

Дакле, f је заиста хомоморфизам група и прва теорема о изоморфизму нам даје изоморфизам $G/\mathrm{Ker}\, f \cong \mathrm{Im}\, f$. Но, $\mathrm{Im}\, f \leqslant \mathbb{S}_{\mathscr{L}_H}$, а $\mathbb{S}_{\mathscr{L}_H} \cong \mathbb{S}_n$, јер је $|\mathscr{L}_{\mathscr{H}}| = |G : H| = n$ (видети став 1.26 у уџбенику), па $|\mathrm{Im}\, f| \mid n!$. Ако са N означимо језгро хомоморфизма f, добијамо да је $|G : N| = |\mathrm{Im}\, f|$, те заиста $|G : N| \mid n!$.

Остало је да се покаже да је $N \subseteq H$. Но, ако $g \in N = \mathrm{Ker}\, f$, онда је $f(g) = \mathrm{id}_{\mathscr{L}_H}$; посебно $f(g)(H) = H$, тј. $gH = H$, из чега следи $g \in H$. 🟥

Подсетимо се да је проста група она група која нема праве нормалне подгрупе (дакле њене једине нормалне подгрупе су она сама и подгрупа састављена само од неутрала).

Date: Јесен 2026.

Последица 3. *Нека је G проста група која има подгрупу индекса n. Тада је она коначна и $|G| \mid n!$.*

✍ Ако је H подгрупа индекса n, онда, на основу претходне теореме постоји нормална подгрупа $N \subseteq H$ тако да $|G : N| \mid n!$. Но, како је H права подгрупа, а $N \subseteq H$, то је и N права подгрупа, а пошто је она нормална и G проста, мора бити $N = \{e\}$. Стога је $|G| = |G : N| \mid n!$, чиме је доказ завршен. 📕

Последица 4. *Нека је G коначна група и p најмањи прост број који дели ред групе G. Ако G има подгрупу индекса p, она је нормална.*

✍ Нека је H подгрупа индекса p. На основу теореме **2**, G има нормалну подгрупу $N \subseteq H$ такву да $|G : N| \mid p!$. То значи да у факторизацији броја $|G : N|$ могу да учествују само прости бројеви мањи од p, као и сам p (а у случају броја p он се може појавити само са експонентом 1). Но, $|G : N| \mid |G|$, па из претпоставке закључујемо да је $|G : N| \in \{1, p\}$. Но, не може бити $|G : N| = 1$, јер би то значило да је $G = N$, а $N \subseteq H \subset G$. Дакле, $|G : N| = p = |G : H|$. Лагранжова теорема даје $|N| \cdot p = |N| \cdot |G : N| = |G| = |H| \cdot |G : H| = |H| \cdot p$, те закључујемо да је $|N| = |H|$, а како су ово коначне групе и $N \subseteq H$, добијамо да је $H = N$, те је $H \triangleleft G$. 📕

Пример 5. Свака група реда 15 је циклична.

👉 Нека је G група реда 15. На основу Кошијеве теореме постоји елемент x ред 3 и елемент y реда 5. Како је $5 = \omega(y) = |\langle y \rangle|$, добијамо да је $\langle y \rangle$ подгрупа индекса 3, па је, на основу претходне последица, она нормална. То, посебно, значи да је $xyx^{-1} \in \langle y \rangle$, те је $xyx^{-1} = y^r$, за неко $r \in \{0, 1, 2, 3, 4\}$. У случају да је $r = 0$, добили бисмо да је $xyx^{-1} = e$, тј. $y = e$ што није тачно.

У случају да је $r = 1$, имамо да је $xyx^{-1} = y$, те је $xy = yx$. Како су редови подгрупа $\langle x \rangle$ и $\langle y \rangle$ узајамно прости добијамо да је $\langle x \rangle \cap \langle y \rangle = \{e\}$. На основу става 1.32 из уџбеника добијамо да је $\omega(xy) = \text{NZS}(\omega(x), \omega(y)) = 15 = |G|$, те закључујемо да је група G циклична.

Остаје да се провери шта се дешава ако је $r \in \{2, 3, 4\}$. Множењем релације $xyx^{-1} = y^r$ слева и здесна елементом x, добијамо:

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

Ако то поновимо још једном добијамо да је $x^3yx^{-3} = y^{r^3}$. Но, $x^3 = e$, па је $y = y^{r^3}$. Дакле, $y^{r^3-1} = e$, па $5 \mid (r^3 - 1)$ (лема 1.11 из уџбеника). Но, имамо да је $\{r^3 - 1 : r \in \{2, 3, 4\}\} = \{7, 26, 63\}$ и како 5 не дели ниједан од тих бројева закључујумо да $r \notin \{2, 3, 4\}$ те нам остаје само да је $r = 1$ и видели смо да је група циклична. 👍

Пример 6. Нека је p непаран прост број и G група реда $2p$. Тада је $G \cong \mathbb{C}_{2p}$ или је $G \cong \mathbb{D}_p$.

👉 На основу Кошијеве теореме у G постоји елемент x реда p и елемент y реда 2. Свакако $y \notin \langle x \rangle$, јер $2 \nmid p$. Стога је $G = \langle x \rangle \sqcup y\langle x \rangle = \{e, x, \ldots, x^{p-1}, y, yx, \ldots yx^{p-1}\}$. Подгрупа генерисана са x је индекса 2, те је стога нормална (став 1.68 из уџбеника или последица **4**). Нека је $\overline{G} = G/\langle x \rangle$ и $\bar{y} = y\langle x \rangle \in \overline{G}$ је генератор цикличне групе $\overline{G}$ реда 2.

Посматрамо елемент yx: $\omega(yx) \mid 2p$, закључујемо да је $\omega(yx) \in \{2, p, 2p\}$ (знамо да $yx \neq e$).

$\omega(yx) = 2p$. Имамо да је група G циклична са генератором yx.

$\omega(yx) = 2$. Дакле, $(yx)^2 = e$, па је $yxyx = e$, из чега следи да је $yx = x^{-1}y^{-1} = x^{p-1}y$ ($x^p = y^2 = e$). Добијамо да је група G изоморфна групи $\mathbb{D}_p$ (y одговара рефлексији σ, а x ротацији ρ).

$\omega(yx) = p$. Но, то нам даје $\omega(\overline{yx}) \mid \omega(yx)$, тј. $\omega(\overline{yx}) \in \{1, p\}$. Како је $\overline{yx} = \bar{y}$ елемент реда 2, видимо да до овог случаја и не долази. 👍

Доказаћемо сада две корисне леме за даљи рад.

Лема 7. *Нека је H непразан подскуп групе G. Тада је H подгрупа у односу на сужење операције у групи G акко важе једнакости: $HH = H$ и $H^{-1} = H$.*

✍ Наравно, $HH = \{xy : x, y \in H\}$, док је $H^{-1} = \{x^{-1} : x \in H\}$.

$\Longrightarrow$. Претпоставимо да је $(H, \cdot) \leqslant (G, \cdot)$. Ако су $x, y \in H$, онда свакако $xy \in H$, а то управо значи да је $HH \subseteq H$. Но, $H = H\{e\} \subseteq H$, па важи једнакост $HH = H$.

Такође, ако је $x \in H$, из чињенице да је H подгрупа, следи да $x^{-1} \in H$, што показује да је $H^{-1} \subseteq H$. Но, одавде следи да је $H = (H^{-1})^{-1} \subseteq H^{-1}$, те је једнакост $H^{-1} = H$ испуњена.

$\Longleftarrow$. Нека $x, y \in H$. Тада $x^{-1}y \in H^{-1}H = HH = H$. 📕

Лема 8. *Нека су H и K подгрупе групе G. Тада је $HK \leqslant G$ акко је $HK = KH$.*

✍ Како $e = e \cdot e \in HK$, имамо да је $HK \neq \emptyset$.

$\Longrightarrow$. Како је $HK \leqslant G$, из претходне леме следи $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$.

$\Longleftarrow$. Имамо да је $(HK)(HK) = H(KH)K = H(HK)K = HHKK = HK$; $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$. 📕

Теорема 9. (Друга теорема о изоморфизму за групе) *Нека је G група, $H \leqslant G$, $K \triangleleft G$. Тада: $HK \leqslant G$, $H \cap K \triangleleft H$ и $HK/K \cong H/H \cap K$.*

✍ Како је K нормална подгрупа, то је $hK = Kh$ за све $h \in G$, те је

$$HK = \cup_{h \in H}\{h\}K = \cup_{h \in H}hK = \cup_{h \in H}Kh = \cup_{h \in H}K\{h\} = KH.$$

На основу претходне леме добијамо да је $HK \leqslant G$. Како је $K = \{e\}K \subseteq HK$, а K је нормална подгрупа у G, онда је она нормална и у HK.

Задајемо $f\colon H \to HK/K$ са: $f(h) = hK$. Лако се провери да је ово хомоморфизам. На основу прве теореме о изоморфизму за групе имамо да је $H/\mathrm{Ker}\, f \cong \mathrm{Im}\, f$. Но, како је, за произвољне $h \in H$, $k \in K$, $hkK = hK = f(h)$, имамо да је f „на”, тј. $\mathrm{Im}\, f = HK/K$. С друге стране,

$$\mathrm{Ker}\, f = \{h \in H : f(h) = K\} = \{h \in H : hK = K\} = \{h \in H : h \in K\} = H \cap K$$

и тражени резултат следи. 📕

Теорема 10. (Трећа теорема о изоморфизму за групе) *Нека су H и K нормалне подгрупе групе G, при чему је $H \subseteq K$. Тада је $K/H \triangleleft G/H$ и $(G/H)/(K/H) \cong G/K$.*

✍ Дефинишемо $f\colon G/H \to G/K$ са: $f(gH) = gK$. Како више елемената одређује леви косет, морамо проверити добру дефинисаност. У ту сврху, нека је $gH = g_1H$; тада је $g^{-1}g_1 \in H$, а како је $H \subseteq K$, имамо да је $g^{-1}g_1 \in K$, што нам даје: $gK = g_1K$. Стога је f добро дефинисано. Уверите се да је f хомоморфизам група. Јасно је да је f „на". Остаје да установимо шта је језгро овог хомоморфизма.

$$\begin{aligned}\operatorname{Ker} f &= \{gH : g \in G, f(gH) = K\} = \{gH : g \in G, gK = K\}\\ &= \{gH : g \in G, gK = K\} = \{gH : g \in G, g \in K\} = \{gH : g \in K\} = K/H.\end{aligned}$$

Прва теорема о изоморфизму нам даје тражени резултат.

Доказаћемо сада и Теорему о кореспонденцији, која ће нам бити корисна да боље предочимо неке резултате.

Теорема 11. *Нека је G група, $N \triangleleft G$; означимо са $\overline{G}$ количничку групу: $\overline{G} = G/N$.*

Подгрупе (нормалне подгрупе) групе $\overline{G}$ су у обострано једнозначној кореспонденцији са подгрупама (нормалним подгрупама) групе G, које садрже подгрупу N.

Прецизније: свака (нормална) подгрупа групе $\overline{G}$ је облика $\overline{K} = K/N = \{g + n : g \in K\}$, где је K (нормална) подгрупа групе G, таква да је $N \subseteq K$.

✍ Посматрамо канонски епиморфизам $p\colon G \to G/N$, задат са: $p(g) = g + N$. Ако је $\mathcal{K} \leqslant \overline{G}$ ($\mathcal{K} \triangleleft \overline{G}$), онда је $K = p^{-1}[\mathcal{K}] \leqslant G$ ($K = p^{-1}[\mathcal{K}] \triangleleft G$). Наравно, јасно је да је $N \subseteq K$, јер се сваки елемент из N при p слика у неутрал, који свакако припада подгрупи.

1. $e \in K = p^{-1}[\mathcal{K}]$, па је $K \neq \emptyset$.

2. $g_1, g_2 \in K \Rightarrow p(g_1^{-1}g_2) = p(g_1)^{-1}p(g_2) \in \mathcal{K}$, јер је $\mathcal{K} \leqslant \overline{G}$.

3. Уколико је $\mathcal{K} \triangleleft \overline{G}$, доказујемо да је $K \triangleleft G$: из $g \in G$ и $k \in K$, следи да $p(k) \in \mathcal{K}$, па $p(gkg^{-1}) = p(g)p(k)p(g)^{-1} \in \mathcal{K}$.

Како је $p[p^{-1}[\mathcal{K}]] = \mathcal{K}$, јер је p „на", имамо да је

$$\mathcal{K} = p[K] = \{g + N : g \in K\} = K/N = \overline{K}.$$

Извод групе и Абелизација

Дефинишемо најпре појам комутатора два елемента у групи и извода групе.

Дефиниција 12. *Нека је G група и $x, y \in G$. Комутатор елемената x и y, у ознаци $[x, y]$ дефинише се са: $[x, y] := x^{-1}y^{-1}xy$. Подгрупу G' генерисану свим комутаторима елемената из G називамо* извод *групе G.*

Дакле $G' = \langle [x, y] : x, y \in G\rangle$. Користи се и ознака $[G, G]$ за ову групу, као и назив комутаторска подгрупа. Докажимо најпре једну лему.

Лема 13. *1. Сваки елемент у G' је производ комутатора.*

2. Сваки конјугат комутатора је комутатор.

✍ 1. Како је подгрупа G' генерисана комутаторима, њу чине, осим неутрала, сви могући производи комутатора и њихових инверза. Но,

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

те је инверз комутатора такође комутатор. Стога ту подгрупу чине производи комутатора.

2. Одредимо произвољни конјугат комутатора.

$$\begin{aligned} g[x,y]g^{-1} = g(x^{-1}y^{-1}xy)g^{-1} &= (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) \\ &= (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) \\ &= [gxg^{-1}, gyg^{-1}]. \end{aligned}$$

Видимо да је конјугат и сам комутатор. 📕

Приметимо да је $[x,y] = e$ ако и само ако је $xy = yx$. То је суштина друге ставке следећег става.

Став 14. *1.* $G' \triangleleft G$.

2. Нека је H нормална подгрупа групе G. Тада је G/H комутативна ако и само ако је $G' \subseteq H$.

✍ 1. директно следи из претходне леме.

2. Нека су $x, y \in G$ произвољни елементи. Тада имамо

$$\begin{aligned} xH \cdot yH = yH \cdot xH \quad &\text{акко} \quad xyH = yxH \\ &\text{акко} \quad (yx)^{-1}xy \in H \\ &\text{акко} \quad x^{-1}y^{-1}xy \in H \\ &\text{акко} \quad [x,y] \in H. \end{aligned}$$

Према томе:

$$\begin{aligned} G/H \text{ је комутативна} \quad &\text{акко} \quad (\forall x \in G)(\forall y \in G)(xH \cdot yH = yH \cdot xH) \\ &\text{акко} \quad (\forall x \in G)(\forall y \in G)([x,y] \in H) \\ &\text{акко} \quad G' \subseteq H, \end{aligned}$$

што се и тражило. 📕

Овај став нам каже да је најефикаснији „прелазак” са дате групе на њој блиску Абелову групу тај да се група „посече” по свом изводу. Управо је то Абелизација групе.

Дефиниција 15. *Абелизација G^{Ab} групе G дефинише се са: $G^{\mathrm{Ab}} := G/G'$.*

Став 16. *Ако је $G \cong H$, онда је $G^{\mathrm{Ab}} \cong H^{\mathrm{Ab}}$.*

✍ Нека је $f\colon G \to H$ изоморфизам и $p\colon H \to H/H' (= H^{\mathrm{Ab}})$ канонски епиморфизам. Посматрамо композицију $p \circ f$. То је наравно епиморфизам, јер су оба хомоморфизма „на”. Одредимо његово језгро:

$x \in \mathrm{Ker}(p \circ f)$ акко $p(f(x)) = H'$

акко $f(x)H' = H'$

акко $f(x) \in H'$

акко $(\exists z_i, t_i \in H)\big(f(x) = [z_1, t_1] \cdots [z_k, t_k]\big)$

акко $(\exists x_i, y_i \in G)\big(f(x) = [f(x_1), f(y_1)] \cdots [f(x_k), f(y_k)]\big)$ (f је „на")

акко $(\exists x_i, y_i \in G)\big(f(x) = f([x_1, y_1]) \cdots f([x_k, y_k])\big)$ (f је хомоморфизам)

акко $(\exists x_i, y_i \in G)\big(f(x) = f([x_1, y_1] \cdots [x_k, y_k])\big)$ (f је хомоморфизам)

акко $(\exists x_i, y_i \in G)(x = [x_1, y_1] \cdots [x_k, y_k])$ (f је „1–1")

акко $x \in G'$.

Дакле, $\mathrm{Ker}(p \circ f) = G'$ и прва теорема о изоморфизму даје тражени изоморфизам $G/G' \cong H/H'$. 📕

Наведимо неке примере.

Пример 17. За све $n \geqslant 2$ је $\mathbb{S}_n^{\mathrm{Ab}} \cong \mathbb{Z}_2$.

👉 Случај $n = 2$ је тривијалан: $\mathbb{S}_2 = \{(1), (12)\}$ што је циклична група реда 2. Она је комутативна те је $\mathbb{S}_2'$ тривијална (сви су комутатори у комутативној групи једнаки неутралу), те је $\mathbb{S}_2^{\mathrm{Ab}} \cong \mathbb{S}_2 \cong \mathbb{Z}_2$.

Тврдимо да је $\mathbb{S}_n' = \mathbb{A}_n$ за све $n \geqslant 3$ (ово је заправо тривијално тачно и за $n = 2$, али рекосмо да је тај случај тривијалан). Јасно је да је сваки комутатор $[\sigma, \pi] = \sigma^{-1}\pi^{-1}\sigma\pi$ парна пермутација, те је $\mathbb{S}_n' \subseteq \mathbb{A}_n$. За доказ обратног укључења, довољно је показати да су сви 3-цикли у $\mathbb{S}_n'$ пошто они генеришу $\mathbb{A}_n$ (видети став 1.31 у уџбенику). Но, директна провера даје $[(ab), (ac)] = (abc)$, где је скуп $\{a, b, c\}$ трочлан скуп.

Дакле, $\mathbb{S}_n^{\mathrm{Ab}} = \mathbb{S}_n/\mathbb{S}_n' = \mathbb{S}_n/\mathbb{A}_n \cong \mathbb{Z}_2$. 👍

Пример 18. Абелизација диедарске групе дата је са:

1. $\mathbb{D}_{2s}^{\mathrm{Ab}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
2. $\mathbb{D}_{2s+1}^{\mathrm{Ab}} \cong \mathbb{Z}_2$.

👉 Као што знамо, $\mathbb{D}_n$ је генерисана са два генератора σ и ρ, који задовољавају услове $\sigma^2 = \rho^n = \varepsilon, \sigma\rho = \rho^{n-1}\sigma$, где је са ε означен неутрал ове групе. Преласком на Абелизацију и адитивну нотацију, добијамо два генератора $\bar{\sigma}$ и $\bar{\rho}$ који задовољавају услове: $2\bar{\sigma} = 0, n\bar{\rho} = 0, \bar{\sigma} + \bar{\rho} = (n-1)\bar{\rho} + \bar{\sigma}$. Последња релација се своди на $(n-2)\bar{\rho} = 0$ и онда из две релације које $\bar{\rho}$ задоваљава, закључујемо да је $2\bar{\rho} = 0$.

Сада имамо два случаја.

1. Ако је $n = 2s$, из $2\bar{\rho} = 0$ следи да је $n\bar{\rho} = 2s\bar{\rho} = 0$, те остајемо са два генератора $\bar{\sigma}$, $\overline{rho}$ и само две релације: $2\bar{\sigma} = 0, 2\overline{rho} = 0$. Закључујемо да је D_{2s}^{Ab} директна сума цикличних група реда 2 генерисаних са $\bar{\sigma}$, $\bar{\rho}$, те је $D_{2s}^{\mathrm{Ab}} \cong \mathbb{Z}_n \times \mathbb{Z}_2$.

2. Ако је $n = 2s + 1$, из $(2s+1)\bar{\rho} = 0$ и $2\bar{\rho} = 0$ добијамо да је $\bar{\rho} = 0$, те D_{2s+1} има само један генератор $\bar{\sigma}$, који је реда 2, те је $D_{2s+1}^{\mathrm{Ab}} \cong \mathbb{Z}_2$. 👍

Аутоморфизми група

У овом одељку ћемо се кратко позабавити аутоморфизмима група, пошто ће нам аутоморфизми бити потребни касније у неким конструкцијама. Ако је G група, са $\operatorname{Aut} G$ означавамо скуп свих аутоморфизама групе G, тј. скуп изоморфизама $G \to G$. Јасно је да је $\operatorname{Aut} G$ група у односу на композицију пресликавања, те говоримо о *групи аутоморфизама*.

Посебно је значајан један тип аутоморфизама, који се називају *унутрашњим аутоморфизмима*. Наиме, ако је G група и $a \in G$, са $u_a(x) = axa^{-1}$ је задат један аутоморфизам $u_a \colon G \to G$. Проверите да је то тако. Са $\operatorname{Inn} G$ означавамо скуп свих унутрашњих аутоморфизама групе G: $\operatorname{Inn} G := \{u_a : a \in G\}$.

Став 19. 1. $\operatorname{Inn} G \triangleleft \operatorname{Aut} G$.

2. $\operatorname{Inn} G \cong G/Z(G)$.

✍ 1. Наравно, $\mathrm{id}_G = u_e \in \operatorname{Inn} G$, па је $\operatorname{Inn} G \neq \emptyset$. Нека су $a, b \in G$. Тада је $(u_a \circ u_b)(x) = u_a(u_b(x)) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = u_{ab}(x)$, па је $u_a \circ u_b = u_{ab} \in \operatorname{Inn} G$. Ово нам показује и да је $u_a^{-1} = u_{a^{-1}} \in \operatorname{Inn} G$, те је $\operatorname{Inn} G \leqslant \operatorname{Aut} G$.

Ако је $\varphi \in \operatorname{Aut} G$ и $a \in G$, онда је

$$(\varphi \circ u_a \circ \varphi^{-1})(x) = \varphi(a\varphi^{-1}(x)a^{-1}) = \varphi(a)\varphi(\varphi^{-1}(x))\varphi(a^{-1}) = \varphi(a)x\varphi(a)^{-1} = u_{\varphi(a)}(x),$$

па је $\varphi \circ u_a \circ \varphi^{-1} = u_{\varphi(a)} \in \operatorname{Inn} G$. Дакле, заиста је $\operatorname{Inn} G$ нормална подгрупа групе $\operatorname{Aut} G$.

2. На основу доказаног, имамо да је пресликавање $f \colon G \to \operatorname{Inn} G$, задато са $f(a) := u_a$ један епиморфизам група. Но, $a \in \operatorname{Ker} f$ акко је $f(a) = \mathrm{id}_G$ акко је за све $x \in G$: $axa^{-1} = x$, што је еквивалентно са $a \in Z(G)$. Прва теорема о изоморфизму завршава доказ. 📕

Како је $\operatorname{Inn} G \triangleleft \operatorname{Aut} G$ можемо посматрати групу $\operatorname{Out} G := \operatorname{Aut} G / \operatorname{Inn} G$, која се назива група *спољашњих аутоморфизама* групе G.

За групу G кажемо да је *савршена* уколико је $\operatorname{Aut} G \cong G$. Приметимо да на основу става **19**, уколико је $Z(G) = \{e\}$, важи: $G \cong \operatorname{Inn} G$, те је у том случају група савршена уколико је сваки аутоморфизам унутрашњи. Знамо да је $Z(\mathbb{S}_n)$ тривијалан за $n \geqslant 3$ и стога се природно поставља питање за које је $n \geqslant 3$ група $\mathbb{S}_n$ савршена, тј. за које је n сваки аутоморфизам групе $\mathbb{S}_n$ унутрашњи. Испоставља се да је то тачно за све $n \neq 6$. Ово није тешко доказати, на основу знања, која имамо, али немамо времена за ту додатну забаву ☺. Но, у оквиру примера који следе, показаћемо да је група $\mathbb{S}_3$ савршена.

Пример 20. $\operatorname{Aut} \mathbb{Z} \cong \mathbb{C}_2$.

👉 Нека је $f \colon \mathbb{Z} \to \mathbb{Z}$ аутоморфизам. Он је потпуно одређен сликом генератора 1. Нека је $f(1) = m \in \mathbb{Z}$. Но, пошто је f аутоморфизам, мора сликати генератор у генератор. Једини генератори у $\mathbb{Z}$ су 1 и -1. Дакле, имамо само два аутоморфизма те је група аутоморфизама циклична реда 2 те је изоморфна са $\mathbb{C}_2 = \{1, -1\}$. Изоморфизам се, заправо, остварује тако што се идентичном придружи 1, а аутоморфизму који 1 слика у -1, придружи се -1. 👍

Пример 21. $\operatorname{Aut}\mathbb{Z}_n \cong U(\mathbb{Z}_n)$.

👉 Овде $U(\mathbb{Z}_n)$ означава групу елемената *прстена* $\mathbb{Z}_n$ који су инвертибилни у односу на множење. Нека је $f \in \operatorname{Aut}\mathbb{Z}_n$. Он је потпуно одређен са $f(1)$ (пошто је $\mathbb{Z}_n$ циклична група са генератором 1) и та слика такође мора бити генератор (пошто је f изоморфизам). Но, то значи да је $f(1)$ узајамно просто са n, те припада $U(\mathbb{Z}_n)$ (видети на страници 111 уџбеника о томе). Ако је $f(1) = k$, означимо то f са f_k. Имамо да је

$$\begin{aligned}(f_k \circ f_l)(1) = f_k(l) = f_k(\underbrace{1 +_n \cdots +_n 1}_{l}) \\ = \underbrace{f_k(1) +_n \cdots +_n f_k(1)}_{l} = \underbrace{k +_n \cdots +_n k}_{l} = k \cdot_n l = f_{k\cdot_n l}(1).\end{aligned}$$

Закључујемо да је $f_k \circ f_l = f_{k\cdot_n l}$. То нам показује да функција $F\colon U(\mathbb{Z}_n) \to \operatorname{Aut}\mathbb{Z}_n$ успоставља тражени изоморфизам. 👍

Посебно имамо да је $(\operatorname{Aut}\mathbb{Z}_p, \circ) \cong (\mathbb{Z}_{p-1}, +_{p-1})$ (видети став 3.46 у уџбенику). Знамо да је $U(\mathbb{Z}_{p_1^{\alpha_1}\cdots p_k^{\alpha_k}}) \cong U(\mathbb{Z}_{p_1^{\alpha_1}}) \times \cdots \times U(\mathbb{Z}_{p_k^{\alpha_k}})$ (видети странице 122–124 уџбеника), док је структура група $U(\mathbb{Z}_{p^r})$ за просте p и $r \geqslant 2$, описана у Додатку III уџбеника.

Пример 22. $(\operatorname{Aut}\mathbb{Q}, \circ) \cong (\mathbb{Q}\setminus\{0\}, \cdot)$

👉 Као и у претходна два примера, означимо са $f_a \in \operatorname{Aut}\mathbb{Q}$, за који је $f_a(1) = a$. Тврдимо да је $f_a(x) = ax$ за све $x \in \mathbb{Q}$. Индукцијом се лако покаже да је ово тачно за све $x \in \mathbb{N}$, а из чињенице да је $f_a(-x) = -f_a(x)$, добијамо да је $f_a(x) = ax$ за све $x \in \mathbb{Z}$. Но,

$$a = f_a(1) = f_a(\underbrace{\tfrac{1}{n} + \cdots + \tfrac{1}{n}}_{n}) = \underbrace{f_a(\tfrac{1}{n}) + \cdots + f_a(\tfrac{1}{n})}_{n} = nf_a(\tfrac{1}{n}),$$

те добијамо да је $f_a(\frac{1}{n}) = a \cdot \frac{1}{n}$. Одавде се индукцијом добија да је $f_a(\frac{m}{n}) = a \cdot \frac{m}{n}$ за све $m \in \mathbb{N}$, а потом и да је ова једнакост тачна за све $m \in \mathbb{Z}$. Како је $n \in \mathbb{N}$ био произвољан, добијамо да је заиста $f_a(x) = a \cdot x = ax$ као што је и наведено. Сада се на исти начин, као и у претходном примеру покаже да је $f_a \circ f_b = f_{a\cdot b}$, а како је јасно да је $f_1 = \mathrm{id}_{\mathbb{Q}}$, имамо да је f_a изоморфизам акко је $a \neq 0$. Тражени резултат следи. 👍

Пример 23. $\operatorname{Aut}\mathbb{S}_3 \cong \mathbb{S}_3$.

👉 На основу горенаведене дискусије желимо да покажемо да је сваки аутоморфизам групе $\mathbb{S}_3$, унутрашњи, тј. да је остварен конјуговањем неким елементом.

У ту сврху, нека је $f \in \operatorname{Aut}S_3$. Сада приметимо две ствари:

1. Група $\mathbb{S}_3$ је генерисана транспозицијама $(1\,2)$ и $(1\,3)$.

2. Аутоморфизам f слика транспозиције у транспозиције, јер мора да слика елементе реда 2 у елементе реда 2, а у групи $\mathbb{S}_3$ једини елементи реда 2 су транспозиције.

Дакле, имамо да је $f((12)) = (ab)$ и $f((13)) = (ac)$, где је $\{a, b, c\} = \{1, 2, 3\}$. То је заиста тако, јер у скупу транспозиција $\{(1\,2), (1\,3), (2\,3)\}$ сваке две имају заједнички елемент и тај елемент напишемо као први. Остаје да нађемо пермутацију π за коју је $\pi(12)\pi^{-1} = (ab)$ и $\pi(13)\pi^{-1} = (ac)$. Но, $\pi(12)\pi^{-1} = (\pi(1)\,\pi(2))$,

а $\pi(13)\pi^{-1} = (\pi(1)\,\pi(3))$. Дакле $\{\pi(1), \pi(2)\} = \{a, b\}$, а $\{\pi(1), \pi(3)\} = \{a, c\}$. Заједнички елементи морају да се поклопе, па је $\pi(1) = a$, те следи да је $\pi(2) = b$, а $\pi(3) = c$. Добили смо тражену пермутацији и тиме завршили доказ. Видимо да је случај $n = 3$ прилично једноставан. 👍

Пример 24. $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathbf{SL}_2(\mathbb{Z}_2)$.

👉 Најпре појашњење ознаке. Скраћеница **SL** стоји за „специјална линеарна (група)", што значи група инвертибилних матрица чија је детерминанта једнака 1; 2 у индексу означава да се ради о матрицама реда 2, а $\mathbb{Z}_2$ да су компоненте у (пољу) $\mathbb{Z}_2$. Ово тврђење је заправо очигледно када се мало размисли!

Наиме, група $\mathbb{Z}_2 \times \mathbb{Z}_2$ је директна сума две цикличне групе реда 2, које су генерисане елементима $a = (1, 0)$ и $b = (0, 1)$: $\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle a \rangle \oplus \langle b \rangle$. Сваки ендоморфизам f групе $\langle a \rangle \oplus \langle b \rangle$ потпуно је одређен сликама генератора a и b: $f(a) = m_{11}a + m_{12}b$, $f(b) = m_{21}a + m_{22}b$. Дакле, природно се појављује матрица

$$\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$$

чије су све компоненте из $\mathbb{Z}_2 = \{0, 1\}$, јер је $2a = 2b = 0$. Имамо да се елемент $(\alpha, \beta) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ слика у елемент

$$\begin{pmatrix} \alpha & \beta \end{pmatrix} \cdot \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} = \begin{pmatrix} m_{11}\alpha + m_{21}\beta & m_{12}\alpha + m_{22}\beta \end{pmatrix}.$$

Овде смо уређени пар (α, β) записали као матрицу формата 1×2. Наиме,

$$\begin{aligned} f(\alpha, \beta) = f(\alpha a + \beta b) = \alpha f(a) + \beta f(b) = \alpha(m_{11}a + m_{12}b) + \beta(m_{21}a + m_{22}b) \\ = (m_{11}\alpha + m_{21}\beta)a + (m_{12}\alpha + m_{22}\beta)b = (m_{11}\alpha + m_{21}\beta)(1, 0) + (m_{12}\alpha + m_{22}\beta)(0, 1) \\ = (m_{11}\alpha + m_{21}\beta, m_{12}\alpha + m_{22}\beta). \end{aligned}$$

Овде нисмо радили ништа друго до оно што радимо у линеарној алгебри када посматрамо матрицу линеарног пресликавања; једина разлика је било што смо желели, због каснијег рада, да не радимо са колона координатама, него са врстама!

Дакле, ово је за ма који ендоморфизам. Ако је то и аутоморфизам, ова матрица мора бити инвертибилна, тј. детерминатна јој мора бити различита од 0. Но, како су компоненте у $\mathbb{Z}_2$, различито од 0 значи да је једнако 1. И тако добијамо горенаведени опис. Наравно, остало је да се провери да се овакво придруживање слаже са композицијом пресликавања, односно множењем матрица, али знамо из линеарне алгебре да је то тако. Заправо, пошто смо овде множили врсте матрицом здесна, ако ту матрицу означимо са $M(f)$, онда би, да би се очувало својство композиције, требало аутоморфизму f придружити инверз ове матрице, $M(f)^{-1}$. Наиме:

$$(g \circ f)(x, y) = g(f(x, y)) = ((x\,y) \cdot M(f)) \cdot M(g) = (x\,y) \cdot (M(f) \cdot M(g)),$$

па је $M(g \circ f) = M(f) \cdot M(g)$. Да би пресликавање $f \to M(f)$ било хомоморфизам, морамо обрнути поредак и придруживање $f \to M(f)^{-1}$ нам то даје: $M(g \circ f)^{-1} = (M(f) \cdot M(g))^{-1} = M(g)^{-1} \cdot M(f)^{-1}$, па је $\Phi \colon \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \to \mathbf{SL}_2(\mathbb{Z}_2)$ задато са: $\Phi(f) = M(f)^{-1}$ хомоморфизам. Ово смо могли да остваримо и придруживањем $f \to M(f)^T$. Но, то је од мањег значаја.

Приметимо да је

$$\mathbf{SL}_2(\mathbb{Z}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}.$$

Заправо, важи изоморфизам $\mathbb{S}_3 \cong \mathbf{SL}_2(\mathbb{Z}_2)$. Ово можемо да констатујемо тако што приметимо да су обе групе реда 6 и да су некомутативне, а знамо из Алгебре 1 да је свака група реда 6 или циклична или је диедарска (а такође знамо да је $\mathbb{D}_3 \cong \mathbb{S}_3$ – свашта ми знамо, или би бар требало да знамо ☺). Занимљиве би било да нађемо директан изоморфизам. Размислите о томе.

Напомена. Последња два примера нам показују да из $\operatorname{Aut} G \cong \operatorname{Aut} H$ **не** следи $G \cong H$.

Коначне p-групе

Најпре дајемо пар дефиниција.

Дефиниција 25. *Нека је p прост број. За коначну групу G кажемо да је једна p-група, уколико је $|G| = p^n$ за неко $n \geqslant 1$.* 👌

Означимо са $\mathcal{P}(G)$ скуп свих подгрупа групе G. Тада G дејствује на скупу $\mathcal{P}(G)$: $g * H := gHg^{-1}$. Ако је $H \leqslant G$, онда је $\Sigma_H = \{g \in G : gHg^{-1} = H\}$. Знамо да је ово подгрупа од G. Користи се ознака $N_G(H)$ за ову подгрупу и назив: нормализатор подгрупе H у групи G. Својства нормализатора описана су следећим ставом.

Став 26. *Нека је G група и $H \leqslant G$.*

1. *$Z(G) \subseteq N_G(H)$.*
2. *$H \triangleleft N_G(H)$.*
3. *Ако је $K \leqslant G$ и $H \triangleleft K$, онда је $K \subseteq N_G(H)$.*
4. *Ако је $K \subseteq N_G(H)$, онда је $KH \leqslant G$, $H \triangleleft KH$ и $KH/H \cong K/(H \cap K)$.*

✍ 1. и 2. директно следе из дефиниције.

3. Како је H нормална подгрупа (под)групе K, онда је $kHk^{-1} = H$ за све $k \in K$, али то управо значи да $k \in N_G(H)$ за свако $k \in K$.

4. Ово је једноставна генерализације друге теореме о изоморфизму за групе. Урадите то за вежбу. 📕

Важи следећа теорема.

Теорема 27. *Нека је G коначна p-група, $|G| = p^n$ и e неутрал у G.*

а) $Z(G) \neq \{e\}$.

б) Постоје нормалне подгрупе $G_0, G_1, \ldots, G_n$ такве да је

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n = G.$$

Тада је $|G_j| = p^j$ за све j.

✍ а) Ово би требало да је доказано у Алгебри 1, али ево ипак доказа. Посматрамо дејство групе G на самој себи задато са: $g * a := gag^{-1}$. Орбите при овом дејству су класе конјугованости у G. Но, знамо да ред орбите дели ред групе, па је ред сваке орбите облика p^r за неко $r \geqslant 0$. Но, орбита је једночлана акко $a \in Z(G)$. Ако су $\Omega_1, \ldots, \Omega_k$ орбите које нису једночлане, онда имамо једнакост

$$|G| = |Z(G)| + |\Omega_1| + \cdots + |\Omega_k|. \tag{1}$$

Но, како $p \mid |G|$ и $p \mid |\Omega_i|$ за све $i = \overline{1,k}$, онда и $p \mid |Z(G)|$, па $Z(G) \neq \{e\}$.

б) Доказ изводимо индукцијом по n. Уколико је $n = 1$, онда је $G \cong \mathbb{C}_p$ и узимамо да је $G_0 = \{1\}$, а $G_1 = G$. Претпоставимо да је тврђење доказано за све групе реда p^s, где је $s < n$ и нека је $|G| = p^n$. По делу под а), $Z(G) \neq \{e\}$, па на основу Кошијеве леме у $Z(G)$ постоји елемент x реда p. Како $x \in Z(G)$, подгрупа $\langle x \rangle$ је нормална у G и можемо посматрати групу $\overline{G} = G/\langle x \rangle$. Но, $|\overline{G}| = p^{n-1}$ и по индуктивној хипотези постоји низ нормалних подгрупа од $\overline{G}$:

$$\{\langle x \rangle\} = \overline{G_0} \subset \overline{G_1} \subset \cdots \subset \overline{G_{n-1}} \subset \overline{G_{n-1}} = \overline{G}.$$

Ако са $\pi \colon G \to G/\langle x \rangle$, означимо канонску пројекцију и ако је $G_{i+1} = \pi^{-1}[\overline{G_i}]$, онда добијамо тражени низ нормалних подгрупа:

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n = G.$$

Наиме, инверзна слика нормалне подгрупе је нормална подгрупа; приметимо да је овде $G_1 = \langle x \rangle$ и да је $|G_j| = p^j$, за све j. 📕

Колико има неизоморфних p-група датог реда? Ево кратке таблице за 2-групе (до 2^{10}).

ред	број класа изоморфизама
4	2
8	5
16	14
32	51
64	267
128	2328
256	56092
512	10494213
1024	49487365422

Ево и једне процене за број класа изоморфизама група реда p^n, у ознаци $v(p^n)$, за ма који прост број p: $v(p^n) = p^{2n^3/27} + O(n^{8/3})$.

Решиве групе

Решиве групе су, генерализација комутативних група. Видећемо да у случају коначних група оне имају нека корисна својства, што их чини прилично значајном класом у оквиру класе свих коначних група.

Најпре наводимо нека додатна својства извода група.

Став 28. *а) Ако је $H \triangleleft G$, онда је и $H' \triangleleft G$.*

б) Ако је $H \leqslant G$, онда је $H' \leqslant G'$.

✍ а) Ако је $H \triangleleft G$, а $x, y \in H$, имамо да $gxg^{-1},\ gyg^{-1} \in H$, па је и $g[x,y]g^{-1} = [gxg^{-1}, gyg^{-1}] \in H'$, те је и $H' \triangleleft G$.

б) Ово је тривијално тачно. 📕

Навели смо дефиницију извода групе. Но, можемо наћи и други извод, и трећи, итд. Наравно, дефиниција је индуктивна (рекурзивна): n-ти извод групе G, у ознаци $G^{(n)}$ дефинишемо са:

$$G^{(0)} := G;$$
$$G^{(n+1)} := (G^{(n)})'.$$

Сада дајемо дефиницију решивих група.

Дефиниција 29. *За групу G кажемо да је решива уколико постоји $n \in \mathbb{N}$ тако да је $G^{(n)} = \{e\}$.* 👌

Приметимо да изводи групе G чине опадајући низ подгрупа од G:

$$G = G^{(0)} \supseteq G' \supseteq G'' \supseteq \cdots$$

при чему је сваки члан у низу, почев од другог, нормална подгрупа претходног и још је количничка група комутативна. Занимљиво је да важи следећа теорема.

Теорема 30. *Група G је решива ако и само ако постоји опадајући низ подгрупа*

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n = \{e\}, \tag{2}$$

при чему је, за све $i = \overline{0, n-1}$: $H_{i+1} \triangleleft H_i$ и H_i/H_{i+1} је комутативна група.

✍ $\Longrightarrow$. За тражени низ можемо узети низ извода: $H_i = G^{(i)}$.

$\Longleftarrow$. Претпоставимо да постоји низ 2. Како је $G/H_1 = H_0/H_1$ комутативна група, на основу става 28 добијамо да је $G' \subseteq H_1$. Докажимо индукцијом да је за све $i = \overline{1, n}$: $G^{(i)} \subseteq H_i$. Базу смо показали. Претпоставимо да је $G^{(i)} \subseteq H_i$. Како је H_i/H_{i+1} комутативна, имамо да је $H_i' \subseteq H_{i+1}$. По индуктивној хипотези је $G^{(i)} \subseteq H_i$, па је $G^{(i+1)} = (G^{(i)})' \subseteq H_i' \subseteq H_{i+1}$. Добијамо да је $G^{(n)} \subseteq H_n = \{e\}$, те закључујемо да је $G^{(n)} = \{e\}$ те је G решива група. 📕

Последица 31. *Коначне p-групе су решиве*

✍ Ово директно следи из претходне теореме и теореме **27** јер су сви количници у низу група који постоји по тој теореми групе реда p, дакле цикличне, тиме и комутативне. 📕

Пример 32. Диедарска група $\mathbb{D}_n$ је решива.

👉 Погледајте пример **1.79** у уџбенику. Ту је показано да је $\mathbb{D}_n' = \langle \rho^2 \rangle$. Како је подгрупа $\langle \rho^2 \rangle$ комутативна, комутатори свака два елемента у њој дају неутрал, те је $\langle \rho^2 \rangle' = \{\varepsilon\}$, тј. $\mathbb{D}_n'' = \{\varepsilon\}$. ✌

Пример 33. Групе $\mathbb{S}_2$, $\mathbb{S}_3$, $\mathbb{S}_4$ су решиве, док групе $\mathbb{S}_n$, за $n \geqslant 5$ нису решиве.

👉 У примеру **1.78** у уџбенику је показано да је, за све $n \geqslant 2$: $\mathbb{S}_n' = \mathbb{A}_n$. За $n = 2$ имамо да је $\mathbb{S}_2' = \{(1)\}$. За $n = 3$ је $\mathbb{S}_3' = \mathbb{A}_3$, а $\mathbb{A}_3 \cong \mathbb{C}_3$, па је $\mathbb{S}_3'' = \{1\}$. У случају $n = 4$, имамо да је $\mathbb{S}_4' = \mathbb{A}_4$, док директан рачун показује да је $\mathbb{A}_4' = V$ (урадите то за вежбу). Како је група V комутативна, то је $V' = \{(1)\}$, те је $G''' = \{(1)\}$.

Но, ствари се битно мењају када је у питању случај $n \geqslant 5$. Наравно, имамо да је $\mathbb{S}_n' = \mathbb{A}_n$, но, за $n \geqslant 5$ важи: $\mathbb{A}_n' = \mathbb{A}_n$. Наиме, ако су $a, b, c, d, e \in \{1, \ldots, n\}$ различити бројеви, имамо да је

$$[(abc), (cde)] = (abc)^{-1}(cde)^{-1}(abd)(cde) = (cba)(edc)(abc)(cde) = (bec).$$

Стога сваки 3-цикл можемо да добијемо као комутатор два 3-цикла, Како 3-цикли генеришу подгрупе $\mathbb{A}_n$ добијамо да је $\mathbb{A}_n' = \mathbb{A}_n$, те ни група $\mathbb{S}_n$ ни група $\mathbb{A}_n$ нису решиве за $n \geqslant 5$. ✌️

Напомена. Придев решива у вези је са решивошћу алгебарске једначине „у радикалима", односно изражавању њених решења као функција коефицијената при чему је дозвољено да се користе једино операције сабирања, одузимања, множења, дељења и налажења корена (отуд радикали), као што нам је познато у случају решења квадратне једначине: ако је једначина $ax^2 + bx + c = 0$, онда је $x_1 = \frac{-b-\sqrt{b^2-4ac}}{2}$, а $x_2 = \frac{-b-\sqrt{b^2+4ac}}{2}$. Постоје и одговарајуће Карданове формуле за случај једначина трећег степена, као и Фераријев метод за свођење једначине четвртог степена на једначину трећег, али у случају једначина степена већег од четвртог, решења се не могу изразити на овај начин. Наиме, Галоа је показао како се свакој једначини може придружити једна група и да је та једначина решива у радикалима ако и само ако је та група решива. Општој једначини n-тог степена придружује се група $\mathbb{S}_n$, а она, видели смо, није решива. 👍

Став 34. *а) Подгрупа решиве групе и сама је решива.*

б) Количничка група решиве групе је решива група.

в) Ако је $N \triangleleft G$, N решива, G/N решива, онда је и G решива.

г) Директан производ коначно много решивих група је решива група.

✍️ а) Ако је $H \leqslant G$, онда је $H^{(n)} \leqslant G^{(n)}$. Како је G решива, то је $G^{(n)} = \{e\}$, за неко n, а тада је и $H^{(n)} = \{e\}$.

б) Нека је $N \triangleleft G$ и $\pi \colon G \to G/N$ канонски епиморфизам: $\pi(g) = gN$. Тада имамо да је $\pi[G'] = (\overline{G})'$. Наиме, како је инверз комутатора комутатор, сваки елемент у комутаторској подгрупи је производ комутатора. Но, сваки комутатор у количничкој групи је слика комутатора у почетној групи (то смо већ користили). Стога ово важи. Индукцијом се лако покаже да је и $\pi[G^{(n)}] = (\overline{G})^{(n)}$ за све $n \geqslant$, те ако је $G^{(n)} = \{e\}$ за неко n, онда је $(\overline{G})^{(n)} = \bar{e} = N$.

в) Из претпоставке да је $\overline{G}$ решива, следи да постоји n тако да је $(\overline{G})^{(n)} = \bar{e} = N$. Но, то заправо значи да је $G^{(n)} = N$. Но, и N је решива, па постоји m тако да је $N^{(m)} = \{e\}$. Тада је $G^{(n+m)} = (G^{(n)})^{(m)} = N^{(m)} = \{e\}$.

г) Операције у директном производу су задате по координатама, па је комутатор елемената у производу уређена k-торка комутатора у одговарајућим групама, те је $(G_1 \times \cdots \times G_k)' = G_1' \times \cdots \times G_k'$. Ако је $G_i^{(n_i)} = \{e_i\}$, онда имамо да је

$$(G_1 \times \cdots \times G_k)^{(n)} = G_1^{(n)} \times \cdots \times G_k^{(n)} = \{e_1\} \times \cdots \times \{e_k\}$$

ако узмемо да је $n = \max\{n_1, \ldots, n_k\}$. 📕

Теореме Силова

Докажимо најпре једну лему.

Лема 35. *Нека је G коначна група и $K \leqslant H \leqslant G$. Тада важи једнакост*

$$|G : K| = |G : H| \cdot |H : K|.$$

✍ На основу Лагранжове теореме имамо следеће једнакости:

$$|G| = |H| \cdot |G : H|, \quad |H| = |K| \cdot |H : K|, \quad |G| = |K| \cdot |G : K|.$$

Из прве две једнакости добијамо: $|G| = |K| \cdot |H : K| \cdot |G : H|$, те онда из треће закључујемо да важи тражена једнакост. 🟥

Дефиниција 36. *Нека је $|G| = p^r m$, где је $r \geqslant 1$ и $p \nmid m$. Тада сваку подгрупу од G реда p^r, ако постоји, називамо* Силовљева p-подгрупа *групе G.* 👌

Испоставља се да таква подгрупа увек постоји. То је садржај следеће теореме.

Теорема 37. *Нека је G коначна група. Тада за сваки прост број p који дели ред групе постоји Силовљева p-подгрупа.*

✍ Нека је p прост број, који дели ред групе G. Доказ изводимо индукцијом по реду групе. База индукције се односи на $|G| = p$ и ту немамо шта да доказујемо. Претпоставимо да је $|G| = n$ и да је тврђење тачно за све подгрупе са мање од n елемената. Разматрамо два случаја.

1. У G постоји права подгрупа H чији индекс није дељив са p. Како је $|H| < |G|$, по индуктивној хипотези постоји Силовљева p-подгрупа од H. Но, ако је $|G| = p^r m$, где $p \nmid m$, како је $|G| = |H| \cdot |G : H|$ по Лагранжовој теореми, а по претпоставци $p \nmid |G : H|$, добијамо да је $|H| = p^r m'$, где $p \nmid m'$. Стога је Силовљева p-подгрупа од H уједно и Силовљева p-подгрупа од G.

2. Претпоставимо да p дели индекс сваке праве подгрупе од G. Као и у доказу у којем смо показали да је центар сваке p-подгрупе нетривијалан, посматрајмо дејство саме групе G на себе конјуговањем. Поново добијамо исту једнакост (1). Но, како је при дејству групе ред орбите једнак индексу стабилизатора, добијамо да поново $p \mid |\Omega_i|$ за све i. Како $p \mid |G|$ добијамо да $p \mid |Z(G)|$. Према Кошијевој теореми у $Z(G)$ постоји елемент x реда p. Поново посматрамо групу $\overline{G} = G/\langle x \rangle$. Како је $\overline{G} = p^{r-1}m$, можемо да применимо индуктивну хипотезу под условом да је $r - 1 > 0$. Но, ако је $r = 1$, онда смо већ добили тражену Силовљеву подгрупу: то је подгрупа $\langle x \rangle$. Дакле, уколико је $r > 1$, по индуктивној хипотези добијамо Силовљеву p-подгрупу $\overline{K} \lhd \overline{G}$. Она је реда p^{r-1}. Но, тада је група $K = \pi^{-1}[\overline{K}]$ реда p^r и то је тражена Силовљева p-подгрупа групе G. 🟥

Дакле, Силовљеве p-подгрупе увек постоје. Сада ће нам требати једна техничка лема.

Лема 38. *Нека p-група H дејствује на коначном скупу X. Тада је*

$$|X^G| \equiv |X| \pmod{p},$$

где је $X^G := \{x \in X : (\forall g \in G) g \cdot x = x\}$.

✍ Како је ред орбите једнак индексу стабилизатора представника те орбите и како је група која дејствује на X једна p-група, то је ред сваке неједночлане орбите дељив са p. Наравно, унија једночланих орбита је баш X^G. Тражени резултат следи. 📕

Теорема 39. *Нека је G коначна група.*

1. *Свака p-подгрупа од G садржана је у некој Силовљевој p-подгрупи.*
2. *Сваке две Силовљеве p-подгрупе су конјуговане једна другој.*
3. *Број Силовљевих p-подгрупа од G при дељењу са p даје остатак 1.*
4. *Број Силовљевих p-подгрупа од G дели ред групе G.*

✍ 1. и 2. Нека је H нека p-подгрупа и P нека Силовљева p-подгрупа. Претпоставимо најпре да је $H \subseteq N_G(P)$. На основу става 26, добијамо: $HP \leqslant G$ и $|HP : P| = |H : H \cap P|$. Уколико би било $|H : H \cap P| > 1$, добили бисмо да је HP једна p-podgrupa која има више елемената од Силовљеве p-подгрупе P што није могуће. Закључујемо да је $|H : H \cap P| = 1$, што значи да је $H = H \cap P$, тј. $H \subseteq P$. Дакле, у овом случају смо добили тражени резултат.

Означимо сада са $\mathcal{S}$ скуп свих конјугата од P и нека G дејствује на $\mathcal{S}$ конјуговањем. Дакле, $\mathcal{S}$ је орбита од P при овом дејству и стога је број елемената у $\mathcal{S}$ једнак индексу стабилизатора. Но, овде је стабилизатор баш $N_G(P)$ и добили смо да је $|\mathcal{S}| = |G : N_G(P)|$. Како је $P \subseteq N_G(P)$, добијамо да $p \nmid |G : N_G(P)|$, те $p \nmid |\mathcal{S}|$.

Нека сада H дејствује на $\mathcal{S}$ конјуговањем. На основу леме имамо да је $|\mathcal{S}^H| \equiv |\mathcal{S}| \pmod p$, те $p \nmid |\mathcal{S}^H|$. То значи да $\mathcal{S}^H \neq \emptyset$, јер свакако $p \mid 0$. Дакле, постоји $Q \in \mathcal{S}^H$. То значи да $(\forall h \in H) hQh^{-1} = Q$, те добијамо да је $H \subseteq N_G(Q)$. На основу првог дела доказа добијамо да је $H \subseteq Q$. Како је $Q \in \mathcal{S}$, то постоји $g \in G$ тако да је $Q = gPg^{-1}$. Дакле, добили смо следеће: ако је H ма која p-подгрупа и P ма која Силовљева p-подгрупа, онда постоји $g \in G$ тако да је $H \subseteq gPg^{-1}$. Како је и gPg^{-1} Силовљева p-подгрупа, добили смо да је свака p-подгрупа садржана у некој Силовљевој p-подгрупи. Но, ако је H и сама Силовљева p-подгрупа, онда из укључења $H \subseteq gPg^{-1}$ следи заправо једнакост $H = gPg^{-1}$ и тиме смо показали да су сваке две Силовљеве p-подгрупе конјуговане.

3. Ми сада знамо да је $\mathcal{S}$ заправо скуп свих Силовљевих p-подгрупа. Нека је H сада нека Силовљева p-подгрупа и нека она дејствује на $\mathcal{S}$ конјуговањем. Нека $K \in \mathcal{S}^H$. Као што смо видели, то значи да је $H \subseteq K$. Но, пошто су обе Силовљеве, добијамо $K = H$, те је заправо $\mathcal{S}^H = \{H\}$. На основу техничке леме добијамо да је $1 = |\mathcal{S}^H| \equiv |\mathcal{S}| \pmod p$ што се и тражило.

4. Како је број Силовљевих p-подгрупа заправо једнак индексу нормализатора ма које од њих, тај број свакако дели ред групе G. 📕

Напомена. Ако са s_p означимо број Силовљевих p-подгрупа и ако је $|G| = p^r m$, онда имамо да је $s_p \equiv 1 \pmod p$, а како $s_p \mid |G|$, имамо да $s_p \mid m$. 👍

Полудиректан производ

Дефиниција 40. *Нека је G група, $H \leqslant G$, $K \triangleleft G$ тако да важи:*

$$G = KH, \quad \text{и} \quad K \cap H = \{e\}.$$

Тада кажемо да је G унутрашњи полудиректан производ K са H *и то означавамо са:* $G = K \rtimes H$. 👌

У случају наведеном у дефиницији, кажемо и да је K нормални комплемент од H. Погледајмо неки пример.

Пример 41. 👉 *а)* $\mathbb{S}_n = \mathbb{A}_n \rtimes \langle (12) \rangle$.
б) $\mathbb{D}_n = \langle \rho \rangle \rtimes \langle \sigma \rangle$. ✌

Анализирајмо мало овај унутрашњи директан производ. Пре свега, пресликавање $f\colon K \times H \to K \rtimes H$, дато са: $f(k,h) = kh$ јесте бијекција. Наиме, јасно је да је „на", а ако је $f(k,h) = f(k_1,h_1)$ имамо да је $kh = k_1h_1$, па је $K \ni k^{-1}k_1 = hh_1^{-1} \in H$, а како је $K \cap H = \{e\}$, добијамо да је $k^{-1}k_1 = e = hh_1^{-1}$, тј. $(k,h) = (k_1,h_1)$. Но, f не мора бити изоморфизам – ако би било тако, имали бисмо да је $G \cong K \times H$, а горњи примери нам показују да то не важи увек.

Погледајмо како да дефинишемо операцију на $K \times H$ тако да f буде изоморфизам. Посматрајмо производ $(kh) \cdot (k_1h_1)$. Наш задатак је да га напишемо у облику $k'h'$, за неке $k' \in K$, $h' \in H$. То није тешко, користимо да је $K \lhd G$:

$$(kh) \cdot (k_1h_1) = khk_1h_1 = \underbrace{(k(hk_1h^{-1}))}_{k'}\underbrace{(hh_1)}_{h'}.$$

Овде имамо да $hk_1h^{-1} \in K$ зато што је $K \lhd G$, па је $hKh^{-1} = K$. Сада видимо како да дефинишемо производ на скупу $K \times H$ да би f био изоморфизам:

$$(k,h) \odot (k_1,h_1) := (k(hk_1h^{-1}), hh_1).$$

Дакле, множење на другој координати се не мења, док се на првој мало „уврне" други фактор. Приметимо да је функција из K у K дефинисана са: $k \mapsto hkh^{-1}$ један аутоморфизам групе K. Дакле, сваком елементу из H придружили смо један аутоморфизам групе . Ово нас доводи до појма спољашњег полудиректног производа.

Нека су $(K,*)$ и $(H,\cdot)$ групе и $\varphi\colon H \to \mathrm{Aut}(K)$ хомоморфизам. На скупу $K \times H$ задајемо операцију множења са:

$$(k,h) \odot (k_1,h_1) := (k * \varphi(h)(k_1), h \cdot h_1).$$

Став 42. *Са овако дефинисаном операцијом,* $K \times H$ *постаје група, коју називамо* спољашњи полудиректни производ групе K са групом H. *Користићемо ознаку* $K \rtimes_\varphi H$. *Осим тога,* $K' = K \times \{e_H\}$ *је нормална подгрупа ове групе,* $H' = \{e_K\} \times H$ *је њена подгрупа и* $K \rtimes_\varphi H$ *је унутрашњи директан производ* K' *са* H'.

✍ Рутински је проверити да је ово група, мада јесте мало дужа провера. Проверимо најпре асоцијативност.

$$\begin{aligned}\big((k,h)\odot(k_1,h_1)\big)\odot(h_2,k_2) &= (k*\varphi(h)(k_1),h\cdot h_1)\odot(k_2,h_2)\\ &= ((k*\varphi(h)(k_1))*\varphi(h\cdot h_1)(k_2),(h\cdot h_1)\cdot h_2)\\ &= (k*(\varphi(h)(k_1)*(\varphi(h)\circ\varphi(h_1))(k_2)),h\cdot(h_1\cdot h_2))\\ &= (k*(\varphi(h)(k_1)*\varphi(h)(\varphi(h_1)(k_2))),h\cdot(h_1\cdot h_2))\\ &= (k*(\varphi(h)(k_1*\varphi(h_1)(k_2))),h\cdot(h_1\cdot h_2))\\ &= (k,h)\odot(k_1*\varphi(h_1)(k_2),h_1\cdot h_2)\\ &= (k,h)\odot\big((k_1,h_1)\odot(k_2,h_2)\big).\end{aligned}$$

Неутрал је (e_K,e_H):

$$(k,h)\odot(e_K,e_H)=(k*\varphi(h)(e_K),h\cdot e_H)=(k*e_K,h)=(k,h).$$

$$(e_K,e_H)\odot(k,h)=(e_K*\varphi(e_H)(k),e_H\cdot h)=(\mathrm{id}_K(k),h)=(k,h).$$

Овде користимо да је $\varphi(e_H)=\mathrm{id}_K$ – неутрал се слика у неутрал. Нађимо инверз. Нека је $(k',h')\odot(k,h)=(e_K,e_H)$. То значи да је $k'*\varphi(h')(k)=e_K$, $h'\cdot h=e_H$. Дакле, $h'=h^{-1}$, док је

$$k'=\big(\varphi(h^{-1})(k)\big)^{-1}=\varphi(h^{-1})(k^{-1}).$$

Провера:

$$\begin{aligned}(k,h)\odot(\varphi(h^{-1})(k^{-1}),h^{-1}) &= (k*\varphi(h)(\varphi(h^{-1}(k^{-1})),h\cdot h^{-1})\\ &= (k*\varphi(h)(\varphi(h^{-1})(k^{-1})),e_H)\\ &= (k*(\varphi(h)\circ\varphi(h^{-1}))(k^{-1}),e_H)\\ &= (k*\varphi(h\cdot h^{-1})(k^{-1}),e_H)\\ &= (k*\varphi(e_H)(k^{-1}),e_H)\\ &= (k*\mathrm{id}_K(k^{-1}),e_H)\\ &= (k*k^{-1},e_H)\\ &= (e_K,e_H).\end{aligned}$$

Дакле, $(k,h)^{-1}=(\varphi(h^{-1})(k^{-1}),h^{-1})$.

Покажимо и да је $K'=K\times\{e_h\}$ нормална подгрупа.

$$\begin{aligned}(k,e_H)^{-1}\odot(k_1,e_H) &= (\varphi(e_H^{-1})(k^{-1}),e_H^{-1})\odot(k_1,e_H)\\ &= (k^{-1},e_H)\odot(k_1,e_H)\\ &= (k^{-1}*\varphi(e_H)(k_1),e_H\cdot e_H)\\ &= (k^{-1}*k_1,e_H)\in K'.\end{aligned}$$

$$\begin{aligned}(k,h)^{-1}\odot(k_1,e_H)\odot(k,h) &= (\varphi(h^{-1})(k^{-1}),h^{-1})\odot(k_1*\varphi(e_H)(k),e_H\cdot h)\\ &= (\varphi(h^{-1})(k^{-1})*\varphi(h^{-1})(k_1*k),h^{-1}\cdot h)\\ &= (\varphi(h^{-1}(k^{-1}*k_1*k)),e_H)\in K'.\end{aligned}$$

Приметимо да је $K'\cong K$. Проверу да је H' подгрупа изоморфна са H остављамо читаоцима. Но, јасно је да $K'\odot H'=K\rtimes_\varphi H$, као и $K'\cap H'=\{(e_K,e_H)\}$. Стога је заиста $K\rtimes_\varphi H=K'\rtimes H'$.

Урадимо неки пример спољашњег полудиректног производа. Дакле, изаберимо групе H и K и хомоморфизам $\varphi\colon H \to \mathrm{Aut}(K)$. Приметимо најпре да, ако је φ константан хомоморфизам, тј. хомоморфизам који све елементе из H слика у id_K, добијамо заправо директан производ – погледајте како операција изгледа у том случају.

Значи, тражимо нешто занимљивије. Но, не може се увек наћи тако нешто. На пример, ако бисмо узели да је $H = \mathbb{Z}_3$, а $K = \mathbb{Z}_8$, не може се наћи нетривијалан хомоморфизам $\varphi\colon \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_8)$. Наиме, сваки аутоморфизам групе $\mathbb{Z}_8$, која је циклична, је потпуно одређен када је задат на генератору, узмимо да је то 1. Но, да бисмо добили бијекцију, тај генератор се мора сликати у генератор, дакле, могућности за аутоморфизам су да се 1 слика у неки од елемената скупа $\{1, 3, 5, 7\}$. То значи да је $|\mathrm{Aut}(\mathbb{Z}_8)| = 4$. Но, $\mathbb{Z}_3$ је такође циклична група и то реда 3. Како ред слике ма ког елемента при хомоморфизму мора да дели ред тог елемента (поновите то из Алгебре 1), ред слике генератора групе $\mathbb{Z}_3$ мора бити или 1 или 3. Ако је 1, то значи да се слика у неутрал, стога претпоставимо да је 3. Али ред елемента дели ред групе, па бисмо добили да $3 \mid 4$. Дакле, овако не можемо добити пример. Но...

Пример 43. Одредити полудиректан производ $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_8$, који није изоморфан директном производу ових група.

👉 Тражимо нетривијалан хомоморфизам $\varphi\colon \mathbb{Z}_8 \to \mathrm{Aut}(\mathbb{Z}_3)$. Но група $\mathbb{Z}_3$ има два аутоморфизма: $x \mapsto x$ и $x \mapsto 2x$. Заправо је $\mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{C}_2$ и генератор је овај други аутоморфизам. Сада немамо проблем, јер је група $\mathbb{Z}_8$ реда 8, а $2 \mid 8$. Дефинишемо $\varphi\colon \mathbb{Z}_8 \to \mathrm{Aut}(\mathbb{Z}_3)$ са: $\varphi(m)(x) := 2^m x$, где $m \in Z_8 = \{0, 1, \ldots, 7\}$, а $x \in Z_3 = \{0, 1, 2\}$. Ево како изгледа операција у групи $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_8$: $(x, m) \oplus (y, n) = (x +_3 2^m y, m +_8 n)$.

Покажимо да ова група није комутативна, те стога није изоморфна са $\mathbb{Z}_3 \times \mathbb{Z}_8$. Имамо да је $(x, 1) \oplus (y, 2) = (x +_3 2y, 1 +_8 2) = (x +_3 2y, 3)$, док је $(y, 2) \oplus (x, 1) = (y +_3 2^2 x, 2 +_8 1) = (y +_3 x, 3)$. Но, $x +_3 2y = y +_3 x$ акко је $y = 0$. Дакле, ако је $y \neq 0$, једнакост не важи. Добили смо једну некомутативну групу реда 24. ✌

Пример 44. Одредити полудиректан производ $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\varphi \mathbb{Z}_3$, који није изоморфан директном производу ових група.

👉 Тражимо нетривијалан хомоморфизам $\varphi\colon \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$. Подсетимо се да је $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathbf{SL}_2(\mathbb{Z}_2)$, и да ову групу чине матрице:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ и } \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Ради краћег писања, тј. да парове не пишемо као колоне, него као врсте, матрице ће дејствовати са десне стране на врсте (као што смо раније и навели). Како је група $\mathbb{Z}_3$ циклична реда 3, тражимо матрице које су, као елементи групе, реда 3. То су заправо последње две матрице у горњем списку:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Дакле, дефинишемо $\varphi\colon \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ са: $\varphi(n)(x, y) = (x, y) \cdot (\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix})^n$. Коначно, операција је на $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\varphi \mathbb{Z}_3$ задата са:

$$((x, y), m) \odot ((u, v), n) = ((x, y) + (u, v)(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix})^m, m +_3 n).$$

Ова група није комутативна:

$$\begin{aligned}((x,y),1)\odot((u,v),2) &= ((x,y)+(u,v)\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right),1+_3 2)\\ &= ((x,y)+(u+_2 v,u),0)\\ &= ((x+_2 u+_2 v, y+_2 u),0).\end{aligned}$$

$$\begin{aligned}((u,v),2)\odot((x,y),1) &= ((u,v)+(x,y)\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)^2,2+_3 1)\\ &= ((u,v)+(x,y)\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right),0)\\ &= ((u,v)+(y,x+_2 y),0)\\ &= ((u+_2 y, v+_2 x+_2 y,0).\end{aligned}$$

Ако узмемо, на пример да је $x=y=0$, $u=v=1$, добијамо најпре да је $((0,0),1)\odot((1,1),2)=((0,1),0)$, а потом и $((1,1),2)\odot((0,0),1)=((1,1),0)$. Дакле, добили смо некомутативну групу која има цикличну подгрупу реда 3, као и нормалну подгрупу изоморфну Клајновој групи. Знате ли о којој се тачно групи ради? ✌️

Наводимо сада, за крај овог одељка, без доказа, једну важну теорему, која говори о постојању нормалног комплемента, као и једну њену примену.

Теорема 45. (Бернсајдова теорема о нормалном комплементу) *Нека је G коначна група, P њена Силовљева подгрупа. Ако је $P\subseteq Z(N_G(P))$, онда P има нормалан комплемент у G.* 📕

Пример 46. Група реда 552 не може бити проста.

Као што неки кажу, ово спада у рекреативну теорију група, али је прилично популарна тема код нас на испитима, па ...🤠

👉 Дакле, треба показати да свака група G реда 552 има неку нетривијалну нормалну подгрупу. Како је $552=2^3\cdot 3\cdot 23$, имамо да је $s_{23}\equiv 1 \pmod{23}$ и да $s_{23}\mid 2^3\cdot 3$ (подсетимо се да је s_{23} број Силовљевих 23-подгрупа). Дакле, $s_{23}\in\{1,24\}$. Ако је $s_{23}=1$, онда је Силовљева 23-подгрупа нормална, а ако је $s_{23}=24$, ако са P означимо неку Силовљеву 23-подгрупу, имамо да је $24=s_{23}=|G:N_G(P)|$, па, како је $P\subseteq N_G(P)$ и $|P|=23$, добијамо да је $P=N_G(P)$. Но, група реда 23 нужно је циклична, стога и комутативна, па је тривијално испуњен услов из Бернсајдове теореме. Стога постоји нормална подгрупа $N\triangleleft G$, која је нормални комплемент од P. ✌️

За крај овог одељка један занимљив, а необавезан пример.

Пример 47. 👉 Сви смо чули за Рубикову (магичну) коцку. Са становишта теорије група, имамо једну подгрупу групе $\mathbb{S}_{48}$ (имамо шест страна коцке обојених са шест различитих боја и на свакој страни имамо по 8 квадратића који се померају – централни се не померају; зато је овде 48), која је генерисана ротацијама страна коцке. Може се показати да је ова група изоморфна групи

$$\left(\mathbb{C}_3^7\times\mathbb{C}_2^{11}\right)\rtimes\left((\mathbb{A}_8\times\mathbb{A}_{12})\rtimes\mathbb{C}_2\right).$$

Само кратко појашњење. Нормална подгрупа изоморфна са $\mathbb{C}_3^7\times\mathbb{C}_2^{11}$ је подгрупа трансформација које не мењају позицију коцкица, само оријентацију. Како имамо 8 коцкица у угловима, њихове три странице можемо да пермутујемо, али

не можемо у потпуности независно, када се изврши пермутација на њих 7, онда је на осмој фиксирано шта се може десити. Зато имамо $\mathbb{C}_3^7$ – циклично пермутујемо те три странице, а има укупно 7 позиција на којима имамо слободу. Слично имамо 12 коцкица које су на средини ивица и оне имају две странице које видимо. Стога имамо $\mathbb{C}_2^{11}$ – на дванаестој је фиксирано шта се може десити када се трансформише преосталих 11.

Подгрупа која није нормална изоморфна је са $(\mathbb{A}_8 \times \mathbb{A}_{12}) \rtimes \mathbb{C}_2$. Ту се ради о подгрупи у којој су трансформације које мењају само позиције малих коцкица, али не и њихове оријентације. Поново, није све произвољно, имамо парне пермутације коцкица у угловима (стога се појављује група $\mathbb{A}_8$), као и парне пермутације коцкица на срединама ивица (стога група $\mathbb{A}_{12}$, а ту је и пермутација реда два која замени две угаоне и две ивичне коцкице (група $\mathbb{C}_2$).

У сваком случају, из горњег приказа можемо израчунати ред ове групе:

$$|\big(\mathbb{C}_3^7 \times \mathbb{C}_2^{11}\big) \rtimes \big((\mathbb{A}_8 \times \mathbb{A}_{12}) \rtimes \mathbb{C}_2\big)| = 3^7 \cdot 2^{11} \cdot \tfrac{8!}{2} \cdot \tfrac{12!}{2} \cdot 2 = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11. \quad ✌$$