АЛГЕБРА 2: ГРУПЕ

ЗОРАН ПЕТРОВИЋ

У овом одељку бавићемо се скоро искључиво коначним групама, тако да сматрамо да су све групе које се овде појављују коначне, сем ако се посебно не истакне да могу бити и бесконачне. Кратка напомена о ознакама: $\subset$ увек означава прави подскуп. У уџбенику *Алгебра за информатичаре* погледајте теореме о изоморфизмима, као и додатак IV.

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

Теорема 1. *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. $e \in K = p^{-1}[\mathcal{K}]$, ра 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

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

📕

Докажимо и једну једноставну лему, коју ћемо у даљем користити.

Лема 2. *Нека је G коначна комутативна група и p прост број, који дели ред те групе. Тада у G постоји елемент реда p.*

✍ Доказ изводимо индукцијом по реду групе G.

$|G| = p$. Тада је G циклична група реда p и њен генератор је реда p.

$< n \to n$. Нека је $|G| = n$ и тврђење испуњено за све групе мањег реда.

Нека $x \in G \setminus \{e\}$ и $\omega(x) = m$; свакако $m \mid |G|$.

$p \mid m$. Тада је $\omega(x^{m/p}) = p$.

$p \nmid m$. Посматрамо групу $\overline{G} = G/\langle x\rangle$. Како $p \nmid m$, имамо да $p \mid |\overline{G}|$ и $|\overline{G}| < n$. По индуктивној хипотези, постоји $y \in G$, такав да $\omega(\bar{y}) = p$ ($\bar{y} = y\langle x\rangle$). Но $\omega(\bar{y}) \mid \omega(y)$ (из $y^{\omega(y)} = e$ следи $\bar{y}^{\omega(y)} = \bar{e}$, па $\omega(\bar{y}) \mid \omega(y)$), те $p \mid \omega(y)$ и $\omega(y^{\omega(y)/p}) = p$. 📕

Date: Јесен 2026.

Напомена. Наравно да је Кошијева лема јачи резултат од овог, али нам заправо пуна Кошијева лема и не треба у даљем.

Коначне p-групе

Најпре дајемо пар дефиниција.

Дефиниција 3. *Нека је p прост број. За коначну групу G кажемо да је једна p-група, уколико је $|G| = p^n$ за неко $n \geqslant 1$.* 👌

Дефиниција 4. *Нека је G група и $H \leqslant G$. За H кажемо да је* максимална *уколико не постоји подгрупа $K \leqslant G$ за коју је $H \subset K \subset G$.* 👌

Приметимо да произвољна група не мора садржати максималну подгрупу.

Пример 5. Група $(\mathbb{Q}, +)$ не садржи максималну подгрупу.

👉 Претпоставимо да је A максимална подгрупа од $\mathbb{Q}$. Како је $(\mathbb{Q}, +)$ Абелова група, свака подгрупа је нормална и можемо посматрати количничку групу $\mathbb{Q}/A$. Једине подгрупе ове групе су цела група и тривијална подгрупа. Наиме, ако би $L \leqslant \mathbb{Q}/A$ била нека подгрупа различита од ове две, онда би $\pi^{-1}[L]$, где је $\pi \colon \mathbb{Q} \to \mathbb{Q}/A$ канонска пројекција, била права подгрупа од $\mathbb{Q}$, која је стриктно већа од A, а то није могуће, јер је A максимална подгрупа од $\mathbb{Q}$.

Дакле, мора бити $\mathbb{Q}/A \cong \mathbb{Z}_p$ за неки прост број p. Нека је $x \in \mathbb{Q} \setminus A$. Тада је $A = p(\frac{x}{p} + A) = x + A$, па бисмо добили да $x \in A$. ✌

У случају коначне групе G, јасно је да постоји максимална подгрупа. Наиме, пођимо од тривијалне подгрупе $H_0 = \{e\}$. Ако она није максимална, онда постоји $H_1 \leqslant G$, тако да је $H_0 \subset H_1$. Уколико ни H_1 није максимална, постоји $H_2 \leqslant G$, тако да је $H_1 \subset H_2$. Но, не можемо наставити тако неограничено, јер је група G коначна, и добијамо $|H_0|, |H_1|, |H_2|, \ldots$ што је строго растући низ природних бројева. Зато се овај процес мора завршити неком максималном подгрупом. Сличан доказ нам даје да је свака права подгрупа коначне групе садржана у некој максималној подгрупи те групе.

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 6. *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 7. *Нека је G коначна p-група, e неутрал у G, K максимална подгрупа у G и $|G| = p^n$.*

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.

в) $K \triangleleft G$ и $|G : K| = p$.

✍ 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 леме **2** 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.

в) Радимо индукцијом по n. За $n = 1$ заиста нема шта да се ради. Нека је $|G| = p^n$ и претпоставимо да тврђење важи за све природне бројеве мање од n.

Претпоставимо да постоји максимална подгрупа K која није нормална подгрупа од G. Како је $K \triangleleft N_G(K)$ закључујемо да $N_G(K) \neq G$, па мора бити $K = N_G(K)$. Како је, на основу претходног става, $Z(G) \subseteq N_G(K)$, закључујемо да је $Z(G) \subseteq K$. Као и у доказу претходног дела, посматрамо $x \in Z(G)$ реда p и канонску пројекцију $\pi \colon G \to \overline{G} = G/\langle x \rangle$. Приметимо да је тада $\overline{K} = \pi[K]$ максимална подгрупа групе $\overline{G}$. Наиме, како је свака подгрупа од $\overline{G}$ облика $\overline{L} = L/\langle x \rangle$ за неку подгрупу L групе G, претпоставимо да је $\overline{K} \subset \overline{L}$. Но, тада је и $K \subseteq L$, но не може важити једнакост $K = L$, јер бисмо тада имали и $\overline{K} = \overline{L}$. Дакле, $K \subset L$, те, како је K максимална, имамо да је $L = G$, те следи да је $\overline{L} = \overline{G}$ и закључујемо да је $\overline{K}$ максимална. Како је $|\overline{G}| = p^{n-1}$, по индуктивној хипотези закључујемо да је $\overline{K} \triangleleft \overline{G}$ и да је $|\overline{G} : \overline{K}| = p$. Но, K је тада нормална подгрупа као

инверзна слика нормалне подгрупе, а π индукује изоморфизам $\widetilde{\pi}\colon G/K \to \overline{G}/\overline{K}$ (уверите се да је то тако), те је $|G:K| = |\overline{G}:\overline{K}| = p$. 📕

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: $v(p^n) = p^{2n^3/27} + O(n^{8/3})$.

Теореме Силова

Докажимо најпре једну лему.

Лема 8. *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 9. *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 10. *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 $\overline{K} \triangleleft \overline{G}$. 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 11. *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 12. *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 6, 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 технике 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 13. *Нека је G група, $H \leqslant G$, $K \triangleleft G$ тако да важи:*

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

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 14. 👉 *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 $K \triangleleft G$:

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

Овде имамо да $hk_1h^{-1} \in K$ зато што је $K \triangleleft G$, 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 15. *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 16. 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 $(y,2)\oplus(x,1) = (y+_3 2^2x, 2+_8 1)=(y+_3 x,3)$. 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 17. 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 $\varphi\colon\mathbb{Z}_3\to\mathrm{Aut}(\mathbb{Z}_2\times\mathbb{Z}_2)$. Група $\mathbb{Z}_2\times\mathbb{Z}_2$ је изоморфна Клајновој групи V и из Алгебре 1 би требало да је познато да је њена група аутоморфизама изоморфна групи $\mathbb{S}_3$. Заправо, у то се није тешко уверити: овде су сви елементи сем неутрала реда 2 и аутоморфизам није ништа друго до пермутација ових елемената. Како их има 3 и све пермутације су дозвољене, група је изоморфна са $\mathbb{S}_3$. Но, овде ћемо другачије поступити. Наиме, група $\mathbb{Z}_2\times\mathbb{Z}_2$ је векторски простор димензије 2 над пољем $\mathbb{Z}_2$ и аутоморфизми ове

групе су заправо изоморфизми овог простора. Но, они су задати инвертибилним матрицама реда 2 над овим пољем. То су заправо следеће матрице:

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

Дакле, има их 6. Ове матрице чине групу у односу на множење. Та група се означава са $\mathbf{SL}_2(\mathbb{Z}_2)$. Ознака **SL** је скраћеница за „специјална линеарна", а то означава матрице чија је детерминанта једнака 1 (како је детерминанта из $\mathbb{Z}_2$, она није једнака 0 акко је једнака 1), 2 у индексу се односи на то да су матрице реда 2, а $\mathbb{Z}_2$ да су компоненте у пољу $\mathbb{Z}_2$. Претходна дискусија нам каже да је ова група изоморфна групи $\mathbb{S}_3$. Пробајте да се у то уверите, можда је корисно да користите изоморфизам $\mathbb{S}_3 \cong \mathbb{D}_3$, па да видите да је она изоморфна диедарској групи.

Ради краћег писања, тј. да парове не пише као колоне, него као врсте, матрице ће дејствовати са десне стране на врсте. 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 $\varphi\colon \mathbb{Z}_3 \to \operatorname{Aut}(\mathbb{Z}_2\times\mathbb{Z}_2)$ са: $\varphi(n)(x,y) = (x,y)\cdot(\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)^n$. Коначно, операција је на $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\varphi \mathbb{Z}_3$ задата са:

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

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? ✌

За неке сложеније примере, добро је знати групу аутоморфизама цикличне групе.

Став 18. $\operatorname{Aut}\mathbb{Z}_n \cong U(\mathbb{Z}_n)$.

✍ 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

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

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 $U(\mathbb{Z}_{p_1^{\alpha_1} \dots p_k^{\alpha_k}}) \cong U(\mathbb{Z}_{p_1^{\alpha_1}}) \times \cdots \times U(\mathbb{Z}_{p_k^{\alpha_k}})$ (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.

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

Теорема 19. (Бернсајдова теорема о нормалном комплементу) *Нека је G коначна ɡрупа, P њена Силовљева подɡрупа. Ако је $P \subseteq Z(N_G(P))$, онда P има нормалан комплемент у G.* 📕

Пример 20. 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 21. 👉 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:

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

Нилпотентне групе

Докажимо најпре једну корисну лему.

Лема 22. (Фратинијев аргумент) *Нека је G коначна група, $K \triangleleft G$ и P Силовљева подгрупа од K, тада је $G = N_G(P)K$.*

✍ Нека је $g \in G$ произвољан елемент. Тада је $g^{-1}Pg \subseteq g^{-1}Kg = K$. Дакле, $g^{-1}Pg$ је подгрупа од K, која има исти број елемената као и њена Силовљева подгрупа P. Стога је и она Силовљева подгрупа од K, па су оне конјуговане у K, тј. постоји $k \in K$ тако да је $k^{-1}(g^{-1}Pg)k = P$, односно $(gk)^{-1}P(gk) = P$, те $gk \in N_G(P)$, па $g \in N_G(P)k^{-1} \subseteq N_G(P)K$. Како је g био произвољан елемент групе G, закључујемо да је $G \subseteq N_G(P)K$, тј. $G = N_G(P)K$. 📕

Изводимо неке последице ове леме.

Последица 23. *Нека је P Силовљева подгрупа коначне групе G и $N_G(P) \leqslant H \leqslant G$. Тада је H* самонормализујућа, *тј. $H = N_G(H)$.*

✍ На основу претпоставке и својстава нормализатора имамо да је

$$P \triangleleft N_G(P) \leqslant H \triangleleft N_G(H) \leqslant G.$$

Како је P Силовљева подгрупа групе G, она је и Силовљева подгрупа свих група у овом низу. Посебно, она је Силовљева подгрупа групе $N_G(H)$, која садржи нормалну подгрупу H. Применом Фратинијевог аргумента добијамо да је $N_G(H) = N_{N_G(H)}(P)H$. Но, $N_{N_G(H)}(P) \subseteq N_G(P) \subseteq H$, те добијамо $N_G(H) \subseteq HH = H$, што даје $N_G(H) = H$. 📕

Последица 24. *Нека је G коначна група и нека су у G све њене максималне подгрупе нормалне. Тада су у G и све њене Силовљеве подгрупе нормалне и група G је изоморфна директном производу својих Силовљевих подгрупа.*

✍ Претпоставимо да G садржи неку Силовљеву подгрупу P која није нормална. Дакле, $N_G(P)$ је права подгрупа од G. Стога је она садржана у некој максималној подгрупи H групе G (можда је и она сама максимална, ништа не смета). По претпоставци је $H \triangleleft G$, а $P \leqslant N_G(P) \leqslant H$, па је P Силовљева подгрупа и од H. Фратинијев аргумент даје: $G = N_G(P)H$. Но, $N_G(P) \subseteq H$, па добијамо да је $G \subseteq HH = H$, тј. $G = H$, што противречи претпоставци да је H максимална

подгрупа од G, дакле, самим тим, и права подгрупа од G. Закључујемо да су у G све Силовљеве погрупе нормалне. Посебно то значи да за сваки прост број p, који дели ред групе, постоји тачно једна Силовљева p-подгрупа од G.

Покажимо сада да је G изоморфна производу својих Силовљевих подгрупа. Neka је $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ и нека је H_i Силовљева p_i-погрупа од G; $|H_i| = p_i^{\alpha_i}$. Докажимо најпре да је $h_i h_j = h_j h_i$ за све $h_i \in H_i$, $h_j \in H_j$, $i \neq j$. Посматрамо комутатор ова два елемента: $[h_i, h_j] = h_i^{-1} h_j^{-1} h_i h_j$. Како је $H_i \triangleleft G$, имамо да $h_j^{-1} h_i h_j \in H_i$, па, како $h_i \in H_i \leqslant G$, добијамо да $[h_i, h_j] \in H_i$. Слично, како је $H_j \triangleleft G$ и $h_j^{-1} \in H_j$, добијамо да $h_i^{-1} h_j^{-1} h_i \in H_j$, те $[h_i, h_j] \in H_j$. Дакле, $[h_i, h_j] \in H_i \cap H_j$. Но, по Лагранжовој теореми имамо да $|H_i \cap H_j| \mid |H_i|$, тј. $|H_i \cap H_j| \mid p_i^{\alpha_i}$. Такође $|H_i \cap H_j| \mid p_j^{\alpha_j}$, те $|H_i \cap H_j| \mid \mathrm{NZD}(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$. Закључујемо да је $H_i \cap H_j = \{e\}$, те је $[h_i, h_j] = e$, тј. $h_i^{-1} h_j^{-1} h_i h_j = e$, из чега следи: $h_i h_j = h_j h_i$.

Дефинишимо $f \colon H_1 \times \cdots \times H_k \to G$ са: $f(h_1, \ldots, h_k) := h_1 \cdots h_k$. Покажимо да је f један хомоморфизам група. Наиме:

$$f((h_1, \ldots, h_k) \cdot (h_1', \ldots, h_k')) = f(h_1 h_1', \ldots, h_k h_k') = h_1 h_1' \cdots h_k h_k'.$$

Но, како елементи из различитих Силовљевих подгрупа комутирају, индукцијом по k се лако показује да је

$$h_1 h_1' \cdots h_k h_k' = (h_1 \cdots h_k) \cdot (h_1' \cdots h_k') = f(h_1, \ldots, h_k) \cdot f(h_1', \ldots, h_k').$$

Дакле, заиста је

$$f((h_1, \ldots, h_k) \cdot (h_1', \ldots, h_k')) = f(h_1, \ldots, h_k) \cdot f(h_1', \ldots, h_k'),$$

те је f хомоморфизам група. На основу прве теореме о изоморфизму група, имамо да је $H_1 \times \cdots \times H_k / \mathrm{Ker}\, f \cong \mathrm{Im}\, f$. Покажимо да је $\mathrm{Ker}\, f = \{(e, \ldots, e)\}$. Наиме, ако је $(h_1, \ldots, h_k) \in \mathrm{Ker}\, f$, имамо да је $h_1 \cdots h_k = e$. Како h_i комутирају, имамо да је $(h_1 \cdots h_k)^m = h_1^m \cdots h_k^m$ за свако $m \in \mathbb{Z}$. Узмимо да је $m = p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Како је $|H_i| = p_i^{\alpha_i}$, имамо да је $h_i^{p_i^{\alpha_i}} = e$ за све i. Стога је $h_i^m = e$ за све $i \geqslant 2$. Добијамо:

$$e = e^m = (h_1 h_2 \cdots h_k)^m = h_1^m h_2^m \cdots h_k^m = h_1^m e \cdots e = h_1^m.$$

Из чињенице да је $\mathrm{NZD}(p_1^{\alpha_1}, m) = 1$, следи да постоје $r, s \in \mathbb{Z}$ такви да је $r p_1^{\alpha_1} + sm = 1$. Тада је:

$$h_1 = h_1^1 = h_1^{r p_1^{\alpha_1} + sm} = \left(h_1^{p_1^{\alpha_1}}\right)^r \cdot (h_1^m)^s = e^r \cdot e^s = e.$$

Уколико узмемо да је $m = \frac{p_1^{\alpha_1} \cdots p_k^{\alpha_k}}{p_i^{\alpha_i}}$, аналогно добијамо је $h_i = e$. Дакле, језгро хомоморфизма f је тривијално. Стога је $H_1 \times \cdots \times H_k \cong \mathrm{Im}\, f \leqslant G$, па је $|\mathrm{Im}\, f| = |H_1 \times \cdots \times H_k| = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = |G|$, те добијамо да је заправо $\mathrm{Im}\, f = G$ и да имамо тражени изоморфизам. ∎

Већ смо се у претходном доказу подсетили комутатора два елемента. Приметимо да је група G комутативна ако и само ако важи:

$$(\forall a_0 \in G)(\forall a_1 \in G)([a_0, a_1] = e).$$

Но, овај поступак можемо итерирати, па посматрати

$$[[a_0, a_1], a_2],\ [[[a_0, a_1], a_2], a_3],\ [[[[a_0, a_1], a_2], a_3], a_4],\ \ldots.$$

Дефиниција 25. *За групу G кажемо да је* нилпотентна *уколико постоји $n > 0$ такав да важи:*

$$(\forall a_0 \in G)(\forall a_1 \in G)\cdots(\forall a_n \in G)([[\ldots[a_0, a_1], a_2], \ldots, a_n] = e).$$

Најмање такво n називамо степен нилпотентности групе G. 👌

Дакле, нетривијална група је комутативна ако и само ако је њен степен нилпотентности једнак 1.

Пример 26. Група $\mathbb{S}_3$ није нилпотентна.

👉 Наиме,

$$\begin{aligned}
[(12),(13)] &= (12)^{-1}(13)^{-1}(12)(13) = (12)(13)(12)(13) = (123);\\
[[(12),(13)],(12)] &= (123)^{-1}(12)^{-1}(123)(12) = (123);\\
[[[(12),(13)],(12)],(12)] &= (123)^{-1}(12)^{-1}(123)(12) = (123);\\
&\vdots
\end{aligned}$$

Видимо да никада не добијамо тривијалну подгрупу. ✌

Пример 27. Кватернионска група Q_8 јесте нилпотентна.

👉 Подсетимо се да је $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ и да је

$$ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j,\ i^2 = j^2 = k^2 = -1.$$

Покажимо да је $[[a, b], c] = 1$ за све $a, b, c \in Q_8$. То ће нам дати да је Q_8 нилпотентна и да је степен нилпотентности једнак 2. Заправо треба показати да $[a, b] \in Z(Q_8) = \{1, -1\}$ за све a, b. Ако је неки од њих већ у центру, комутатор је једнак 1. Стога претпоставимо да они нису у центру. Но, за $x \in Q_8 \setminus \{1, -1\}$ имамо да је $x^{-1} = -x$, па је $[a, b] = a^{-1}b^{-1}ab = (-a)(-b)ab = (ab)^2 \in \{1, -1\} = Z(G)$. ✌

Пример 28. Диедарска група $\mathbb{D}_4$ јесте нилпотентна и то степена 2.

👉 У уџбенику *Алгебра за информатичаре* можете наћи да је, за све $x, y \in \mathbb{D}_4$: $[x, y] \in \langle \rho^2 \rangle = Z(G)$. Стога тражено следи. ✌

Овде смо имали пример две групе реда $8 = 2^3$ које су нилпотентне. У следећем ставу доказујемо знатно општији резултат.

Став 29. *Свака p-група, где је p прост број, јесте нилпотентна.*

✍ Дакле, нека је G група реда p^n. Доказ изводимо индукцијом по n.

Уколико је $n = 1$, имамо групу реда p која је нужно циклична, па тиме и комутативна, па тиме и нилпотентна.

Претпоставимо да је тврђење тачно за све p-групе са мање од p^n елемената и нека је $|G| = p^n$. Претпоставимо такође да она није комутативна (пошто за комутативне немамо шта да радимо). Знамо да је $Z(G) \neq \{e\}$ (видети теорему 7). Означимо са $\overline{G}$ количничку групу $G/Z(G)$. Како је $|\overline{G}| = p^k$, за неко $1 < k < n$, по индуктивној хипотези имамо да је $\overline{G}$ нилпотентна. Неке је њен степен нилпотентности n и нека су $a_0, \ldots, a_n \in G$ произвољни елементи. Ако са $\bar{x}$ означимо класу елемента x у количничкој групи $\overline{G}$, имамо да је

$$[[[\overline{a_0}, \overline{a_1}], \overline{a_2}], \ldots, \overline{a_n}] = \bar{e}(= Z(G)).$$

Но, $[[[\overline{a_0},\overline{a_1}],\overline{a_2}],\ldots,\overline{a_n}] = \overline{[[[a_0,a_1],a_2],\ldots,a_n]}$ и горња једнакост заправо значи да је $[[[a_0,a_1],a_2],\ldots,a_n] \in Z(G)$. Но, то нам даје да је

$$[[[[a_0,a_1],a_2],\ldots,a_n],a_{n+1}] = e,$$

за све $a_{n+1} \in G$, те је G нилпотентна са степеном нилпотентности $n+1$. 📕

Став 30. *а) Подгрупа нилпотентне групе и сама је нилпотентна.*
б) Количничка група нилпотентне групе је такође нилпотентна.
в) Ако су G и H нилпотентне, онда је и $G \times H$ нилпотентна.

✍ а) Дакле, нека је G нилпотентна група и L ма која њена подгрупа. Како је G нилпотентна, постоји $n > 0$ тако да је $[[\ldots[a_0,a_1],a_2],\ldots,a_n] = e$ за све $a_i \in G$. Но, тада је та једнакост тривијално испуњена и за све $a_i \in L$, па је и L нилпотентна.

б) Нека је G нилпотентна група и $N \triangleleft G$. Нека је $\overline{G} = G/N$. Како је G нилпотентна, то постоји $n > 0$ тако да је $[[\ldots[a_0,a_1],a_2],\ldots,a_n] = e$ за све $a_i \in G$. Тада је

$$[[\ldots[\overline{a_0},\overline{a_1}],\overline{a_2}],\ldots,\overline{a_n}] = \overline{[[[a_0,a_1],a_2],\ldots,a_n]} = \bar{e}(= N).$$

Но, како је сваки елемент из $\overline{G}$ облика $\bar{x}$ за неко $x \in G$, добијамо да је и $\overline{G}$ нилпотентна.

в) Претпоставимо да је G степена нилпотентности m, а H степена нилпотентности n. Но, ако је $[[\ldots[a_0,a_1],a_2],\ldots,a_n] = e$, за све $a_i \in G$, онда је и

$$[[\ldots[a_0,a_1],a_2],\ldots,a_k] = e,$$

за све $k \geqslant n$ и све $a_i \in G$. Стога, ако је $N = \max\{m,n\}$, имамо да је за све $g_i \in G$, $h_j \in H$:

$$[[\ldots[g_0,g_1],g_2],\ldots,g_N] = e_G \text{ као и } [[\ldots[h_0,h_1],h_2],\ldots,h_N] = e_H.$$

Стога је и

$$[[\ldots[(g_0,h_0),(g_1,h_1)],(g_2,h_2)],\ldots,(g_N,h_N)] = (e_G,e_H) = e_{G\times H},$$

Овде смо користили једнакост $[(g_0,h_0),(g_1,h_1)] = ([g_0,g_1],[h_0,h_1])$ 📕

Сада ћемо формулисати и доказати теорему која даје више критеријума за нилпотентност коначних група.

Теорема 31. *Нека је G коначна група. Следећи услови су еквивалентни.*

а) *G је нилпотентна.*
б) *Ако је H права подгрупа од G, онда је H права подгрупа и од $N_G(H)$.*
в) *Све максималне подгрупе од G су нормалне.*
г) *Све Силовљеве подгрупе од G су нормалне.*
д) *G је изоморфна директном производу својих Силовљевих подгрупа, које одговарају различитим простим делиоцима $|G|$.*

✍ а) $\Longrightarrow$ б). Наравно, ако је G комутативна, онда је све јасно: свака подгрупа је нормална, па је нормализатор сваке подгрупе једнак целој групи и ако је подгрупа права, она не може бити једнака свом нормализатору.

Претпоставимо стога да G није комутативна. Приметимо да је $Z(G) \neq \{e\}$. Наиме, нека је G степена нилпотентности n, а како G није комутативна, мора бити $n > 1$ и морају постојати $a_0,\ldots,a_{n-1}$ такви да је $[\ldots[a_0,a_1],\ldots,a_{n-1}] \neq e$,

али да за све $x \in G$ важи: $[[\dots[a_0, a_1], \dots, a_{n-1}], x] = e$. То заправо значи да $[\dots[a_0, a_1], \dots, a_{n-1}] \in Z(G) \setminus \{e\}$, па центар није тривијалан.

Уколико $Z(G) \not\subseteq H$, постоји $x \in Z(G) \setminus H$, али, пошто је $Z(G) \subseteq N_G(H)$, закључујемо да је $x \in N_G(H) \setminus H$ и доказ је завршен.

У супротном, $Z(G) \subseteq H$ и радимо индукцијом по степену нилпотентности од G. База индукције се односи на ситуацију када је G комутативна и то смо објаснили. Посматрамо $\overline{G} = G/Z(G)$. Јасно је да је она мањег степена нилпотентности – погледати објашњење зашто је центар нилпотентне групе нетривијалан. Како је $\overline{H} = H/Z(G)$ права подгрупа од $\overline{G}$, на основу индуктивне хипотезе закључујемо да је $\overline{H}$ права подгрупа од $N_{\overline{G}}(\overline{H})$. Дакле, постоји $\bar{x} \in N_{\overline{G}}(\overline{H}) \setminus \overline{H}$, за неки $x \in G$. Имамо да је $\bar{x}\overline{H}\bar{x}^{-1} = \overline{H}$, али $\bar{x} \notin \overline{H}$. Из друге релације следи да $x \notin H$. Покажимо да $x \in N_G(H)$. Уколико то не би било тачно, постојао би $h \in H$ такав да $xhx^{-1} \notin H$. Но, $\bar{x}\bar{h}\bar{x}^{-1} \in \overline{H}$, што значи да је $\bar{x}\bar{h}\bar{x}^{-1} = \overline{h_1}$ за неки $h_1 \in H$. Дакле, важи једнакост (подсетимо се да је $\bar{a} = aZ(G)$): $(xhx^{-1})Z(G) = h_1Z(G)$, те је $xhx^{-1} \in h_1Z(G)$. Но, $Z(G) \subseteq H$, $h_1 \in H$, па је $h_1Z(G) \subseteq H$ и добили бисмо да $xhx^{-1} \in H$, а знамо да то није тачно. Закључујемо да $x \in N_G(H) \setminus H$, те је заиста H права подгрупа од $N_G(H)$.

б) $\Longrightarrow$ в). Нека је M максимална подгрупа од G. Посебно, она је права подгрупа од G. На основу б) она је права подгрупа свог нормализатора $N_G(M)$. Но, како је M максимална подгрупа од G, не може постојати подгрупа „између" M и G, те мора бити $N_G(M) = G$, па закључујемо да је $M \triangleleft G$.

в) $\Longrightarrow$ г). Доказано у последици 24.

г) $\Longrightarrow$ д). Доказано у последици 24.

д) $\Longrightarrow$ а). На основу става 30 имамо да је производ две нилпотентне и сама нилпотентна група. Јасно је да се индукцијом онда може показати да је производ коначно много нилпотентних нилпотентна група. Но, Силовљеве подгрупе групе G су p-групе за неке просте бројеве p, а на основу става 29 имамо да су све p-групе нилпотентне и резултат следи. ∎

Следећи став нам даје још један потребан и довољан услов да би коначна група била нилпотентна.

Став 32. *Нека је G коначна група. Она је нилпотентна ако и само ако свака два елемента, чији су редови узајамно прости бројеви, комутирају.*

✍ Претпоставимо најпре да је група G нилпотентна и нека је $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. На основу претходне теореме, имамо да је $G \cong P_1 \times \cdots \times P_k$, где је P_i Силовљева p_i-подгрупа. Ако су x и y елементи групе такви да је

$$\mathrm{NZD}(\omega(x), \omega(y)) = 1,$$

где се са $\omega(a)$ означава ред елемента $a \in G$, можемо, због поједностављења ознака, претпоставити да смо поређали просте бројеве p_i тако да је $\omega(x) = p_1^{\beta_1} \cdots p_r^{\beta_r}$, $\omega(y) = p_{r+1}^{\beta_{r+1}} \cdots p_k^{\beta_k}$, где је $0 \leqslant \beta_i \leqslant \alpha_i$. Ако са x', односно y' означимо елементе производа $P_1 \times \cdots \times P_k$, који одговарају елементима x и y при горњем изоморфизму, онда је јасно да је

$$x' = (u_1, \dots, u_r, e, \dots, e) \text{ и } y' = (e, \dots, e, u_{r+1}, \dots, u_k),$$

за неке $u_i \in P_i$. Но, тада је:

$$x' \cdot y' = (u_1, \ldots, u_r, e, \ldots, e) \cdot (e, \ldots, e, u_{r+1}, \ldots, u_k) = (u_1, \ldots u_r, u_{r+1}, \ldots, u_k)$$
$$= (e, \ldots, e, u_{r+1}, \ldots, u_k) \cdot (u_1, \ldots, u_r, e, \ldots, e) = y' \cdot x';$$

следи да је и $x \cdot y = y \cdot x$.

Обратно, ако претпоставимо да елементи узајамно простих редова комутирају, можемо да искористимо доказ последице 24. Наиме, ту смо користили чињеницу да су Силовљеве подгрупе нормалне да бисмо доказали да је f хомоморфизам и да му је језгро тривијално. Но, нормалност нам је служила баш за то да покажемо да елементи Силовљевих подгрупа, које одговарају различитим простим бројевима, комутирају, а то овде већ имамо по претпоставци. Стога доказ пролази и у овом случају. 📕

За крај овог одељка докажимо једну занимљиву чињеницу о коначним нилпотентним групама.

Став 33. *Нека је G коначна нилпотентна група реда n. Тада у G важи обрат Лагранжове теореме, тј. ако $d \mid n$, онда G садржи подгрупу реда d.*

✍ Нека је $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ и $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$ и нека су, као и горе, P_i Силовљеве p_i-подгрупе. На основу теореме 7 постоје $H_i \triangleleft P_i$ такве да је $|H_i| = p_i^{\beta_i}$. Тада је $H_1 \cdots H_k$ тражена подгрупа реда d. 📕

Фратинијева подгрупа

Све групе које овде разматрамо су коначне.

Дефиниција 34. *Нека је G (коначна) група. Фратинијева подгрупа, у ознаци $\Phi(G)$ дефинише се као пресек свих максималних подгрупа од G.* 👌

Дефиниција 35. *За елемент $x \in G$, иде је G група, кажемо да је* негенератор *уколико за сваки подскуп $X \subseteq G$ важи: $\langle X \rangle = G \Rightarrow \langle X \setminus \{x\} \rangle = G$.* 👌

Подсетимо да $\langle X \rangle$ означава подгрупу генерисану скупом X – то је најмања подгрупа која садржи X као свој подскуп. Видимо да се негенератор дефинише као елемент који се може изоставити из ма ког генераторног скупа групе, а да остатак и даље генерише групу. На пример, неутрал се може изоставити из сваког генераторног скупа.

Став 36. *Скуп свих негенератора у G једнак је $\Phi(G)$.*

✍ Претпоставимо да је $a \in G$ негенератор и H максимална подгрупа од G. Желимо да докажемо да је $a \in H$. Нека је $X = H \cup \{a\}$. Ако $a \notin H$, имамо да је $\langle X \rangle$ подгрупа од G, која садржи H као своју подгрупу, а садржи и елемент који не припада H, па је $H \subset \langle X \rangle$. Како је H максимална подгрупа, мора бити $\langle X \rangle = G$. Но, $\langle X \setminus \{a\} \rangle = \langle H \rangle = H \neq G$, што противречи претпоставци да је a негенератор. Закључујемо да $a \in H$. Како је H била произвољна максимална подгрупа од G, добијамо да $a \in \Phi(G)$.

Обратно, нека је $a \in \Phi(G)$. Желимо да докажемо да је a негенератор. У ту сврху, нека је $X \subset G$ подскуп који не садржи a и нека је $\langle X \cup \{a\} \rangle = G$. Докажимо да је тада и $\langle X \rangle = G$. У супротном, $\langle X \rangle$ је права подгрупа од G, па је она садржана

у неком максималној подгрупи $M < G$ (ознака $<$ овде означава праву подгрупу). Но, како $a \in \Phi(G) \subseteq M$, имамо да $a \in M$. То значи да је $X \cup \{a\} \subseteq M$, па мора бити $G = \langle X \cup \{a\} \rangle \subseteq M$, што је наравно немогуће. Тиме смо доказали да је a негенератор. 📕

Лема 37. $\Phi(G) \triangleleft G$.

✍ Довољно је да покажемо да је, за свако $x \in G$ и максималну подгрупу $M < G$, подгрупа xMx^{-1} такође максимална. Наравно, јасно је да $xMx^{-1} \neq G$, јер би из једнакости следило да је $M = G$. Зато је $xMx^{-1} \subseteq M'$ за неку максималну подгрупу $M' < G$. Но, тада добијамо да је $M \subseteq x^{-1}M'x$, те из чињенице да је M максимална подгрупа, следи да је $M = x^{-1}M'x$, те је $xMx^{-1} = M'$, тј. xMx^{-1} је максимална подгрупа. 📕

Следећа лема је веома занимљива и корисна.

Лема 38. *Ако је $H \leqslant G$, $H\Phi(G) = G$, онда је $H = G$.*

✍ Уколико је H права подгрупа од G, онда је она садржана у некој максималној подгрупи M. Но, и $\Phi(G) \subseteq M$, па добијамо $G = H\Phi(G) \subseteq MM = M$, што није могуће. Закључујемо да је $H = G$. 📕

Теорема 39. *$\Phi(G)$ је нилпотентна.*

✍ Уколико је $\Phi(G) = \{e\}$, немамо шта да доказујемо. Претпоставимо да је $\Phi(G) \neq \{e\}$. Докажимо да је свака Силовљева подгрупа од $\Phi(G)$ нормална. У ту сврху, нека је P Силовљева подгрупа од $\Phi(G)$. Како је $\Phi(G) \triangleleft G$, Фратинијев аргумент нам даје: $G = N_G(P)\Phi(G)$. Но, тада из леме 38 добијамо да је $N_G(P) = G$, па је P нормална. 📕

Следећа теорема, коју због недостатка времена нећемо доказивати, даје нам два нова критеријума за нилпотентност коначних група. Ознака G' означава комутаторску подгрупу од G, тј. подгрупу генерисану свим комутаторима. Том подгрупом ћемо се више бавити у наредном одељку.

Теорема 40. *Нека је G коначна група.*

а) G је нилпотентна акко је $G/\Phi(G)$ нилпотентна.

б)G је нилпотентна акко је $G' \leqslant \Phi(G)$. 📕

Решиве групе

Решиве групе су, као и нилпотентне, генерализација комутативних група. Видећемо да су, у случају коначних група, она мало више „удаљене" од комутативних, али да имају и нека додатна корисна својства, што их чини прилично значајном класом у оквиру класе свих коначних група. За почетак нека понављања из Алгебре 1, уз нешто ново.

Дефиниција 41. *Нека је G група. Дефинишемо* извод *групе G, у ознаци G' са:* $G' := \langle [x, y] : x, y \in H \rangle$. 👌

Користи се и ознака $[G, G]$ за ову подгрупу, као и термин комутаторска подгрупа.

Лема 42. *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 треће ставке следећег става.

Став 43. *а) Ако је $H \triangleleft G$, онда је и $H' \triangleleft G$.*

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

в) Ако је $N \triangleleft G$, онда је G/N комутативна ако и само ако $G' \subseteq N$.

✍ 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.

в) Нека су $x, y \in G$. Као и раније, означимо количничку групу G/N са $\overline{G}$ а класу елемента a са $\bar{a}$. Тада:

$$\begin{aligned} \overline{G} \text{ је комутативна акко } &(\forall x \in G)(\forall y \in G)([\bar{x},\bar{y}] = \bar{e}) \\ \text{акко } &(\forall x \in G)(\forall y \in G)(\overline{[x,y]} = N) \\ \text{акко } &(\forall x \in G)(\forall y \in G)([x,y] \in N) \\ \text{акко } &G' \subseteq N. \end{aligned}$$

■

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

Став 45. *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 46. 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 47. 👉Абелизација диедарске групе дата је са:

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

Погледати пример 1.79 у уџбенику.

Докажимо сада, као примену ових резултата, теорему која повезује три важне подгрупе сваке коначне групе: центар, комутаторску подгрупу и Фратинијеву подгрупу.

Теорема 48. *Ако је G коначна грӯпа, онда је $G' \cap Z(G) \leqslant \Phi(G)$.*

✍ Треба показати да је $G' \cap Z(G)$ подскуп сваке максималне подгрупе од G. Претпоставимо да то није тако, тј. да постоји максимална подгрупа H групе G тако да $G' \cap Z(G) \not\subseteq H$. Дакле, постоји $a \in (G' \cap Z(G)) \setminus H$. Како је $a \in Z(G)$, то је $\langle a \rangle \triangleleft G$, те је $\langle a \rangle H \leqslant G$. Но, H је максимална, $a \notin H$, те закључујемо да је

$$\langle a \rangle H = G. \tag{2}$$

Но, из ове једнакости и чињенице да је $a \in Z(G)$ добијамо да је $H \triangleleft G$. Наиме, ако је $g \in G$ произвољан елемент, онда постоје $m \in \mathbb{Z}$ и $h \in H$ тако да је $g = a^m h$.

Тада је

$$gH = a^m hH = a^m H = Ha^m = Hha^m = Ha^m h = Hg, \tag{3}$$

па је $H \triangleleft G$. Сада нам једнакост (3) показује да је G/H циклична са генератором aH – добили смо да за свако $g \in G$ постоји $m \in \mathbb{Z}$ тако да је $gH = a^m H = (aH)^m$. Но, како је G/H циклична, она је комутативна, па на основу става 43 добијамо да $G' \subseteq H$. Но, $a \in G'$, па бисмо добили да је $a \in H$ што противречи избору елемента a. Ова контрадикција завршава доказ. 📕

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 49. *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 50. *Група G је решива ако и само ако постоји опадајући низ подгрупа*

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n = \{e\}, \tag{4}$$

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 4. Како је $G/H_1 = H_0/H_1$ комутативна група, на основу става 43 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. 📕

Пример 51. 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 52. 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). Kako je grupa 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 53. *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 $n = \max\{n_1, \ldots, n_k\}$. 📕

Следећи став појашњава оно што смо на почетку рекли о вези између нилпотентних и коначних решивих група.

Став 54. *Свака коначна нилпотентна група је решива.*

✍️ На основу теореме 7 и теореме 53 имамо да је свака коначна p-група решива. Како је, по теореми 31 свака коначна нилпотентна група изоморфна директном производу решивих, тражено следи из става 53. 📕