АЛГЕБРА 2

Групе

Решиве групе

Зоран Петровић

27. март 2012.

Пажљив читалац би могао да примети да смо за сада доказали постојање Силовљевих p-подгрупа, као и подгрупа реда p (уколико прост број p дели ред групе G). Но, мада смо ми причали о свим p-подгрупама дате групе, ипак нисмо експлицитно показали да постоје p-подгрупе свих могућих редова. Нпр. ако је $|G| = p^5 m$, где p не дели m, ми знамо да у G постоје подгрупе реда p и реда p^5. Али, да ли заиста постоје подгрупе реда p^2, p^3 и p^4? Одговор је наравно потврдан, а доказаћемо и више од тога.

Пре свега, уведимо неке неопходне појмове.

За опадајући низ подгрупа

$$G = G_0 \supset G_1 \supset \cdots \supset G_m,$$

групе G кажемо да је нормалан низ уколико је $G_{i+1} \triangleleft G_i$ за све $i = \overline{0, m-1}$. Овај низ је Абелов уколико је нормалан и уколико је G_i/G_{i+1} Абелова група за све $i = \overline{0, m-1}$. Он је цикличан уколико је нормалан и уколико је G_i/G_{i+1} циклична група за све $i = \overline{0, m-1}$.

Дефиниција 1 Група G је решива уколико постоји Абелов низ

$$G = G_0 \supset G_1 \supset \cdots \supset G_m,$$

за који је $G_m = \{e\}$.

Приметимо да је решива група једна генерализација Абелове групе. Профињење низа

$$G = G_0 \supset G_1 \supset \cdots \supset G_m,$$

је низ који се добија „уметањем" нових подгрупа између већ постојећих у низу. Важи следећи став.

Став 2 Нека је G коначна група. Тада за сваки Абелов низ

$$G = G_0 \supset G_1 \supset \cdots \supset G_m,$$

постоји профињење, које је цикличан низ.

Доказ. Ово заправо није тешко доказати. Све се своди на следеће. Нека је G група и H њена нормална подгрупа тако да је G/H коначна комутативна група. Тада постоји цикличан низ подгрупа

$$G = G_0 \supset H_1 \supset \cdots \supset H_k = H. \qquad (*)$$

Уметањем оваквих низова између сваке две групе у почетном низу, добија се тражено циклично профињење.

Докажимо егзистенцију наведеног цикличног низа. Заправо доказујемо да постоји цикличан низ који почиње групом $G' = G/H$ и завршава се тривијалном групом. „Подизањем" овог низа до групе G завршавамо доказ. Радимо индукцијом по реду групе G'. Узмимо ма који елемент $x' \in G'$. Уколико је $G' = \langle x' \rangle$, доказ је готов. У супротном, група $G'/\langle x' \rangle$ је коначна комутативна група мањег реда од G'. По индуктивној претпоставци, постоји цикличан низ

$$G'/\langle x' \rangle = K_0'' \supset K_1'' \supset \cdots \supset K_l'',$$

при чему је $K_l' = \{\langle x' \rangle\}$ тривијална подгрупа од $G'/\langle x' \rangle$ (шта је неутрал у количничкој групи?). Налажењем инверзних слика подгрупа овог низа при канонском епиморфизму $p : G' \to G'/\langle x' \rangle$, добијамо нормалан низ

$$G/H = G' = K_0' \supset K_1' \supset \cdots \supset K_l', \qquad (**)$$

за који је $K_i'/K_{i+1}' \cong K_i''/K_{i+1}''$, а то су све цикличне групе. Наравно, група K_l' је циклична са генератором $x'(= xH)$. Налажењем инверзних слика при канонском епиморфизму $\pi : G \to G/H(= G')$ подгрупа у низу $(**)$ добијамо тражени цикличан низ $(*)$. □

Напомена. У овом доказу користимо следећи резултат: ако је $f\colon K \to L$ епиморфизам група и ако су L_1 и L_2 подгрупе од L при чему је $L_1 \triangleleft L_2$, онда је и $f^{-1}[L_1] \triangleleft f^{-1}[L_2]$ и $f^{-1}[L_2]/f^{-1}[L_1] \cong L_2/L_1$. Докажимо га.

Да бисмо поједноставили запис, уведимо ознаке $K_i = f^{-1}[L_i]$. Нека су $x \in K_2$ и $y \in K_1$ произвољни елементи. Треба проверити да $xyx^{-1} \in K_1 = f^{-1}[L_1]$. Но, $f(xyx^{-1}) = f(x)f(y)f(x)^{-1}$. Како $y \in K_1 = f^{-1}[L_1]$, то $f(y) \in L_1$, а како је $L_1 \triangleleft L_2$, то и $f(x)f(y)f(x)^{-1} \in L_1$, што је и требало показати. Приметимо да овде нисмо користили чињеницу да је f „на".

За доказ траженог изоморфизма $K_2/K_1 \cong L_2/L_1$, посматрајмо композицију рестрикције хомоморфизма f на K_2 и природног епиморфизма $p\colon L_2 \to L_2/L_1$:

$$K_2 \xrightarrow{f|_{K_2}} L_2 \xrightarrow{p} L_2/L_1.$$

Означимо је са g. Јасно је да је g „на" (пошто су оба хомоморфизма у композицији таква), док је такође лако проверити да је $\mathrm{Ker}(g) = K_1$. Прва теорема о изоморфизму завршава доказ. ◇

Следећи став разрешава претходно споменута неразјашњена питања.

Став 3 Свака p-група је решива.

Доказ. Нека је G једна p-група. Радимо индукцијом по реду групе. Свака p-група има нетривијалан центар. Група $G/Z(G)$ је такође p-група и њен ред је мањи од реда групе G. По индуктивној хипотези, постоји Абелов низ подгрупа

$$G/Z(G) = G_0' \supset G_1' \supset \cdots \supset G_m' = \{Z(G)\}.$$

Подизањем овог низа помоћу канонског епиморфизма добијамо Абелов низ

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = Z(G).$$

Како је $Z(G)$ Абелова група, то можемо додати тривијалну групу на крај, што показује да је група G решива. □

Зашто овај став разрешава раније постављена питања? Како је свака p-група решива, то свака p-група има и цикличан низ. Но, свака циклична група има (тачно) једну подгрупу за сваки делилац реда те групе. То значи да заправо за сваку p-групу G постоји опадајући низ нормалних подгрупа

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset \{e\}.$$

при чему је G_i/G_{i+1} циклична група реда p (размислите зашто). Но, тада следи да, ако је $|G| = p^n$, онда је $|G_i| = p^{n-i}$, те у p-групи постоје подгрупе свих могућих редова. Резултат за произвољну коначну групу добијамо применом чињенице да Силовљева p-подгрупа увек постоји.

Следећи став је веома важан у применама теорије група на проблем решивости алгебарских једначина.

Став 4 Група $\mathbb{S}_n$ није решива ако је $n \geq 5$.

Доказ. Подсетимо се два позната резултата:

1. $[\mathbb{S}_n, \mathbb{S}_n] = A_n$
2. Ако је H нормална подгрупа групе G и G/H комутативна, онда је $[G, G] \subseteq H$.

Претпоставимо да је $n \geq 5$ и да је $\mathbb{S}_n$ решива група. Посебно, то значи да постоји нормална подгрупа H од $\mathbb{S}_n$ таква да је $\mathbb{S}_n/H$ Абелова. Но, према 2. то значи да $[S_n, S_n] \subseteq H$, а према 1. да је $A_n \subseteq H$. Дакле, ако је $\mathbb{S}_n/H$ нетривијална, мора бити $H = A_n$.

Докажимо да је за $n \geq 5$: $[A_n, A_n] = A_n$. Ово заправо није тешко доказати. Наиме,

$$(abc)(cde)(abc)^{-1}(cde)^{-1} = (adc),$$

где су a, b, c, d, e међусобно различити. Дакле, сваки 3-цикл можемо добити као комутатор нека друга два 3-цикла, па, како је A_n генерисано 3-циклима, добијамо да је $[A_n, A_n] = A_n$.

Сада је јасно зашто $\mathbb{S}_n$ не може бити решива. Наиме, Абелов низ почиње са: $\mathbb{S}_n \supset A_n$ и поставља се питање како га наставити. Ако је K нормална подгрупа од A_n таква да је A_n/K Абелова група, онда $[A_n, A_n] \subseteq K$, но, како је $[A_n, A_n] = A_n$, то мора бити $K = A_n$ и не можемо наставити наш низ. Како A_n није комутативна, добијамо да $\mathbb{S}_n$ није решива група. □

Групе $\mathbb{S}_n$ за $n \leq 4$ јесу решиве. Уколико је $n = 4$, онда је Абелов низ дат са: $\mathbb{S}_4 \supset A_4 \supset V \supset \{(1)\}$, пошто је Клајнова група V Абелова. Остали случајеви су још лакши. Чињеница да су ове групе решиве омогућава решавање једначина другог, трећег и четвртог степена „у радикалима“, али то је прича за касније.

Урадимо за крај неколико примера.

Пример 5 Свака група реда pq, где су p и q прости бројеви, је решива.

Решење. Наравно, једино је занимљив случај када је $p \neq q$ (зашто?). Но, и он је лак. Нека је $|G| = pq$ и $p < q$. На основу Кошијеве теореме, у групи G постоји елемент x реда q. Ако је H подгрупа генерисана са x, онда је $[G : H] = p$, а како је p најмањи прост број који дели ред групе G, H мора бити нормална. Стога Абелов (заправо и цикличан) низ: $G \supset H \supset \{e\}$ показује да је група G решива. ♣

Пример 6 Свака група реда p^2q, где су p и q прости бројеви, је решива.

Решење. И овде имамо нешто ново само ако је $p \neq q$.

1. $p > q$. Ако са s_p означимо број Силовљевих p-подгрупа од G, онда знамо да је $s_p \equiv 1 \pmod{p}$ и да $s_p \mid q$. Но, ако је $s_p = q$, онда $p \mid (q-1)$, што није могуће, јер је $p > q$. Стога је $s_p = 1$ и једина Силовљева p-подгрупа је нормална. Ако је означимо са H, добијамо Абелов низ: $G \supset H \supset \{e\}$. Наиме, G/H је реда q, па је циклична, а H је, као група реда p^2 комутативна.

2. $p < q$. Знамо да је $s_q \equiv 1 \pmod{q}$ и да $s_q \mid p^2$. Уколико је $s_q = 1$, поступамо као у претходном случају. Претпоставимо да је $s_q \neq 1$.

а) $s_q = p$. Тада $q \mid (p-1)$, што није могуће, јер је $q > p$.

б) $s_q = p^2$. То значи да $q \mid (p^2-1)$, тј. $q \mid (p-1)(p+1)$. Како је q прост број, то $q \mid (p-1)$, или $q \mid (p+1)$. Пошто је $q > p$, мора бити $q \mid (p+1)$, али и то је могуће једино у случају да је $q = p+1$. С обзиром да су p и q прости бројеви, мора бити $p = 2$, $q = 3$. Дакле, наша група G је реда 12. Осим тога, $s_3 = 4$. Уколико је $s_2 = 1$, добијамо Абелов низ, стога претпостављамо да је $s_2 = 3$. Нека су H_1, H_2, H_3, H_4 Силовљеве 3-подгрупе. Како је $H_i \cap H_j = \{e\}$, за $i \neq j$, то добијамо да је $|H_1 \cup H_2 \cup H_3 \cup H_4| = 4 \cdot 2 + 1 = 9$. Нека су K_1, K_2, K_3 Силовљеве

2-подгрупе. С обзиром да је $|K_i| = 4$, то у $K_1 \cup K_2$, сем неутрала, има бар још $4+4-2 = 6$ елемената. Тако смо добили да у нашој групи има бар 15 елемената. Како је она реда 12, то смо дошли до контрадикције и тиме је доказ завршен. ♣

Пример 7 Свака група реда $2pq$, где су p и q прости бројеви, је решива.

Решење. Јасно је да имамо нешто ново само уколико су p и q различити непарни прости бројеви. Нека је $p < q$.

Уколико је $s_p = 1$, или $s_q = 1$, све је јасно. Наиме, тада је једна од Силовљевих подгрупа нормална, те је и производ те Силовљеве подгрупе и Силовљеве подгрупе, која одговара другом простом броју такође подгрупа, а како је индекса 2, та подгрупа је нормална. Тако добијамо Абелов низ: $G \supset HK \supset H \supset \{e\}$ (где смо са H и K означили одговарајуће Силовљеве подгрупе). Дакле, у даљем претпостављамо да је $s_p \neq 1$ и $s_q \neq 1$. Како је $p < q$, мора бити $s_q = 2p$ (зашто?). Нека су $H_1, \ldots, H_{2p}$ Силовљеве q-подгрупе. У њиховом унији има (сем неутрала) $2p(q-1)$ елемената. Како је $s_p > 1$ по претпоставци, то има бар q Силовљевих p-подгрупа. Означимо их са $K_1, \ldots, K_q$. У њима сем неутрала има $q(p-1)$ елемената. Закључујемо да у унији $H_1 \cup \ldots \cup H_{2p} \cup K_1 \ldots \cup K_q$ има $2p(q-1)+q(p-1)+1$ елемената. Остављамо читаоцима за вежбу да докажу да је $2p(q-1)+q(p-1)+1 > 2pq$, те смо тако добили контрадикцију. ♣