АЛГЕБРА 2

Групе

Теореме Силова

Зоран Петровић

17. март 2012.

Нека је G група и H нека њена подгрупа. Уочимо скуп X свих подгрупа од G конјугованих са H.

$$X = \{gHg^{-1} : g \in G\}.$$

На овом скупу G дејствује конјуговањем:

$$g \cdot (xHx^{-1}) := (gx)H(gx)^{-1}.$$

Јасно је да је ово дејство транзитивно (има само једну орбиту), док је стабилизатор подгрупе H подгрупа од G, која се зове нормализатор подгрупе H и означава са $N(H)$:

$$N(H) = \{g \in G : gHg^{-1} = H\}.$$

Својства нормализатора дата су у следећем ставу.

Став 1 1. $H \triangleleft N(H)$.

2. Ако је $K \leq G$ и $H \triangleleft K$, онда је $K \subseteq N(H)$.

3. Ако је $K \leq N(H)$, онда је $KH \leq G$, $H \triangleleft KH$ и $KH/H \cong K/(H \cap K)$.

Доказ. 1. Ово директно следи из дефиниције нормализатора.

2. Претпоставимо да је K подгрупа од G таква да је $H \triangleleft K$ и $k \in K$. Како је $H \triangleleft K$, то је $kHk^{-1} = H$, а то управо значи да је $k \in N(H)$. Дакле, $K \subseteq N(H)$.

3. Јасно је да $e \in KH$. Нека $x, y \in KH$. То значи да је $x = kh$ и $y = k_1h_1$, за неке $k, k_1 \in K$ и $h, h_1 \in H$. Тада је

$$x^{-1}y = (kh)^{-1}(k_1h_1) = h^{-1}k^{-1}k_1h_1.$$

Како је $zHz^{-1} = H$ за све $z \in K$, то значи да је и $Hz = zH$ за све $z \in K$. Посебно: $h^{-1}(k^{-1}k_1) = (k^{-1}k_1)h'$ за неки $h' \in H$. Стога је

$x^{-1}y = (k^{-1}k_1)(h'h_1)$, па $x^{-1}y \in KH$. Закључујемо да је KH заиста подгрупа од G. Но, H је очигледно садржана у KH и лако је проверити да је H нормална подгрупа од KH. Нека $k \in K$ и $h \in H$. Тада:

$$\begin{aligned}(kh)H(kh)^{-1} &= k(hHh^{-1})k^{-1} \\ &= kHk^{-1} \text{ (јер је } hH = H = Hh^{-1}) \\ &= H \text{ (јер } k \in N(H)).\end{aligned}$$

Изоморфизам $KH/H \cong K/(H \cap K)$ доказује се на исти начин на који се доказује такав изоморфизам у доказу друге теореме о изоморфизму (ово је заправо једна општија формулација те теореме). □

Сваку коначну групу чији је ред степен простог броја p зовемо p-група. Сетимо се да смо раније доказали да свака нетривијална p група има нетривијалан центар. То ћемо користити у даљем раду.

Сада ћемо дати неке теореме које више говори о структури коначних група, но што су то дали досадашњи резултати. Подсетимо се Кошијеве теореме: уколико $p \mid |G|$, где је p прост број, онда у G постоји елемент реда p. Заправо можемо закључити доста више од тога о постојању p-подгрупа у групи G уколико p дели ред те групе.

Дефиниција 2 Нека је група G реда n. Уколико је $n = p^r m$, где p не дели m (дакле, уколико је p^r највећи степен броја p који дели ред групе G), онда подгрупу групе G реда p^r (уколико она постоји) зовемо Силовљевом p-подгрупом групе G.

Испоставља се да Силовљева p-подгрупа увек постоји. То је садржај следеће теореме.

Теорема 3 Нека је G коначна група. За сваки прост број p који дели ред групе G постоји Силовљева p-подгрупа те групе.

Доказ. Нека је p прост број и нека $p \mid |G|$. Уколико је $|G| = p$, резултат је тривијалан. Доказ изводимо индукцијом по $|G|$. Базу индукције смо урадили. Претпоставимо да је $|G| = n$ и да је тврђење тачно за све групе са мање од n елемената. Разматрамо два случаја.

1. У G постоји права подгрупа H чији индекс није дељив са p. Како је $|H| < |G|$, то постоји Силовљева p-подгрупа од H. Но, највећи степен од p који дели ред групе G исти је као и највећи степен од p који дели $|H|$: $|G| = |H|[G : H]$, а p не дели $[G : H]$. Стога је Силовљева p-подгрупа од H заправо и Силовљева p-подгрупа од G. Дакле, у овом случају она постоји.

2. Претпоставимо сада да p дели индекс сваке праве подгрупе од G. Уколико G дејствује на самој себи конјуговањем, онда су орбите при том дејству класе коњугованости елемената из G, а унија једночланих орбита једнака је центру те групе (подсетите се доказа нетривијалности центра p-групе, који је урађен у Алгебри 1):

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

при чему је $C_i = \Omega(x_i) = [G : G_{x_i}]$. Како p по претпоставци дели индекс сваке праве подгрупе, добијамо да $p \mid |C_i|$ за све i. Закључујемо да $p \mid |Z(G)|$ (посебно: $Z(G) \neq \{e\}$). Према Кошијевој теореми, у $Z(G)$ постоји елемент реда p. Означимо га са x. Подгрупа $H = \langle x \rangle$ је нормална у G пошто $x \in Z(G)$, па комутира са свим елементима из G. Тада је $|G/H| = \frac{n}{p} < n = |G|$. По индуктивној хипотези у G/H постоји Силовљева p-подгрупа. Означимо је са K'. Уочимо канонски епиморфизам $\pi : G \to G/H$, $\pi(g) = gH$. Није тешко проверити да је $K = \pi^{-1}[K']$ подгрупа од G (проверите!). Но, K садржи H (зашто?) и заправо је $K/H = K'$ (уколико K/H видимо као подскуп од G/H). Стога је $|K| = p|K'|$ и како је и $|G| = p|G/H|$, а K' је Силовљева p-подгрупа од G/H, то је K Силовљева p-подгрупа од G. □

Напомена 1. У овом доказу смо користили Кошијеву теорему. Но, заправо смо могли и без ње. Наиме, једино нам је био потребан резултат да свака коначна Абелова група чији је ред дељив са p (радило се о центру групе G) садржи елемент реда p. А та се чињеница лако доказује помоћу класификације коначних Абелових група, коју смо урадили у Алгебри 1.

Дакле, показали смо да Силовљеве p-подгрупе увек постоје. Пре него што наставимо, докажимо једну техничку лему.

Лема 4 Нека p-група H дејствује на коначном скупу X. Тада је

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

где је са X^G означен скуп фиксних тачака од G:

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

Доказ. Како је ред орбите једнак индексу стабилизатора елемента те орбите, и како је група која дејствује једна p-група, то је број елемената у свакој неједночланој орбити дељив са p. Унија једночланих орбита је заправо скуп фиксних тачака X^G. Дакле,

$$|X| = |X^G| + |\Omega_1| + \cdots + |\Omega_k|$$

. где $p \mid |\Omega_i|$ за све $i = \overline{1,k}$. Следи да је $|X| - |X^G|$ заиста дељиво са p.□

Теорема 5 Нека је G коначна група.

1. Свака p-подгрупа од G садржана је у некој Силовљевој p-подгрупи од G.
2. Све Силовљеве p-подгрупе од G су међусобно конјуговане.
3. Број Силовљевих p-подгрупа од G конгруентан је са 1 по модулу p.
4. Број Силовљевих подгрупа дели ред групе G.

Доказ. 1. Нека је H нека p-подгрупа од G и P Силовљева p-подгрупа. Размотримо најпре случај када је $H \subseteq N(P)$. Према доказаном ставу добијамо да је HP подгрупа од G (заправо је HP подгрупа од $N(P)$ – размислите зашто) и $[HP : P] = [H : H \cap P]$. Уколико је $[H : H \cap P] \neq 1$, с обзиром да је H једна p-подгрупа, добијамо да је и HP једна p-подгрупа и да је $|HP| > |P|$, што није могуће с обзиром да је P Силовљева p-подгрупа. Закључујемо да је $[H : H \cap P] = 1$, те је $H = H \cap P$, па је $H \subseteq P$. Дакле, у овом случају смо добили тражени резултат.

Посматрамо сада скуп S свих конјугата од P. Нека G дејствује на S конјуговањем. Добијамо да је $|S| = [G : N(P)]$ (погледајте почетак предавања и присетите се да је број елемената у орбити индекс стабилизатора). Како је $P \subseteq N(P)$ и P је Силовљева p-подгрупа, то $[G : N(P)]$ није дељиво са P (уколико $H \subseteq K \subseteq G$, то је $[G : H] = [G : K] \cdot [K : H]$ за коначну групу G и њене подгрупе K и H – доказ касније!), те ни $|S|$ није дељиво са p.

Нека сада H дејствује на S конјуговањем. На основу леме, $|S| \equiv |S^H| \pmod{p}$. Како p не дели $|S|$, то p не дели ни $|S^H|$. То посебно значи да $S^H \neq \emptyset$. Нека је $Q \in S^H$. То значи да је $hQh^{-1} = Q$, па је $H \subseteq N(Q)$. На основу првог дела доказа, закључујемо да је $H \subseteq Q$. Како је Q подгрупа конјугована подгрупи P, она је и сама Силовљева p-подгрупа (има исти број елемената као и P), а то значи да је заиста p-подгрупа H садржана у некој Силовљевој p-подгрупи Q.

2. Ово смо заправо већ доказали. Наиме, ако у претходном доказу за H узмемо неку Силовљеву p-подгрупу, видимо да смо доказали да је $H \subseteq Q(= xPx^{-1})$. Како је $|H| = |P|$, то добијамо да је $H = xPx^{-1}$. Дакле, S је заправо скуп свих Силовљевих p-подгрупа.

3. Нека је поново H нека Силовљева p-подгрупа, која дејствује на S конјуговањем. Свакако $H \in S^H$. Претпоставимо да $K \in S^H$. То значи да је $hKh^{-1} = K$ за све $k \in H$, па је $H \subseteq N(K)$. На основу првог дела доказа добијамо да је $H \subseteq K$, па мора бити $H = K$. Дакле, $S^H = \{H\}$. Тада, помоћу леме, добијамо да је $|S| \equiv 1 \pmod{p}$ што и завршава доказ.

4. Број Силовљевих подгрупа једнак је индексу нормализатора било које од њих, те стога дели ред групе G. □

Напомена 2. У доказу смо користили следећи резултат. Ако је K подгрупа од H коначног индекса $[H : K]$ и H подгрупа од G коначног индекса $[G : H]$, онда је

$$[G : K] = [G : H] \cdot [H : K].$$

Докажимо га.

Пре свега, нека је $[G : H] = m$ и $[H : K] = n$. Показаћемо да је $[G : K] = mn$. Како је $[G : H] = m$, то постоје елементи $g_1, g_2, \ldots, g_m \in G$ такви да је

$$G = g_1H \sqcup g_2H \sqcup \ldots \sqcup g_mH. \tag{1}$$

Такође постоје и елементи $h_1, h_2, \ldots, h_n \in H$ за које је

$$H = h_1K \sqcup h_2K \sqcup \ldots \sqcup h_nK. \tag{2}$$

Заменом (2) у (1), добијамо

$$G = g_1h_1K \cup g_1h_2K \cup \ldots \cup g_1h_nK \cup \ldots \cup g_mh_1K \cup g_mh_2K \cup \ldots \cup g_mh_nK. \tag{3}$$

Ако покажемо да су скупови у наведеној унији различити (подсетимо се да су различити косети обавезно дисјунктни), доказ ће бити завршен. Но, заиста је тако. Наиме, претпоставимо да је

$$g_ih_jK = g_kh_lK, \tag{4}$$

за неке индексе i, j, k, l. Тада је и

$$g_ih_jKH = g_kh_lKH,$$

а како је $KH = H$ (зашто?), то мора бити

$$g_ih_jH = g_kh_lH,$$

па је

$$g_iH = g_kH.$$

Но, то је могуће једино ако је $i = k$. Множењем (4) слева са g_i^{-1} добијамо

$$h_jK = h_lK,$$

но то је могуће једино ако је $j = l$.

Напомена 3. Нека је $|G| = p^rm$, где p не дели m. Ако са s_p означимо број Силовљевих p-подгрупа, онда, на основу претходне теореме, знамо да је $s_p \equiv 1 \pmod{p}$ и да $s_p \mid |G|$. Но, из чињенице $s_p \equiv 1 \pmod{p}$ следи да $s_p \mid m$.