Математичка гимназија

МАТУРСКИ РАД

-из математике-

Теорија група

Ученик:
Ђорђе Јовановић IVa

Ментор:
Сандра Андрић

Београд, мај 2023.

Садржај

1

Увод

Теорија група је област чије јасне почетке можемо наћи у неколико различитих грана математике, од којих се најранији налазе у класичној алгебри. Из класичне алгебре прве идеје потичу од Лагранжа[1] који је посматрао пермутације да би тражио корене полинома. На његов рад су се после надовезали и напредовали Абел[2] и Галоа[3], од који је Галоа први у чијем се раду помиње термин група у контексту сличном данашњој дефиницији.

У овом раду ћемо се бавити основама теорије група. Прво ћемо дефинисати групу, доказати основна својства која следе директно из дефиниције, дефинисати ред елемента као и појам хомоморфизма група. Потом ћемо дефинисати појам подгрупе, као и доказати критеријум којим утврђујемо да ли је подскуп подгрупа. У овом раду је стављен фокус на проучавање и својства количничких група и нормалних подгрупа, којима се бавимо у трећем поглављу. Доказујемо Лагранжову теорему и на крају наводимо и доказујемо теореме о изоморфизму.

[1]француско-италијански математичар Ј. Л. Лагранж (1736 - 1813).
[2]норвешки математичар Н. Х. Абел (1802 - 1829).
[3]француски математичар Е. Галоа (1811 - 1832).

2

Основни појмови и тврђења

Дефиниција 2.1.

(1) *Бинарна операција* $\star$ на скупу G је функција $\star : G \times G \to G$. За свако $a, b \in G$ пишемо $a \star b$ уместо $\star(a, b)$.

(2) Бинарна операција $\star$ на скупу G је *асоцијативна* ако за свако $a, b, c \in G$ важи $a \star (b \star c) = (a \star b) \star c$.

(3) Бинарна операција $\star$ на скупу G је *комутативна* ако за свако $a, b \in G$ важи $a \star b = b \star a$.

Дефиниција 2.2. *Група* је уређени пар $(G, \star)$ скупа G и бинарне операције $\star$ над скупом G тако да су задовољене следеће аксиоме:

(i) $a \star (b \star c) = (a \star b) \star c$ за свако $a, b, c \in G$, односно $\star$ је асоцијативна,

(ii) постоји елемент $e \in G$ који називамо *неутрал*, тако да за свако $a \in G$ важи $a \star e = e \star a = a$,

(iii) за свако $a \in G$ постоји елемент $a^{-1} \in G$, који називамо *инверзом* елемента a, тако да важи $a \star a^{-1} = a^{-1} \star a = e$.

За групу кажемо да је абелова ако задовољава аксиому:

(iiii) $a \star b = b \star a$ за свако $a, b \in G$.

За групу $(G, \star)$ ћемо рећи да је група G са операцијом $\star$. Из аксиоме (ii) се може закључити да је група увек непразна. За групу G кажемо да је *коначна* група када је скуп G коначан.

Пример 2.1. 1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ и $\mathbb{C}$ са операцијом $+$ су групе, са $e = 0$, $a^{-1} = -a$, за свако a.

2. $\mathbb{Q}\setminus\{0\}, \mathbb{R}\setminus\{0\}, \mathbb{C}\setminus\{0\}, \mathbb{R}^+, \mathbb{Q}^+$ су групе са операцијом множења, са $e=1$, $a^{-1}=\dfrac{1}{a}$, за свако a.

3. Скуп класа еквиваленције остатака при дељењу са n, $\mathbb{Z}/n\mathbb{Z}$ са операцијом сабирања класа остатака $+$ је група. Неутрал ове групе је елемент $\overline{0}$, а за свако $a\in\mathbb{Z}/n\mathbb{Z}$ инверзни елемент од $\overline{a}$ је $\overline{-a}$.

4. Нека је n позитиван цео број и нека је T скуп $\{1,2,\ldots,n\}$. Нека је S_n скуп свих пермутација скупа T (односно бијекција из T у T). Како је композиција две бијективне функције такође бијекција, S_n је затворено при операцији композиција функција. Композиција функција је асоцијативна, и свака бијекција има инверзну функцију при композицији. Пермутација која слика сваки елемент у себе самог је неутрал групе S_n и S_n зовемо *симетричном групом*. Ред групе S_n је $n!$.

5. Прошли пример можемо лако генерализовати. Нека је T неки непразни скуп. Нека је $A(T)$ скуп свих пермутација скупа T (свих бијекција из T у T). Све аргументе коришћене за S_n можемо користити и за $A(T)$ и показују нам да је $A(T)$ група са операцијом композиција функција.

Тврђење 2.1. Ако је G група са операцијом $\star$ онда важи следеће:

(1) неутрал групе G је јединствен,

(2) за свако $a\in G$, a^{-1} је једнозначно одређено,

(3) $(a^{-1})^{-1}=a$ за свако $a\in G$,

(4) $(a\star b)^{-1}=(b^{-1})\star(a^{-1})$

(5) за $a_1,a_2,\ldots,a_n\in G$, вредност израза $a_1\star a_2\star\cdots\star a_n$ не зависи од тога како поставимо заграде (важи општи асоцијативни закон).

Доказ.

(1) Ако су i и j неутрали онда по аксиоми (ii) дефиниције групе важи $i\star j=i$ (узмимо $a=i$ и $e=j$). По истој аксиоми је и $i\star j=j$ (узмимо $a=j$ и $e=i$). Онда је $i=j$, па је неутрал јединствен.

(2) Нека су a' и a'' инверзи елемента a и нека је e неутрал групе G. По аксиоми (iii), $a \star a' = e$ и $a'' \star a = e$. Онда је

$$\begin{aligned} a'' &= a'' \star e \\ &= a'' \star (a \star a') \\ &= (a'' \star a) \star a' \\ &= e \star a' \\ &= a' \end{aligned}$$

(3) Да бисмо показали да је $(a^{-1})^{-1} = a$ показаћемо да је a инверз елемента a^{-1}. Из дефиниције групе можемо видети да a задовољава сва својства инверза за елемент a^{-1}, па је a његов инверз.

(4) Нека је $c = (a \star b)^{-1}$, па је по дефиницији $(a \star b) \star c = e$. По асоцијативном закону је

$$a \star (b \star c) = e.$$

Множењем са леве стране са a^{-1} добијамо

$$a^{-1} \star (a \star (b \star c)) = a^{-1} \star e.$$

Применом асоцијативног закона на левој страни и по дефиницији e добијамо

$$\begin{aligned} (a^{-1} \star a) \star (b \star c) &= a^{-1} \\ e \star (b \star c) &= a^{-1} \\ b \star c &= a^{-1} \end{aligned}$$

Множењем са b^{-1} на левој страни и применом асоцијативног закона и дефиниција се добије

$$\begin{aligned} b^{-1} \star (b \star c) &= b^{-1} \star a^{-1} \\ (b^{-1} \star b) \star c &= b^{-1} \star a^{-1} \\ e \star c &= b^{-1} \star a^{-1} \\ c &= b^{-1} \star a^{-1} \end{aligned}$$

што је и тврђено.

(5) Индукцијом по n.

База: $n = 1$: $(a) = a$ $n = 2$: $((a_1)\star(a_2)) = (a_1\star a_2$ $n = 3$: по дефиницији групе и остатку базе $((a_1 \star a_2) \star a_3) = (a_1 \star (a_2 \star a_3)) = a_1 \star a_2 \star a_3$.

Индуктивна хипотеза: За свако $k \leq n$ било каква поставка заграда израза $b_1 \star b_2 \star \cdots \star b_k$ се може редуковати на $b_1 \star (b_2 \star (b_3 \star (\cdots \star b_k)) \cdots)$.

Индуктивни корак: Било која поставка заграда на израз $a_1 \star a_2 \star a_3 \star \cdots a_n$ мора поделити израз на два подизраза, $(a_1 \star a_2 \star \cdots \star a_k) \star (a_{k+1} \star a_{k+2} \star \cdots \star_n)$ где сваки од њих има постављене заграде на неки начин. Применом индуктивне хипотезе на ова два подизраза и редукувањем добијамо израз облика $a_1 \star (a_2 \star (b_3 \star (\cdots \star a_n)) \cdots)$ □

За групе у којима није потребно експлицитно навести операцију сматраћемо да је операција $\cdot$ и за $a \cdot b$ ћемо писати ab. За неку групу G и $x \in G$, $n \in \mathbb{Z}^+$ производ $xx \cdots x$ (n чланова) ћемо писати као x^n, а производ $x^{-1}x^{-1} \cdots x^{-1}$ (n чланова) као x^{-n} . Нека је $x^0 = e$.

Тврђење 2.2. Нека је G група са операцијом $\star$ и $a, b \in G$. Леви и десни закон скраћивања важе у G, односно:

(1) ако је $au = av$ онда је $u = v$ и,

(2) ако је $ub = vb$ онда је $u = v$.

Доказ. Множењем израза $au = av$ са a^{-1} са леве стране и применом закона асоцијативности и дефиниција лако се добије $u = v$. Слично се доказује и десни закон скраћивања. □

Дефиниција 2.3. За групу G и елемент $x \in G$ *ред елемента* x дефинишемо као најмањи позитиван цео број n тако да је $x^n = e$,у ознаци $|x| = n$. За елемент x кажемо да је реда n. Ако не постоји позитиван цео број који испуњава овај услов ред елемента x је бесконачно и x је бесконалног реда.

Пример 2.2.

1. Елемент групе је реда 1 ако и само ако је он неутрал те групе.

2. У адитивним групама $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ и $\mathbb{C}$ сваки елемент различит од нуле је бесконачног реда.

Сада ћемо увести појмове који нам помажу да поредимо структуре две групе.

Дефиниција 2.4. Нека су $(G, \star)$ и $(H, \diamond)$ групе. Пресликавање $\varphi : G \to H$ такво да за свако $x, y \in G$ важи

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y)$$

зове се *хомоморфизам*.

Када операције у групама G и H нису експлицитно дате услов хомоморфизма пишемо као

$$\varphi(xy) = \varphi(x)\varphi(y)$$

где је производ xy са леве стране рачунат у G, а производ $\varphi(x)\varphi(y)$ са десне стране рачунат у H.

Дефиниција 2.5. Пресликавање $\varphi : G \to H$ зовемо *изоморфизмом* и групе G и H су *изоморфне* у ознаци $G \cong H$ ако је

(1) φ хомоморфизам, и

(2) φ бијекција,

3

Подгрупе

Једна од метода изучавања структура математичких објеката који су дефинисани неким скупом аксиома је проучавање подскупова тог објекта за који важи исти скуп аксиома. У проучавању група овакви подскупови се зову *подгрупе*.

Дефиниција 3.1. Нека је G група. Подскуп H групе G је *подгрупа* групе G, у ознаци $H \leq G$, ако H формира групу са операцијом групе G.

Како су неутрал и инверз елемента јединствени и једнозначно одређени у G, јасно је да су неутрал групе G и подгрупе H исти, као и да је инверз елемента $a \in H$ у H исти као његов инверз у G.

Пример 3.1.

1. $\mathbb{Z} \leq \mathbb{Q}$ и $\mathbb{Q} \leq \mathbb{R}$ са операцијом сабирања.
2. Свака група има две подгрупе, $H = G$ и $H = \{e\}$, где другу зовемо тривијалном подгрупом и обележавамо је само са e.
3. Скуп свих парних целих бројева је подгрупа групе свих целих бројева са операцијом сабирања.

Проверавање свих аксиома група са неки скуп и бинарну операцију се показало напорним, док је проверити да ли је подскуп групе погрупа знатно лакше. Довољно је показати да је подскуп затворен под операцијом групе и да у њему постоји инверз за сваки његов елемент, што можемо објединити у следеће тврђење.

Тврђење 3.1. Подскуп H групе G је подгрупа ако и само ако

(1) $H \neq \emptyset$, и

(2) за свако $a, b \in H$, $ab^{-1} \in H$.

Ако је H коначно довољно је показати да је H непразно и затворено под операцијом групе.

Доказ. Ако је H подгрупа групе G онда (1) и (2) важе јер H садржи неутрал групе G, инверз сваког свог елемента и јер је H затворена под операцијом групе.

Остаје да покажемо да важи и обрнуто, ако H задовољава и (1) и (2) да је онда $H \leq G$. Нека је $x \in H$ (такво x постоји по својству (1)). Нека је $y = x$, применом својства (2) добијамо $e = xx^{-1} \in H$, односно да H садржи неутрал групе G. Применом својства (2) на e и x добијамо $x^{-1} = ex^{-1} \in H$, односно да у H постоји инверз за сваки елемент. Ако су x и y неки елементи H, онда H садржи x и y^{-1}, па по својству (2) $xy = x(y^{-1})^{-1} \in H$, односно H је затворено под операцијом групе. Како је H подскуп групе по аксиоми групе асоцијативан закон важи и у H. H је затворено под операцијом групе, важи асоцијативан закон, садржи неутрал групе и садржи инверз сваког свог елемента па је по дефиницији H подгрупа групе G.

Претпоставимо да је H коначно и затворено под операцијом групе и нека је x неки елемент H. Онда постоји коначно много различитих елемената облика $x, x^2, x^3, \ldots$ па је $x^a = x^b$ за неке целе бројеве a, b, $b > a$. Ако је $n = b - a$, онда је $x^n = 1$ па је сваки елемент из H коначног реда. Онда је $x^{n-1} = x^{-1}$ елемент H, па у H постоји инверз за сваки елемент. □

3.1 Централизатор, центар и нормализатор

Увешћемо неке фамилије подгрупа које ће нам бити важне у следећем поглављу. Нека је G група и A неки непразан подскуп групе G.

Дефиниција 3.2. Дефинишимо $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ за свако } a \in A\}$. Овај подскуп групе G се зове *централизатор* скупа A у групи G. Како је $gag^{-1} = a$ ако и само ако $ga = ag$, $C_G(A)$ је скуп елемената групе G који комутују са сваким елементом скупа A.

Показаћемо да је $C_G(A)$ подгрупа групе G. $C_G(A) \neq \emptyset$ јер је $e \in C_G(A)$, по дефиницији неутрала је $ea = ae$, за свако $a \in G$ (односно за свако $a \in A$), па e задовољава услов припадности $C_G(A)$. Нека су $x, y \in C_G(A)$, па је за свако $a \in A$, $xax^{-1} = a$ и $yay^{-1} = a$. Посматрајмо прво $yay^{-1} = a$, множењем са леве стране са y^{-1} па множењем са десне са y добијамо $a = y^{-1}ay$ однаосно да је $y^{-1} \in C_G(A)$, па у $C_G(A)$ постоји инверз за сваки елемент. Сада

$$\begin{aligned}(xy)a(xy)^{-1} &= (xy)a(y^{-1}x^{-1}) \\ &= x(yay^{-1})x^{-1} \\ &= xax^{-1} \\ &= a\end{aligned}$$

па је $xy \in C_G(A)$ и $C_G(A)$ је затворено под операцијом групе, па је $C_G(A) \leq G$.

У посебном случају кад је $A = \{a\}$ пишемо $C_G(a)$ уместо $C_G(A)$. У овом случају је $a^n \in C_G(a)$ за свако $n \in \mathbb{Z}$.

Дефиниција 3.3. Дефинишимо $Z(G) = \{g \in G \mid gx = xg \text{ за свако } x \in G\}$, скуп елемената који комутују са свим елементима групе G. Овај подскуп групе G се зове *центар* групе G.

Како је $Z(G) = C_G(G)$, показавши да је $C_G(A) \leq G$ смо показали и да је $Z(G) \leq G$ као специјалан случај.

Дефиниција 3.4. Дефинишимо $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. Дефинишимо *нормализатор* скупа A у групи G као скуп $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$.

Приметимо да ако $g \in C_G(A)$ онда $gag^{-1} = a \in A$ за свако $a \in A$ па је $C_G(A) \leq N_G(A)$. Доказ да је $N_G(A)$ подгрупа групе G је сличан доказу $C_G(A)$ да је подгрупа групе G па га нећемо навести.

Пример 3.2. Ако је G абелова група онда је $Z(G) = G$. Такође је $C_G(A) = N_G(A) = G$ за сваки подскуп A групе G јер је $gag^{-1} = gg^{-1}a = a$ за свако $g \in G$ и за свако $a \in A$.

4

Хомоморфизми и количничке групе

Осим подгрупа, увешћемо количничке групе групе G које ће нам помоћи у изучавању структуре групе G. Проучавање количничких група се у ствари своди на проучање хомоморфизама групе G. Ако је φ хомоморфизам из G у групу H, посматраћемо скупове свих елемената из G који се сликају у исти елемент групе H.

Операција групе H нам даје начин да множимо два елемента у слици хомоморфизма φ. То нас наводи ка томе да постоји природан начин множења горе наведених скупова па можемо начинити групу од скупа скупова елемената из G који се сликају у један елемент у H. Нека је X_a скуп елемената који се сликају у елемент a, а X_b скуп елемената који се сликају у b. Производ ових скупова ћемо дефинисати као скуп X_{ab} чији се елементи сликају у ab. Овакво множење је асоцијативно јер је множење у H асоцијативно, неутрал је скуп елемената који се сликају у неутрал групе H и инверз је скуп који се слика у инверзни елемент (за X_a то је скуп елемената који се сликају у a^{-1}). Група G је подељена на овакве скупове где они имају структуру групе, коју зовемо количничка група групе G, за који ћемо касније навести формалну дефиницију.

4.1 Својства хомоморфизма

Да би смо формално дефинисали количничку групу потребно нам је да дефинишемо и покажемо нека својства хомоморфизма.

Дефиниција 4.1. Ако је φ хомоморфизам $\varphi : G \to H$, онда је *језгро* хомоморфизма φ скуп

$$\{g \in G \mid \varphi(g) = e\}$$

у ознаци $\ker \varphi$ (где је e неутрал групе H).

Тврђење 4.1. Нека су G и H групе и нека је $\varphi : G \to H$ хомоморфизам.

(1) $\varphi(e_G) = e_H$, где су e_G и e_H редом неутрали група G и H.

(2) $\varphi(g^{-1}) = \varphi(g)^{-1}$ за свако $g \in G$.

(3) $\varphi(g^n) = \varphi(g)^n$ за свако $n \in \mathbb{Z}$.

(4) $\ker \varphi$ је подгрупа групе G.

(5) $\mathrm{im}(\varphi)$, слика групе G под φ, је подгрупа групе H.

Доказ. (1) Како је $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$, применом закона скраћивања добијамо $e_H = \varphi(e_G)$.

(2) $\varphi(e_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$, и по делу (1) је $e_H = \varphi(e_G)$ односно $e_H = \varphi(g)\varphi(g^{-1})$. Множењем са леве стране са $\varphi(g)^{-1}$ добијамо $\varphi(g)^{-1} = \varphi(g^{-1})$.

(3) Индукцијом по $n \in \mathbb{Z}^+$.
База: За $n = 1$ је очигледно $\varphi(g^1) = \varphi(g)^1$.
Индуктивна хипотеза: Нека је $\varphi(g^n) = \varphi(g)^n$.
Индуктивни корак: $\varphi(g^{n+1}) = \varphi(g^n g) = \varphi(g^n)\varphi(g)$ што је по индуктивној хипотези једнако $\varphi(g)^n\varphi(g) = \varphi(g)^{n+1}$ односно $\varphi(g^{n+1}) = \varphi(g)^{n+1}$.

По делу (2) важи и за негативне вредности n.

(4) Како је $e_G \in \ker \varphi$ језгро од φ је непразно. Нека су $x, y \in \ker \varphi$, $\varphi(x) = \varphi(y) = e_H$. Онда

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = e_H e_H^{-1} = e_H$$

па је $xy^{-1} \in \ker \varphi$. По Тврђењу 3.1 је $\ker \varphi \leq G$.

(5) Како је $\varphi(e_G) = e_H$, неутрал групе H је у слици од φ, па је $\mathrm{im}(\varphi)$ непразно. Ако су x и y у $\mathrm{im}(\varphi)$, рецимо $x = \varphi(a)$, $y = \varphi(b)$ онда је $y^{-1} = \varphi(b^{-1})$ по (2) па је $xy^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1})$ јер је φ хомоморфизам. xy^{-1} је такође у слици од φ, па је $\mathrm{im}(\varphi)$ подгрупа групе H по Тврђењу 3.1.

□

Један од важних резултата теорије група је Кејлијева[1] теорема коју наводимо без доказа.

Теорема (Кејлијева теорема)**.** Свака група G је изоморфна некој групи пермутација. Конкретно, коначна група реда n је изоморфна подгрупи од S_n.

4.2 Количничке групе и нормалне подгрупе

Дефиниција 4.2. Нека је $\varphi : G \to H$ хомоморфизам са језгром K. *Количничка група* или *фактор група*, G/K (читамо G *mod* K), је група чији су елементи скупови елемената из G који се сликају у исти елемент из H са операцијом дефинисаном на почетку поглавља: ако је X скуп елемената који се сликају у a и Y скуп елемената који се сликају у b онда је производ X и Y дефинисан као скуп елемената који се сликају у производ ab.

Оваквом нотацијом је наглашено да је језгро K само један елемент групе G/K. Можемо гледати групу G/K као да је добијена дељењем са K (прецизније *modulo* K).

Дефиниција операције количничке групе захтева да пресликавање φ буде експлицитно дефинисано. Могуће је дефинисати множење у количничкој групи коришћењи само репрезентативне елементе оних скупова. Прво чемо показати да сваки од тих скупова може да се изрази преко језгра хомоморфизма.

Тврђење 4.2. Нека је $\varphi : G \to H$ хомоморфизам група са језгром K. Нека је $X \in G/K$ скуп елемената који се слика у a, односно $X = \varphi^{-1}(a)$. Онда је

(1) За било које $u \in X$, $X = \{uk \mid k \in K\}$

[1] По британском математичару А. Кејлију (1821 - 1895).

(2) За било које $u \in X$, $X = \{ku \mid k \in K\}$.

Доказ. Нека је $u \in X$, па је по дефиницији X $\varphi(u) = a$. Нека је $uK = \{uk \mid k \in K\}$. Прво чемо показати да је $uK \subseteq X$. За неко $k \in K$,

$$\begin{aligned}\varphi(uk) &= \varphi(u)\varphi(k)\\ &\text{`} = \varphi(u)e\\ &= a,\end{aligned}$$

па је $uk \in X$. Овим смо показали да је $uK \subseteq X$. Да би смо показали и обрнуто претпоставимо да је $g \in X$ и нека је $k = u^{-1}g$. Онда је

$$\begin{aligned}\varphi(k) &= \varphi(u^{-1})\varphi(g) = \varphi(u)^{-1}\varphi(g)\\ &= a^{-1}a = e.\end{aligned}$$

Па је $k \in \ker\varphi$. Kako je $k = u^{-1}g$, $g = uk \in uK$ онда је и $X \subseteq uK$ ра је $X = uK$.

(2) се доказује слично. □

Скупови описани у Тврђењу 4.2 су дефинисани за било коју подгрупу K групе G не само за језгро хомоморфизма и зову се:

Дефиниција 4.3. За неко $N \leq G$ и неко $g \in G$ нека су редом

$$gN = \{gn \mid n \in N\}$$

$$Ng = \{ng \mid n \in N\}$$

леви косет и *десни косет* подгрупе N у групи G. Неки елемент косета зовемо *репрезентативним елементом* тог косета.

Са овом дефиницијом, Тврђење 4.2 нам показује да су скупови описани у дефиницији количничке групе у ствари леви (односно десни) косети језгра, односно елементи количничке групе G/K су леви косети gK, $g \in G$. Следећом теоремом ћемо показати да производ левих косета X и Y у G/K рачунамо тако што бирамо репрезентативни елемент u од X и репрезентативни елемент v од Y, множимо u и v у G и формирамо косет $(uv)K$.

Теорема 4.1. Нека је G група и нека је K језгро неког хомоморфизма из G у другу групу. Онда скуп чији су елементи леви косети од K у G са операцијом дефинисаном као

$$uK \circ vK = (uv)K$$

формира групу, G/K. Операција је добро дефинисана у смислу да ако је u_1 неки елемент uK и v_1 неки елемент vK онда је $u_1v_1 \in uvK$ односно $u_1v_1K = uvK$, тако да множење не зависи од избора репрезентативних елемената косета. Ова теорема важи и за десне косете.

Доказ. Нека су $X, Y \in G/K$ и нека је $Z = XY$ у G/K тако да су по Тврђењу 4.2(1), X, Y и Z (леви) косети од K. K је језгро неког хомоморфизма $\varphi : G \to H$ тако да је $X = \varphi^{-1}(a)$ и $Y = \varphi^{-1}(b)$ за неко $a, b \in H$. По дефиницији операције у G/K, $Z = \varphi^{-1}(ab)$. Нека су u и v неки репрезентативни елементи косета X и Y тако да је $\varphi(u) = a$, $\varphi(v) = b$ и $X = uK$, $Y = vK$. Морамо показати да је $uv \in Z$.

$$\begin{aligned} uv \in Z &\iff uv \in \varphi^{-1}(ab) \\ &\iff \varphi(uv) = ab \\ &\iff \varphi(u)\varphi(v) = ab \end{aligned}$$

Како је последња једнакост тачна $uv \in Z$ па је Z (леви) косет uvK. Овим смо показали да је производ косета X и Y косет uvK за било који избор репрезенративних елемената $u \in X$, $v \in Y$ чиме смо доказали прво тврђење теореме. Друго тврђење одмах следи јер су по Тврђењу 4.2 $uK = Ku$ и $vK = Kv$ за свако u и v из G. □

Како производ не зависи од избора репрезентативних елемената косета корисна нотација за означавање косета uK је $\overline{u}$. Са оваквом нотацијом количничку групу G/K означавако са $\overline{G}$ а производ елемената $\overline{u}$ и $\overline{v}$ је косет који садржи uv, односно $\overline{uv}$.

Пример 4.1.

1. Ако је $\varphi : G \to H$ изоморфизам онда је $K = 1$ и количничка група $G/1 \cong G$.

2. Нека је G нека група и $H = e_H$ група реда 1 и дефинишимо $\varphi : G \to H$ са $\varphi(g) = e_H$ за свако $g \in G$. Јасно је да је φ хомоморфизам. Ово пресликавање се зове *тривијалан хомоморфизам.* У овом случају је $\ker \varphi = G$ и G/G је група са једним елементом, целим G.

По Теореми 4.1, ако нам је дата подгрупа K групе G за коју знамо да је језгро неког хомоморфизма, можемо дефинисати количничку групу G/K без осврtања на хомоморфизам тако што множимо $uKvK = uvK$. Поставља се питање да ли је могуће урадити исто са било којом подгрупом N групе G. У општем случају се показало да то није могуће јер

множење косета није добро дефинисано. Касније ћемо показати да је могуће дефинисати структуру групе на косетима од N ако и само ако је N језгро неког хомоморфизма.

Прво ћемо показати да косети неке подгрупе групе G гормирају партицију групе G (односно њихова унија даје цео G, а пресек свака два различита косета је празан скуп).

Тврђење 4.3. Нека је N нека подгрупа групе G. Скуп левих косета од N у G формира партицију групе G. За свако $u, v \in G$, $uN = vN$ ако и само ако $v^{-1}u \in N$ и нарочито, $uN = vN$ ако и само ако су u и v репрезентстивни елементи истог косета.

Доказ. Како је N подгрупа групе G, $e \in N$. Онда је $g = ge \in gN$ за свако $g \in G$ односно

$$G = \bigcup_{g \in G} gN$$

Да бисмо показали да су различити косети дисјунктни претпоставимо да је $uN \cap vN \neq \emptyset$. Показаћемо да је онда $uN = vN$. Нека је $x \in uN \cap vN$. Онда је $x = un = um$ за неко $n, m \in N$. Множењем са десне стране са n^{-1} добијамо $u = vmu^{-1} = vm_1$ где је $m_1 = mn^{-1} \in N$. Сад за неки елемент $ut \in uN$ $(t \in N)$, $ut = (vm_1)t = v(m_1t) \in vM$. Овим смо показали да је $uN \subseteq vN$. Аналогним постпуком (заменом u и v) добијамо и $vN \subseteq uN$, па је $uN = vN$ чиме смо показали да су два косета за непразним пресеком једнака.

По првом делу тврђења $uN = vN$ ако и само ако $u \in vN$ ако и само ако $u = vn$ за неко $n \in N$ ако и само ако $v^{-1}u \in N$. $v \in uN$ је еквивалентно томе да је v репрезентативни елемент косета uN, па је $uN = vN$ ако и само ако су u и v репрезентативни елементи истог косета. □

Тврђење 4.4. Нека је G група и N подгрупа групе G.

(1) Операција на скуп левих косета од N у G описана са

$$uN \cdot vN = (uv)N$$

је добро дефинисана ако и само ако је $gng^{-1} \in N$ за свако $g \in G$ и за свако $n \in N$.

(2) Ако је горе наведена операција добро дефинисана онда чини групу са скупом левих косета од N у G. Неутрал ове групе је косет eN и инверз косета gN је косет $g^{-1}N$ односно $(gN)^{-1} = g^{-1}N$.

Доказ. (1) Претпоставимо да је ова операција добро дефинисана односно да за свако $u, v \in G$, ако су $u, u_1 \in uN$ и $v, v_1 \in vN$ онда је $uvN = u_1v_1N$. Нека је g неки елемент групе G и нека је n неки елемент из N. Нека је $u = e$, $u_1 = n$ и $v = v_1 = g^{-1}$, применом горе неведене претпоставке добијамо да је $eg^{-1}N = ng^{-1}N$ односно $g^{-1}N = ng^{-1}N$. Како је $e \in G$, $ng^{-1} \cdot e \in ng^{-1}N$. Онда је $ng^{-1} \in g^{-1}N$ па је $ng^{-1} = g^{-1}n_1$ за неко $n_1 \in N$. Множењем са леве стране са g дпбијамо $gng^{-1} = n_1 \in N$.

Обрнуто, претпоставимо да је $gng^{-1} \in N$ за свако $g \in G$ и за свако $n \in N$. Да би смо показали да је горе наведена операција добро дефинисана нека је $u, u_1 \in uN$ и $v, v_1 \in vN$. Можемо написати $u_1 = un$ и $v_1 = vm$, за неко $n, m \in N$. Морамо доказати да је $u_1v_1 \in uvN$:

$$\begin{aligned} u_1v_1 &= (un)(vm) = u(vv^{-1})nvm \\ &= (uv)(v^{-1}nv)m = (uv)(n_1m), \end{aligned}$$

где је $n_1 = v^{-1}nv = (v^{-1})n(v^{-1})^{-1}$ елемент N по претпоставци. Као је N затворено под операцијом групе, $n_1m \in N$. Онда је $u_1v_1 = (uv)n_2$, за неко $n_2 \in N$. Онда леви косети uvN и u_1v_1N садрже исти елемент u_1v_1. По прошлом тврђењу ови косети су једнаки чиме смо доказали да је горе наведена операција добро дефинисана.

(2) Ако је операција на косетима добро дефинисана аксиоме група се лако проверавју и директно следе и аксиома групе G.

□

Подгрупе N које задовољавају услов наведен у Тврђењу 4.4 за које је природна структура групе за количничку групу G/N имају посебан назив:

Дефиниција 4.4. Елемент gng^{-1} се назива *коњугатом* елемента $n \in N$ елементом g. Скуп $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ се назива *коњугатом* скупа N елементом g. За елемент g кажемо да *нормализује* скуп N ако $gNg^{-1} = N$. Подгрупа N групе G се назива *нормалном* ако сваки елемент групе G нормализује N, односно ако $gNg^{-1} = N$ за свако $g \in G$. Ако је N нормална подгрупа пишемо $N \trianglelefteq G$.

Теорема 4.2. Нека је N подгрупа групе G. Следећа тврђења су еквивалентна:

(1) $N \trianglelefteq G$

(2) $N_G(N) = G$

(3) $gN = Ng$ за свако $g \in G$

(4) операција на леве косете описана у Тврђењу 4.4 чини скуп левих косета групом

(5) $gNg^{-1} \subseteq N$ за свако $g \in G$

Доказ. Прво ћемо показати да је (1) $\iff$ (2). Ако је $N_G(N) = G$ онда је по дефиницији $N_G(N) = \{g \in G \mid gNg^{-1} = N\}$, односно видимо да је $gNg^{-1} = N$ за свако $g \in G$ па је $N \trianglelefteq G$. Ако је $N \trianglelefteq G$ онда је по дефиницији нормалне подгрупе $gNg^{-1} = N$ за свако $g \in G$, па је из дефиницији нормализатора $N_G(N) = G$.

(1) $\iff$ (3) : Ако је $N \trianglelefteq G$ онда је $gNg^{-1} = N$ за свако $g \in G$ односно за свако $g \in G$ је $gn_1g^{-1} = n_2$ за неко $n_1, n_2 \in N$. Множењем са десне стране са g добијамо $gn_1 = n_2g$ па јасно видимо да су за свако $g \in G$ леви и десни косети једнаки. Обрнуто, ако је $gN = Ng$ за свако $g \in G$ знамо да за свако $g \in G$ постоји неко $n_1, n_2 \in N$ тако да је $gn_1 = n_2g$. Множењем са десне стране са g^{-1} добијамо $gn_1g^{-1} = n_2$ односно да за свако $g \in G$ и за свако $n \in N$ $gng^{-1} \in N$ odnosno $gNg^{-1} = N$ па је $N \trianglelefteq G$.

(1) $\iff$ (4) : По Тврђењу 4.4 да би операција на леве косете формирала групу са скупом левих косета она мора бити добро дефинисана што је по Тврђењу 4.4(1) еквивалентно са тим да је $gng^{-1} \in N$ за свако $g \in G$ и за свако $n \in N$ што је по дефиницији нормална подгрупа.

(1) $\iff$ (5) : Ако је $N \trianglelefteq G$ онда је $gNg^{-1} = N$ odnosno $gNg^{-1} \subseteq N$ за свако $g \in G$. Обрнуто, ако је $gNg^{-1} \subseteq N$ за свако $g \in G$, за свако $n \in N$ је $gng^{-1} \in N$ односно постоји $n_1 \in N$ тако да је $gng^{-1} = n_1$. Множењем леве и десне стране са g^{-1} односно g добијамо $n = g^{-1}n_1g = g^{-1}n_1(g^{-1})^{-1} \in gNg^{-1}$ па је $N \subseteq gNg^{-1}$ односно $N = gNg^{-1}$ па је $N \trianglelefteq G$. □

Сада ћемо показати да су нормалне групе језгра хомоморфизама.

Тврђење 4.5. Подгрупа N групе G је нормална ако и само ако је она језгро неког хомоморфизма.

Доказ. Ако је N језгро неког хомоморфизма φ, онда су по Тврђењу 4.2 леви и десни косети једнаки. По Теореми 4.2(3) је онда N нормална подгрупа.

Обрнуто, ако је $N \trianglelefteq G$, нека је $H = G/N$ и дефинишимо $\pi : G \to G/N$ са $\pi(g) = gN$ за свако $g \in G$. Онда је по дефиницији операције у G/N $\pi(g_1g_2) = (g_1g_2)N = g_1Ng_2N = \pi(g_1)\pi(g_2)$ чиме смо показали да је π хомоморфизам. Сада је језгро овог хомоморфизма:

$$\begin{aligned}\ker\pi &= \{g \in G \mid \pi(g) = eN\}\\ &= \{g \in G \mid gN = eN\}\\ &= \{g \in G \mid g \in N\} = N,\end{aligned}$$

што значи да је N језгро хомоморфизма π. □

Пример 4.2. Нека је G група.

1. Подгрупе e и G су увек нормалне подгрупе групе G, $G/e \cong G$ и $G/G \cong e$.

2. Ако је G абелова група онда је било која подгрупа N групе G нормална јер за свако $n \in N$ и за свако $g \in G$:

$$gng^{-1} = gg^{-1}n = n \in N.$$

4.3 Лагранжова теорема и још нека својства косета

Када се бавимо коначним групама њихов ред на је од велике важности. Показаћемо да је ред количничке групе неке коначне групе једнак $|G/N| = \dfrac{|G|}{|N|}$. Ово је последица једног општијег тврђења, Лагранжове теореме. Ова теорема је једна од најважнијих комбинаторних резултата коначне теорије група.

Теорема 4.3 (Лагранжова теорема)**.** Ако је G коначна група и H подгрупа групе G, онда ред од H дели ред од G и број левих косета од H у G је $\dfrac{|G|}{|H|}$.

Доказ. Нека је $|H| = n$ и нека је број левих косета од H у G k. По Тврђењу 4.3 скуп левих косета од H у G формира партицију скупа G. По дефиницији левог косета пресликавање $H \to gH$ дефинисано са

$h \mapsto gh$ је сурјективно из H у неки леви косет gH. Из левог закона скраћивања добијамо да је ово пресликавање инјективно јер ако $gh_1 = gh_2$ следи да је $h_1 = h_2$. Ово нам показује да су gH и H истог реда односно $|H| = |gH| = n$. Скуп левих косета формира партицију од G тако што га дели на k дисјунктних подскупова, сваки каридиналности n, па је $|G| = kn$. Онда је $k = \dfrac{|G|}{n} = \dfrac{|G|}{|H|}$. □

Дефиниција 4.5. Ако је G група и $H \leq G$, број левих косета од H у G зове се *индекс* подгрупе H у групи G у ознаци $|G : H|$.

За коначне групе индекс од H у G је $\dfrac{|G|}{|H|}$. За групу G бесконачног реда количник $\dfrac{|G|}{|H|}$ нема смисла. Бесконачне групе могу имати подгрупе и коначног и бесконачног индекса.

Пример 4.3. Нека је G нека група која има подгрупу H индекса 2. Показаћемо да је $H \trianglelefteq G$. Нека је $g \in G \setminus H$, па су по претпоставци два лева косета H у G eH и gH. Како је $eH = H$ и леви косети формирају партицију скупа G мора да буде $gH = G \setminus H$. Десни косети од H у G су He и Hg. Како је $He = H$ онда мора бити $Hg = G \setminus H$. Добили смо да је $gH = G \setminus H = Hg$ односно да су леви и десни косети једнаки па је по Теореми 4.2 $H \trianglelefteq G$.

Потпуно обрнуто тврђење Лагранжовој теореми у општем случају није тачно. Односно ако је G коначна група и n дели ред групе G, G не мора да има подгрупу реда n. Постоје нека парцијална обрнута тврђења Лагранжовој теореми која јесу тачна. На пример, за коначне абелове групе важи потпуно обрнуто тврђење. Најјаче обрнуто тврђење Лагранжовој теореми је Силовљева[2] теорема коју наводимо без доказа.

Теорема 4.4 (Силовљева теорема)**.** Ако је G коначна група реда $p^\alpha m$, где је p прост број и p не дели m, онда G има подгрупу реда p^α.

Показаћемо неке комбинаторне резлтате косета.

Дефиниција 4.6. Нека су H и K подгрупе неке групе, дефинишимо

$$HK = \{hk \mid h \in H, k \in K\}$$

.

[2]по норвешком математичар П. Л. Силов (1832 - 1918)

Тврђење 4.6. Ако су H и K коначне подгрупе неке групе онда је

$$|HK| = \frac{|H||K|}{|H \cup K|}.$$

Доказ. Приметимо да је HK унија левих косета од K односно

$$HK = \bigcup_{h \in H} hK.$$

Како сваки косет има $|K|$ елемената довољно је наћи број различитих левих косета облика hK, $h \in H$. $h_1K = h_2K$, за неко $h_1, h_2 \in H$ ако и само ако је $h_2^{-1}h_1 \in K$, па је

$$h_1K = h_2K \iff h_2^{-1}h_1 \in H \cap K \iff h_1(H \cap K) = h_2(H \cap K).$$

Број различитих левих косета облика hK, за $h \in H$ је исти као број различитих левих косета облика $h(H \cap K)$, за $h \in H$, што је по Лагранжовој теореми једнако $\frac{|H|}{|H \cap K|}$. HK се састоји од $\frac{|H|}{|H \cap K|}$ различитих косета од K, што нам даје горе наведену формулу. □

Тврђење 4.7. Ако су H и K подгрупе неке групе, HK је подгрупа ако и само ако је $HK = KH$.

Доказ. Претпоставимо прво да је $HK = KH$ и нека је $a, b \in HK$. Доказаћемо да је $ab^{-1} \in HK$ да би HK била подгрупа по Тврђењу 3.1. Нека је $a = h_1k_1$ и $b = h_2k_2$, за неко $h_1, h_2 \in H$ и $k_1, k_2 \in K$. Онда је $b^{-1} = k_2^{-1}h_2^{-1}$, па је $ab^{-1} = h_1k_1k_2^{-1}h_2^{-1}$. Нека је $k3 = k_1k_2^{-1}$ и $h_3 = h_2^{-1}$. Онда је $ab^{-1} = h_1k_3h_3$. Како је $HK = KH$, $k_3h_3 = h_4k_4$ за неко $h_4 \in H$ и $k_4 \in K$. Онда је $ab^{-1} = h_1h_4k_4 = h_5k_4 \in HK$ за $h_5 = h_1h_4$.

Обрнуто, претпоставимо да је HK подгрупа групе G. Како је $H \leq HK$ и $K \leq HK$, $KH \subseteq HK$. Да би смо показали и да је $HK \subseteq KH$, узмимо неко $hk \in HK$. Како је HK подгрупа нека је $hk = a^{-1}$ за неко $a \in HK$. Ако је $a = h_1k_1$ онда је $hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$. □

Последица 4.1. Ако су H и K подгрупе групе G и $H \leq N_G(K)$ онда је HK подгрупа групе G. Ако је $K \trianglelefteq G$, $HK \leq G$ за било које $H \leq G$.

Доказ. Доказаћемо да је $HK = KH$. Нека су $h \in H$, $k \in K$. Како је $hkh^{-1} \in K$ па је $hk = (hkh^{-1})h \in KH$, што показује да је $HK \subseteq KH$. Слично $kh = h(h^{-1}kh) \in HK$, чиме добијамо да је $HK = KH$. Остатак последице добијамо из прошлог тврђења. □

Дефиниција 4.7. Ако је A подскуп од $N_G(K)$ (или $C_G(K)$) кажемо да A *нормализује* K (*централизује* K).

Са овом терминологијом, Последица 4.1 нам каже да је HK подгрупа ако H нормализује K (слично, HK је подгрупа ако K нормализје H).

Кроз ово поглавље смо се бавили и доказивалин својства левих косета. Сва својства важе и за десне косете и слично се доказују. За нормалне подгупе је тривијално јер су леви и десни косети исти. Лагранжова теорема важи и за десне косете и из ње добијамо да је за коначну групу G и њену подгрупу H број левих и десних косета од H у G исти. Кад се бавимо косетима у комбинаторне сврхе можемо користити и леве и десне косете али не оба ако је потребна партиција од G.

4.4 Теореме о изоморфизму

Овде ћемо се бавити неким последицама основних релација између количничких група и хомоморфизама показаних у 4.1 и 4.2.

Теорема 4.5 (Прва теорема о изоморфизму)**.** Ако је $\varphi : G \to H$ хомоморфизам група, онда је $\ker\varphi \trianglelefteq G$ и $G/\ker\varphi \cong \varphi(G)$.

Доказ. Како је $\ker\varphi$ језгро хомоморфизма по Теореми 4.5 $\ker\varphi$ је нормална подгрупа групе G.

Покушаћемо да конструишемо пресликавање $\theta : G/\ker\varphi \to \varphi(G)$ са $\theta(aK) = \varphi(a)$. Морамо показати да вредност од θ зависи само од косета а не од репрезентативног елемента који изаберемо. Претпоставимо да је $aK = bK$, онда је по Тврђењу 4.3 $b^{-1}a \in K$ па је $\varphi(b^{-1}a) = e_H$ па је

$$\varphi(b)^{-1}\varphi(a) = \varphi(b^{-1})\varphi(a) = \varphi(b^{-1}a) = e_H.$$

Множењем са леве стране са $\varphi(b)$ добијамо да је $\varphi(a) = \varphi(b)$. Како је $\varphi(a) = \varphi(b)$ онда мора и $\theta(aK) = \theta(bK)$, па је пресликавање $\theta : G/\ker\varphi \to \varphi(G)$, дефинисано са $\theta(aK) = \varphi(a)$, добро дефинисано пресликавање.

Из дефиниције од θ јасно видимо да је пресликавање сурјективно (пресликавање из G у $\varphi(G)$ је јасно сурјективно а како је $\theta(gK) = \varphi(g)$, за свако $g \in G$ мора и θ да буде сурјективно). Да бисмо показали да је пресликавање θ инјективно, претпоставимо да је $\theta(aK) = \theta(bK)$. Онда је $\varphi(a) = \varphi(b)$ ра је, обрнутим поступком горе урађеним, $b^{-1}a \in K$. По

Тврђењу 4.3 је $aK = bK$ па је θ инјективно. Остаје само да покажемо да је θ хомоморфизам:

$$\theta(aKbK) = \theta(abK) = \varphi(ab) = \varphi(a)\varphi(b) = \theta(aK)\theta(bK).$$

Показали смо да је $\theta : G/\ker\varphi \to \varphi(G)$ изоморфизам. □

Последица 4.2. Нека је $\varphi : G \to H$ хомоморфизам група.

(1) φ је инјективно ако и само ако је $\ker\varphi = e_G$

(2) $|G : \ker\varphi| = |\varphi(G)|$

Доказ. (1) Прво претпоставимо да је φ инјективно пресликавање. Нека су $a, b \in \ker\varphi$, онда је $\varphi(a) = \varphi(b) = e_H$ па како је φ инјективно $a = b$. Како је $\varphi(e_G) = e_H$ мора да је $\ker\varphi = e_G$. Обрнуто, претпоставимо да је $\ker\varphi = e_G$. Морамо доказати да ако је $\varphi(a) = \varphi(b)$ онда је и $a = b$. Множењем прве једнакости са десне стране са $\varphi(b)^{-1}$ добијамо:

$$\varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) = \varphi(b)\varphi(b)^{-1} = e_H.$$

По дефиницији језгра хомоморфизма је $ab^{-1} \in \ker\varphi$, а како је $\ker\varphi = e_G$ $ab^{-1} = e_G$. Множењем са десне стране са b добијамо $a = b$, односно да је φ инјективно.

(2) По Првој теореми о изоморфизму је $G/\ker\varphi \cong \varphi(G)$, па је $|G/\ker\varphi| = |\varphi(G)|$. Елементи групе $G/\ker\varphi$ су леви косети од $\ker\varphi$ у G, а по дефиницији индекса $|G : \ker\varphi|$ је једнако броју левих косета од $\ker\varphi$ у G, па је $|\varphi(G)| = |G/\ker\varphi| = |G : \ker\varphi|$.

□

Теорема 4.6 (Друга теорема о изоморфизму)**.** Нека је G група и нека су A и B подгрупе и претпоставимо да је $A \leq N_G(B)$. Онда је AB подгрупа групе G, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ и $AB/B \cong A/A \cap B$.

Доказ. По Последици 4.1, AB је подгрупа групе G. Како је $A \leq N_G(B)$ (по претпоставци) и $B \leq N_G(B)$ (тривијално) онда је и $AB \leq N_G(B)$ па је B нормална подгрупа подгрупе AB.

Како је B нормално у AB количничка група AB/B је добро дефинисана. Дефинишимо пресликавање $\varphi : A \to AB/B$ са $\varphi(a) = aB$. Како је операција групе у AB/B добро дефинисана лако је видети да је φ хомоморфизам:

$$\varphi(a_1a_2) = a_1a_2B = a_1Ba_2B = \varphi(a_1)\varphi(a_2).$$

Јасно је из дефиниције AB да је φ сурјективно. Неутрал у AB/B је косет eB па се језгро од φ састоји од елемената $a \in A$, $aB = eB$, који су по Тврђењу 4.3 елементи $a \in B$, односно $\ker\varphi = A \cap B$. По Првој теореми о изоморфизму, $A \cap B \trianglelefteq A$ и $A/A \cap B \cong AB/B$. □

Трећа теорема о изоморфизму се бави количничким групама количничких груопа.

Теорема 4.7 (Трећа теорема о изоморфизму)**.** Нека је G група и H и K нормалне подгрупе групе G и $H \leq K$. Онда је $K/H \trianglelefteq G/H$ и

$$(G/H)/(K/H) \cong G/K.$$

Ако количник са H означимо цртом, ово можемо записати са

$$\overline{G}/\overline{K} \cong G/K.$$

Доказ. Прво ћемо показати да је $K/H \trianglelefteq G/H$. Односно да је за свако $k \in K$ и $g \in G$ $gHkHg^{-1}H = (gkg^{-1})H = K/H$. Како је $K \trianglelefteq G$ $gkg^{-1} = k_1$ за неко $k_1 \in K$, па је $(gkg^{-1})H = k_1H \in K/H$, па је $K/H \trianglelefteq G/H$.

Дефинишимо:

$$\varphi : G/H \to G/K$$
$$(gH) \mapsto gK$$

Да бисмо показали да је φ добро дефинисано претпоставимо да је $g_1H = g_2H$. Онда је $g_1h = g_2h$ за неко $h \in H$. Како је $H \leq K$, h је такође елемент K, па је $g_1K = g_2K$, односно $\varphi(g_1H) = \varphi(g_2H)$ чиме смо показали да је φ добро дефинисано. Како g можемо насумично изабрати из G, φ је сурјективан хомоморфизам. На крају,

$$\begin{aligned}\ker\varphi &= \{gH \in G/H \mid \varphi(gH) = eK\}\\ &= \{gH \in G/H \mid gK = eK\}\\ &= \{gH \in G/H \mid g \in K\} = K/H.\end{aligned}$$

По Првој теореми о изоморфизму је $(G/H)/(K/H) \cong G/K$. □

5

Закључак

У овом раду смо дотакли само површину теорије група. Посебну пажњу смо посветили количничким групама и нормалним подгрупама, и на крају смо доказали теореме о изоморфизму које су важне у даљем изучавању стурктура и својства група.

Групе су најпростија стуктура којој се придаје велики значај у модерној алгебри. Теорија група има примене у криптографији, хемији и физици. Надам се да смо овим радом поставили основе и заинтересовали читаоца за даље изучавање ове области.

Желим да се захвалим ментору Сандри Андрић на издвојеном времену и датим саветима током израде овог рада, као и на пренетом знању током пет година којих ми је предавала.

Литература

[1] D. S. Dummit, R. M. Foote, *Abstract Algebra, third edition*, John Wiley & Sons, 2003.

[2] Thomas W. Hungerford, *Abstract Algebra: An Introduction, third edition*, Cengage Learning, 2012.

[3] Israel Kleiner, *A History of Abstract Algebra*, Birkhäuster Boston, 2007.

[4] Nataša Božović, Žarko Mijailović, *Uvod u Teoriju Grupa, прво издање*, Naučna knjiga, 1983.