Лекція 14. Теорема Лагранжа для скінченних груп.

Нехай H – підгрупа групи G, g – фіксований елемент у G. Лівим суміжним класом групи G за підгрупою H (з представником g) називаємо множину елементів вигляду gh, де h пробігає всі елементи підгрупи H. Цю множину позначатимемо через gH. Аналогічно визначаємо правий суміжний клас Hg групи G за підгрупою H.

Далі наведено приклади суміжних класів:

1) нехай $G = S_3$ – група підстановок з трьох елементів. Кількість елементів у вказаній групі дорівнює 6. Позначимо елементи цієї групи так: $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

Два числа i та j в нижньому рядку підстановки складають інверсію, якщо $i > j$, але число i знаходиться раніше від j. Підстановку називають парною, якщо загальна кількість інверсій в її нижньому рядку парна, і непарною в протилежному випадку. Зауважимо, що означення парності підстановки не залежить від форми запису цієї підстановки. Множина парних підстановок $H = \{e, a, f\}$ є підгрупою групи S_3. Разом з тим множина непарних підстановок $K = \{b, c, d\}$ підгрупу групи S_3 не утворює.

Таблиця Келі виконання операції композиції підстановок для групи S_3 наведена в табл. 10. З цієї таблиці видно, що операція у вказаній групі не є комутативною, бо скажімо $a \circ b = d$, але $b \circ a = c$, тобто композиції $a \circ b$ та $b \circ a$ не співпадають.

Табл. 10. Таблиця Келі групи підстановок S_3.

$\circ$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	f	d	b	c	e
b	b	c	e	a	f	d
c	c	d	f	e	a	b
d	d	b	a	f	e	c
f	f	e	c	d	b	a

Ліві суміжні класи групи підстановок з трьох елементів за підгрупою H парних підстановок мають такий вигляд:

eH={ e, a, f}, aH={ e, a, f}, fH={ e, a, f},
bH={ b, c, d}, cH={ b, c, d}, dH={ b, c, d}.

Праві суміжні класи групи підстановок з трьох елементів за підгрупою H парних підстановок мають наведений далі вигляд:

He={ e, a, f}, Ha={ e, a, f}, Ha^2={ e, a, f},
Hb={ b, c, d}, Hc={ b, c, d}, Hd={ b, c, d}.

Як бачимо, у даному прикладі $eH = He$, $aH = Ha$, $bH = Hb$, $cH = Hc$, $dH = Hd$, $fH = Hf$, тобто ліві суміжні класи співпадають з відповідними правими суміжними класами.

Проте таке співпадіння не завжди має місце, як показує такий приклад:

2) нехай $G = S_3$, $H_1 = \{e, b\}$. Лівий суміжний клас, породжений елементом d, складається з двох елементів: $dH_1 = \{de, db\} = \{d, a\}$. Правий суміжний клас виглядає так $H_1d = \{ed, bd\} = \{d, f\}$. Як бачимо, в цьому випадку відповідні суміжні класи є різними: $dH_1 \neq H_1d$.

3) нехай $G = \mathbf{Z}$, H – підгрупа цілих чисел, кратних числу 5. Суміжний клас, утворений числом 1, є множиною $1 + 5\mathbf{Z} = \{1, 1\pm5, 1\pm2\cdot5, \ldots\}$. Це всі цілі числа, які при діленні на 5 дають остачу 1.

Очевидно, що існує тільки 5 різних класів групи $\mathbf{Z}$ за підгрупою $5\mathbf{Z}$, а саме: $5\mathbf{Z}$, $1 + 5Z$, $2 + 5\mathbf{Z}$, $3 + 5\mathbf{Z}$, $4 + 5\mathbf{Z}$.

Зафіксуємо деяку підгрупу H групи G і розглянемо всі можливі ліві суміжні класи за цією підгрупою, утворені елементами групи G. Перш за все ясно, що кожний елемент $g \in G$ належить до деякого класу , а саме, до класу gH, бо $g = ge \in gH$.

Далі, якщо підгрупа H скінченна і має n елементів, то кожен суміжний клас також має n елементів. Дійсно, якщо $h_1 \neq h_2$, то $gh_1 \neq gh_2$, бо за законом скорочення із $gh_1 = gh_2$ отримуємо $h_1 = h_2$.

Для нескінченної підгрупи ці міркування означають, що множини gH та H рівнопотужні. Тоді й ліві суміжні класи рівнопотужні.

Усе раніше сказане справедливе й для правих суміжних класів.

Лема 1. Усякі два суміжні класи за однією і тією ж підгрупою або не перетинаються або співпадають.

Доведення. Щоб довести лему, треба довести таке: із $g_1H \cap g_2H \neq \varnothing$ випливає $g_1H = g_2H$. Нехай $g_0 \in g_1H \cap g_2H$, тобто $g_0 = g_1h_1 = g_2h_2$, де $h_1, h_2 \in H$. Тоді

$g_1H \subseteq g_2H$. Це випливає з низки рівностей, які справедливі для будь-якого $h \in H$: $g_1h = g_1(h_1(h_1)^{-1})h = g_0h' = g_2h_2h' = g_2h'' \in g_2H$.

Аналогічно можна довести, що $g_2H \subseteq g_1H$. Тоді отримуємо, що дійсно $g_1H = g_2H$.

Теорема 5 (Лагранж). Кількість елементів будь-якої підгрупи H скінченої групи G є дільником кількості елементів групи.

Доведення. Кожен елемент $g \in G$ належить принаймні до одного класу, а саме до класу gH. Тому суміжні класи утворюють покриття групи. За доведеною лемою бачимо, що група є об'єднанням суміжних класів, які не перетинаються. Кількість класів позначатимемо через j і назвемо індексом підгрупи H у групі G. Оскільки всі класи мають однакову кількість елементів, то $n = j\,m$, де n – кількість елементів групи G, а m – кількість елементів підгрупи H. Теорему доведено.

Наслідок 2. a) Група простого порядку не має жодних підгруп, крім тривіальних.

b) Порядок елемента скінченої групи ділить порядок групи.

c) Група простого порядку завжди циклічна.

Доведення. a) Випливає з того, що просте число p має лише два можливих дільники: числа 1 та p.

b) Розглянемо циклічну підгрупу, породжену якимось елементом групи. Кількість елементів цієї підгрупи дорівнює порядку елемента. Далі застосовуємо теорему 5.

c) Візьмемо довільний елемент групи простого порядку, який не дорівнює нейтральному елементу цієї групи. У циклічний підгрупі, породженій вказаним елементом, є більше, ніж один елемент. Тоді застосовуємо наслідок 2 a.

Не слід думати, що для будь-якого дільника m кількості елементів групи завжди у цій групі існує підгрупа з кількістю елементів m. Так, у групі A_4 (підгрупа парних підстановок групи S_4), яка має 12 елементів, не існує підгруп з 6 елементів.

Підгрупа H групи G називається нормальною підгрупою, якщо $gH = Hg$ для всіх $g \in G$. Остання умова означає, що відповідні ліві й праві суміжні класи за нормальною підгрупою співпадають. Сукупність суміжних класів за нормальною підгрупою утворює групу. Операція множення суміжних класів визначається за допомогою рівності $g_1H \bullet g_2H = (g_1\,g_2)H$. Ця група називається

фактор-групою групи G за нормальною підгрупою H і позначається G / H. Нормальність потрібна для того, щоб показати коректність визначення добутку суміжних класів (тобто незалежність результату від вибору представників g_1, g_2 суміжних класів).

Зрозуміло, що у випадку абелевої групи кожна підгрупа є нормальною. Таку ситуацію, зокрема, маємо коли беремо як групу $G = \mathbf{Z}$ множину цілих чисел відносно додавання, а як підгрупу H підмножину цілих чисел, кратних числу 5. Як зауважено раніше, існує 5 різних класів групи $\mathbf{Z}$ за підгрупою $5\mathbf{Z}$, тобто фактор-група $\mathbf{Z} / 5\mathbf{Z}$ складається з 5 елементів, а саме: $\overline{0}=5\mathbf{Z}$, $\overline{1}=1+5\mathbf{Z}$, $\overline{2}=2+5\mathbf{Z}$, $\overline{3}=3+5\mathbf{Z}$, $\overline{4}=4+5\mathbf{Z}$. Таблиця Келі для цієї групи цілих чисел за модулем числа 5 наведена в табл. 9.

Розглянемо також приклад неабелевої групи $G = S_n$ підстановок з n елементів (n – довільне натуральне число не менше, ніж 3) відносно операції композиції підстановок. Як підгрупу беремо множину парних підстановок $H=A_n$. Тоді фактор-група S_n / A_n складається з двох класів: парні підстановки $\overline{p} = pH$ та непарні підстановки $\overline{n} = nH$. В якості n можна взяти довільну парну підстановку (наприклад, тотожну), а в якості p – довільну непарну підстановку. Таблиця Келі для цієї групи показана в табл. 11.

Табл. 11.

•	$\overline{p}$	$\overline{n}$
$\overline{p}$	$\overline{p}$	$\overline{n}$
$\overline{n}$	$\overline{n}$	$\overline{p}$