[4] *Чичкарёв Е.А.* Компьютерная математика с Maxima. Руководство для школьников и студентов / Е.А. Чичкарёв. – М.: ALT Linux, 2009. – 233 с.
[5] *Шнайер Б.* Разделение секрета : [пер. с англ.] / Б. Шнайер // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – С. 93 – 96.
[6] *Шнайер Б.* Алгоритмы разделения секрета : [пер. с англ.] / Б. Шнайер // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – С. 588 – 591.

УДК 512.53

Рябухо О.М., Турка Т.В., Литвиненко Л.П.

[1] *канд. фіз.-мат. наук, доцент, зав. кафедри алгебри, СДПУ*

[2] *асистент кафедри алгебри, СДПУ*

[3] *студентка 5 курсу фізико-математичного факультету, СДПУ*

e-mail: kafedra_algebry_sdpu@mail.ru

НАПІВГРУПА ВІДПОВІДНОСТЕЙ СКІНЧЕННОЇ ГРУПИ

Дослідження полягає у вивченні напівгрупи відповідностей скінченної групи, зокрема обчислено порядки напівгрупи відповідностей знакозмінної групи четвертого порядку $S(A_4)$ та групи кватерніонів восьмого порядку $S(Q_8)$.

Ключові слова: *напівгрупа відповідностей, порядок напівгрупи, знакозмінна група, група кватерніонів.*

Вступ

Поняття напівгрупи та відповідний термін виникли на початку XX століття, а систематичні дослідження напівгруп почалися в кінці 20-х років. До 60-х років теорія напівгруп сформувалася в область алгебри, що динамічно розвивається, з багатою проблематикою і різноманітними застосуваннями. В ці роки з'явилися і перші монографії, які цілком присвячені теорії напівгруп.

Першим задачу вивчення напівгруп відповідностей поставив Курош О.Г. в своєму курсі з теорії універсальних алгебр (див. [1]). Однак зроблено в цьому напрямку небагато. Є кілька робіт (наприклад, Іскандер [2], [3]), де вивчалася будова напівгрупи $S(G)$ як решітки відносно природного часткового порядку. Але напівгрупи відповідностей конкретних універсальних алгебр майже не досліджувалися.

У роботі [4] обчислено порядок напівгруп $S(G)$, коли G є скінченною групою. Зокрема, явно вказано порядок $|S(G)|$ для трьох класичних серій скінченних груп: циклічних, діедральних та елементарних абелевих.

Продовжуючи роботу над вивченням напівгруп відповідностей скінченних груп, ми обчислили порядок напівгруп відповідностей знакозмінної групи степеня чотири $S(A_4)$ та групи кватерніонів восьмого порядку $S(Q_8)$.

Порядок напівгрупи відповідностей

Нехай G — універсальна алгебра. Якщо підалгебру з $G \times G$ розглядати як бінарне відношення на G, то множина $S(G)$ всіх підалгебр з $G \times G$ є напівгрупою відносно деморганівського добутку відношень. Напівгрупа $S(G)$ називається *напівгрупою відповідностей* алгебри G.

У роботі [4] показано, що коли G — група, то елементи напівгрупи $S(G)$ можна ототожнити з п'ятірками вигляду $(H_1, G_1, H_2, G_2, \varphi)$, де $H_1 \lhd G_1 < G$, $H_2 \lhd G_2 < G$, а φ — ізоморфізм факторгрупи G_1/H_1 на факторгрупу G_2/H_2. При цьому відповідний елемент напівгрупи $S(G)$ — як підмножина із $G \times G$ — має вигляд

$$(H_1, G_1, H_2, G_2, \varphi) = \bigcup_{a \in G_1} (aH_1 \times \varphi(aH_1)).$$

Множини вигляду $aH_1 \times bH_2$, де $bH_2 = \varphi(aH_1)$ є блоками елемента $A = (H_1, G_1, H_2, G_2, \varphi)$.

Якщо $H, N \leq G$ і $N \lhd H$, то факторгрупа H/N називається фактором групи G. Вибираємо з кожного класу ізоморфних факторів групи G по представнику і позначаємо через $\mathfrak{F}(G)$ множину цих представників. Тоді для кожного з можливих факторів $F \in \mathfrak{F}$ число K_F є потужністю відповідного класу ізоморфних факторів, тобто

$$K_F = |\{(N, H) | N \lhd H \ i \ H/N \simeq F\}|.$$

Теорема 1. *Для будь-якої скінченної групи G порядок напівгрупи відповідностей $S(G)$ дорівнює*

$$|S(G)| = \sum_{F \in \mathfrak{F}(G)} K_F^2 \cdot |\mathrm{Aut}\ F|. \qquad (1)$$

Порядок напівгрупи відповідностей $S(A_4)$.

A_4 — група парних підстановок степеня 4. Підгрупи E, A_4 і K_4 є нормальними в групі A_4. Група $K_4 = \{\varepsilon, (12)(34), (13)(24), (14)(23)\}$, так звана четверна група Кляйна, має підгрупи E, K_4, $\langle(12)(34)\rangle$, $\langle(13)(24)\rangle$, $\langle(14)(23)\rangle$. Всі вони будуть нормальними в групі K_4.

Скориставшись теоремою про порядок напівгрупи відповідностей скінченної групи знайдемо порядок напівгрупи відповідностей групи парних підстановок степеня 4, тобто $|S(A_4)|$.

Задача 1. *Обчислити порядок напівгрупи відповідностей* $S(A_4)$ *знакозмінної групи* A_4, *тобто* $|S(A_4)|$.

Розв'язання. Згідно теореми 2 [4] для будь-якої скінченної групи, зокрема групи A_4, порядок напівгрупи відповідностей $S(A_4)$ дорівнює

$$|S(A_4)| = \sum_{F \in \mathfrak{F}(A_4)} K_F^2 \cdot |Aut\ F|, \tag{2}$$

де $\mathfrak{F}(A_4)$ — множина всіх представників класів ізоморфних факторів F групи A_4:

$$\mathfrak{F}(A_4) = \{E, C_2, C_3, K_4, A_4\}.$$

До кожної підгрупи групи A_4, класи ізоморфних факторів, їх потужність (число K_F) та потужність групи автоморфізмів проілюструємо за допомогою таблиці:

$H \leq A_4 \times A_4$	$\lvert H\rvert$	F	K_F	$\lvert\text{Aut } F\rvert$
E	1	E	$K_E = 10$	$\lvert\text{Aut } E\rvert = 1$
C_2	3	E, C_2	$K_{C_2} = 6$	$\lvert\text{Aut } C_2\rvert = 1$
C_3	4	E, C_3	$K_{C_3} = 5$	$\lvert\text{Aut } C_3\rvert = 2$
K_4	1	E, C_2, K_4	$K_{K_4} = 1$	$\lvert\text{Aut } K_4\rvert = 6$
A_4	1	E, K_4, A_4	$K_{A_4} = 1$	$\lvert\text{Aut } A_4\rvert = 12$

Тепер скориставшись формулою 3 обчислимо потужність напівгрупи відповідностей знакозмінної групи степеня 4.

$$|S(A_4)| = K_E^2 \cdot |\text{Aut } E| + K_{C_2}^2 \cdot |\text{Aut } C_2| + K_{C_3}^2 \cdot |\text{Aut } C_3| +$$
$$+ K_{K_4}^2 \cdot |\text{Aut } K_4| + K_{A_4}^2 \cdot |\text{Aut } A_4| =$$
$$= 10^2 \cdot 1 + 6^2 \cdot 1 + 5^2 \cdot 2 + 1^2 \cdot 6 + 1^2 \cdot 12 = 204.$$

Порядок напівгрупи відповідностей $S(Q_8)$.

В теорії груп, група кватерніонів Q_8 є неабелевою групою порядку 8, ізоморфною множині восьми визначенним кватерніонам з операцією множення. В групі Q_8 маємо підгрупи E, Q_8, $\{\pm 1\}$, $< i >$, $< j >$, $< k >$. Всі вони є нормальними.

Задача 2. *Обчислити порядок напівгрупи відповідностей* $S(Q_8)$ *групи кватерніонів* Q_8, *тобто* $|S(Q_8)|$.

Розв'язання. Згідно теореми 1 для будь-якої скінченної групи Q_8 порядок напівгрупи відповідностей $S(Q_8)$ дорівнює

$$|S(Q_8)| = \sum_{F \in \mathfrak{F}(Q_8)} K_F^2 \cdot |Aut\ F|, \tag{3}$$

де $\mathfrak{F}(Q_8)$ — множина всіх представників класів ізоморфних факторів F групи Q_8:

$$\mathfrak{F}(Q_8) = \{E, C_2, C_4, K_4, Q_8\}.$$

До кожної підгрупи групи Q_8, класи ізоморфних факторів, їх потужність (число K_F) та потужність групи автоморфізмів проілюструємо за допомогою наступної таблиці

$H \leq Q_8 \times Q_8$	$\lvert H\rvert$	F	K_F	$\lvert\text{Aut } F\rvert$
E	1	E	$K_E = 6$	$\lvert\text{Aut } E\rvert = 1$
C_2	1	E, C_2	$K_{C_2} = 7$	$\lvert\text{Aut } C_2\rvert = 1$
C_4	3	E, C_2, C_4	$K_{C_4} = 3$	$\lvert\text{Aut } C_4\rvert = 2$
Q_8	1	E, C_2, K_4, Q_8	$K_{K_4} = 1$ $K_{Q_8} = 1$	$\lvert\text{Aut } K_4\rvert = 6$ $\lvert\text{Aut } Q_8\rvert = 24$

Тепер скориставшись формулою 3 обчислимо потужність напівгрупи відповідностей групи кватерніонів порядку 8.

$$\begin{gathered}|S(Q_8)| = K_E^2 \cdot |\text{Aut } E| + K_{C_2}^2 \cdot |\text{Aut } C_2| + K_{C_4}^2 \cdot |\text{Aut } C_4| + \\ + K_{K_4}^2 \cdot |\text{Aut } K_4| + K_{Q_8}^2 \cdot |\text{Aut } Q_8| = \\ = 6^2 \cdot 1 + 7^2 \cdot 1 + 3^2 \cdot 2 + 1^2 \cdot 6 + 1^2 \cdot 24 = 133.\end{gathered}$$

Висновки

В роботі ми продовжили вивчати порядок напівгруп відповідностей $S(G)$, коли G є скінченною групою. Зокрема, обчислили порядки напівгруп відповідностей знакозмінної групи $|S(A_4)|$ та групи кватерніонів $|S(Q_8)|$.

Література

[1] *Курош А.Г.* Общая алгебра / А.Г. Курош. – М.: Наука, 1974. – 160 с.

[2] *Искандер А.А.* Структура соответствий универсальной алгебры. – Изв. АНСССР, сер. матем. – 1965. – т.29. – С. 1357 – 1372.

[3] *Искандер А.А.* Частичные универсальные алгебры с заданными структурами подалгебр и соответствий / А. А. Искандер // Матем. сборник. – 1960. – т. 70. – С. 438 – 456.

[4] *Ганюшкін О.Г.* Порядок напівгрупи відповідностей скінченної групи / О.Г. Ганюшкін, Т.В. Турка // Вісник Київського університету. Серія : фіз.-мат. науки. – 2009. – вип. № 3. – С. 9 – 13.