2. *Що таке електронний цифровий підпис? [Урядовий портал]. URL: https://www.kmu.gov.ua/usi-pitannya-po-e-poslugam/sho-tak-elektronnij-cifrovij-pidpis-ecp*
3. *ЕЦП або КЕП: чим підписувати електронні документи? URL: https://biz.ligazakon.net/analitycs/200366_etsp-abo-kep-chim-pdpisuvati-elektronn-dokumenti*
4. *Піддубна Л. В., Павліченко В. М., Інформаційна безпека в системах електронного документообігу. Науковий вісник Полтавського університету економіки і торгівлі. 2019. № 4 (95) http://journal.puet.edu.ua/index.php/nven/article/viewFile/1588/1422*
5. *Станісла Лур'є. Безпечність використання електронного цифрового підпису URL: https://investgazeta.ua/blogs/bezpechnist-vikoristannya-elektronnogo-tsifrovogo-pidpisu*

УДК 546.07

Сохацький Ф.М., д.ф.-м.н., доцент, доцент кафедри прикладної математики
Луценко А.В., асистент кафедри прикладної математики

МАТРИЧНІ IP-КВАЗІГРУПИ 4-ГО ПОРЯДКУ

Донецький національний університет імені Василя Стуса, м. Вінниця

Центральні квазігрупи в класі квазігруп відіграють таку ж саму роль, що і комутативні групи в класі всіх груп. Крім того, центральні квазігрупи є лінійними ізотопами комутативних груп, що дозволяє значно поглибити результати про оборотність, сформульовані авторами в [2, 3], зокрема, стосовно ізотопів груп, отриманих у [4]. Матричні квазігрупи є одним із видів центральних квазігруп, а в деяких випадках збігаються з матричними квазігрупами. Тому вивчення центральних і матричних квазігруп викликає значний інтерес.

Означення 1 [1]. *Квазігрупою* називається групоїд $(Q;\cdot)$ такий, що для довільних a,b кожне з рівнянь $a\cdot x=b$, $y\cdot a=b$ має єдиний розв'язок.

Квазігруповою (оборотною) операцією називають функцію, визначену на скінченній чи нескінченній множині, якщо вона оборотна за кожною своєю змінною.

Нехай K - довільне комутативне кільце з одиницею і $K^n=K\times\ldots\times K$. Групоїд $(K^n;f)$ визначений рівністю

$$f(\bar{x},\bar{y})=\bar{x}A+\bar{y}B+\bar{a},$$

де A, $B\in M_n(K)$ і $\bar{a}\in K^n$ називається *матричною квазігрупою* над

кільцем K, якщо квадратні матриці A, B оборотні.

Означення 2. Квазігрупа $(Q;\cdot)$ називається: *середньою, лівою та правою IP квазігрупою,* якщо відповідно існують відображення λ, ρ, μ, такі, що для всіх x, y виконуються рівності

$$x \cdot y = \mu(y \cdot x); \quad \lambda(x) \cdot xy = y; \quad yx \cdot \rho(x) = y;$$

λ, ρ, μ називаються *лівою, правою* та *середньою функцією оборотності*.

В праці [2] було повністю описано квазігрупи з властивостями оборотності відповідно до рівностей множин трансляцій та отримано 9 многовидів, які розподілені у три парастрофні орбіти: IP квазігруп, CIP квазігруп та дзеркальних квазігруп. В класі матричних квазігруп досить розглянути дві парастрофні орбіти, оскільки всі дзеркальні квазігрупи є IP квазігрупами.

Класифікація матричних IP та CIP квазігруп подано в праці [3]. Для описання центральних квазігруп з інверсною властивістю (IP) потрібно розв'язати матричне рівняння $X^2 = E$. Дане рівняння цілком розв'язане над множиною матриць другого порядку, які визначені над полем лишку 2. Зокрема, отримано таке твердження.

Твердження. *Для описання центральних середніх IP квазігруп (а отже, лівих і правих IP квазігруп) досить розв'язати матричне рівняння*

$$X^2 = E.$$

Лема [3]**.** Множина U всіх розв'язків матричного рівняння $X^2 = E$ над множиною квадратних матриць $M_2(\mathbb{Z}_2)$, де $\mathbb{Z}_2 = \{0, 1\}$, дорівнює

$$U = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}.$$

Наслідок [3]**.** Кількість різних матричних IP квазігруп над полем $\mathbb{Z}_2^2$ подано в таблиці:

середня IP	96
ліва IP	96
права IP	96
ліво-середня IP	64
право-середня IP	64
ліво-права IP	64
тристороння IP	40
Всього	136

Список використаних джерел

1. *Белоусов В.Д. Основы теории квазигрупп и луп // М.: Наука, 1967. - 223с.*

2. *Sokhatsky F.M., Lutsenko A.V. Classification of quasigroups according to directions of translations II. Commentationes Mathematicae Universitatis Carolinae. 2021. Vol. 62, No 3. P. 309-323.*
3. *Sokhatsky F.M., Lutsenko A.V., Fryz I.V. Constructing quasigroups with invertibility property, Math. Methods and Physic. Fields, 64 (2021), No.4 (in Ukrainian).*
4. *Lutsenko A.V. Classification of group isotopes according to their inverse properties. Applied problems of mechanics and mathematics. - 2020. - Vol. 13, 48-62. DOI:10.15407/apmm2020.18.48-61*

УДК 512.548

Сохацький Ф.М., д.ф.-м.н., доцент,
доцент кафедри прикладної математики
Фриз І.В., к.ф.-м.н., ст. викладач
кафедри прикладної математики

ПОБУДОВА МЕДІАЛЬНИХ ТОТАЛЬНО-ПАРАСТРОФНО ОРТОГОНАЛЬНИХ ТЕРНАРНИХ КВАЗІГРУП

Донецький національний університет імені Василя Стуса, м. Вінниця

Квазігрупові алгебри з властивістю ортогональності знаходять своє застосування як в алгебрі, так і в комбінаториці, геометрії, криптографії, теорії кодування тощо, зокрема зв'язок між ортогональністю та максимально дистанційно роздільними (МДР) кодами описаний в [1]. Проте проблема їх побудови досі є відкритою. Це питання для операцій арності більше двох вивчалося у [2, 3, 4], для квазігруп – у [5].

Тернарна операція f, яка визначена на множині Q порядку m, називається *оборотною*, а групоїд $(Q; f)$ називається *квазігрупою* порядку m, якщо для будь-яких $a, b \in Q$ кожен з термів $f(x, a, b)$, $f(a, x, b)$, $f(a, b, x)$ визначає підстановку множини Q. Кожній тернарній квазігрупі порядку m відповідає *латинський куб* порядку m, тобто тривимірний масив m різних символів із Q, кожен з яких зустрічається точно один раз у кожній лінії.

Трійка тернарних операцій f_1, f_2, f_3, які визначені на множині Q, називаються *ортогональними* [2], якщо система

$$\begin{cases} f_1(x_1, x_2, x_3) = a, \\ f_2(x_1, x_2, x_3) = b, \\ f_3(x_1, x_2, x_3) = c \end{cases}$$

має єдиний розв'язок для всіх $a, b, c \in Q$. Множина тернарних операцій $\Sigma = \{f_1, f_2, f_3, \dots, f_s\}$ називається *ортогональною*, якщо кожна трійка різних операцій із Σ є ортогональною, де $s \geq 3$. Ортогональність трьох операцій