УДК 512.548.7

Ф. М. Сохацький, А. В. Луценко[✉], І. В. Фриз

ПОБУДОВА КВАЗІГРУП ІЗ ВЛАСТИВОСТЯМИ ОБОРОТНОСТІ

Розглядаються лінійні ізотопи комутативних груп, тобто центральні квазігрупи. Вивчаються умови оборотності та ортогональності, які, як виявилось, достатньо вивчати лише для унітарних ізотопів, тобто для ізотопів, які мають ідемпотент. Знайдено критерії наявності кожної із властивостей оборотності (інверсна властивість, схрещена інверсна властивість і дзеркальність) в унітарних центральних і матричних квазігрупах. Зокрема, для матриць другого порядку описано відповідні матричні квазігрупи над полями характеристик 2 і 3. Встановлено критерії ортогональності матричних квазігруп із зазначеними властивостями оборотності.

Ключові слова: *квазігрупа, напівгрупа, автоморфізм, ендоморфізм, конгруенція, матричне рівняння, кільце, матрична квазігрупа, тепліцева матриця, повна матриця.*

Вступ. У класі квазігруп центральні квазігрупи відіграють ту саму роль, що й комутативні групи в класі всіх груп. У той же час центральні квазігрупи є лінійними ізотопами комутативних груп, що дозволяє значно поглибити результати про оборотність, сформульовані авторами в [7−11], зокрема, стосовно ізотопів груп, отриманих у [4]. Матричні квазігрупи є одним із видів центральних квазігруп, а в деяких випадках (наприклад, лінійні ізотопи елементарних абелевих груп) збігаються з матричними квазігрупами. Тому вивчення центральних і матричних квазігруп становить значний інтерес.

У цій статті наведено критерії оборотності та ортогональності для матричних квазігруп. Зокрема, показано, що для опису квазігруп з інверсною властивістю (IP-квазігруп) потрібно розв'язати матричне рівняння $X^2 = E$. Це рівняння цілком розв'язане над множиною матриць другого порядку, які визначені над полями лишків 2 і 3. Тим самим описано відповідні центральні квазігрупи. Отримані критерії ортогональності дають новий метод побудови ортогональних квазігруп і латинських квадратів.

1. Додаткові відомості.

***Означення 1* [1].** *Квазігрупою* називають групоїд $(Q;\cdot)$ такий, що для довільних $a, b \in Q$ система 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 Q є базовою множиною для операцій, які розглядаються. Бінарна операція f називається *оборотною*, якщо вона є оборотним елементом в обох моноїдах: *лівому симетричному моноїді* $(\Omega;\underset{\ell}{\oplus},e_\ell)$ і *правому симетричному моноїді* $(\Omega;\underset{r}{\oplus},e_r)$ бінарних операцій, де Ω є множиною всіх бінарних операцій і

$$(g\underset{\ell}{\oplus}h)(x,y) := g(h(x,y),y), \qquad e_\ell(x,y) := x\,,$$

$$(g\underset{r}{\oplus}h)(x,y) := g(x,h(x,y)), \qquad e_r(x,y) := y\,. \tag{1}$$

Означення 2. Дві бінарні операції f і g, визначені на множині Q, називають *ортогональними*, якщо система

[✉] lucenko.alla32@gmail.com

$$\begin{cases} f(x,y) = a, \\ g(x,y) = b \end{cases}$$

має єдиний розв'язок для всіх $a, b \in Q$.

У статті розглядаються оборотні матриці, які є, зокрема, повними.

Нагадаємо, що матриця $A \in M_2(K)$ називається *повною*, якщо $M_2(K) \cdot A \cdot M_2(K) = M_2(K)$, де $M_2(K)$ − кільце матриць порядку 2 над кільцем K [13].

Означення 3 **[**1, 5, 9**]**. Квазігрупу $(Q;\cdot)$ називають *середньою, лівою* та *правою IP-квазігрупою,* якщо відповідно існують відображення λ, ρ, μ такі, що для всіх x, y виконуються рівності

$$x \cdot y = \mu(y \cdot x), \qquad \lambda(x) \cdot xy = y, \qquad yx \cdot \rho(x) = y.$$

Відображення λ, ρ, μ називають *лівою, правою* та *середньою функціями оборотності*, відповідно.

Означення 4 **[**11**]**. Квазігрупу $(Q;\cdot)$ називають *середньою, лівою* та *правою квазігрупою зі схрещеною інверсною властивістю* (*CIP-квазігрупою*), якщо відповідно існують відображення ψ, υ, γ такі, що для всіх x, y виконуються рівності

$$\psi(x) \cdot yx = y, \qquad yx \cdot y = \upsilon(x), \qquad y \cdot xy = \gamma(x).$$

Відображення ψ, υ, γ називають *лівою, правою* та *середньою функціями оборотності.*

Означення 5 **[**11**]**. Квазігрупу $(Q;\cdot)$ називають *середньою, лівою* та *правою дзеркальною квазігрупою*, якщо відповідно існують відображення φ, δ, ξ такі, що для всіх x, y виконуються рівності

$$\varphi(x) \cdot y = y \cdot x, \qquad y \cdot yx = \delta(x), \qquad xy \cdot y = \xi(x).$$

Відображення φ, δ, ξ називають *лівою, правою* та *середньою функціями оборотності.*

2. (Унітарні) групові ізотопи. *Груповим ізотопом* називають квазігрупу, яка є ізотопною деякій групі. Про групові ізотопи відомо таке твердження.

Теорема 1 [3**]**. *Нехай* $(Q;\bullet)$ − *груповий ізотоп* і 0 − *довільний елемент із* Q. *Тоді існує четвірка* $(+,\alpha,\beta,a)$ *така, що* ***1***) $(Q;+,0)$ − *група,* ***2***) α, β − *унітарні підстановки, тобто* $\alpha 0 = \beta 0 = 0$, *та елемент* $a = 0 \bullet 0$ *такі, що*

$$x \bullet y = \alpha(x) + a + \beta(y). \tag{2}$$

При цьому праву частину цієї рівності називають 0-*канонічним розкладом*, підстановки α і β − коефіцієнтами, елемент a − вільним членом, а $(Q;+,0)$ − групою канонічного розкладу.

Ізотоп групи назвемо *унітарним*, якщо він має одноелементну підалгебру. Якщо $\{0\}$ позначає одноелементну підалгебру у групового ізотопа $(Q;\circ)$, то цей ізотоп позначатимемо $(Q;\circ,0)$. Інакше кажучи, 0 є ідемпотентом для операції $(\circ)$: $0 \circ 0 = 0$. Із (2) випливає рівність $a = 0 \circ 0$, тому справджується таке твердження.

Наслідок 1. *Груповий ізотоп* $(Q;\circ)$ *має одноелементну підалгебру* 0 *тоді й тільки тоді, коли в* 0-*канонічному розкладі вільний член дорівнює* 0, *тобто канонічний розклад* (2) *має вигляд*

$$x \circ y = \alpha(x) + \beta(y). \tag{3}$$

Нехай $(Q;\bullet)$ − довільний груповий ізотоп із канонічним розкладом (2) і нехай $(Q;\circ)$ − груповий ізотоп, отриманий із $(Q;\bullet)$ заміною вільного члена нулем, тобто ізотоп, канонічним розкладом якого є (3). Тоді унітарний груповий ізотоп $(Q;\circ,0)$ назвемо *відповідним* груповому ізотопу $(Q;\bullet)$.

Квазігрупа $(Q;\circ)$ називається

- *лінійною*, якщо вона є лінійним ізотопом групи, тобто в її канонічному розкладі (2) перетворення α і β є автоморфізмами групи $(Q;+,0)$;
- *центральною*, якщо вона є лінійним ізотопом абелевої групи;
- *медіальною*, якщо виконується тотожність

  $(x\circ y)\circ(u\circ v)=(x\circ u)\circ(y\circ v)$;
- *абелевою*, якщо вона є медіальною і має одноелементну підалгебру, наприклад, $\{0\}$, тобто 0 є її ідемпотентом: $0\circ 0=0$. Таку абелеву квазігрупу позначатимемо $(Q;\circ,0)$.

Повну класифікацію многовидів лінійних квазігруп наведено в роботі [8], а лінійні ізотопи циклічних груп досліджено в праці [12]. У теоремі Брука − Тойоди знайдено канонічний розклад медіальної квазігрупової операції, проте ця теорема випливає з більш загального результату, отриманого у [6] для медіальних та абелевих універсальних алгебр. Сформулюємо теорему Брука − Тойоди у зручному вигляді.

Теорема 2 [1]. *Квазігрупа є медіальною тоді й тільки тоді, коли вона є центральною і коефіцієнти канонічного розкладу комутують.*

3. Центральні квазігрупи з властивістю оборотності. У праці [4] досліджено групові ізотопи з властивостями оборотності. Зокрема, знайдено умови, коли груповий ізотоп буде *IP*-квазігрупою, *CIP*-квазігрупою та дзеркальною квазігрупою. У цьому параграфі проведемо дослідження для центральних квазігруп, тому переформулюємо теореми, які були доведені в [4] для групових ізотопів.

Теорема 3 [4]. *Нехай* $(Q;\circ)$ − *центральна квазігрупа і* (2) − *її канонічний розклад. Тоді*

1) $(Q;\circ)$ *є середньою IP-квазігрупою тоді й тільки тоді, коли існує інволютивний автоморфізм* θ *такий, що* $\beta=\theta\alpha$. *Функція оборотності* μ *обчислюється за формулою*

   $\mu(x)=\theta(x)+a+\theta(a)$;

2) $(Q;\circ)$ *є лівою IP-квазігрупою тоді й тільки тоді, коли* β *є інволютивним автоморфізмом групи* $(Q;+)$. *Функція оборотності* λ *обчислюється за формулою*

   $\lambda(x)=-\alpha^{-1}\beta(a)-\alpha^{-1}\beta\alpha(x)-\alpha^{-1}(a)$;

3) $(Q;\circ)$ *є правою IP-квазігрупою тоді й тільки тоді, коли* α *є інволютивним автоморфізмом групи* $(Q;+)$. *Функція оборотності* ρ *обчислюється за формулою*

   $\rho(x)=-\beta^{-1}(a)-\beta^{-1}\alpha\beta(x)-\beta^{-1}\alpha(a)$.

Для унітарної центральної квазігрупи отримуємо такий

Наслідок 2. *Нехай* $(Q;\circ,0)$ − *унітарна центральна квазігрупа і* (3) − *її канонічний розклад. Тоді*

1) $(Q;\circ)$ *є середньою IP-квазігрупою тоді й тільки тоді, коли існує інволютивний автоморфізм* θ *такий, що* $\alpha=\theta\beta$, $\theta^2=\iota$. *Функція оборотності* μ *обчислюється за формулою* $\mu=\theta$;
2) $(Q;\circ)$ *є лівою IP-квазігрупою тоді й тільки тоді, коли* β *є інволютивним автоморфізмом групи* $(Q;+)$. *Функція оборотності* λ *обчислюється за формулою* $\lambda=-\alpha^{-1}\beta\alpha$;

3) $(Q;\circ)$ *є правою IP-квазігрупою тоді й тільки тоді, коли α є інволютивним автоморфізмом групи $(Q;+)$. Функція оборотності ρ обчислюється за формулою $\rho = -\beta^{-1}\alpha\beta$.*

Д о в е д е н н я випливає з означення унітарної центральної квазігрупи та теореми 3. ♦

Групові ізотопи з властивістю схрещеної оборотності досліджено в працях [2, 4]. Для центральних *CIP*-квазігруп переформулюємо таку теорему.

Теорема 4 [4]. *Нехай $(Q;\circ)$ – центральна квазігрупа і її канонічний розклад визначається формулою* (2). *Тоді*

1) $(Q;\circ)$ *є середньою CIP-квазігрупою тоді й тільки тоді, коли $\beta = \alpha^{-1}$. Функція оборотності ψ обчислюється за формулою*

$$\psi(x) = -\alpha^{-2}(a) - \alpha^{-3}(x) - \alpha^{-1}(a);$$

2) $(Q;\circ)$ *є лівою CIP-квазігрупою тоді й тільки тоді, коли $\beta = -\alpha^{2}$. Функція оборотності υ обчислюється за формулою*

$$\upsilon(x) = \alpha\beta(x) + \alpha(a) + a;$$

3) $(Q;\circ)$ *є правою CIP-квазігрупою тоді й тільки тоді, коли $\alpha = -\beta^{2}$. Функція оборотності γ обчислюється за формулою*

$$\gamma(x) = a + \beta(a) + \beta\alpha(x).$$

Наслідок 3. *Нехай $(Q;\circ,0)$ – унітарна центральна квазігрупа і* (3) *– її канонічний розклад. Тоді*

1) $(Q;\circ)$ *є середньою CIP-квазігрупою тоді й тільки тоді, коли $\beta = \alpha^{-1}$. Функція оборотності ψ обчислюється за формулою $\psi = -\alpha^{-3}$;*

2) $(Q;\circ)$ *є лівою CIP-квазігрупою тоді й тільки тоді, коли $\beta = -\alpha^{2}$. Функція оборотності υ обчислюється за формулою $\upsilon = \alpha\beta$;*

3) $(Q;\circ)$ *є правою CIP-квазігрупою тоді й тільки тоді, коли $\alpha = -\beta^{2}$. Функція оборотності γ обчислюється за формулою $\gamma = \beta\alpha$.*

Д о в е д е н н я випливає з означення унітарної центральної квазігрупи та теореми 4. ♦

Наслідок 4. *Якщо центральна квазігрупа є середньою, лівою чи правою CIP-квазігрупою, то вона є медіальною.*

Д о в е д е н н я випливає з теореми Брука – Тойоди та теореми 4.♦

Випадок, коли груповий ізотоп має властивість дзеркальності, досліджено в праці [4]. Як висновок з отриманих там результатів можемо сформулювати таку теорему.

Теорема 5 [4]. *Нехай $(Q;\circ)$ – центральна квазігрупа і* (2) *– її канонічний розклад. Тоді*

1) $(Q;\circ)$ *є середньою дзеркальною квазігрупою тоді й тільки тоді, коли вона є комутативною;*

2) $(Q;\circ)$ *є лівою дзеркальною квазігрупою тоді й тільки тоді, коли вона є ліво-симетричною;*

3) $(Q;\circ)$ *є правою дзеркальною квазігрупою тоді й тільки тоді, коли вона є право-симетричнаою.*

Отже, центральна квазігрупа з властивістю дзеркальності є центральною квазігрупою з відповідною властивістю оборотності, тому надалі будемо розглядати центральні лише *IP*-квазігрупи та *CIP*-квазігрупи.

4. Матричні квазігрупи. Серед центральних квазігруп особливу роль відіграють матричні квазігрупи. Нехай K − довільне комутативне кільце з одиницею. Бінарну операцію f, яка визначена над комутативною групою $(K^n;+)$, назвемо

- *матричною*, якщо існують квадратні матриці A, B порядку n над m-елементним кільцем K і $\overline{a} \in K^n = K \times \ldots \times K$ такі, що для всіх $\overline{x}, \overline{y} \in K^n$ виконується рівність
$$f(\overline{x}, \overline{y}) = \overline{x}A + \overline{y}B + \overline{a}, \qquad (4)$$
при цьому пару $(K^n; f)$ назвемо *матричним групоїдом порядку* m^n;
- *унітарною матричною*, якщо існують квадратні матриці A, B порядку n над кільцем K порядку m такі, що для всіх $\overline{x}, \overline{y} \in K^n$ виконується рівність
$$f(\overline{x}, \overline{y}) = \overline{x}A + \overline{y}B, \qquad (5)$$
при цьому пару $(K^n; f)$ назвемо *унітарним матричним групоїдом порядку* m^n.

Твердження 1. *Матричний групоїд є квазігрупою тоді й тільки тоді, коли матриці A і B є оборотними.*

Д о в е д е н н я. Оборотність операції f означає, що кожне з рівнянь
$$f(\overline{x}, \overline{y}) = \overline{c}, \qquad f(\overline{b}, \overline{y}) = \overline{c}.$$
має єдиний розв'язок. Відповідно до (4) ці рівняння рівносильні рівнянням
$$\overline{x}A + \overline{b}B + \overline{a} = \overline{c}, \qquad \overline{b}A + \overline{y}B + \overline{a} = \overline{c},$$
тобто
$$\overline{x}A = \overline{c} - \overline{b}B - \overline{a}, \qquad \overline{y}B = \overline{c} - \overline{b}A - \overline{a}.$$

Однозначна розв'язність цих рівнянь рівносильна оборотності матриць A і B. ♦

Наслідок 5. *Кожна матрична квазігрупа є центральною.*

Д о в е д е н н я. Оскільки множення матриць дистрибутивне, то множення на матрицю є ендоморфізмом, а тому множення на оборотну матрицю є автоморфізмом відповідної групи. ♦

Із означення унітарної матричної квазігрупи та теореми 3 випливає таке твердження.

Теорема 6. *Нехай $(K^n; f, \overline{0})$ − унітарна матрична квазігрупа і (4) − її канонічний розклад. Тоді*

1) $(K^n; f, \overline{0})$ *є середньою IP-квазігрупою тоді й тільки тоді, коли існує оборотна матриця C така, що $C^2 = E$, $B = AC$. Функція оборотності μ обчислюється за формулою*
$$\mu(\overline{x}) = \overline{x}C;$$
2) $(K^n; f, \overline{0})$ *є лівою IP-квазігрупою тоді й тільки тоді, коли $B^2 = E$. Функція оборотності λ обчислюється за формулою*
$$\lambda(\overline{x}) = -\overline{x}ABA^{-1};$$
3) $(K^n; f, \overline{0})$ *є правою IP-квазігрупою тоді й тільки тоді, коли $A^2 = E$. Функція оборотності ρ обчислюється за формулою*
$$\rho(\overline{x}) = -\overline{x}BAB^{-1}.$$

Теорема 7. *Нехай* $(K^n; f, \overline{0})$ *– унітарна матрична квазігрупа і* (4) *– її канонічний розклад. Тоді*

1) $(K^n; f, \overline{0})$ *є середньою CIP-квазігрупою тоді й тільки тоді, коли* $B = A^{-1}$. *Функція оборотності* ψ *обчислюється за формулою*
$\psi(\overline{x}) = -\overline{x}A^{-3}$;

2) $(K^n; f, \overline{0})$ *є лівою CIP-квазігрупою тоді й тільки тоді, коли* $B = -A^2$. *Функція оборотності* λ *обчислюється за формулою*
$\upsilon(\overline{x}) = -\overline{x}A^3$;

3) $(K^n; f, \overline{0})$ *є правою CIP-квазігрупою тоді й тільки тоді, коли* $A = -B^2$. *Функція оборотності* ρ *обчислюється за формулою*
$\gamma(\overline{x}) = -\overline{x}B^3$.

Д о в е д е н н я випливає з означення унітарної матричної квазігрупи та теореми 4. ♦

Нагадаємо такий відомий факт.

Твердження 2. *Відображення* θ *є ендоморфізмом групи* $(K^n; +)$ *тоді й тільки тоді, коли для деякої матриці* A *виконується рівність* $\theta(\overline{x}) = \overline{x}A$. *Відображення* θ *є автоморфізмом тоді й тільки тоді, коли матриця* A *є оборотною над кільцем* K.

Враховуючи цей факт та теореми 3, 4, маємо такі наслідки.

Наслідок 6. *Кількість IP-квазігруп над кільцем* K *дорівнює кількості пар матриць* (A, C), *де* A *– оборотна матриця над кільцем* K, *а матриця* C *є розв'язком рівняння* $X^2 = E$.

Д о в е д е н н я випливає з твердження 2 та теореми 3. ♦

Наслідок 7. *Кількість CIP-квазігруп над кільцем* K *дорівнює кількості автоморфізмів групи* $(K^n; +)$, *тобто кількості оборотних матриць порядку* n *над кільцем* K.

Д о в е д е н н я випливає з твердження 2 та теореми 4. ♦

Для того щоб знайти вигляд односторонньої, двосторонньої матричної *IP*-квазігрупи та тристоронньої *IP*-квазігрупи потрібно довести таке твердження.

Твердження 3. *Кожна матрична IP-квазігрупа над кільцем* K *має такий вигляд*:

середня IP-квазігрупа	$f(\overline{x}, \overline{y}) = \overline{x}A + \overline{y}AC + \overline{a}$
ліва IP-квазігрупа	$f(\overline{x}, \overline{y}) = \overline{x}A + \overline{y}C + \overline{a}$
права IP-квазігрупа	$f(\overline{x}, \overline{y}) = \overline{x}C + \overline{y}A + \overline{a}$
ліво-середня IP-квазігрупа	$f(\overline{x}, \overline{y}) = \overline{x}C_1C_2 + \overline{y}C_1 + \overline{a}$
право-середня IP-квазігрупа	$f(\overline{x}, \overline{y}) = \overline{x}C_1 + \overline{y}C_1C_2 + \overline{a}$
ліво-права IP-квазігрупа	$f(\overline{x}, \overline{y}) = \overline{x}C_1 + \overline{y}C_2 + \overline{a}$
тристороння IP-квазігрупа	$f(\overline{x}, \overline{y}) = \overline{x}C_1 + \overline{y}C_2 + \overline{a}$, $C_1C_2 = C_2C_1$

Тут A *– оборотна матриця над кільцем* K; C, C_1, C_2 *– уніпотентні матриці*; $\overline{a} \in K^n$.

Д о в е д е н н я. Згідно з рівністю (5) і теоремою 6, середня, ліва та права *IP*-квазігрупи матимуть вигляд

$$f(\overline{x}, \overline{y}) = \overline{x}A + \overline{y}AC + \overline{a}\ ,$$
$$f(\overline{x}, \overline{y}) = \overline{x}A + \overline{y}C + \overline{a}\ ,$$
$$f(\overline{x}, \overline{y}) = \overline{x}C + \overline{y}A + \overline{a}\ ,$$

відповідно.

Розглянемо двосторонні IP-квазігрупи. У середній IP-квазігрупі лівий коефіцієнт має бути уніпотентною матрицею, тому право-середні матриці визначаються рівностями

$$f(\overline{x}, \overline{y}) = \overline{x}C_1 + \overline{y}C_1C_2 + \overline{a}\ , \tag{6}$$

де C_1, C_2 – уніпотентні матриці, тобто вони є розв'язками рівняння $X^2 = E$. Аналогічно утворюються формули для ліво-середніх та праволівих IP-квазігруп.

Для визначення тристоронніх IP-квазігруп розглянемо право-середню IP-квазігрупу (6), де C_1, C_2 – уніпотентні матриці. Вона є лівою IP-квазігрупою тоді й тільки тоді, коли правий коефіцієнт є уніпотентною матрицею, тобто $(C_1C_2)^2 = E$. Помноживши цю рівність справа на матрицю C_2, а потім на матрицю C_1, отримаємо

$$C_1C_2 = C_2C_1\,.$$

Отже, матричні тристоронні IP-квазігрупи мають вигляд (6), коли матриці C_1 і C_2 комутують. ♦

5. Матричні квазігрупи 4-го порядку. З теореми 6 та наслідку 6 випливає таке

Твердження 4. *Для опису центральних середніх IP-квазігруп (а отже, лівих і правих IP-квазігруп) достатньо розв'язати матричне рівняння*

$$X^2 = E\,.$$

Д о в е д е н н я. Згідно з теоремою 6, щоб описати центральні середні (ліві і праві) IP-квазігрупи, треба знайти матриці, які будуть задовольняти умову $C^2 = E$ для середніх IP-квазігруп, $B^2 = E$ для лівих IP-квазігруп та $A^2 = E$ для правих IP-квазігруп. А це й означає, що треба знайти розв'язки матричного рівняння $X^2 = E$. ♦

Розв'язки цього рівняння над групою Клейна $\mathbb{Z}_2^2$ подаємо в такій лемі.

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

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

Д о в е д е н н я. Нехай $C := \begin{pmatrix} x & y \\ u & v \end{pmatrix}$ є розв'язком матричного рівняння $C^2 = E$, тобто

$$\begin{pmatrix} x & y \\ u & v \end{pmatrix} \cdot \begin{pmatrix} x & y \\ u & v \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Звідси маємо таку систему рівнянь:

$$\begin{cases} x^2 + yu = 1, \\ xy + yv = 0, \\ ux + vu = 0, \\ yu + v^2 = 1. \end{cases}$$

1. Нехай $y = 1$, тоді з другого рівняння маємо, що $v = x$. Отже, система рівносильна рівнянню

$$x^2 + yu = 1. \tag{7}$$

1′. Нехай $x = 1$, тоді з рівняння (7) маємо, що $yu = 0$. Звідси $v = 1$, $u = 0$. Отже, матриця матиме вигляд

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

1″. Нехай $x = 0$, тоді $v = 0$, а $yu = 1$. Звідси $u = 1$. Отже, матриця матиме вигляд

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

2. Нехай $y = 0$, тоді система матиме вигляд

$$\begin{cases} x^2 = 1, \\ ux + vu = 0, \\ v^2 = 1. \end{cases}$$

Оскільки $\mathbb{Z}_2$ – поле, то з першого і третього рівнянь маємо $x = 1$ і $v = 1$, а з другого рівняння випливає, що $u = 0$ або $u = 1$. Тоді матриці матимуть вигляд

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Отже, отримали множину розв'язків U. Лему доведено. ♦

Зауважимо, що всі матриці із множини U є тепліцевими. Нагадаємо, що матриця другого порядку над комутативним кільцем K називається *тепліцевою*, якщо її діагональні елементи однакові.

Отримані результати дозволяють обчислювати матричні квазігрупи скінченного порядку. Для групи Клейна маємо такий наслідок.

Наслідок 8. *Кількість різних матричних IP-квазігруп над полем* $\mathbb{Z}_2$ *подано в таблиці*:

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

Д о в е д е н н я. Оскільки група Клейна має 6 автоморфізмів, то згідно з твердженням 2 і наслідком 6 кількість односторонніх *IP*-квазігруп над групою Клейна $\mathbb{Z}_2^2$ буде дорівнювати $6 \times 4 \times 4 = 96$.

Оскільки в двосторонніх квазігрупах є 3 незалежних параметри, то кількість двосторонніх квазігруп дорівнює $4 \times 4 \times 4 = 64$. Для визначення тристоронніх матричних квазігруп із тристоронньою властивістю оборотності потрібно знайти кількість комутуючих пар матриць у множині U. Безпосередньою перевіркою переконуємось, що кожна матриця комутує лише сама зі собою та з одиничною матрицею. Тому маємо 4 пари, в яких матриці збігаються, це пари вигляду (C, C), та 6 пар, у яких матриці різні, це пари вигляду (C, E) і (E, C), де $C \neq E$. Отже, всього 10 пар матриць. Враховуючи вільний член, отримуємо 40 матричних квазігруп.

Для обчислення всіх різних матричних квазігруп, які мають одну з властивостей оборотності, скористаємось загальною формулою для обчислення кількості елементів із трьох множин X, Y, Z:

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|.$$

Нехай X, Y, Z − множини матричних відповідно середньої, лівої та правої IP-квазігруп. Тоді

$$|X \cup Y \cup Z| = 3 \times 96 - 3 \times 64 + 40 = 136.$$

Твердження доведено. ♦

6. Матричні квазігрупи 9-го порядку. Розглянемо центральну квазігрупу 9-го порядку $\mathbb{Z}_3^2$. Знайдемо розв'язки рівняння $X^2 = E$, яке є умовою для того, щоб квазігрупа була IP-квазігрупою.

Лема 2. *Множина U всіх розв'язків матричного рівняння $X^2 = E$ над множиною квадратних матриць $M_2(\mathbb{Z}_3)$, де $\mathbb{Z}_3 = \{0,1,2\}$, є такою*:

$$U = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \right.$$

$$\left. \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix} \right\}.$$

Д о в е д е н н я. Нехай $C = \begin{pmatrix} x & y \\ u & v \end{pmatrix}$ і $C^2 = E$. Тоді

$$\begin{pmatrix} x & y \\ u & v \end{pmatrix} \cdot \begin{pmatrix} x & y \\ u & v \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Перепишемо цю рівність у вигляді системи рівнянь:

$$\begin{cases} x^2 + yu = 1, \\ xy + yv = 0, \\ ux + vu = 0, \\ yu + v^2 = 1. \end{cases}$$

Розглянемо два випадки: $y \neq 0$ і $x = 0$.

1. Нехай $y \neq 0$, тобто $y \in \{1,2\}$. Тоді з другого рівняння системи випливає, що $v = -x = 2x$, і система рівносильна рівнянню

$$x^2 + yu = 1.$$

Можливі такі випадки: $x \neq 0$ і $x = 0$.

1′. Нехай $x \neq 0$, тобто $x \in \{1,2\}$. Тоді $x^2 = 1$ і, оскільки $y \neq 0$, то $u = 0$. Отже, маємо перші чотири матриці із множини U:

$$\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}.$$

1″. Нехай $x = 0$. Тоді система має такий вигляд:

$$\begin{cases} yu = 1, \\ yv = 0, \\ vu = 0, \\ yu + v^2 = 1. \end{cases}$$

Із першого рівняння випливає, що $y = u \in \{1,2\}$, тоді з другого рівняння системи маємо $v = 0$. Ці умови задовольняють дві матриці:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}.$$

2. Нехай $y = 0$. Тоді система матиме вигляд

$$\begin{cases} x^2 = 1, \\ u(x+v) = 0, \\ v^2 = 1. \end{cases}$$

Із першого і третього рівнянь випливає, що $x, v \in \{1,2\}$.

2′. Якщо $u = 0$, то маємо чотири матриці:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

2″. Якщо ж $u \neq 0$, то з другого рівняння маємо $x = -v = 2v$, тому ці умови задовольняють також чотири матриці:

$$\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix}.$$ ♦

Отже, кожна матрична IP-квазігрупа порядку 3^2 над кільцем $\mathbb{Z}_3$ збігається з однією із таких квазігруп:

$$f(\overline{x}, \overline{y}) = \overline{x}A + \overline{y}AC + \overline{a},$$

$$f(\overline{x}, \overline{y}) = \overline{x}A + \overline{y}C + \overline{a},$$

$$f(\overline{x}, \overline{y}) = \overline{x}C + \overline{y}A + \overline{a},$$

де C − матриця з множини U, A − довільна оборотна матриця.

7. Ортогональність матричних квазігруп. Розглянемо умови ортогональності двох матричних квазігруп над скінченним кільцем K. Очевидно, що розв'язність відповідної системи рівнянь не залежить від вільного члена, тому для знаходження таких умов достатньо обмежитися розглядом унітарних матричних квазігруп.

Твердження 5. *Дві матричні квазігрупи* $(K^n; f)$ і $(K^n; g)$, *де*

$$f(\overline{x}, \overline{y}) = \overline{x}A + \overline{y}B + \overline{a}, \qquad g(\overline{x}, \overline{y}) = \overline{x}C + \overline{y}D + \overline{b}, \tag{8}$$

є ортогональними тоді й тільки тоді, коли ортогональними є унітарні матричні квазігрупи $(K^n; f_1)$ *і* $(K^n; g_1)$, *де*

$$f_1(\overline{x}, \overline{y}) = \overline{x}A + \overline{y}B, \qquad g_1(\overline{x}, \overline{y}) = \overline{x}C + \overline{y}D.$$

Надалі будемо використовувати такий факт.

Твердження 6. *Над скінченним кільцем добуток матриць є оборотним тоді й тільки тоді, коли кожний співмножник є оборотною матрицею.*

Д о в е д е н н я. Істинність цього твердження випливає з того факту, що це твердження справджується в довільному скінченному моноїді. ♦

Сформулюємо критерій ортогональності матричних квазігруп.

Теорема 8. *Дві матричні квазігрупи* $(K^n; f)$ і $(K^n; g)$, *які визначені рівностями* (8), *є ортогональними тоді й тільки тоді, коли* $BA^{-1} - DC^{-1}$ (*або* $CD^{-1} - AB^{-1}$) *є оборотною матрицею.*

Д о в е д е н н я. Ортогональність f і g, з огляду на означення 2 і твердження 5, є рівносильною однозначності розв'язку системи

$$\begin{cases}\bar{x}A + \bar{y}B = \bar{a},\\ \bar{x}C + \bar{y}D = \bar{b}\end{cases}$$

для всіх $\bar{a}, \bar{b} \in K^n$. Ця система рівносильна такій:

$$\begin{cases}\bar{x} + \bar{y}BA^{-1} = \bar{a}A^{-1},\\ \bar{x} + \bar{y}DC^{-1} = \bar{b}C^{-1}.\end{cases}$$

Застосуємо перетворення I, де $I\bar{x} = -\bar{x}$, до другого рівняння системи, після чого перше рівняння додамо до другого, використовуючи комутативність операції «+»:

$$\begin{cases}\bar{x} + \bar{y}BA^{-1} = \bar{a}A^{-1},\\ \bar{y}(BA^{-1} + IDC^{-1}) = \bar{a}A^{-1} + I\bar{b}C^{-1}.\end{cases}$$

Очевидно, що ця система має єдиний розв'язок тоді й тільки тоді, коли $BA^{-1} - DC^{-1}$ є оборотною матрицею. А це, в свою чергу, еквівалентне ортогональності операцій f і g.

Оскільки $CD^{-1}(BA^{-1} - DC^{-1})AB^{-1} = CD^{-1} - AB^{-1}$, то на підставі твердження 6, матриці $BA^{-1} - DC^{-1}$ і $CD^{-1} - AB^{-1}$ є оборотними одночасно. ♦

Наведемо деякі наслідки теореми 8.

Нагадаємо, що універсальну квазігрупову алгебру $(Q;\Omega)$ називають *медіальною*, якщо кожна операція із множини Ω є медіальною, і всі їхні коефіцієнти попарно комутують. Зокрема, нехай операції f і g визначені рівностями (8), тоді алгебра $(K^n; f, g)$ є медіальною, якщо матриці A, B, C та D попарно комутують. Детальнішу інформацію про медіальні та абелеві алгебри можна знайти в [6].

Наслідок 9. *Нехай $(K^n; f, g)$ − медіальна квазігрупова алгебра, де f і g визначені рівностями* (8). *Операції f і g ортогональні тоді й тільки тоді, коли матриця $AD - BC$ є оборотною.*

Д о в е д е н н я. Справді, кожна пара матриць A, B, C та D комутує, тому

$$-AC(BA^{-1} - DC^{-1}) = -ACBA^{-1} + ACDC^{-1} = AD - BC.$$

Отже, матриці $BA^{-1} - DC^{-1}$ і $AD - BC$ є оборотними одночасно. ♦

Користуючись канонічними розкладами, вигляд яких встановлено в теоремі 7 і твердженні 3, можна уточнити доведені твердження для матричних *CIP*- та *IP*-квазігруп.

Наслідок 10. *Дві матричні середні CIP-квазігрупи $(K^n; f, \bar{0})$ і $(K^n; g, \bar{0})$ із канонічними розкладами*

$$f(\bar{x}, \bar{y}) = \bar{x}A + \bar{y}A^{-1}, \qquad g(\bar{x}, \bar{y}) = \bar{x}D + \bar{y}D^{-1}$$

та умовою $AD = DA$ є ортогональними тоді й тільки тоді, коли обидві матриці $D - A$ і $D + A$ є оборотними.

Д о в е д е н н я. Згідно з теоремою 8, ортогональність f і g рівносильна оборотності $A^{-2} - D^{-2}$, але

$$A^2(A^{-2} - D^{-2})D^2 = D^2 - A^2 = (D - A)(D + A).$$

Звідси та з твердження 6 випливає істинність твердження. ♦

Наслідок 11. *Дві матричні ліві CIP-квазігрупи $(K^n; f, \bar{0})$ і $(K^n; g, \bar{0})$ із канонічними розкладами*

$$f(\overline{x},\overline{y}) = \overline{x}A - \overline{y}A^2, \qquad g(\overline{x},\overline{y}) = \overline{x}D - \overline{y}D^2,$$

ортогональні тоді й тільки тоді, коли матриця $D - A$ *є оборотною.*

Д о в е д е н н я. За теоремою 8, ортогональність f і g рівносильна оборотності $IA^2A^{-1} - ID^2D^{-1} = D - A$. ♦

Наслідок 12. *Дві матричні праві CIP-квазігрупи* $(K^n; f, \overline{0})$ *і* $(K^n; g, \overline{0})$ *із канонічними розкладами*

$$f(\overline{x},\overline{y}) = -\overline{x}B^2 + \overline{y}B, \qquad g(\overline{x},\overline{y}) = -\overline{x}D^2 + \overline{y}D$$

ортогональні тоді й тільки тоді, коли матриця $D - B$ *є оборотною.*

Д о в е д е н н я. Згідно з теоремою 8, ортогональність f і g рівносильна оборотності $BIB^{-2} - DID^{-2} = D - B$. ♦

Наслідок 13. *Дві матричні середні IP-квазігрупи* $(K^n; f)$ *і* $(K^n; g)$ *із канонічними розкладами*

$$f(\overline{x},\overline{y}) = \overline{x}A + \overline{y}AC_1 + \overline{a}, \quad g(\overline{x},\overline{y}) = \overline{x}D + \overline{y}DC_2 + \overline{b}, \tag{9}$$

де C_1, C_2 *− уніпотентні матриці, є ортогональними тоді і тільки тоді, коли* $C_1 - A^{-1}DC_2D^{-1}A$ *є оборотною матрицею.*

Д о в е д е н н я. Згідно з теоремою 8, f і g ортогональні тоді й тільки тоді, коли матриця $AC_1A^{-1} - DC_2D^{-1}$ є оборотною. З того, що

$$A^{-1}(AC_1A^{-1} - DC_2D^{-1})A = C_1 - A^{-1}DC_2D^{-1}A,$$

випливає істинність цього наслідку. ♦

Наслідок 14. *Дві медіальні матричні середні IP-квазігрупи* $(K^n; f)$ *і* $(K^n; g)$ *із канонічними розкладами* (9), *де* C_1, C_2 *− уніпотентні матриці, є ортогональними тоді й тільки тоді, коли матриця* $C_1 - C_2$ *оборотна.*

Д о в е д е н н я. З медіальності випливає, що коефіцієнти в розкладах (9) комутують, тому $A \cdot AC_1 = AC_1 \cdot A$. Скоротивши на A, отримаємо $AC_1 = C_1A$. Аналогічно $BC_2 = C_2B$. Відповідно до теореми 8, ортогональність функцій f і g рівносильна оборотності матриці

$$AC_1A^{-1} - DC_2D^{-1} = C_1AA^{-1} - C_2DD^{-1} = C_1 - C_2.$$

Твердження доведено. ♦

Наслідок 15. *Дві матричні ліві IP-квазігрупи* $(K^n; f)$ *і* $(K^n; g)$ *із канонічними розкладами*

$$f(\overline{x},\overline{y}) = \overline{x}A + \overline{y}C_1 + \overline{a}, \quad g(\overline{x},\overline{y}) = \overline{x}D + \overline{y}C_2 + \overline{b},$$

де C_1, C_2 *− уніпотентні матриці, є ортогональними тоді й тільки тоді, коли* $C_1A^{-1} - C_2D^{-1}$ *є оборотною матрицею.*

Якщо в умові цього наслідку покласти $C_1 = C_2 = C$, то маємо

$$CA^{-1} - CD^{-1} = C(A^{-1} - D^{-1}),$$

тобто ортогональність f і g рівносильна оборотності $A^{-1} - D^{-1}$, яка оборотна одночасно з матрицею

$$A(A^{-1} - D^{-1})D = D - A.$$

Наслідок 16. *Дві матричні праві IP-квазігрупи* $(K^n; f)$ *і* $(K^n; g)$ *із канонічними розкладами*

$$f(\overline{x}, \overline{y}) = \overline{x}C_1 + \overline{y}B + \overline{a}, \qquad g(\overline{x}, \overline{y}) = \overline{x}C_2 + \overline{y}D + \overline{b},$$

де C_1, C_2 *– уніпотентні матриці, є ортогональними тоді й тільки тоді, коли* $BC_1^{-1} - DC_2^{-1}$ *є оборотною матрицею.*

Якщо в умові цього наслідку покласти $C_1 = C_2 = C$, то маємо

$$BC^{-1} - DC^{-1} = (B - D)C^{-1},$$

тобто ортогональність f і g рівносильна оборотності матриці $B - D$.

1. *Белоусов В. Д.* Основы теории квазигрупп и луп. – Москва: Наука, 1967. – 223 с.
2. *Белоусов В. Д., Цуркан В. Д.* Скрещенно-обратимые квазигруппы (*CI*-квазигруппы) // Изв. вузов. Математика. – 1969. – № 3(82). – С. 21–27.
3. *Сохацький Ф. М.* Про ізотопи груп. II // Укр. мат. журн. – 1995. – **47**, № 12. – С. 1692–1703.
   Те саме: *Sokhatskii F. N.* On isotopes of groups. II // Ukr. Math. J. – 1995. – **47**, No. 12. – P. 1935–1948. – https://doi.org/10.1007/BF01060967.
4. *Lutsenko A. V.* Classification of group isotopes according to their inverse properties // Прикл. проблеми механіки і математики. – 2020. – Вип. 18. – С. 48–61.
   – https://doi.org/10.15407/apmm2020.18.48-61.
5. *Pflugfelder H. O.* Quasigroups and loops: Introduction. – Sigma Series in Pure Math., Vol. 7. – Berlin: Heldermann Verlag, 1990. – 147 p.
6. *Sokhatsky F. M.* Factorization of operations of medial and abelian algebras // Вісн. Донецьк. нац. ун-ту. Сер. А: Природн. науки. – 2017. – № 1-2. – С. 84–96.
   – https://doi.org/10.31558/1817-2237.2017.1-2.7.
7. *Sokhatsky F. M., Fryz I. V.* Invertibility criterion of composition of two multiary quasigroups // Comment. Math. Univ. Carolin. – 2012. – **53**, No. 3. – P. 429–445.
8. *Sokhatsky F. M., Krainichuk H. V., Sydoruk V. A.* Semi-lattice of varieties of quasigroups with linearity // Algebra Discrete Math. – 2021. – **31**, No. 2. – P. 261–285. – https://doi.org/10.12958/adm1748.
9. *Sokhatsky F. M., Lutsenko A. V.* The bunch of varieties of inverse property quasigroups // Вісн. Донецьк. нац. ун-ту. Сер. А: Природн. науки. – 2018. – № 1-2. – С. 56–69. – https://doi.org/10.31558/1817-2237.2018.1-2.4.
10. *Sokhatsky F., Lutsenko A.* Classification of quasigroups according to directions of translations. I // Comment. Math. Univ. Carolin. – 2020. – **61**, No. 4. – P. 567–579.
11. *Sokhatsky F., Lutsenko A.* Classification of quasigroups according to directions of translations. II // Comment. Math. Univ. Carolin. – 2021. – **62**, No. 3. – P. 309–323.
12. *Sokhatskyj F., Syvakivskyj P.* On linear isotopes of cyclic groups // Quasigroups & Related Systems. – 1994. – **1**, No. 1(1). – P. 66–76.
13. *Zabavsky B. V., Domsha O. V., Romaniv O. M.* Clear rings and clear elements // Мат. студії. – 2021. – **55**, № 1. – С. 3–9. – https://doi.org/10.30970/ms.55.1.3-9.

CONSTRUCTION OF QUASIGROUPS WITH INVERTIBILITY PROPERTIES

Linear isotopes of commutative groups, that is, central quasigroups are considered. The conditions of invertibility and orthogonality are studied which, as it turned out, are sufficient to study only for unitary isotopes, i.e., isotopes having an idempotent. The criteria for the existence of each from properties of invertibility (inverse property, crossed inverse property, and mirroring) in unitary central and matrix quasigroups are found. In particular, for second-order matrices the corresponding matrix quasigroups over fields of characteristics 2 and 3 are described. Criteria of the orthogonality for matrix quasigroups with the indicated invertibility properties are also found.

Key words: *quasigroup, semigroup, automorphism, endomorphism, congruence, matrix equation, ring, matrix quasigroup, Toeplitz matrix, full matrix.*

Донец. нац. ун-т ім. В. Стуса, Вінниця

Одержано
09.12.21