CZU 517.518.2

MULȚIMI DE PARASTROFI AI QUASIGRUPULUI CARACTERIZAT DE OPERAȚIA $A(x,y) = ax + by \ (mod\ 9)$

Vadim POGOR, *student, Facultatea de Științe Reale, Economice și ale Mediului, Universitatea de Stat „Alecu Russo" din Bălți*
Conducător științific: **Tatiana ROTARI,** *asist. univ.*

Abstract: *Quasigroup theory is a fairly young branch of contemporary algebra, applied in code theory and cryptology. For this purpose, a special class of quasigroups is studied, called T-quasigroups, which has the following form* $A(x,y) = ax + by + c$. *This article presents a study of a class of quasigroups determined by the followinig operation* $A(x,y) = ax + by \ (mod\ n)$, *in particular, when n is a compound number, especially for* $n = 9$. *This article also presents a study of conjugate sets of the following quasigroup* $A(x,y) = ax + by \ (mod\ 9)$.

Keywords: *quasigroup, T-quasigroup, parastrophe set, TS-quasigroup, loop.*

Teoria quasigrupurilor reprezintă o ramură destul de tânără a algebrei contemporane, ce a apărut în anii '30 ai sec. XX, odată cu publicarea lucrărilor lui Routh Maufang, în care este arătată legătura dintre planele proiective nedesangruene și pătratele latine [3].

Fie Q – o mulțime, A – o lege de compoziționile definită pe mulțimea Q, conform căreia fiecărui element $(x,y) \in Q^2$ i se pune în corespondență elementul $A(x,y) \in Q$.

Definiție 1. Perechea ordonată (Q,A) se numește quasigrup, dacă ecuațiile

$$A(a,x) = b \text{ și } A(y,a) = b, \tag{1}$$

sunt rezolvabile, univoc pentru orice $\forall a,b \in Q$ [1].

De rând cu fiecare operație algebrică A, se definește un sistem de operații inverse, numit sistem de operații conjugate (parastrofi) și anume

$$\sum(A) = \{A,\ {}^{l}A,\ {}^{r}A,\ {}^{lr}A,\ {}^{rl}A,\ {}^{s}A\}, \tag{2}$$

unde $A(x,y) = z$, ${}^{l}A(z,y) = x$, ${}^{r}A(x,z) = y$, ${}^{lr}A(y,z) = x$, ${}^{rl}A(z,x) = y$, ${}^{s}A(y,x) = z$.

Mulțimea de parastrofi a unui quasigrup, din punct de vedere a suprapunerii acestora (egalității parastrofilor) este studiată în lucrarea [1].

În funcție de operația algebrică definită pe mulțimea Q și proprietățile ei, au fost studiate diverse clase de quasigrupuri. Una dintre cele mai populare clase este clasa T-quasigrupurilor, definită astfel:

Definiție 2. Un quasigrup (Q, A) se numește T-quasigrup, dacă există grupul abelian $Q(+)$, automorfismele acestuia a și b și un element fixat c, astfel încât $A(x, y) = ax + by + c$, pentru orice $\forall x, y \in Q$ [2].

Un caz particular al T-quasigrupurilor reprezintă quasigrupurile definite de operația

$$A(x, y) = ax + by \ (mod\ n),$$

definită pe inelul claselor de resturi $\mathbb{Z}_n$. În acest caz, elementele a și b reprezintă automorfisme ale inelului $\mathbb{Z}_n$, dacă a și b sunt reciproc prime cu n.

După cum este cunoscut, mulțimea de parastrofi a unui quasigrup poate conține 1, 2, 3 sau 6 parastrofi distincți. Mulțimea de parastrofi distincți cu variantele de suprapunere sunt arătate în lucrările [1, 2, 4].

Teorema 1. Un quasigrup (Q, A) admite următoarele mulțimi posibile de parastrofi:

$\bar{\Sigma}_1(A) = \{A\}$

$\bar{\Sigma}_2(A) = \{A,\ {}^{s}A\} = \{A = {}^{lr}A = {}^{rl}A,\ {}^{l}A = {}^{r}A = {}^{s}A\}$

$\bar{\Sigma}_6^1(A) = \{A,\ {}^{l}A,\ {}^{r}A, {}^{lr}A, {}^{rl}A,\ {}^{s}A\}$

$\bar{\Sigma}_3(A) = \{A, {}^{lr}A, {}^{rl}A\}$, cu următoarele 3 posibilități:

$\bar{\Sigma}_3^1(A) = \{A = {}^{r}A,\ {}^{l}A = {}^{lr}A, {}^{rl}A = {}^{s}A\}$

$\bar{\Sigma}_3^2(A) = \{A = {}^{l}A,\ {}^{r}A = {}^{rl}A, {}^{lr}A = {}^{s}A\}$

$\bar{\Sigma}_3^3(A) = \{A = {}^{s}A,\ {}^{l}A = {}^{rl}A,\ {}^{r}A = {}^{lr}A,\}$

În aceleași lucrări, sunt arătate formele generale ale mulțimilor de parastrofi caracterizate de operația $A(x, y) = ax + by\ (mod\ n)$, pentru fiecare dintre mulțimile indicate. Pentru fiecare dintre ele se indică ordinul operației pentru care acestea există, predominant pentru modul prim.

O problemă acută reprezintă determinarea mulțimilor de parastrofi distincți în raport cu modulul compus, deoarece în raport cu modul prim, elementele a^{-1} totdeauna există. În continuare vor fi determinate mulțimile de parastrofi ai quasigrupurilor generate de operația $A(x, y) = ax + by\ (mod\ 9)$.

Reieșind din faptul, că orice parastrof dintr-o mulțime $\sum(A)$, generează un alt parastrof din aceeași mulțime, este suficient de determinat toate combinațiile posibile de coeficienți, iar dacă combinația (a, b) generează o operație, atunci parastroful ${}^{s}A$ are coeficienții (b, a).

Definiție 3. Fie $(Q, \cdot)$ – un inel. Elementul nenul $a \in Q$ se numește divizor al lui zero, dacă există elementul nenul $b \in Q$, astfel încât $a * b = 0$.

De exemplu, în inelul Z_6, elementele 2, 3, 4 sunt divizori ai lui zero în acest inel, deoarece $2 * 3 = 0$, $3 * 4 = 0$. În inelul Z_7 nu există divizori ai lui zero. În caz general, inelul Z_p, unde p – un număr prim, este lipsit de divizorii lui zero.

Corolar. Elementul $a \in Z_n$, $n \in \mathbb{N}$, $n \geq 3$, este automorfism al grupului abelian $(Z_n, +)$, dacă și numai dacă a este coprim cu n.

În baza acestui corolar, se obține că operația $A(x, y) = ax + by \ (mod\ 9)$ (6) definește un quasigrup pe inelul Z_n, dacă și numai dacă numerele a și b sunt coprime cu n. Deci pentru a determina mulțimea de parastrofi distincți ai quasigrupului se va ține cont de divizorii lui zero în inelul corespunzător.

Mulțimea de parastrofi distincți în inelul Z_9

Numărul 9 este un număr compus, reiese că acest inel admite divizori ai lui zero și anume 0, 3, 6. Astfel, coeficienții operației algebrice pot fi 1, 2, 4, 5, 7, 8. În total există 36 operații algebrice de forma indicată. Însă, dacă o anumită operație aparține unei mulțimi de parastrofi, atunci orice parastrof al acesteia generează aceeași mulțime. După cum a fost arătat în lucrările [1, 2, 4], mulțimile de parastrofi ai unui quasigrup poate fi de tipul $\bar{\Sigma}_1(A)$, $\bar{\Sigma}_2(A)$, $\bar{\Sigma}_3^1(A)$, $\bar{\Sigma}_3^2(A)$, $\bar{\Sigma}_3^3(A)$, $\bar{\Sigma}_6(A)$. În continuare, pentru fiecare operație se va stabili tipul mulțimii de parastrofi căruia îi aparține.

În rezultatul calculelor s-a stabilit că există un singur quasigrup de ordinul 9, mulțimea de parastrofi a căruia conține un singur parastrof și anume (Z_9, A): $A(x, y) = 8x + 8y \ (mod\ 9)$ (8). Acest quasigrup se numește quasigrup total simetric sau TS-quasigrup.

În lucrarea [3], Belousov definește conceptul de TS-quasigrup în felul următor.

Definiție 4. Quasigrupul (Q, A) se numește TS-qusigrup dacă pentru orice $\forall x, y \in Q$ au loc relațiile:

$$A(x, y) = A(y, x) \text{ și } A(x, A(x, y)) = y \qquad (9)$$

În aceeași lucrare, Belousov demonstrează că mulțimea de parastrofi distincți ai unui TS-quasigrup conține o singură operație. Vom arăta că operația definită de (8) este TS-quasigrup, adică satisface relațiile (9). Deoarece $(Z_9, +)$ este grup abelian, reiese că operația „+” este comutativă. În rezultat obținem:

$$A(x, y) = 8x + 8y \ (mod\ 9) = 8y + 8y \ (mod\ 9) = A(y, x)$$

$$A\big(x, A(x, y)\big) = 8x + 8(8x + 8y) \ (mod\ 9) = 8x + 64x + 64y \ (mod\ 9) =$$
$$= 72x + 64y \ (mod\ 9)$$

Însă $72x = 9 * 8x \equiv 0 \ (mod\ 9)$ și $64y = 63y + y \ (mod\ 9)$, iar $63y = 9 * 7y \equiv 0 \ (mod\ 9)$, obținem că $64y = y \ (mod\ 9)$.

$$A\big(x, A(x, y)\big) = 0 + y = y \ (mod\ 9)$$

Astfel, cele două relații (9) sunt satisfăcute, iar operația $A(x, y) = 8x + 8y \ (mod\ 9)$ definește un TS-quasigrup.

Există un singur quasigrup de ordinul 9, definit de operația $A(x,y) = ax + by\ (mod\ 9)$, mulțimea de parastrofi a căruia este de tipul $\bar{\Sigma}_2$. Acest quasigrup este generat de operația

$$A(x,y) = 2x + 5y\ (mod\ 9)$$

Conform formei mulțimii de parastrofi de tipul $\bar{\Sigma}_2(A)$, avem că:

$$\bar{\Sigma}_2(A) = \{A,\ {}^{s}A\} = \{A = {}^{lr}A = {}^{rl}A,\ {}^{l}A = {}^{r}A = {}^{s}A\}$$

În lucrările [1, 2, 4] este demonstrat că, dacă mulțimea de parastrofi ai quasigrupului este de tipul $\bar{\Sigma}_2(A)$, atunci operația este $A(x,y) = a^{-1}x + ay\ (mod\ n)$, unde $a \neq n-1$, $a \neq a^{-1}$ și $a^3 = n-1$ în Z_n. Calculele directe arată că doar $2^3 \equiv 8\ (mod\ 9)$ și $2^{-1} \equiv 5\ (mod\ 9)$.

Astfel mulțimea de parastrofi ai acestui quasigrup este

$$\bar{\Sigma}_2(A) = \{2x + 5y\ (mod\ 9), 5x + 2y\ (mod\ 9)\}$$

Alte quasigrupuri în inelul Z_9 ce au mulțimea de parastrofi de tipul $\bar{\Sigma}_2(A)$ nu sunt.

În cazul în care mulțimea de parastrofi a unui quasigrup este de tipul $\bar{\Sigma}_3(A)$, atunci sunt posibile 3 variante de suprapunere a parastrofilor

$$\bar{\Sigma}_3^1(A) = \{A = {}^{r}A,\ {}^{l}A = {}^{lr}A, {}^{rl}A = {}^{s}A\}$$
$$\bar{\Sigma}_3^2(A) = \{A = {}^{l}A,\ {}^{r}A = {}^{rl}A, {}^{lr}A = {}^{s}A\}$$
$$\bar{\Sigma}_3^3(A) = \{A = {}^{s}A,\ {}^{l}A = {}^{rl}A,\ {}^{r}A = {}^{lr}A\}$$

Mulțimele de parastrofi $\bar{\Sigma}_3^1(A), \bar{\Sigma}_3^2(A), \bar{\Sigma}_3^3(A)$ sunt mulțimi izomorfe prin transformări parastrofice, adică, considerând, o transformare parastrofică de la o mulțime se obține una dintre celelalte mulțimi sau însăși mulțimea. Din aceste considerente, din punct de vedere al studierii operațiilor ce reprezintă un sistem de parastrofi distincți, este suficient de studiat una dintre aceste forme de parastrofi.

Evident că, dacă $A = {}^{s}A$, atunci operația algebrică este comutativă. Astfel, pentru a determina quasigrupurile ce au mulțimile de parastrofi de tipul $\bar{\Sigma}_3^3(A)$ este suficient de studiat operațiile $A(x,y) = ax + ay\ (mod\ 9)$, unde $a \neq 8$. Dintre toate operațiile definite pe Z_9, operațiile $A_1(x,y) = x + y\ (mod\ 9)$, $A_2(x,y) = 2x + 2y\ (mod\ 9)$, $A_3(x,y) = 4x + 4y\ (mod\ 9)$, $A_4(x,y) = 5x + 5y\ (mod\ 9)$, $A_5(x,y) = 7x + 7y\ (mod\ 9)$ au mulțimea de parastrofi de tipul $\bar{\Sigma}_3^3(A)$. În plus, mulțimile de parastrofi ale acestor qusigrupuri sunt:

$$\bar{\Sigma}_3^3(A_1) = \{x + y\ (mod\ 9), x + 8y\ (mod\ 9), 8x + y\ (mod\ 9)\}$$
$$\bar{\Sigma}_3^3(A_2) = \{2x + 2y\ (mod\ 9), 5x + 8y\ (mod\ 9), 8x + 5y\ (mod\ 9)\}$$
$$\bar{\Sigma}_3^3(A_3) = \{4x + 4y\ (mod\ 9), 7x + 8y\ (mod\ 9), 8x + 7y\ (mod\ 9)\}$$
$$\bar{\Sigma}_3^3(A_4) = \{5x + 5y\ (mod\ 9), 2x + 8y\ (mod\ 9), 8x + 2y\ (mod\ 9)\}$$
$$\bar{\Sigma}_3^3(A_5) = \{7x + 7y\ (mod\ 9), 4x + 8y\ (mod\ 9), 8x + 4y\ (mod\ 9)\}$$

Definiție 5. Quasigrupul (Q, A) se numește idempotent, dacă pentru orice $\forall x \in Q$ are loc relația

$$A(x,x) = x \tag{10}$$

Analizând mulțimile de parastrofi de mai sus, observăm că există o singură operație ce satisface relația (10) și anume $A(x,y) = 5x + 5y \ (mod\ 9)$.

Într-adevăr, $A(x,x) = 5x + 5x = 10x = x \ (mod\ 9)$. În plus, fiecare parastrof al acestui quasigrup este idempotent (vezi Tabelul 1).

Tabelul 1. *Idempotența quasigrupurilor* $\bar{\Sigma}_3^3(A_4)$

	0	1	2	3	4	5	6	7	8
0	0	5	1	6	2	7	3	8	4
1	5	1	6	2	7	3	8	4	0
2	1	6	2	7	3	8	4	0	5
3	6	2	7	3	8	4	0	5	1
4	2	7	3	8	4	0	5	1	6
5	7	3	8	4	0	5	1	6	2
6	3	8	4	0	5	1	6	2	7
7	8	4	0	5	1	6	2	7	3
8	4	0	5	1	6	2	7	3	8

$A = {}^{s}A$
$= 5x + 5y \ (mod\ 9)$

	0	1	2	3	4	5	6	7	8
0	0	8	7	6	5	4	3	2	1
1	2	1	0	8	7	6	5	7	3
2	4	3	2	1	0	8	7	6	5
3	6	5	4	3	2	1	0	8	7
4	8	7	6	5	4	3	2	1	0
5	1	0	8	7	6	5	4	3	2
6	3	2	1	0	8	7	6	5	4
7	5	4	3	2	1	0	8	7	6
8	7	6	5	4	3	2	1	0	8

${}^{r}A = {}^{lr}A$
$= 2x + 8y \ (mod\ 9)$

	0	1	2	3	4	5	6	7	8
0	0	2	4	6	8	1	3	5	7
1	8	1	3	5	7	0	2	4	6
2	7	0	2	4	6	8	1	3	5
3	6	8	1	3	5	7	0	2	4
4	5	7	0	2	4	6	8	1	3
5	4	6	8	1	3	5	7	0	2
6	3	5	7	0	2	4	6	8	1
7	2	4	6	8	1	3	5	7	0
8	1	3	5	7	0	2	4	6	8

${}^{l}A = {}^{rl}A$
$= 8x + 2y \ (mod\ 9)$

Celelalte mulțimi de parastrofi nu conțin quasigrupuri idempotente. În același timp, mulțimile de parastrofi de tipul $\bar{\Sigma}_3^1(A)$ si $\bar{\Sigma}_3^2(A)$ sunt aceleași ca și $\bar{\Sigma}_3^3(A)$, doar că operația inițială este considerată unul dintre parastrofii operației $A(x,y) = ax + y \ (mod\ 9)$.

Un caz important de quasigrupuri o reprezintă clasa DC-quasigrupurilor (distinct conjugates quasigrups). Această clasă se caracterizează prin faptul că mulțimea de parastrofi ai acestui quasigrup este completă, adică conține 6 parastrofi distincți.

În inelul Z_9 există trei mulțimi de parastrofi ce sunt complete. Toate celelalte mulțimi de parastrofi distinți sunt generate de unul dintre parastorfii acestor quasigrupuri. Operațiie de bază ce generează DC-quasigrupuri în Z_9 sunt: $A_6(x,y) = x + 2y \ (mod\ 9)$, $A_7(x,y) = x + 4y \ (mod\ 9)$, $A_8(x,y) = 2x + 4y \ (mod\ 9)$.

Mulțimile de parastrofi ale acestor quasigrupuri sunt:

$$\bar{\Sigma}_6^1(A_6) = \{x + 2y \ (mod\ 9), 2x + y \ (mod\ 9), x + 7y \ (mod\ 9), 7x + y \ (mod\ 9), 4x + 5y \ (mod\ 9), 5x + 4y \ (mod\ 9)\}$$

$$\bar{\Sigma}_6^2(A_7) = \{x + 4y \ (mod\ 9), 4x + y \ (mod\ 9), x + 5y \ (mod\ 9), 5x + y \ (mod\ 9), 2x + 7y \ (mod\ 9), 7x + 2y \ (mod\ 9)\}$$

$$\bar{\Sigma}_6^3(A_8) = \{2x + 4y \ (mod\ 9), 4x + 2y \ (mod\ 9), 4x + 7y \ (mod\ 9), 7x + 4y \ (mod\ 9), 5x + 7y \ (mod\ 9), 7x + 5y \ (mod\ 9)\}$$

Nici unul dintre quasigrupurile respective, precum și nici unul dintre parastrofii acestora nu este idempotent.

Definiție 6. Fie (Q, A) – un quasigrup. Elementrul e se numește element neutru la dreapta, dacă petru orice $\forall x \in Q$ are loc relația $A(x, e) = x$ [3]. Elementul f se numește element neutru la stânga, dacă pentru orice $\forall x \in Q$ are loc relația $A(f, x) = x$. Dacă $f = e$, atunci avem un quasigrup cu unitate ce se numește buclă.

Dintre toate quasigrupurile reprezentate, avem o buclă ce este generată de operația $A(x, y) = x + y \ (mod\ 9)$ cu unitatea 0, o serie de quasigrupuri cu unitate la dreapta ce au forma $A(x, y) = x + ay \ (mod\ 9)$ și o serie de quasigrupuri ce au unitate la stânga descrise de operațiile $A(x, y) = ax + y \ (mod\ 9)$, unde $a \neq \{0, 1, 3, 6\}$.

În Tabelul 2, sunt prezentate exemple ale quasigrupurilor cu unitatea 0, cu unitate la stânga și unitate la dreapta.

Tabelul 2. *Quasigrupurile cu: a. unitatea 0, b. unitatea la stânga, c. unitatea la dreapta*

a	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

$A(x, y) = x + y \ (mod\ 9)$

b	0	1	2	3	4	5	6	7	8
0	0	2	4	6	8	1	3	5	7
1	1	3	5	7	0	2	4	6	8
2	2	4	6	8	1	3	5	7	0
3	3	5	7	0	2	4	6	8	1
4	4	6	8	1	3	5	7	0	2
5	5	7	0	2	4	6	8	1	3
6	6	8	1	3	5	7	0	2	4
7	7	0	2	4	6	8	1	3	5
8	8	1	3	5	7	0	2	4	6

$A(x, y) = x + 2y \ (mod\ 9)$

c	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	2	3	4	5	6	7	8	0	1
2	4	5	6	7	8	0	1	2	3
3	6	7	8	0	1	2	3	4	5
4	8	0	1	2	3	4	5	6	7
5	1	2	3	4	5	6	7	8	0
6	3	4	5	6	7	8	0	1	2
7	5	6	7	8	0	1	2	3	4
8	7	8	0	1	2	3	4	5	6

$A(x, y) = 2x + y \ (mod\ 9)$

Bibliografie:

1. BELEAVSCAYA, G., POPOVICH, T. Conjugate sets of loops and quasi-groups. DC-quasigroups. In: *Buletinul Academiei de Științe a Republicii Moldova, 2012*, nr. 1(68), pp. 21-31. ISSN 1024-7696
2. POPOVICH, T. On the conjugate sets of quasigroups. In: *Buletinul Academiei de Științe a Republicii Moldova, 2011*, nr. 3(67), pp. 69-76. ISSN 1024-7696
3. БЕЛОУСОВ, В. Д. Основы теории квазигрупп и луп. Москва, Изд. Наука, 1967. – 225 стр., УДК 519.4:512.8
4. ПОПОВИЧ, Т. Неполные множества ортогональных парастрофов T-квазигрупп. [online] https://www.math.md/files/download/news/2015/Seminar_V_D_Belousov_Popovici_2015.pdf