Despre AGC – cuasigrupuri

V. Izbaș

1. Introducere

Se ştie că grupurile au apărut în matematică ca grupuri de automorfisme. Rolul automorfismelor este remarcabil şi bine cunoscut. La studierea diverselor structuri matematice speciale, de carecter algebric, geometric şi chiar extramatematic, se întâlnesc, adesea, diferite simetrii, care joacă un rol foarte important. Toate aceste simetrii, ale diferitor obiecte de natură atât matematică cât şi fizică, pot fi definite şi descrise doar folosind limbajul automorfismelor. Astfel grupurile de automorfisme se prezintă ca un aparat matematic special pentru descrierea simetriilor. Grupul de automorfisme al unei structuri algebrice concrete în mare parte determină starea structurei însăşi. Deasemenea grupurile de automorfisme sunt folosite şi pentru clasificarea diferitor obiecte matematice.

Se ştie că orice grup poate fi reprezentat ca grup de automorfisme al unui grupoid. Există un număr mare de lucrări, care conţin construcţii a diferitor structuri Q astfel încât grupul de automorfisme $AutQ$ este izomorf cu un grup G predefinit. Aceste rezultate pot fi interpretate ca construcţii a structurilor Q cu simetrii predefinite. Se pare că numărul de orbite al grupului $AutQ$ măsoară gradul de asimetrie a structurii Q, şi este înţeleasă dorinţa de încercare de a măsura acestă asimetrie. Din acest punct de vedere cele mai simetrice structuri Q sunt acelea, care au grupul $AutQ$ tranzitiv, adică Q este singura orbită a grupului $AutQ$. Aceasta este echivalent cu faptul că pentru orice elemente $a, b \in Q$ există un automorfism $\varphi \in AutQ$ astfel încât $\varphi(a) = b$.

Pentru cuasigrupuri sunt cunoscute unele rezultate care descriu unele cuasigrupuri cu grupul de automorfisme tranzitiv. Însă problema descrierii tuturor cuasigrupurilor cu grupul de automorfisme tranzitiv este în caz general nesoluţionată.

În această comunicare se prezintă un studiu al $AGC-$grupoizilor şi $AGC-$cuasigrupurilor (grupoizi sau cuasigrupuri automorfe de grup ciclic) , definite de savantul francez Albert Sade, care formează o clasă largă de grupoizi şi cuasigrupuri speciale, care au subgrupul de automorfisme ciclic și tranzitiv. Unele rezultate sunt prezentate şi demonstrate într-un cadru mai general decât cel conţinut în lucrările lui A. Sade.

2. Noţiuni şi rezultate preliminare

Definiție A : *Grupoidul* $(G,\times)$ *pentru care* $x \times y = f(x-y)+y, \forall\, x,y \in G$, *unde* $(G,\ +)$ *este un grup cu element neutru* 0, *iar* $f: G \to G$ *o funcție arbitrară se numește* $AG-$*grupoid. Dacă* $(G,\ +)$ *este un grup ciclic atunci* $(G,\times)$ *se numește* $AGC-$*grupoid.*

Propoziție: *Ușor se verifică că că* $f = R_0^{\times}$ *și* $RM(G,\ +) \leq Aut(G,\ \times)$, *unde*

$$RM(G,+) = \{R_a^{+} \mid R_a^{+}(x) = x + a, \forall\, a, x \in G\},$$

deci $(G,\times)$ *are grupul de automorfisme tranzitiv .*

Propoziție: *Orice grupoid* $(G,\times)$ *care are un subgrup ciclic de automorfisme tranzitiv de ordinul* $|G|$ *este de forma datș în Definiție A. Există o corespondență biunivocă între AGC – grupoizi și totalitatea funcțiilor pe mulțimea G.*

Corolar: *Pentru* $|Q| = n$ *există exact* n^n *AGC – grupoizi definiți pe* Q.

Corolar: *Dacă* f *este bijecție atunci* $R_a^{\times}$ *este bijecție pentru orice* $a \in G$.

Teoremă: $AG-$*grupoidul* $(G,\times)$ *este cuasigrup la dreapta dacă și numai dacă* f *– bijectivă.*

Teoremă: *Un AGC – grupoid* $(Q,\ *)$ *este cuasigrup atunci și numai atunci cînd funcția ce-l determină* $x * 0 = f(x)$ *satisface următoarele condiții:*

$$\begin{cases} (i)\ f(x) = f(y) \Leftrightarrow x = y \\ (ii)\ x - f(x) = y - f(y) \Leftrightarrow x = y \end{cases}$$

(unde operațiile " + " și " – " sunt modulo n *în cazul cînd* Q *este finit de ordinul* n.*)*

Teoremă: *Orice AGC – cuasigrup finit* $(G, \times)$ *este de ordin impar*.

Propoziție: *Pentru orice număr impar există un AGC – cuasigrup.*

Exemplu: Astfel se obţine, că grupoidul definit de aplicaţia $x \to x^2, \forall x \in Q$ prin relaţia $x * y = f(x-y) + y, \forall x, y \in Q$ într-un grup ciclic de ordin impar este $AGC-$cuasigrup.

Exemplu: Fie $Q = 2N = \{2k | k \in N\}$. Atunci $(Q, \times)$ definit pe Q de următoarea operație:

$$x \times y = \begin{cases} \frac{1}{2}(x+y),\ dacă\ x, y, \frac{1}{2}(x+y) sunt\ pare \\ \frac{1}{2}(x+y)+1, dacă\ x, y - pare, \frac{1}{2}(x+y) - impar \end{cases};$$

este AGC – grupoid.

Exemplu: Fie $Q = 2Z$ numerele întregi pare. Atunci se știe că $(Q, +)$ este grup ciclic. Definim funcția $f: 2Z \to 2Z$ astfel:

$$f(x) = \begin{cases} -x,\ \ x \in (-\infty.\ 0] \cap 2Z,\ adică\ \ x < 0 \\ -x-2,\ \ x \in (0, +\infty) \cap 2Z, adică\ \ x > 0 \end{cases};$$

Observăm că f nu este surjectivă, dar este injectivă, deoarece ecuația $f(x) = -2$ nu are soluții:

$$f(x) = -2 \Leftrightarrow \begin{cases} -x = -2,\ \ x \in (-\infty, 0] \cap 2Z \\ -x-2 = -2,\ \ x \in (0, +\infty) \cap 2Z \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} x = 2,\ \ x \in (-\infty, 0] \cap 2Z \\ x = 0,\ \ x \in (0, +\infty) \cap 2Z \end{cases} \Leftrightarrow x \in \emptyset$$

Propoziție: *Nu există un AGC – grup netrivial (care conține cel puțin două elemente).*

Deseori în loc de $AGC-$cuasigrupul definit de permutarea f se spune scurt $AGC-$cuasigrupul f.

3. Transformări ce păstrează invariantă proprietatea grupoidului de a fi AGC – grupoid.

Cu $Ort(Q,+)$ notăm mulţimea tuturor permutărilor f ale mulţimei Q, care definesc în modul stabilit AGC – cuasigrupuri și astfel încît $g: G \to G, g(x) = x - f(x)$ este bijecție. Este adevărată următoarea afirmaţie.

Teoremă: Dacă $f \in Ort(Q,+)$, atunci avem aplicaţiile

$$
\begin{aligned}
&a : Ort(Q,+) \to Ort(Q,+),\ f \to a(f),\ a(f)(x) = x - f(x),\ \forall x, y \in Q;\\
&b : Ort(Q,+) \to Ort(Q,+),\ f \to b(f),\ b(f)(x) = -f(-x),\ \forall x, y \in Q;\\
&ab : Ort(Q,+) \to Ort(Q,+),\ f \to ab(f),\ ab(f)(x) = x + f(-x),\ \forall x, y \in Q;\\
&c : Ort(Q,+) \to Ort(Q,+),\ f \to c(f),\ c(f)(x) = f^{-1}(x),\ \forall x, y \in Q;\\
&D_h : Ort(Q,+) \to Ort(Q,+),\ f \to D_h(f),\ D_h(f)(x) = f(x-h),\ \forall x, y, h \in Q;\\
&E_h : Ort(Q,+) \to Ort(Q,+),\ f \to E_h(f),\ E_h(f)(x) = f(x) + h,\ \forall x, y, h \in Q
\end{aligned}
$$

care sunt permutări ale mulţimei $Ort(Q,+)$, şi care formează un grup diedral de ordinul 12.

Remarcă: Aceste relații rămîn adevărate și pentru orice grup abelian $(Q,+)$ inclusiv infinit.

Remarcă: *Dacă $\boldsymbol{f} \in \boldsymbol{Ort}(\boldsymbol{G},+)$ atunci AGC – cuasigrupul determinat de funcția $\boldsymbol{f}$ îl vom nota cu* $\left(\underset{f}{\times}\right)$ *sau* $(\boldsymbol{G}, \underset{f}{\times})$.

Propoziție: *Pentru orice $h \in Q$ și orice $f \in Ort(G,+)$ AGC – cuasigrupurile determinate de funcțiile $D_h(f)$ și $E_h(f)$ sunt izotopi ai AGC – cuasigrupului determinat de f.*

Notăm $M = \{f: Z_n \to Z_n \mid f(x) = ax + b;\ a, b \in Z_n, (a,n) = 1, (a-1,n) = 1\}$;

Lemă: *Mulțimea M este invariantă față de transformările a, b, c, D_h și E_h.*

Exemplu: Dacă $n = 2k+1$ și $a = \frac{n+1}{2}$ atunci pentru $f: Z_n \to Z_n$ cu $f(x) = ax + b \ (mod\ n), b \in Z_n$, AGC – grupoidul (cuasigrupul) $(Z_n, \underset{f}{\times})$ este comutativ.

Propoziție: *Pentru orice n impar există un AGC – grupoid comutativ.*

Exemplu: Pentru $n = 3$ toate AGC – cuasigrupurile sunt date de funcțiile:

$$f(x) = 2x \ (mod\ 3); \qquad g(x) = (2x+1)(mod\ 3); \qquad r(x) = (2x+2)(mod\ 3);$$

4. Compoziția AGC – cuasigrupurilor

Teoremă [2]: *Fie* $f \in Ort(Z_p, +)$ *și* $\rho_x \in Ort(Z_m, +), \forall\, x \in Z_p$. *Atunci aplicația*

$$F: Z_{mp} \to Z_{mp}, F(x + py) = f(x) + p\rho_x(y), \forall\, x \in Z_p, \forall\, y \in Z_m$$

este ortomorfism al grupului $(Z_{mp}, +)$.

Propoziție: *Dacă* $a \in Z_p$ *și* $a \underset{f}{\times} a = a$ *atunci* $\left(C_a, \underset{F}{\times}\right)$ *este subcuasigrup normal în* $\left(Z_{mp}, \underset{F}{\times}\right)$.

Corolar: *Dacă* $a \in \left(Z_p, \underset{f}{\times}\right)$ *și* $a \underset{f}{\times} a = a$ *atunci* $x \underset{f}{\times} x = x$, *oricare ar fi* $x \in Z_p$.

Teoremă [2]: *Fie* Ort *mulțimea tuturor ortomorfismelor grupurilor* $Z_p, p = 1, 2, 3, 4, \ldots$. *Atunci* $(Ort,*)$ *este semigrup necomutativ cu unitate în raport cu operația* $(*)$ *definită prin egalitatea*

$$f * \rho = f + p\rho, f \in Ort\, Z_p, \rho \in Ort\, Z_m$$

$$(f * \rho)(a + px) = f(a) + p\rho(x), \forall\, a \in Z_p, \forall x \in Z_m.$$

Corolar: *Fie* $(M,\cdot) = \langle p, p' \rangle$ - *subsemigrupul semigrupului* $(N^+,\cdot)$ *generat de numerele* p *și* p'. *Atunci* $Ort' = \bigcup_{p \in M} Ort\, Z_p$ *este subsemigrup al semigrupului* $(Ort,*)$.

Corolar: *Dacă* $f \in Ort\, Z_q$, *atunci subsemigrupul semigrupului* $(Ort,*)$ *generat de elementul* f *este izomorf cu grupul aditiv al numerelor naturale* $(N, +)$.

5. Parastrofii AGC – cuasigrupului

Notăm cu "$\backslash_f$" și "$/_f$" parastrofii AGC – cuasigrupului $(Q, \underset{f}{\times})$, adică

$$x \underset{f}{\times} y = 2 \Leftrightarrow x \backslash_f z = y \Leftrightarrow z /_f y = x, \forall\, x, y \in Q.$$

Propoziție: *Parastrofii AGC – cuasigrupului sunt tot AGC – cuasigrupuri.*

Propoziție: *Dacă $(Q, \underset{f}{\times})$ este AGC – cuasigrup, atunci $(\backslash_f) = (\underset{f^{-1}}{\times})$ și $(/_f) = (\underset{(ba(f^{-1}))^{-1}}{\times})$.*

Corolar: *Clasa AGC – cuasigrupurilor este închisă în raport cu transformarea de parastrofie.*

Teoremă: *Dacă $f \in Ort(Q,+)$ atunci aplicația $h: Q \to Q, h(x) = 0 \underset{f}{\times} x$ este ortomorfism, $h \in Ort(Q,+)$.*

Corolar: *Dacă $f \in Ort(Q,+)$ atunci aplicația $h: Q \to Q, h(x) = 0 \underset{f^{-1}}{\times} x$ este ortomorfism, $h \in Ort(Q,+)$.*

Teoremă: *Dacă $(Q,\times)$ este un AGC – cuasigrup, de ordinul $|Q| = n$, dacă elementul $h \in Q$ este soluție a unei din următoarele trei ecuații $0 \times 0 = x, x \times 0 = 0, 0 \times x = 0$ și h este reciproc prim cu n atunci $Aut(Q,\times) = C = \{R_a^+ | a \in Q\}$, unde $R_a^+ x = a + x$, unde "$+$" se ia după modulul n.*

Teorema: *Dacă AGC – cuasigrupul finit* $(Q, \times)$ *de ordin* n *nu este generat de nici un element al său, atunci:*

1. *Fiecare element al său genereaza un subcuasigrup de acelaşi ordin constant* m $(mp = n)$*;*
2. *Există exact* m *subcuasigrupuri astfel definite (monogenerate), care este generat de orice element al său;*
3. *Toate aceste* p *– subcuasigrupuri sunt disjuncte, izomorfe între ele şi toate se obţin din oricare altul aplicînd automorfismele* $R_h^+ : Q \to Q, h \in \{0, 1, 2, \dots, p-1\}$*;*
4. *Subcuasigrupul generat de elementul* 0 *este:* $D = 0, p, 2p, 3p, \dots, n-p$*, şi el se obţine prin înmulţirea cu* p*, fără a schimba legea de compoziţie a unui cuasigrup oarecare de ordin* m *automorf de acelaşi grup ciclic de ordin* m*, adică generat de unul din elementele sale;*
5. *Toate aceste subcuasigrupuri au acelaşi grup de automorfisme, şi anume grupul ciclic de ordinul* m*, şi anume grupul ciclic generat de* $R_p^+ : Q \to Q, x \to x + p$.

Bibliografie

1. В.Д. Белоусов. *Основы теории квазигрупп и луп:* Изд. Наука, Москва, 1967.
2. A. Sade. Groupoides automorphes par le groupe cyclique, *Can. J. Math.*, 9 (1957), 321-335.
3. S. K. Stein. On the foundation of quasigroups, *Trans. Amer. Math. Soc. vol.* 85 (1957) pp. 228-256.
4. S. K. Stein. Homogeneous quasigroups. *Pacific J. Math.* **14** 1964 1091–1102. 20.95
5. M. Hosszu. Homogeneous groupoids. *Ann. Univ. Sci. Budapest. Eötvös. Sect. Math.* **3-4** 1960/1961 95–99.