Известия НАН Армении, Математика, том 58, н. 2, 2023, стр. 68 – 81.

ТЕОРЕМЫ ТИПА ШАУФЛЕРА

Ю. М. МОВСИСЯН, Д. Н. АРУТЮНЯН

Ереванский Государственный Университет[1]
E-mails: *movsisyan@ysu.am;* *david.harutyunyan96@gmail.com*

Аннотация. В данной работе теорема Белоусова о линейности обратимых алгебр с $\forall\exists(\forall)$-тождеством Шауфлера распространяется на регулярные алгебры с делением для других $\forall\exists(\forall)$-тождеств ассоциативности. Для рассматриваемых формул мы также доказываем теоремы типа Шауфлера. Полученные результаты применимы в криптографии(ср. [1],[2],[3]).

MSC2020 number: 03C05; 03C85; 20N05.

Ключевые слова: $\forall\exists(\forall)$-тождество; регулярная и делимая алгебра; эндо-линейная алгебра; квазиэндоморфизм.

1. Введение

Будем называть группоид $Q(\cdot)$ с делением, если для любого $a \in Q$ левые и правые умножения будут сюръекциями. Если $Q(\cdot)$–группоид с делением то его операция называется делимой. Бинарная алгебра $(Q;\Sigma)$ называется делимой, если каждая операция $A \in \Sigma$ является делимой операцией.

Назовем группоид $(Q;\cdot)$ лево-регулярным, если

$$ca = cb \Rightarrow R_a = R_b,$$

где $a, b, c \in Q$. Аналогично определяется право-регулярный группоид. Назовем группоид регулярным, если он одновременно лево-регулярный и право-регулярный. Если $Q(\cdot)$-регулярный группоид, то его операция называется регулярной. Бинарная алгебра $(Q;\Sigma)$ называется регулярной, если каждая операция $A \in \Sigma$ является регулярной операцией.

Скажем, что группоид $(Q;A)$ гомотопен группоиду $(Q;B)$, если существуют такие отображения $\alpha, \beta, \gamma : Q \to Q$, что имеет место равенство $\gamma A(x,y) = B(\alpha x, \beta y)$ для любых $x, y \in Q$. Тогда тройка (α, β, γ) называется гомотопией из $(Q;A)$ в $(Q;B)$. Если $\gamma = id_Q$, то группоиды называются главно гомотопными.

[1]Первый автор был частично финансирован комитетом по науке Республики Армения, гранты: 10-3/1-41, 21T-1A213.

Если α, β, γ сюръективные отображения, то группоиды называются эпитопными или главно эпитопными соотвественно. Скажем, что алгебра $(Q;\Sigma)$ гомотопна (эпитопна) группоиду $(Q;\cdot)$, если для каждого $A \in \Sigma$ группоид $(Q;A)$ гомотопен (эпитопен) группоиду $(Q;\cdot)$. Таким же образом определяется главная гомотопность (эпитопность) алгебры $(Q;\Sigma)$ группоиду $(Q;\cdot)$.

Алгебру $(Q;\Sigma)$ будем называть r-алгеброй, если она регулярна, с делением и существует хотя бы одна обратимая операция $A \in \Sigma$.

Бинарная алгебра $(Q;\Sigma)$ называется лево(право)-линейной на группоиде $(Q;\cdot)$, если каждая ее операция линейна слева (справа) на группоиде $(Q;\cdot)$, то есть для любой операции $A \in \Sigma$ существуют автоморфизм ϕ_A группоида $(Q;\cdot)$ и перестановка α_A множества Q такие, что

$$A(x,y) = \phi_A x \cdot \alpha_A y$$
$$(A(x,y) = \alpha_A x \cdot \phi_A y)$$

для любых $x, y \in Q$. Если ϕ_A будет эндомофизмом, а α_A отображением из Q в Q то алгебру будем называть лево(право)-эндолинейной на группоиде $(Q;\cdot)$.

Бинарная алгебра $(Q;\Sigma)$ называется линейной (эндолинейной) на группоиде $(Q;\cdot)$, если каждая ее операция линейна (эндолинейна) на группоиде $(Q;\cdot)$, то есть для любой операции $A \in \Sigma$ существуют автоморфизмы (эндоморфизмы) ϕ_A и ψ_A группоида $(Q;\cdot)$ и элемент $t_A \in Q$ такие, что

$$A(x,y) = (\phi_A x \cdot t_A) \cdot \psi_A y$$

для любых $x, y \in Q$.

В [4] доказано, что обратимая алгебра $(Q;\Sigma)$ со следующими $\forall\exists(\forall)$-тождествами ассоциативности:

$$\forall X, Y \exists X', Y' \forall x, y, z X(Y(x,y),z) = X'(x, Y'(y,z)),$$
$$\forall X, Y \exists X', Y' \forall x, y, z X(x, Y(y,z)) = X'(Y'(x,y), z),$$

линейна на группе.

Пусть Ω_Q–класс всех обратимых(квазигрупповых) операций определенных на Q.

Теорема 1.1. *(Шауфлер) В $(Q;\Omega_Q)$ имеет место одна из следующих формул:*

$$\forall X, Y \exists X', Y' \forall x, y, z X(Y(x,y),z) = X'(x, Y'(y,z)),$$
$$\forall X, Y \exists X', Y' \forall x, y, z X(x, Y(y,z)) = X'(Y'(x,y), z),$$

тогда и только тогда, когда мощность $|Q| \leq 3$.

В [5] доказано, что обратимая алгебра $(Q;\Sigma)$ со следующими $\forall\exists(\forall)$-тождествами ассоциативности:

$$\forall X,Y\exists X',Y'\forall x,y,zX(Y'(x,y),z)=X'(x,Y(y,z)),$$
$$\forall X,Y\exists X',Y'\forall x,y,zX(x,Y'(y,z))=X'(Y(x,y),z),$$
$$\forall X,Y\exists X',Y'\forall x,y,zY'(x,X(y,z))=X'(Y(x,y),z),$$
$$\forall X,Y\exists X',Y'\forall x,y,zX(x,Y'(y,z))=Y(X'(x,y),z),$$

также линейна на группе, более того в [5] доказаны следующие аналоги теоремы Шауфлера (см. также [6],[7],[8]).

Теорема 1.2. *B $(Q;\Omega_Q)$ имеет место одно из следующих $\forall\exists(\forall)$-тождеств:*

$$\forall X,Y\exists X',Y'\forall x,y,zX(Y'(x,y),z)=X'(x,Y(y,z)),$$
$$\forall X,Y\exists X',Y'\forall x,y,zX(x,Y'(y,z))=X'(Y(x,y),z),$$
$$\forall X,Y\exists X',Y'\forall x,y,zY'(x,X(y,z))=X'(Y(x,y),z),$$
$$\forall X,Y\exists X',Y'\forall x,y,zX(x,Y'(y,z))=Y(X'(x,y),z),$$

тогда и только тогда, когда $|Q|\leq 3$.

В настоящей статье доказываются аналогичные результаты в регулярных алгебрах с делением и в r-алгебрах.

2. ПРЕДВАРИТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

Определение 2.1. *Отображение $\phi:Q\to Q$ называется квазиэндоморфизмом группы $(Q;\cdot)$, если*

$$\phi(x\cdot y)=\phi x\cdot(\phi 1)^{-1}\cdot\phi y$$

для всех $x,y\in Q$, где 1 – единица группы $(Q;\cdot)$.

Если ϕ также биекция из Q в Q, то ϕ называется квазиавтоморфизмом группы $(Q;\cdot)$.

Лемма 2.1. *Каждый квазиэндоморфизм ϕ группы $(Q;\cdot)$ имеет вид $\phi=L_a\phi'$, где $L_ax=a\cdot x$, $a\in Q$, и ϕ' является эндоморфизмом группы $(Q;\cdot)$. Верно и обратное утверждение, если ϕ эндоморфизм группы $(Q;\cdot)$, тогда произвольное отоброжение $\phi'=L_a\phi$ из Q в Q будет квазиэндоморфизмом группы $(Q;\cdot)$.*

Доказательство. Пусть $\phi 1 = k$. Покажем, что $\phi' = L_{k^{-1}}\phi$ является эндоморфизмом. Имеем:

$$\phi'(ab) = L_{k^{-1}}\phi(ab) = k^{-1}\cdot\phi a\cdot(\phi 1)^{-1}\cdot\phi b$$
$$= (k^{-1}\cdot\phi a)\cdot(k^{-1}\cdot\phi b) = \phi' a\cdot\phi' b.$$

□

Лемма 2.2. *Пусть $(Q;\cdot)$ – группа и α является главной эпитопией данной группы, тогда α является сюръективным квазиэндоморфизмом этой группы, более того, если:*

$$\alpha(x\cdot y) = \beta x\cdot\gamma y, \tag{2.1}$$

тогда β и γ также будут квазиэндоморфизмами.

Доказательство. Сделав по очереди в (2.1) замены: 1) $x = 1$, 2) $y = 1$, 3) $x = y = 1$, получаем:

$$\alpha y = \beta 1\cdot\gamma y,\quad \alpha x = \beta x\cdot\gamma 1,\quad \alpha 1 = \beta 1\cdot\gamma 1: \tag{2.2}$$

Преобразуем равенство (2.1), учитывая равенства (2.2):

$$\alpha(xy) = \alpha x\cdot(\gamma 1)^{-1}\cdot(\beta 1)^{-1}\alpha y = \alpha x\cdot(\beta 1\cdot\gamma 1)^{-1}\cdot\alpha y = \alpha x\cdot(\alpha 1)^{-1}\cdot\alpha y,$$

т. е. α – квазиэндоморфизм.

Из (2.1) также имеем:

$$\beta(x\cdot y) = \alpha(x\cdot y)\cdot(\gamma 1)^{-1} = \alpha x\cdot(\alpha 1)^{-1}\cdot(\alpha y\cdot(\gamma 1)^{-1}) =$$
$$(\alpha x\cdot(\gamma 1)^{-1})\cdot(\beta 1)^{-1}\beta y = \beta x\cdot(\beta 1)^{-1}\cdot\beta y.$$

Таким же образом доказывается, что γ также является квазиэндоморфизмом группы $(Q;\cdot)$. □

Лемма 2.3. *Пусть $(Q;\cdot)$ – группа. Если для биекций α,β,γ и сюръекций σ,δ,τ имеет место следующее тождество:*

$$\beta(\alpha(a\cdot b)\cdot c) = \gamma a\cdot\delta(\sigma b\cdot\tau c),\ \ \forall a,b,c\in Q, \tag{2.3}$$

тогда β,α,γ будут квазиавтоморфизмами.

Доказательство. Пусть $b = e$ и a заменим на $\alpha^{-1}a$. Тогда из (2.3) следует, что $\beta(a\cdot c) = \gamma\alpha^{-1}a\cdot\lambda c$, где $\lambda = \delta L_{\sigma_e}\tau$. Таким образом, из леммы 2.1 следует, что β квазиавтоморфизм. Положим $c = e$, тогда из (2.3) получим:

$$\beta\alpha(a\cdot b) = \gamma a\cdot\delta R_{\tau_e}\sigma b. \tag{2.4}$$

Из леммы 2.1 следует, что $\theta = \beta\alpha$ квазиавтоморфизм. Все квазиавтоморфизмы группы являются группой, поэтому $\alpha = \beta^{-1}\theta$ также является квазиавтоморфизмом. Из (2.4) и леммы 2.2 следует, что γ является квазиавтоморфизмом. □

Лемма 2.4. [9] *Если лупа $(Q;\circ)$ главно гомотопна группе $(Q;\cdot)$, то они изоморфны. Если группа $(Q;\circ)$ главно гомотопна группе $(Q;\cdot)$, следовательно они изоморфны.*

Лемма 2.5. *Пусть $(Q;\cdot)$ – группа. Если ϕ,ψ квазиэндоморфизмы группы $(Q;\cdot)$, тогда $\alpha = \phi\psi$ тоже будет квзаиэндоморфизмом группы $(Q;\cdot)$.*

Доказательство. Поскольку ϕ и ψ – квазиэндоморфизмы группы $(Q;\cdot)$, то имеем

$$\alpha(x\cdot y) = \phi(\psi(x\cdot y)) = \phi((\psi x\cdot(\psi 1)^{-1})\cdot\psi y) = \phi(\psi x\cdot(\psi 1)^{-1})\cdot(\phi_1)^{-1}\cdot\phi\psi y = \phi\psi x\cdot(\phi 1)^{-1}\cdot\phi(\psi 1)^{-1}\cdot(\phi_1)^{-1}\cdot\phi\psi y. \tag{2.5}$$

Сделав замены $x = y = 1$ в (2.5), получаем

$$\phi\psi 1 = \phi\psi 1\cdot(\phi 1)^{-1}\cdot\phi(\psi 1)^{-1}\cdot(\phi_1)^{-1}\cdot\phi\psi 1,$$

то есть

$$(\phi\psi 1)^{-1} = (\phi 1)^{-1}\cdot\phi(\psi 1)^{-1}\cdot(\phi_1)^{-1}. \tag{2.6}$$

Из (2.5) и (2.6) получаем

$$\alpha(x\cdot y) = \phi\psi x\cdot(\phi\psi 1)^{-1}\phi\psi y = \alpha x\cdot(\alpha 1)^{-1}\cdot\alpha y.$$

□

Определение 2.2. *Скажем, что тернарная операция T представима на множестве Q, если существуют бинарные операции A и B определенные на том же множестве Q такие, что справедливо тождество*

$$T(x_1,x_2,x_3) = A(x_i,B(x_j,x_k))$$

или тождество

$$T(x_1,x_2,x_3) = A(B(x_i,x_j),x_k),$$

где i,j,k попарно различные и $i,j,k\in\{1,2,3\}$.

Будем определять левую, серединную и правую подстановки тернарной операции T следующим образом:

$$\lambda_{xy}z = \mu_{xz}y = \rho_{yz}x = T(x, y, z).$$

Множество всех отоброжений из Q в Q обозначим через τ_Q и определим:

$$\tau_1 = \{\rho_{yz} | y \in Q, z \in Q\},$$
$$\tau_2 = \{\mu_{xz} | x \in Q, z \in Q\},$$
$$\tau_3 = \{\lambda_{xy} | x \in Q, y \in Q\}.$$

Теорема 2.1. [12] *Тернарная операция T на множестве Q представима тогда и только тогда, когда $|\tau_1| \leq |Q|$, или $|\tau_2| \leq |Q|$, или $|\tau_3| \leq |Q|$.*

Теорема 2.2. [9] *Пусть $(Q; A), (Q; B), (Q; C), (Q; D)$ группоиды с делением, а $(Q; A)$ и $(Q; C)$ - регулярны. Тогда, если имеет место тождество*

$$A(x, B(y, z)) = C(D(x, y), z), \tag{2.7}$$

то алгебра $(Q; \{A, B, C, D\})$ будет эпитопна некоторой группе $(Q; \cdot)$. Более того, существуют такие сюръективные отображения $A_1, A_2, B_1, B_2, C_1, C_2, D_1, D_2$, что имеют место следующие тождества:

$$\begin{cases} A(x, y) = A_1x \cdot A_2y, \\ A_2B(x, y) = A_2B_1x \cdot A_2B_2y, \\ C(x, y) = C_1x \cdot C_2y, \\ C_2D(x, y) = C_2D_1x \cdot C_2D_2y, \end{cases} \quad \text{и} \quad \begin{cases} A_1 = C_1D_1, \\ A_2B_1 = C_1D_2, \\ A_2B_2 = C_2. \end{cases}$$

3. ЭНДОЛИНЕЙНЫЕ ПРЕДСТАВЛЕНИЯ

Теорема 3.1. *Пусть $(Q; \Sigma)$-r-алгебра. Если для произвольных $A, B \in \Sigma$ существуют $C, D \in \Sigma$ такие, что имеет место тождество (2.7), тогда существует группа $(Q; \cdot)$ такая, что произвольная операция $A \in \Sigma$ будет эндолинейной над группой $(Q; \cdot)$. Группа $(Q; \cdot)$ определяется единственным образом с точностью до изоморфизма.*

Доказательство. Пусть $A \in \Sigma$–обратимая операция, тогда из теоремы 2.2 следует, что существуют операции $C_A, D_A \in \Sigma$ и группа $(Q; \cdot)$ такая, что имеет место

тождество $A(x, A(y, z)) = C_A(D_A(x, y), z)$, а также:

$$\begin{cases} A(x, y) = \alpha x \cdot \beta y, \\ \beta A(x, y) = \beta\gamma x \cdot \beta\delta y, \\ C_A(x, y) = \lambda x \cdot \theta y, \\ \lambda D_A(x, y) = \lambda\nu x \cdot \lambda\mu y, \end{cases}$$

где $\alpha, \beta, \gamma, \delta, \lambda, \theta, \nu, \mu$ – сюръективные отображения. В доказательстве теоремы 2.2 были рассмотрены элементы $p, q, r \in Q$ и определены $\alpha x = R_{A_b} x = A(x, b)$ и $\beta y = L_{A_p} y = A(p, y)$, где $b = A(q, r)$. Из вышеупомянутых определений следует, что α и β являются биекциями. Помимо этого, имеет место следующее тождество:

$$\beta(\alpha x \cdot \beta y) = \beta\gamma x \cdot \beta\delta y,$$

или

$$\beta(x \cdot y) = \beta\gamma\alpha^{-1} x \cdot \beta\delta\beta^{-1} y,$$

из которого следует, что β является квазиавтоморфизмом.

Из теоремы 2.2 следует, что для произвольного $B \in Q$ существуют операции $C, D \in \Sigma$ и группа $(Q; \cdot_B)$ такая, что имеют место равенства $A(x, B(y, z)) = C(D(x, y), z)$ и

$$\begin{cases} A(x, y) = \alpha_B x \cdot_B \beta_B y, \\ \beta_B B(x, y) = \beta_B\gamma_B x \cdot_B \beta_B\delta_B y, \\ C(x, y) = \lambda_B x \cdot_B \theta_B y, \\ \lambda_B D(x, y) = \lambda_B\nu_B x \cdot_B \lambda_B\mu_B y, \end{cases}$$

где $\alpha_B, \beta_B, \gamma_B, \delta_B, \lambda_B, \theta_B, \nu_B, \mu_B : Q \hookrightarrow Q$ сюръективные отображения.

Однако, из доказательства теоремы 2.2 следует, что $\beta_B y = A(p, y) = \beta y$, т.е. $\beta_B = \beta$.

Заметим, что $A(x, y) = \alpha_B x \cdot_B \beta y$, а также $A(x, y) = \alpha x \cdot \beta y$, откуда следует, что $x \cdot_B y = \alpha h_{\alpha_B} x \cdot y$, где h_{α_B} – правое обратное отображение для α_B.

Таким образом, для произвольного $B \in \Sigma$ получаем:

$$\beta B(x, y) = \beta\gamma_B x \cdot_B \beta\delta_B y = \alpha h_{\alpha_B} \beta\gamma_B x \cdot \beta\delta_B y \implies$$
$$B(x, y) = \beta^{-1}(\alpha h_{\alpha_B} \beta\gamma_B x \cdot \beta\delta_B y).$$

Заметив, что β^{-1} также является квазиавтоморфизмом, получим:

$$B(x, y) = \beta^{-1}\alpha h_{\alpha_B} \beta\gamma_B x \cdot (\beta^{-1} e)^{-1} \cdot \delta_B y = \beta^{-1}\alpha h_{\alpha_B} \beta\gamma_B x \cdot L_{(\beta^{-1}e)^{-1}} \delta_B y, \tag{3.1}$$

где $e \in Q$ единица группы $(Q; \cdot)$ и $L_{(\beta^{-1}e)^{-1}}$ левое умножение группы $(Q; \cdot)$.

Таким образом, для произвольного $B \in \Sigma$ существуют сюръекции σ_B, τ_B для которых выполняется следующее равенство $B(x,y) = \sigma_B x \cdot \tau_B y$. Откуда следует, что существует группа $(Q;\cdot)$ такая, что

$$\begin{cases} A(x,y) = \alpha_A x \cdot \beta_A y, \\ B(x,y) = \alpha_B x \cdot \beta_B y, \\ C(x,y) = \alpha_C x \cdot \beta_C y, \\ D(x,y) = \alpha_D x \cdot \beta_D y, \end{cases}$$

где $\alpha_A, \alpha_B, \alpha_C, \alpha_D, \beta_A, \beta_B, \beta_C, \beta_D$ - сюръекции. Делая замены в выражении (2.7) получим следующее равенство:

$$\alpha_A x \cdot \beta_A(\alpha_B y \cdot \beta_B z) = \alpha_C(\alpha_D x \cdot \beta_D y) \cdot \beta_C z.$$

После замены элементов $x = h_{\alpha_A} e$, $y = h_{\alpha_B} y$, $z = h_{\beta_B} z$, где $h_{\alpha_A}, h_{\alpha_B}, h_{\beta_B}$ являются правыми обратными операциями для α_A, α_B и β_B, а e единичный элемент группы $(Q;\cdot)$, имеем:

$$\beta_A(x \cdot y) = \alpha_C(\alpha_D h_{\alpha_A} e \cdot \beta_D h_{\alpha_B} y) \cdot \beta_C h_{\beta_B} z = \mu y \cdot \nu z,$$

где $\mu = \alpha_C L_{\alpha_D h_{\alpha_A} e} \beta_D h_{\alpha_B} y$ и $\nu = \beta_C h_{\beta_B}$. Это означает, что β_A является квазиэндоморфизмом, а из леммы 2.1 следует, что существует эндоморфизм ϕ_A такой, что $\beta_A = L_a \phi_A$:

$A(x,y) = \alpha_A x \cdot L_a \phi_A y = R_a \alpha_A x \cdot \phi_A y = \sigma_A x \cdot \phi_A y$, где $\sigma_A = R_a \alpha_A$.

Отсюда следует, что существует группа $(Q;\cdot)$ такая, что:

$$\begin{cases} A(x,y) = \sigma_A x \cdot \phi_A y, \\ B(x,y) = \sigma_B x \cdot \phi_B y, \\ C(x,y) = \sigma_C x \cdot \phi_C y, \\ D(x,y) = \sigma_D x \cdot \phi_D y, \end{cases}$$

где $\sigma_A, \sigma_B, \sigma_C, \sigma_D$ - сюръекции, $\phi_A, \phi_B, \phi_C, \phi_D$ – эндоморфизмы группы $(Q;\cdot)$.

Делая замены в выражении (2.7) получим следующее равенство:

$$\sigma_A x \cdot \phi_A(\sigma_B y \cdot \phi_B z) = \sigma_C(\sigma_D x \cdot \phi_D y) \cdot \phi_C z.$$

После замены $z = e$, где e единичный элемент группы $(Q;\cdot)$, имеем:

$$\sigma_A x \cdot \phi_A \sigma_B y = R_{\phi_C e} \sigma_C(\sigma_D x \cdot \phi_D y)$$

Из леммы 2.2 следует, что $\theta = \phi_A \sigma_B$ является квазиэндоморфизмом.

Пусть A является обратимой операцией, тогда ϕ_A будет автоморфизмом группы $(Q;\cdot)$ и $\sigma_B = \phi_A^{-1}\theta$, где ϕ_A^{-1} автоморфизм группы $(Q;\cdot)$, а θ квазиэндоморфизм группы $(Q;\cdot)$. Из леммы 2.5 следует, что σ_B является квазиэндоморфизмом, а из

леммы 2.1 известно, что существует эндоморфизм σ_{B_0} и элемент $t_B \in Q$ такие, что $\sigma_B x = t_B \cdot \sigma_{B_0} x$, $\forall x \in Q$. Таким образом, для любого $B \in \Sigma$ имеем следующее равенство:

$$B(x,y) = t_B \cdot \sigma_{B_0} x \cdot \phi_B y, \forall x, y \in Q,$$

где σ_{B_0} и ϕ_B являются сюръективными эндоморфизмами группы $(Q;\cdot)$ и t_B– некоторый элемент из Q. □

Аналогично доказывается следующая теорема.

Теорема 3.2. *Пусть $(Q;\Sigma)$–r-алгебра. Если для произвольных $C, D \in \Sigma$ существуют $A, B \in \Sigma$ такие, что выполняется тождество (2.7), то существует группа $(Q;\cdot)$ такая, что произвольная операция $A \in \Sigma$ будет эндолинейной над группой $(Q;\cdot)$. Группа $(Q;\cdot)$ определяется единственным образом с точностью до изоморфизма.*

Теорема 3.3. *Пусть $(Q;\Sigma)$–r-алгебра. Если для произвольных $A, D \in \Sigma$ существуют $B, C \in \Sigma$ такие, что имеет место (2.7), тогда существует группа $(Q;\circ)$ такая, что любая операция $A \in \Sigma$ является эндолинейной над этой группой. Группа $(Q;\circ)$ определяется единственным образом с точностью до изоморфизма.*

Доказательство. Пусть $D = A$ является обратимой операцией. Из теоремы 2.4 следеут, что существуют $B_A, C_A \in \Sigma$ и группа $(Q;\cdot)$ такие, что

$$\begin{cases} A(x,y) = \alpha x \cdot \beta y, \\ \beta B_A(x,y) = \beta\gamma x \cdot \beta\delta y, \\ C_A(x,y) = \lambda x \cdot \theta y, \\ \lambda A(x,y) = \lambda\nu x \cdot \lambda\mu y. \end{cases}$$

Из доказательства теоремы 2.2 известно, что α и β являются биекциями. Зафиксировав операцию A, получим, что для любого $D \in \Sigma$ существуют группа $(Q;\cdot_D)$ и операции $B_D, C_D \in \Sigma$ такие, что

$$\begin{cases} A(x,y) = \alpha_D x \cdot_D \beta_D y, \\ \beta_D B_D(x,y) = \beta_D\gamma_D x \cdot_D \beta_D\delta_D y, \\ C_D(x,y) = \lambda_D x \cdot_D \theta_D y, \\ \lambda_D D(x,y) = \lambda_D\nu_D x \cdot_D \lambda_D\mu_D y. \end{cases}$$

Из доказательства теоремы 2.2 также известно, что α_D и β_D биекции, и $\alpha_D = \lambda_D \circ \nu_D$. Таким образом, $\lambda_D = \alpha_D \circ h_{\nu_D}$, где h_{ν_D} правая обратная операция

ν_D. Из ее определения известно, что это инъекция, поэтому λ_D также является инъекцией. Из теоремы 2.2 следует, что λ_D сюръекция, то есть λ_D биекция.

Заметим, что $A(x,y) = \alpha_D x \cdot_D \beta_D y$ и $A(x,y) = \alpha x \cdot \beta y$, откуда следует, что $x \cdot_D y = \alpha\alpha_D^{-1}x \cdot \beta\beta_D^{-1}y$, где α_D^{-1} и β_D^{-1} – обратные отображения для α_D и β_D.

Таким образом, для любого $D \in \Sigma$ имеем $D(a,b) = \lambda_D^{-1}(\lambda_D\nu_D x \cdot_D \lambda_D\mu_D y) = \lambda_D^{-1}(\alpha\alpha_D^{-1}\alpha_D x \cdot \beta\beta_D^{-1}\lambda_D\mu_D y) = \lambda_D^{-1}(\alpha x \cdot \sigma_D)$, где $\sigma_D = \beta\beta_D^{-1}\lambda_D\mu_D$, а λ_D и α являются биекциями.

Откуда следует, что существует группа $(Q;\cdot)$ такая, что

$$\begin{cases} A(x,y) = \alpha_A^{-1}(\beta_A x \cdot \gamma_A y), \\ B(x,y) = \alpha_B^{-1}(\beta_B x \cdot \gamma_B y), \\ C(x,y) = \alpha_C^{-1}(\beta_C x \cdot \gamma_C y) \\ D(x,y) = \alpha_D^{-1}(\beta_D x \cdot \gamma_D y), \end{cases}$$

где $\alpha_A, \beta_A, \alpha_B, \beta_B, \alpha_C, \beta_C, \alpha_D, \beta_D \in \Sigma$ - биекции, $\gamma_A, \gamma_B, \gamma_C, \gamma_D \in \Sigma$ – сюръекции. Из (2.7) имеем

$$\alpha_A^{-1}(\beta_A x \cdot \gamma_A\alpha_B^{-1}(\beta_B y \cdot \gamma_B z)) = \alpha_C^{-1}(\beta_C\alpha_D^{-1}(\beta_D x \cdot \gamma_D y) \cdot \gamma_C z).$$

Делая следующие замены: $x = \beta_D^{-1}x$, $y = h_{\gamma_D}y$, $z = h_{\gamma_C}z$, где $h_{\gamma_D}, h_{\gamma_C}$ являются правыми обратными для γ_D, γ_C, получим следующее равенство:

$$\alpha_A\alpha_C^{-1}(\beta_C\alpha_D^{-1}(x \cdot y) \cdot z) = \beta_A\beta_D^{-1}x \cdot \gamma_A\alpha_B^{-1}(\beta_B h_{\gamma_D}y \cdot \gamma_B h_{\gamma_C}z).$$

Известно, что $\alpha_A\alpha_C^{-1}, \beta_C\alpha_D^{-1}, \beta_A\beta_D^{-1}$ – биекции, поэтому из леммы 2.3 следует, что они являются квазиавтоморфизмами. Определим следующие отображения $\theta_1 = \beta_C\alpha_D^{-1}$ и $\theta = \beta_A\beta_D^{-1}$. Зафиксировав $A = C$, получим, что $\theta_2 = \beta_C\alpha_D^{-1}$ также является квазиавтоморфизмом, и для любого $D \in \Sigma$:

$$D(x,y) = \alpha_D^{-1}(\beta_D x\gamma_D y) = \beta_C^{-1}\theta_1(\theta_2^{-1}\beta_C x \cdot \gamma_D y) =$$
$$\beta_C^{-1}(\theta_1(\theta_2^{-1}\beta_C x) \cdot (\theta_1 e)^{-1} \cdot \theta_1\gamma_D y) = \beta_C^{-1}(\phi_D\beta_C x \cdot \delta_D y),$$

где $\phi_D x = \theta_1\theta_2^{-1}x \cdot (\theta_1\theta_2^{-1}e)^{-1}$ и $\delta_D y = \theta_1\theta_2^{-1}e \cdot (\theta_1 e)^{-1} \cdot \theta_1\gamma_D y$. Из определения ϕ следует, что оно является автоморфизмом группы $(Q;\cdot)$.

Определим операцию $(\circ)$ на Q следующим образом:

$$x \circ y = \beta_C^{-1}(\beta_C x \cdot \beta_C y), \forall x, y \in Q.$$

$(Q;\circ)$ будет группой, поскольку она изоморфна группе $(Q;\cdot)$. Таким образом, имеем:

$$D(x,y) = \beta_C^{-1}\phi_D\beta_C x \circ \beta_C^{-1}\delta_D y = \psi x \circ \sigma_D y, \forall x, y \in Q,$$

где $\psi x = \beta_C^{-1}\phi_D\beta_C x$ и $\sigma_D y = \beta_C^{-1}\delta_D y$.

Для произвольных $x, y \in Q$ имеем

$$\psi(x \circ y) = \beta_C^{-1}\phi\beta_C(x \circ y) = \beta_C^{-1}\phi\beta_C\beta_C^{-1}(\beta_C x \cdot \beta_C y) =$$
$$\beta_C^{-1}(\phi\beta_C x \cdot \phi\beta_C y) = \beta_C^{-1}(\beta_C\psi x \cdot \beta_C\psi y) = \psi x \circ \psi y.$$

Откуда следует, что ψ является автоморфизмом группы $(Q;\circ)$. Следовательно, существуют автоморфизмы $\psi_A, \psi_b, \psi_C, \psi_D$ группы $(Q;\circ)$ и сюръекции $\sigma_A, \sigma_B, \sigma_C, \sigma_D \in \Sigma$ такие, что:

$$\begin{cases} A(x,y) = \psi_A x \circ \sigma_A y, \\ B(x,y) = \psi_B x \circ \sigma_B y, \\ C(x,y) = \psi_C x \circ \sigma_C y, \\ D(x,y) = \psi_D x \circ \sigma_D y. \end{cases}$$

Из тождества (2.7) следует:

$$\phi_A x \circ \sigma_A(\phi_B y \circ \sigma_B z) = \phi_C(\phi_D x \circ \sigma_D y) \circ \sigma_C z.$$

Зафиксировав $x = f$, где f единичный элемент группы $(Q;\circ)$, имеем:

$$\sigma_A(\psi_B y \circ \sigma_B z) = \psi_C\sigma_D y \circ \sigma_C z.$$

Из леммы 2.2 следует, что σ_A является квазиэндоморфизмом, а из леммы 2.1 известно, что существует эндоморфизм σ_{A_0} и элемент $t_A \in Q$ такие, что $\sigma_A x = \sigma_{A_0} x \circ t_A$, $\forall x \in Q$. Таким образом, для любого $A \in \Sigma$ имеем следующее равенство:

$$A(x,y) = \psi_A x \circ \sigma_{A_0} y \circ t_A, \forall x, y \in Q,$$

где ψ_A является автоморфизмом группы $(Q;\circ)$, σ_{A_0} является сюръективным эндоморфизмом группы $(Q;\circ)$ и t_A некоторый элемент в Q. □

Аналогично доказываются следующие теоремы.

Теорема 3.4. *Пусть $(Q;\Sigma)$–r-алгебра. Если для произвольных $B, C \in \Sigma$ существуют $A, D \in \Sigma$ такие, что выполняется* (2.7)*, то существует группа $(Q;\circ)$ такая, что любая операция $A \in \Sigma$ является эндолинейной над этой группой. Группа $(Q;\circ)$ определяется единственным образом с точностью до изоморфизма.*

Теорема 3.5. *Пусть $(Q;\Sigma)$–регулярная алгебра с делением и для любых $A, C \in \Sigma$ существуют $B, D \in \Sigma$ такие, что имеет место тождество* (2.7)*. Тогда существует группа $(Q;\cdot)$ такая, что алгебра $(Q;\Sigma)$ эндолинейна над этой группой. Группа $(Q;\cdot)$ определяется единственным образом с точностью до изоморфизма.*

Теорема 3.6. *Пусть $(Q;\Sigma)$–регулярная алгебра с делением и для любых $B, D \in \Sigma$ существуют $A, C \in \Sigma$ такие, что имеет место тождество* (2.7)*. Тогда существует группа $(Q;\cdot)$ такая, что для каждой операции $A \in \Sigma$ имеет место:*

$$\gamma_A A(x,y) = \theta_A(\alpha_A x \cdot \beta_A y),$$

где $\gamma_A, \theta_A, \alpha_A, \beta_A$ сюръекции из Q в Q.

4. ТЕОРЕМЫ ТИПА ШАУФЛЕРА ДЛЯ ГРУППОИДОВ И ДЛЯ РЕГУЛЯРНЫХ ОПЕРАЦИЙ С ДЕЛЕНИЕМ

Пусть дано непустое множество Q. Систему всех регулярных операций с делением, определенных над множеством Q обозначим через R_Q, а систему всех бинарных операции на Q - через G_Q.

Теорема 4.1. *B $(Q;R_Q)$ имеет место одно из следующих $\forall\exists(\forall)$-тождеств:*

(1) $\forall A, C \exists B, D \forall x, y, z A(x, B(y, z)) = C(D(x, y), z)$,
(2) $\forall A, D \exists B, C \forall x, y, z A(x, B(y, z)) = C(D(x, y), z)$,
(3) $\forall B, C \exists A, D \forall x, y, z A(x, B(y, z)) = C(D(x, y), z)$,
(4) $\forall A, B \exists C, D \forall x, y, z A(x, B(y, z)) = C(D(x, y), z)$,
(5) $\forall C, D \exists A, B \forall x, y, z A(x, B(y, z)) = C(D(x, y), z)$,

тогда и только тогда, когда $|Q| \leq 3$.

Доказательство. Докажем для первого тождества, для остальных доказательство будет аналогичным.

Из теоремы 3.5 следует, что существует группа $(Q;\cdot)$ такая, что любая операция $A \in R_Q$ эндолинейна над этой группе, откуда следует, что все лупы в R_Q эндолинейны над этой группе, поэтому они будут главно гомотопными этой группе. Из леммы 2.4 следует, что они будут изоморфными этой группе, однако из теорем Альберта ([10],[11]) следует, что неассоцативная лупа, не изоморфна какой-либо группе, поэтому $|Q| < 5$. Известно, что на конечном множестве каждое сюръективное преобразование будет биекцией, поэтому каждая регулярная операция с делением будет обратимой операцией, т.е. любая операция в R_Q будет обратимой, а из теоремы 1.1 следует, что $|Q| \leq 3$ (см. также [8]). □

Теорема 4.2. *B $(Q;G_Q)$ верны следующие утверждения:*

(1) $\forall A, C \in G_Q$ $\exists B, D \in G_Q$ *такие, что имеет место* (2.7) *тогда и только тогда, когда $|Q| = 1$,*

(2) $\forall A, D \in G_Q\ \exists B, C \in G_Q$ *такие, что имеет место* (2.7) *тогда и только тогда, когда* $|Q| = 1$,

(3) $\forall B, C \in G_Q\ \exists A, D \in G_Q$ *такие, что имеет место* (2.7) *тогда и только тогда, когда* $|Q| = 1$,

(4) *для произвольного множества* Q, $\forall B, D \in G_Q\ \exists A, C \in G_Q$ *такие, что имеет место* (2.7),

(5) $\forall C, D \in G_Q\ \exists A, B \in G_Q$ *такие, что имеет место* (2.7) *тогда и только тогда, когда* $|Q| = 1$ *или* Q *бесконечна,*

Доказательство. (1) Если $|Q| > 1$, то существуют $a_1, a_2 \in Q$ такие, что $a_1 \neq a_2$. Пусть операции A и C такие, что $\forall x, y \in Q$

$$A(x, y) = a_1,$$
$$C(x, y) = a_2,$$

следовательно, тождество (2.7) не будет выполняться.

(2) Пусть $|Q| > 1$ и операции A и D такие, что $\forall x, y \in Q$:

$$A(x, y) = x,$$
$$D(x, y) = y.$$

Таким образом $\forall B, C \in G_Q$ и $\forall x, y, z \in Q$ имеем:

$$A(x, B(y, z)) = x,$$
$$C(D(x, y), z) = C(y, z).$$

Из $|Q| > 1$ вытикает, что существуют $a_1, a_2 \in Q$ такие, что $a_1 \neq a_2$. Если зафиксируем $x = a_1, y = a_1$ и $z = a_2$, то получим, что $C(a_1, a_2) = A(a_1, B(a_1, a_2)) = a_1$, и если $x = a_2, y = a_1$ и $z = a_2$, тогда получим $C(a_1, a_2) = A(a_2, B(a_1, a_2)) = a_2$, что является противоречием.

(3) Доказательство идентично случаю 2.

(4) $\forall B, D \in G_Q$ возьмем $A, C \in G_Q$ такие, что:

$$A(x, y) = a, \forall x, y \in Q,$$
$$C(x, y) = a, \forall x, y \in Q,$$

где a – некоторый элемент из Q.

Получим следующее равенство:

$$\forall x, y, z \in Q, A(x, B(y, z)) = a = C(D(x, y), z).$$

(5) Доказывается с использованием теоремы 2.1.

□

Abstract. In this paper, Belousov's theorem on the linearity of invertible algebras with the Shcaufler $\forall\exists(\forall)$-identity extends to regular division algebras for other Schaufler like associativity $\forall\exists(\forall)$-identities. For the considered new formulas, we also prove Schauffler like theorems. The results obtained are applicable in cryptography (cf. [1],[2],[3]).

Список литературы

[1] R. Schauffler, Eine Anwendung zyklischer Permutationen and ihreTheorie. Ph.D. Thesis, Marburg University (1948).
[2] R. Schauffler, "Über die Bildung von Codewörtern", Arch. elekt. Übertragung, **10**, 303 – 314 (1956).
[3] R. Schauffler, "Die Associativität im Ganzen, besonders bei Quasigruppen", Math. Z., **67**, 428 – 435 (1957).
[4] V. D. Belousov, "Globally associative systems of quasigroups", Mat. Sb., N.S., **55**(97)(2), 221 -– 236 (1961).
[5] Yu. Movsisyan, "Hyperidentities: Boolean and De Morgan Structures", World Scientific (2022), doi:10.1142/12796
[6] Yu. Movsisyan, Introduction to the Theory of Algebras With Hyperidentities [in Russian], Yerevan State University Press, Yerevan (1986).
[7] Yu. Movsisyan, Hyperidentities and Hypervarieties in Algebras [in Russian], Yerevan State University Press, Yerevan (1990).
[8] Yu. Movsisyan, "On a theorem of Schauffler", Math. Notes, **53**, 172 – 179 (1993).
[9] S. Davidov, A. Krapež, Yu. Movsisyan, "Functional equations with division and regular operations", Asian-European Journal of Mathematics, **11**, no. 03, 1 – 14 (2018).
[10] A. A. Albert, "Quasigroups I", Trans. Amer. Math. Soc. **54**, 507 – 519 (1943).
[11] A. A. Albert, "Quasigroups II", Trans. Amer. Math. Soc. **55**, 401 – 419 (1944).
[12] A. Krapež, "Generalized associativity on groupoids", Publ. Inst. Math. (Beograd), N.S. **28**(42), 105 -– 112 (1980).

Поступила 16 августа 2022
После доработки 6 декабря 2022
Принята к публикации 28 декабря 2022