CONGRUENCES AND AUTOMORPHISMS IN CELLS OF POST ALGEBRAS

I. A. Mal'tsev

UDC 517.11

Let P_k be the collection of all functions defined on the set $E_k = \{0,1,\ldots,k-1\}$ with values in this set, let $\mathcal{P}_k = \langle P_k; \zeta, \tau, \Delta, \nabla, * \rangle$ be the Post algebra of finite rank k [2], and let $\mathfrak{A}$ be a subalgebra of the algebra $\mathcal{P}_k$. It will be assumed throughout that $k \geq 3$. We denote by $\mathfrak{A}^t$, $t \neq 0$, the set of all functions of $\mathfrak{A}$ dependent on precisely t variables, and by $\mathfrak{A}^{(s)}$ $(1 \leq s \leq k)$ the set of all functions of $\mathfrak{A}$, taking not more than s values. We denote by $\mathcal{L}$ the algebra generated by the set of all the functions of $\mathcal{P}_k$, which are expressible in the form $f(f_1(x_1) \oplus \cdots \oplus f_n(x_n))$, where $\oplus$ denotes addition $mod\, 2$, and the functions $f, f_1, \ldots, f_n$ belong to $\mathcal{P}_k^1$. Given any function $f \in \mathcal{P}_k$ we write f^n to denote that $f \in \mathcal{P}_k^n$ and write δf for the set of values of the function f. We shall call the algebras $\mathcal{L}^{(2)}, \mathcal{P}_k^{(2)}, \mathcal{P}_k^{(3)}, \ldots, \mathcal{P}_k^{(k-1)}$ cells of the algebra $\mathcal{P}_k$.

We introduce into $\mathcal{L}^{(2)}$ the equivalence relation $\varkappa_p$ putting functions f_1 and f_2 in the same class if one of the following conditions is satisfied:

1) the functions f_1 and f_2 are identical,

2) the functions f_1 and f_2 belong to $\mathcal{P}_k^{(1)}$ and depend on the same number of variables,

3) $\delta f_1 = \delta f_2$, while there exists a function $h \in \mathcal{P}_k^1$, taking two values in the set δf_2 and such that $f_1 = h(f_2)$.

The functions f_1 and f_2 will be called dual if $f_1 \equiv_{\varkappa_p} f_2$.

The relation $\varkappa_p$ is clearly stable with respect to the operations ζ, τ, Δ, ∇. Let $g_1^* = g_1 * h_1$, $g_2^* = g_2 * h_2$, $g_1 \equiv_{\varkappa_p} g_2$, $h_1 \equiv_{\varkappa_p} h_2$. If the functions g_1 and g_2 belong to $\mathcal{L}^{(2)}$, then

$$
\begin{aligned}
g_1^*(x_1,\ldots,x_{m+n-1}) &= f_{10}(f_{11}(h_1(x_1,\ldots,x_m)) \oplus f_{12}(x_{m+1}) \oplus \ldots \oplus f_{1m+n-1}(x_{n+m-1})), \\
g_2^*(x_1,\ldots,x_{m+n-1}) &= f_{20}(f_{21}(h_2(x_1,\ldots,x_m)) \oplus f_{22}(x_{m+1}) \oplus \ldots \oplus f_{2m+n-1}(x_{n+m-1})).
\end{aligned} \tag{1}
$$

It can easily be seen that, if g_1, g_2 and h_1, h_2 are each a pair of dual functions, then it follows from Eqs. (1) that g_1^*, g_2^* is a pair of dual functions. Hence the relation $\varkappa_p$ is also stable with respect to the operation $*$, i.e., $\varkappa_p$ is a congruence in $\mathcal{L}^{(2)}$.

It was shown by A. I. Mal'tsev in [2] that there are three congruences in any subalgebra of the algebra $\mathcal{P}_k$, namely, $\varkappa_0$, which is the same as the equality relation, $\varkappa_1$, which is the same as the identically true relation, and $\varkappa_a$, under which two functions are put in the same class if they depend on the same number of variables. It was also shown in [2] that there are no other congruences in the algebra $\mathcal{P}_k$. We shall show that this is likewise true for cells of the algebra $\mathcal{P}_k$, other than $\mathcal{L}^{(2)}$, and that there are just four congruences in $\mathcal{L}^{(2)}$.

<u>THEOREM 1.</u> If $\mathfrak{A}$ is a cell of the algebra $\mathcal{P}_k$, different from $\mathcal{L}^{(2)}$, then there are just three congruences in it: $\varkappa_0$, $\varkappa_1$, $\varkappa_a$. In the cell $\mathcal{L}^{(2)}$ there are just four congruences: $\varkappa_0$, $\varkappa_1$, $\varkappa_a$, $\varkappa_p$.

Theorem 1 is a consequence of the following three lemmas.

Translated from Algebra i Logika, Vol. 11, No. 6, pp. 666-672, November-December, 1972. Original article submitted November 14, 1972.

LEMMA 1. Let $\mathfrak{x}$ be a congruence in the algebra $\mathfrak{B} \leq \mathcal{K}_k$, containing the cell $\mathfrak{A} \neq \mathcal{L}^{(2)}$. If there exist in $\mathfrak{B}$ two distinct $\mathfrak{x}$-congruent functions f_1, f_2 dependent on the same number of variables, then any two functions of $\mathfrak{A}$, which depend on the same number of variables, are $\mathfrak{x}$-congruent.

By hypothesis, there exist in E_k numbers $a_1, \ldots, a_n$, b_1, b_2 such that $b_1 \neq b_2$ and

$$f_1(a_1, \ldots, a_n) = b_1 \;, \; f_2(a_1, \ldots, a_n) = b_2 \;.$$

We denote by $c_i(x_1, \ldots, x_n) (i = 0, \ldots, k-1)$ the function identically equal to i. Obviously,

$$c_{b_1}(x) = f_1(c_{a_1}(x), \ldots, c_{a_n}(x)), \; c_{b_2}(x) = f_2(c_{a_1}(x), \ldots, c_{a_n}(x)).$$

Since $\mathfrak{A} \supset \mathcal{K}_k^{(1)}$, we have $c_{b_1} \equiv_{\mathfrak{x}} c_{b_2}$. The following functions belong to the algebra $\mathfrak{A}$:

$$t_{uzv}(x) = \begin{cases} z \;, & \text{if} \quad x = u \;, \\ v \;, & \text{if} \quad x \neq u \;. \end{cases}$$

Since, for any numbers a, b on E_k we have $(t_{b_1ab}(c_{b_1}(x)) \equiv_{\mathfrak{x}} t_{b_1ab}(c_{b_2}(x))$, i.e., $c_a(x) \equiv_{\mathfrak{x}} c_b(x)$, all the functions of $\mathcal{K}_k^{(1)}$, which depend on the same number of variables, are $\mathfrak{x}$-congruent.

Let g be an arbitrary n-place function of $\mathfrak{A}$, $g \notin \mathcal{K}_k^{(1)}$. We shall show that g is $\mathfrak{x}$-congruent with an n-place function of $\mathcal{K}_k^{(1)}$. Let d and h be fixed numbers from the set δg. We introduce the functions

$$q(x,y) = \begin{cases} y \;, & \text{if } x \neq d \text{ and } y \in \delta g; \\ d & \text{otherwise}, \end{cases}$$

$$p(x) = \begin{cases} x \;, & \text{if} \quad x \in \delta g, \\ d & \text{otherwise}. \end{cases}$$

These functions obviously belong to the algebra $\mathfrak{A}$. Since $c_d(x) \equiv_{\mathfrak{x}} c_h(x)$, we have $q(x, c_d(x)) \equiv_{\mathfrak{x}} q(x, c_h(x))$, i.e., $c_d(x) \equiv_{\mathfrak{x}} t_{ddh}(x)$; hence

$$q(c_d(x), x) \equiv_{\mathfrak{x}} q(t_{ddh}(x), x),$$

$$c_d(x) \equiv_{\mathfrak{x}} p(x),$$

and consequently,

$$p(g(x_1, \ldots, x_n)) \equiv_{\mathfrak{x}} c_d(g(x_1, \ldots, x_n)),$$

$$g(x_1, \ldots, x_n) \equiv_{\mathfrak{x}} c_d(x_1, \ldots, x_n).$$

<u>LEMMA 2.</u> Let $\mathfrak{x}$ be a congruence in the algebra $\mathcal{L}^{(2)}$. If there exist in $\mathcal{L}^{(2)}$ two distinct $\mathfrak{x}$-congruent functions f_1, f_2, dependent on the same number of variables, then $\mathfrak{x} \geq \mathfrak{x}_p$ if the functions f_1 and f_2 are dual; or $\mathfrak{x} \geq \mathfrak{x}_a$, otherwise.

As in Lemma 1, it is easily shown that any two functions of $\mathcal{L}^{(1)}$, dependent on the same number of variables, are $\mathfrak{x}$-congruent. It follows from the truth of the congruence

$$g(x_1, \ldots, x_n) \oplus c_a(x_1, \ldots, x_n) \equiv_{\mathfrak{x}} g(x_1, \ldots, x_n) \oplus c_0(x_1, \ldots, x_n) \; (\delta g = \{0,1\})$$

that, if $g_1^n = g_2^n \oplus c_a^n$ and $\delta g_2 = \{0,1\}$, then $g_2 \equiv_{\mathfrak{x}} g_1$. Let h be an arbitrary function of $\mathcal{L}^{(2)}$, $h \notin \mathcal{K}_k^{(1)}$, and $\delta h = \{a_1, a_2\}$. We introduce the three functions

$$f(x_1, \ldots, x_n) = \begin{cases} 0 \;, & \text{if} \quad h(x_1, \ldots, x_n) = a_1; \\ 1 \;, & \text{if} \quad h(x_1, \ldots, x_n) = a_2; \end{cases}$$

$$g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \oplus 1;$$

$$u(x) = \begin{cases} a_1, & \text{if} \quad x = 0 \;; \\ a_2 & \text{otherwise}. \end{cases}$$

Since $u(f)=h$, the function $u(g)$ is dual to the function h and distinct from h, and $u(f(x_1,\dots,x_n)) \equiv_{\varkappa} u(g(x_1,\dots,x_n))$, so that $\varkappa \geq \varkappa_p$.

Assume now that the functions f_1 and f_2 are not dual. Let $f_1, f_2 \in \mathcal{R}_K^n$. The fact that f_1 and f_2 are not dual implies that one of them does not belong to $\mathcal{R}_K^{(1)}$, and also, that one of the following conditions is satisfied:

a) $\delta f_1 \notin \delta f_2$ and $\delta f_2 \notin \delta f_1$;

b) $\delta f_1 \subseteq \delta f_2$ or $\delta f_2 \subseteq \delta f_1$ and there exist in E_K numbers $a_{11},\dots,a_{1n},a_{21},\dots,a_{2n}$ such that

$$f_1(a_{11},\dots,a_{1n})=f_2(a_{11},\dots,a_{1n}),\; f_1(a_{21},\dots,a_{2n})\neq f_2(a_{21},\dots,a_{2n}).$$

We shall show that case a) reduces to case b). Assume that $f_1 \notin \mathcal{R}_K^{(1)}$ and let $\delta f_1=\{d_1,d_2\}$, $\delta f_1 \cap \delta f_2 = d_2$ or alternatively, $\delta f_1 \cap \delta f_2 = \phi$. We choose in $\mathcal{R}_K^{1(2)}$ a function g such that $g(d_1)=d_1$, $g(x)=d_2$ if $x\neq d_1$. Obviously, the functions $g(f_1)$, $g(f_2)$ are not dual, and they satisfy condition b).

Take the case b). Let $f_1(a_{11},\dots,a_{1n})\neq f_1(a_{21},\dots,a_{2n})$ (if not, then this is true for f_2). We choose in $\mathcal{L}^{(2)}{}_n$ the functions

$$u_i(x) = \begin{cases} a_{1i}, & \text{if } x=0, \\ a_{2i}, & \text{if } x\neq 0, \end{cases} \quad (i=1,\dots,n)$$

and let

$$t_1(x)=f_1(u_1(x),\dots,u_n(x)),\; t_2(x)=f_2(u_1(x),\dots,u_n(x)).$$

The functions t_1, t_2 are not dual, $t_2 \in \mathcal{R}_K^{(1)}$, $\delta t_1=\delta f_1$, and $t_1 \equiv_{\varkappa} t_2$.

Let $h(x)$ be any function of $\mathcal{L}^{1(2)} \setminus \mathcal{R}_K^{(1)}$ and $\delta h=\{b_1,b_2\}$. We introduce the functions

$$h_1(x)=\begin{cases} 0, & \text{if } h(x)=b_1, \\ 1 & \text{otherwise,} \end{cases}$$

$$h_2(x)=\begin{cases} b_1, & \text{if } x=t_1(0), \\ b_2 & \text{otherwise.} \end{cases}$$

Obviously, $h_2(t_1(h_1)) \equiv_{\varkappa} h_2(t_2(h_1))$. It can easily be seen that $h_2(t_1(h_1))=h$, and for some $a\in E_K$, we have $h_2(t_2(h_1))=c_a$, so that $h\equiv_{\varkappa} c_a$. Hence any two functions of $\mathcal{R}_K^{1(2)}$ are $\varkappa$-congruent.

Now let q^n be an arbitrary essentially multi-place function of $\mathcal{L}^{(2)}$. There exist in $\mathcal{R}_K^1$ functions $p, p_1, \dots, p_n$ such that

$$q(x_1,\dots,x_n)=p(p_1(x_1)\oplus\dots\oplus p_n(x_n)).$$

With each number $i=1,\dots,n$ we associate the number 0, if the function $p_i(x)$ takes values of only one parity; otherwise, we associate with it two numbers b_1^i, b_2^i, such that the number $p_i(b_1^i)$ is even, and the number $p_i(b_2^i)$ odd. We introduce the functions $(i=1,\dots,n)$:

$$q_i(x)=\begin{cases} 0, & \text{if } p_i(x) \text{ takes values of just one parity;} \\ b_1^i, & \text{if } p_i(x) \text{ is even;} \\ b_2^i, & \text{if } p_i(x) \text{ is odd.} \end{cases}$$

We have the congruences

$$p(p_1(q_1(x_1))\oplus\dots\oplus p_n(q_n(x_n))) \equiv_{\varkappa} p(p_1(c_0(x_1))\oplus\dots\oplus p_n(c_0(x_n))),$$

$$q(x_1,\dots,x_n)\equiv_{\varkappa} c_a(x_1,\dots,x_n),$$

where $a=q(0,\dots,0)$. Lemma 2 is proved.

LEMMA 3. Let $\varkappa$ be a congruence in the algebra $\mathfrak{B} \subseteq \mathcal{P}_k$ containing the cell $\mathfrak{A}$. If there exist in $\mathfrak{B}$ two $\varkappa$-congruent functions f_1, f_2, dependent on different numbers of variables, then any two functions of $\mathfrak{A}$ will be $\varkappa$-congruent.

Let $f \in \mathcal{P}_k^m$, $f_2 \in \mathcal{P}_k^n$, $m < n$ and $a \in E_k$. We have the congruences

$$c_a(f_1) \equiv_\varkappa c_a(f_2), \quad \text{i.e.,} \quad c_a^m \equiv_\varkappa c_a^n,$$
$$\Delta^{n-2} c_a^m \equiv_\varkappa \Delta^{n-2} c_a^n, \quad \text{i.e.,} \quad c_a^1 \equiv_\varkappa c_a^2. \tag{2}$$

We introduce the two-place function g:

$$g(x_1, x_2) = \begin{cases} 0, & \text{if } x_2 \text{ is even,} \\ 1, & \text{if } x_2 \text{ is odd.} \end{cases}$$

From (2) we obtain the congruence

$$(\tau(g * c_a^1)) * c_a^1 \equiv_\varkappa (\tau(g * c_a^2)) * c_a^1.$$

We denote $(\tau(g * c_a^1)) * c_a^1$ by g_1, and $(\tau(g * c_a^2)) * c_a^1$ by g_2. Obviously, $g_1 \in \mathcal{P}_k^{2(1)}$, $g_2 \in \mathcal{P}_k^3$ and

$$g_2(x, y, z) = \begin{cases} 0, & \text{if } z \text{ is even,} \\ 1, & \text{if } z \text{ is odd} \end{cases}$$

Notice that the functions $\Delta(\Delta g_1)$, $\Delta(\Delta g_2)$ belong to $\mathcal{L}^{(2)}$, that they are not dual and are one-place, and that

$$\Delta(\Delta g_1) \equiv_\varkappa \Delta(\Delta g_2).$$

On applying Lemmas 1 and 2, we obtain the proof of Lemma 3.

We denote by φ a one-to-one mapping of the set E_k onto itself and with every function $f \in \mathcal{P}_k$ we associate a function $f^\alpha \in \mathcal{P}_k$, such that

$$f^\alpha(x_1, \ldots, x_n) = [f(x_1\varphi^{-1}, \ldots, x_n\varphi^{-1})]\varphi. \tag{3}$$

The mapping $\alpha : f \to f^\alpha$ is an automorphism of the algebra $\mathcal{P}_k$; automorphisms of this kind, of subalgebras of the algebra $\mathcal{P}_k$ which are invariant under the mapping α, will be called internal automorphisms of these subalgebras [2]. A. I. Mal'tsev showed in [2] that all automorphisms of the algebra $\mathcal{P}_k$ are internal. The following theorem shows that all automorphisms of cells of the algebra $\mathcal{P}_k$ are likewise internal.

THEOREM 2. If the subalgebra $\mathfrak{A}$ of the algebra $\mathcal{P}_k$ contains the algebra $\mathcal{P}_k^{(1)}$, then all its automorphisms are internal.

Let α be an automorphism of the algebra $\mathfrak{A}$. Since duality of functions is invariant under isomorphisms, α is an automorphism of the semi-group $\mathfrak{A}^1$ [2]. We shall show that here, corresponding to functions of $\mathfrak{A}^{1(1)}$, we again have functions of $\mathfrak{A}^{1(1)}$. For this, we only need to show that functions of $\mathfrak{A}^1 \setminus \mathfrak{A}^{(1)}$ do not map into functions of $\mathfrak{A}^{(1)}$. Assume the contrary, i.e., that there exists a function $f \in \mathfrak{A}^1$ such that $f \notin \mathfrak{A}^{(1)}$ and that for some a of E_k we have $f^\alpha = c_a$; then

$$(f * c_\alpha)^\alpha = f^\alpha * c_\alpha^\alpha,$$

i.e., for some b we have $c_b^\alpha = c_a$, which is impossible.

There thus exists for every x of E_k a unique y of E_k such that $c_x^\alpha = c_y$, i.e., corresponding to the automorphism α we have a one-to-one mapping $\varphi : x \to y$ of the set E_k onto itself. In turn, the mapping φ generates an isomorphism of the type (3) of the algebra $\mathfrak{A}$. In order to show that α is the same as α_φ, we shall show that all functions in $\mathfrak{A}$ remain invariant under the mapping $\gamma = \alpha\alpha_\varphi^{-1}$.

This is obvious for functions of $\mathfrak{A}^{1(1)}$. Let $f \in \mathfrak{A}^n$ and

$$[f(x_1, \ldots, x_n)]^\gamma = g(x_1, \ldots, x_n).$$

In view of the invariance of the functions of $\mathfrak{A}^{1(1)}$, for arbitrary $a_1, \ldots, a_n$ of E_k we have

$$[f(c_{a_1}(x),\ldots,c_{a_n}(x))]^{r}=g(c_{a_1}(x),\ldots,c_{a_n}(x)),$$
$$[f(c_{a_1}(x),\ldots,c_{a_n}(x))]^{r}=f(c_{a_1}(x),\ldots,c_{a_n}(x)),$$

so that the functions f and g are identical.

COROLLARY. If $\mathfrak{A}$ is a cell of the algebra $\mathcal{R}_k$, there exist precisely $k!$ distinct automorphisms of the algebra $\mathfrak{A}$, and all these automorphisms are internal.

LITERATURE CITED

1. A. I. Mal'tsev, Algebraic Systems [in Russian], Nauka (1970).
2. A. I. Mal'tsev, "Iterative algebras and Post manifolds," Algebra i Logika, 5, No. 2, 5-24 (1966).
3. S. V. Yablonskii, "Functional constructions in a k-valued logic," Trudy MIAN im. V. A. Steklova, 51, 5-142 (1958).