COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE
26,3 (1885)

SOME AUTOMORPHISMS OF NATURAL NUMBERS IN THE ALTERNATIVE SET THEORY

J. MLČEK

Abstract: A method of construction of automorphisms of natural numbers is presented. It is based on a saturation of the structure in question and on some properties of indiscernibles in this one. Majorizing and minorizing automorphisms are constructed.

Key words: Alternative set theory, natural numbers, automorphism, indiscernibles.

Classification: 03E70, 03C50, 03H15

Introduction. It is known that there exist non-trivial automorphisms of natural numbers in the alternative set theory. There are several possibilities, how to construct these ones. In the paper presented, we introduce one method of such a construction, based on a saturation of natural numbers and on some properties of indiscernibles. A description of this method is contained in the section "Proofs".

By using this method, we can, for example, construct to a given class X of natural numbers and a collection $\mathcal{F}$ of functions, an automorphism of natural numbers which majorize (minorize resp.) every function from $\mathcal{F}$ on X. A precise formulation of this vague description is given in the section "Main results".

Preliminaries. By a language we mean a countable first-order language $\mathcal{L}$ with equality. The set of formulas of this language is obtained by a usual construction on FN. Writing $\varphi \in \mathcal{L}$ we mean that φ is a formula of $\mathcal{L}$.

We use $\mathbb{M}, \mathbb{N}, \ldots$ as symbols that range over structures for $\mathcal{L}$. If $\mathbb{M}$ is such a model then M is the universe of this one.

Having $\mathbb{M}_i \models \mathcal{L}$, $i = 1,2$, and a mapping $H \subseteq M_2 \times M_1$, we say that H is a similarity between $\mathbb{M}_1$ and $\mathbb{M}_2$ iff the following holds: $(\forall \varphi \in \mathcal{L})(\forall a_1, \ldots \in \mathrm{dom}(H))(\mathbb{M}_1 \models \varphi(a_1, \ldots) \Longleftrightarrow$ $\Longleftrightarrow M_2 \models \varphi(H(a_1), \ldots))$. Recall the following fact: if $\mathbb{M}$ is a fully revealed model for $\mathcal{L}$, then every 1-type of $\mathcal{L}(C)$-formulas, where $C \subseteq M$ is at most countable, is realized in M. Thus, every at most countable similarity between two infinite fully revealed models for $\mathcal{L}$ can be extended to an isomorphism of these ones. Note that every revealment of a class X is a fully revealed class. (See [3].)

Let $\mathcal{J}$ denote the language of Peano arithmetic and let $\mathbb{N}$ be the structure $\langle \mathbb{N}, +, \cdot, 0, 1, < \rangle$ for $\mathcal{J}$. We use $\alpha, \beta, \gamma, \delta, \varsigma$ (possibly indexed) as variables ranging over natural numbers. Assuming $\alpha \leq \beta$, we denote $[\alpha, \beta]$ the interval $\{\gamma; \alpha \leq \gamma \leq \beta\}$ and $\check{\alpha}$ the class $\{\gamma; \gamma > \alpha\}$.

Suppose that H is an automorphism of the model $\mathbb{M}$, $\mathbb{M} \models \mathcal{J}$. This property of H can be expressed in an extension $\mathcal{J}'$ of $\mathcal{J}$, $\mathcal{J}' = \mathcal{J} \cup \{h\}$, where h is a new unary function symbol. Indeed, let $\langle \mathbb{M}, H \rangle$ be the expansion of $\mathbb{M}$ to the structure for $\mathcal{J}'$. Then H is an automorphism of $\mathbb{M}$ iff $\langle \mathbb{M}, H \rangle \models \{\varphi(x_1, \ldots) \longleftrightarrow$ $\longleftrightarrow \varphi(h(x_1), \ldots); \varphi \in \mathcal{J}\} \cup \{(\forall x)(\exists y)(F(y) = x)\}$.

Main results. Throughout this paper, $\mathcal{F}_0, \mathcal{F}_1, \mathcal{F}_2$ denote at most countable classes of functions such that

$F \in \mathcal{F}_0 \cup \mathcal{F}_1 \cup \mathcal{F}_2 \longrightarrow F:N \longrightarrow N$ and there exist $\varphi(x,y,z) \in \mathcal{J}$ and γ with $F(\alpha) = \beta \longleftrightarrow \varphi(\alpha, \beta, \gamma) \& (\forall \alpha)(\exists ! \beta)\varphi(\alpha, \beta, \gamma)$.
Let $H:N \longrightarrow N$ be a function, $X \subseteq N$. H <u>majorizes</u> (<u>minorizes</u> resp.) $\mathcal{F}_0$ <u>on</u> X if $(\forall \alpha \in X)(\forall G \in \mathcal{F}_0)(G(\alpha) \leq H(\alpha))$ $(\forall \alpha \in X)(\forall G \in \mathcal{F}_0)(G(\alpha) \geq H(\alpha))$ resp.) holds.
H is <u>over constants</u> if $(\forall \alpha)(\exists \beta)(\forall \gamma > \beta)(H(\gamma) > \alpha)$. $\mathcal{F}_0$ is over constants if $(\forall F \in \mathcal{F}_0)$(F is over constants).

<u>Theorem 1</u>. $(\forall \gamma)(\exists \delta)(\exists H)$[(H is an automorphism of $\mathbb{N}$) & (H is identic on γ) & (H majorizes $\mathcal{F}_1$ on $\check{\delta}$)].

<u>Theorem 2</u>. Let $\mathcal{F}_2$ be over constants. Then $(\forall \gamma)(\exists \delta)(\exists H)$[(H is an automorphism of $\mathbb{N}$) & (H is identic on γ) & (H minorizes $\mathcal{F}_2$ on $\check{\delta}$)] holds.

An interval $[\alpha, \beta]$ is $\mathcal{F}_0$<u>-large</u> iff $(\forall F \in \mathcal{F}_0)(F(\alpha) < \beta)$.

<u>Theorem 3</u>. Assume that $\mathcal{F}_2$ is over constants. Then $(\forall \gamma)(\exists H)$ {(H is an automorphism of $\mathbb{N}$) & (H is identic on γ) & & $(\forall \alpha)$ [$(\exists U) \subseteq \check{\alpha}$)(U is an $\mathcal{F}_0$-large interval & H majorizes $\mathcal{F}_1$ on U) & $(\exists U \subseteq \check{\alpha})$(U is an $\mathcal{F}_0$-large interval & H minorizes $\mathcal{F}_2$ on U) & $(\exists \beta > \alpha)(H(\beta) = \beta)$]} .

<u>Remark</u>. Each of Theorems 1, 2,3 guarantees that for every α, the mapping $Id \wedge \alpha$ can be extended to a non-trivial automorphism of $\mathbb{N}$.

<u>Proofs</u>

<u>Notation</u>. Let $\{B_k\}_{k \in FN}$ be an indexed sequence of classes. We shall write more briefly $\{B_k\}_k$ only.

Suppose that $\mathcal{F}_i = \{F_{ik}\}_k$, i=0,1,2. Assume that for i = = 0,1,2 and $k \in N$, $\Psi_{ik}(x,y,z)$ and γ_{ik} are such that the statements

$$F_{1k}(\alpha) = \beta \leftrightarrow \psi_{1k}(\alpha, \beta, \gamma_{1k}) \& (\forall \gamma)(\exists ! \delta)\psi_{1k}(\gamma, \delta, \gamma_{1k})$$

hold.

To simplify some following notations, we put

$$\delta_{1k} = \gamma_{1k},\ \delta_{2k} = \gamma_{2k},\ k \in FN \text{ and } \delta_{3k} = \gamma_{i\ell} \leftrightarrow i=0,1,2 \ \& \ \& \ k = 3\cdot\ell + i.$$

Let $\mathcal{K}$ be the extension of $\mathcal{J}$ of the form

$$\mathcal{K} = \mathcal{J} \cup \{h\} \cup \{c_o, c_1\} \cup \{d_k\}_k,$$

where h is a new unary function and c_1, d_k are new constants. Let $\mathcal{T}_1$ be the following theory, formulated in $\mathcal{K}$:

$$\{\varphi(x_1,\dots) \leftrightarrow \varphi(h(x_1),\dots); \varphi \in \mathcal{J}\} \cup \{(\forall x)(\exists y)(h(y)=x)\} \cup$$

$$\cup \{x < c_o \rightarrow h(x)=x\} \cup \{c_1 < x \rightarrow (\forall y)\ (\psi_{1k}(x,y,d_k) \rightarrow y < h(x)); k\}.$$

It is easy to see that the theorem 1 is equivalent to the following proposition:

$$(\forall \gamma_o)(\exists \gamma_1)(\exists H{:}N \rightarrow N)(\langle \mathbb{N}, H, \gamma_o, \gamma_1, \{\delta_{1k}\}_k \rangle \models \mathcal{T}_1).$$

We can construct quite analogously the theories $\mathcal{T}_2$ and $\mathcal{T}_3$ in $\mathcal{K}$ such that the theorem 2 is equivalent to the proposition

$$(\forall \gamma_o)(\exists \gamma_1)(\exists H{:}N \rightarrow N)(\langle \mathbb{N}, H, \gamma_o, \gamma_1, \{\delta_{2k}\}_k \rangle \models \mathcal{T}_2$$

and the theorem 3 is equivalent to

$$(\forall \gamma_o)(\exists H{:}N \rightarrow N)(\langle \mathbb{N}, H, \gamma_o, 0, \{\delta_{3k}\}_k \rangle \models \mathcal{T}_3.$$

Now, let i be fixed.

Assume that to given γ_o, there exist

γ_1, a substructure $\mathbb{M}$ of $\mathbb{N}$ and a mapping $G{:}M \rightarrow M$

such that

(A) $\{\gamma_o, \gamma_1\} \cup \{\delta_{ik}\}_k \subseteq M$

(B) $\mathbb{M} \prec \mathbb{N}$

(C) $\langle \mathbb{M}, G, \gamma_o, \gamma_1, \{\delta_{ik}\}_k \rangle \models \mathcal{T}_i$.

Then there exists a mapping $H: N \to N$ such that

$$\langle \mathbb{N}, H, \gamma_0, \gamma_1, \{\sigma_{1k}\}_k \rangle \models \mathcal{T}_1$$

and, consequently, Theorem 1 is true.

Proof. Put $\widetilde{\mathbb{M}} = \langle \mathbb{M}, G, \gamma_0, \gamma_1, \{\sigma_{1k}\}_k \rangle$. Then a revealment $\widetilde{\mathbb{M}}^*$ of $\widetilde{\mathbb{M}}$ has the form $\langle \mathbb{M}^*, G^*, \gamma_0, \gamma_1, \{\sigma_{1k}\}_{k \in FN^*} \rangle$, where X^* is the revealment of X. We have $\widetilde{\mathbb{M}} \prec_{\mathcal{K}} \widetilde{\mathbb{M}}^*$ and, especially, $\mathbb{M} \prec_{\mathcal{J}} \mathbb{M}^*$ is true, too. We deduce from this, (A) and (B), that $Id \upharpoonright (\{\gamma_0, \gamma_1\} \cup \{\sigma_{1k}\}_k)$ is a similarity between $\mathbb{N}$ and $\mathbb{M}^*$. Let Z be an isomorphism of $\mathbb{N}$ and $\mathbb{M}^*$ which is identical on $\{\gamma_0, \gamma_1\} \cup \{\sigma_{1k}\}_k$. Put $H(\alpha) = \beta \leftrightarrow G^*(Z(\alpha)) = Z(\beta)$. Then Z is an isomorphism between $\langle \mathbb{N}, H, \gamma_0, \gamma_1, \{\sigma_{1k}\}_k \rangle$ and $\widetilde{\mathbb{M}}^*$. We deduce from this that the assertion in question holds.

To finish our proof of Theorem 1 it suffices to find, to a given γ_0, a number γ_1, a substructure $\mathbb{M}$ of $\mathbb{N}$ and $G: M \to M$ such that (A), (B), and (C) hold. We shall construct γ_1, $\mathbb{M}$ and G in question by using some properties of indiscernibles in AST. Recall that there exists <u>an unbounded</u> π<u>-class</u> J <u>of strong indiscernibles</u> in N. (See [2].) We start with two lemmas which will be used frequently in the sequel. Let us introduce the following notation. Let $X \subseteq N$. We denote by $\mathbb{N}_X$ <u>the smallest substructure of</u> $\mathbb{N}$ <u>such that the universe of</u> $\mathbb{N}_X$ <u>contains</u> X <u>as a subclass</u>.

<u>Lemma 1</u>. Let I be a class of strong indiscernibles in N. Assume that $Z \subseteq N$ has the property $(\forall e \in I)(Z \subseteq e)$.

(1) Let G_0 be an automorphism of $\langle Z \cup I, < \rangle$ which is identic on Z. Then there exists an automorphism G of the structure $\mathbb{N}_{Z \cup I}$ and $G \supseteq G_0$ hold.

(2) Assume, moreover, that I has no last element and $I \subseteq J$. Then I is cofinal in $N_{Z \cup I}$.

Proof. (1) We define the mapping G as follows: Suppose that $a \in N_{Z \cup I}$ is definable by the formula $\varphi(x,e_1,\ldots,z_1,\ldots)$ where $e_1,\ldots$ is an increasing sequence from I (i.e. $e_1 < e_2 < \ldots$ and $e_1 \in I$, $e_2 \in I,\ldots$), $z_1 \in Z,\ldots$ and $\varphi(x,y_1,\ldots,x_1,\ldots) \in \mathcal{J}$. We put $G(a) = b$ iff $\varphi(b,G(e_1),\ldots,z_1,\ldots)$ holds.

If $b \in N_{Z \cup I}$ is definable by $\psi(x,e_1,\ldots,z_1,\ldots)$ in $\mathbb{N}$, where $e_1,\ldots$ is an increasing sequence from I and $z_1 \in Z,\ldots$, then there exists an element $a \in N_{Z \cup I}$ such that $\psi(a,G_0^{-1}(e_1),\ldots,z_1,\ldots)$ holds. Therefore, the mapping G is onto $N_{Z \cup I}$.

To finish the proof, it suffices to prove the following: If $a_1,\ldots \in N_{Z \cup I}$, $\varphi(x_1,\ldots) \in \mathcal{J}$ then $\mathbb{N}_{Z \cup I} \models \varphi(a_1,\ldots) \Longleftrightarrow \mathbb{N}_{Z \cup I} \models \varphi(G(a_1),\ldots)$. But $\mathbb{N}_{Z \cup I} \prec \mathbb{N}$ and, consequently, we have to prove: If $a_1,\ldots \in N_{Z \cup I}$, $\varphi(x_1,\ldots) \in \mathcal{J}$ then $\mathbb{N} \models \varphi(a_1,\ldots) \Longleftrightarrow \mathbb{N} \models \varphi(G(a_1),\ldots)$. Assume that $\psi_i(x_i,e_1^i,\ldots,z_1^i,\ldots)$ defines a_i in $\mathbb{N}$, $e_1^i,\ldots$ is an increasing sequence from I and $z_1^i,\ldots \in Z$. We have

$$\varphi(a_1,\ldots) \Longleftrightarrow (\exists x_1\ldots)(\bigwedge_i \psi_i(x_i,e_1^i,\ldots,z_1^i,\ldots) \,\&\, \varphi(x_1,\ldots)) \Longleftrightarrow$$
$$\Longleftrightarrow (\exists x_1\ldots)(\bigwedge_i \psi_i(x_i,G_0(e_1^i),\ldots,z_1^i,\ldots) \,\&\, \varphi(x_1,\ldots)) \Longleftrightarrow$$
$$\Longleftrightarrow \varphi(G(a_1),\ldots).$$

(2) Assume a is definable by $\varphi(x,e_1,\ldots,z_1,\ldots)$ in $\mathbb{N}$, $e_1,\ldots$ is an increasing sequence from I, $z_1,\ldots \in Z$. Suppose that $e \in I$ has the property: $\{e_1,\ldots\} \leq e$. We can easily see that $a < e$ holds.

<u>Lemma 2</u>. Let $F: N \longrightarrow N$ be a function, definable by the formula $\varphi(x,y,\gamma) \in \mathcal{J}(\{\gamma\})$ in $\mathbb{N}$. Suppose that I is a class of strong indiscernibles in N which is unbounded in N. Let $e_0 < e_1 < e_2 < e_3$ be an increasing sequence from I, $\gamma < e_0$.

Then (1) $F''[e_1,e_2] \subseteq e_3$ and

(2) if F is over constants, then $F''[e_1,e_2] \subseteq \check{e}_0$.

Proof. (1) Let $\chi(e_2,e_2,e_3)$ be the formula

$$(\exists x \in [e_1,e_2])(F(x) \geq e_3).$$

Then $\chi(e_1,e_2,e_3) \longrightarrow ((e \in I \,\&\, e > e_3) \longrightarrow \chi(e_1,e_2,e))$, which is impossible.

(2) Let $\chi(e_0,e_1,e_2)$ be the formula

$$(\exists x \in [e_1,e_2])(F(x) \leq e_0).$$

Then $\chi(e_0,e_1,e_2) \longrightarrow ((e,f \in I \,\&\, e_2 < e < f) \longrightarrow \chi(e_0,e,f))$, which contradicts the assuming property of F.

Let $\gamma_0 \in N$, $i \in [0,2]$. We are looking for γ_1, a substructure $\mathbb{M}$ of $\mathbb{N}$ and $G: M \longrightarrow M$ such that (A),(B), and (C) hold. Let K denote the class of all finite integers.

Case $i = 1$. Choose $\varsigma \in N$ with $\{\gamma_0\} \cup \{\delta_{1k}\}_k \subseteq \varsigma$ and $I \subseteq J$ of the form $I = \{e_c\}_{c \in K}$ such that $(\forall c \in K)(\varsigma < e_c)$ holds. Put $M = N_{\varsigma \cup I}$. Let G_0 be an automorphism of $\langle \varsigma \cup I, < \rangle$, satisfying: G_0 is identical on ς and $G_0(e_c) = e_{c+2}$ holds for every $c \in K$. Let $G \supseteq G_0$ be an automorphism of $\mathbb{M}$. Assume that $x \in [e_k,e_{k+1}] \cap M$. We can see, by using Lemma 2, that $G(x) \geq$ $\geq G(e_k) = e_{k+2} > F_{1i}(x)$ holds for every i, k. The class I is cofinal in M and, consequently, $\gamma_1 = e_0$, $\mathbb{M}$ and G have the required properties (A),(B), and (C).

Case $i = 2$. Choose again $\varsigma \in N$ with $\{\gamma_0\} \cup \{\delta_{2k}\}_k \subseteq \varsigma$ and I, M as above. Let G_0 be identical on ς and let $G_0(e_c) =$ $= e_{c-2}$ hold for every $c \in K$. Suppose that $G \supseteq G_0$ is an automorphism of $\mathbb{M}$. We can see analogously as above (by using the presumption that $\mathcal{F}_2$ is over constants) that $x \in [e_k,e_{k+1}] \cap M \longrightarrow$ $\longrightarrow F_{2k}(x) > G(x)$ holds for every i, k. We can conclude that

$\gamma_1 = e_o$, $\mathbb{M}$ and G have the required properties.

Case i = 3. Let again $\xi \in N$ be such that $\{\gamma_o\} \cup \{\delta_{3k}\}_k \subseteq$ $\subseteq \xi$. Choose $I \subseteq J$ of the form $I = \{e_{kc}\}$ $k \in FN$, $c \in K$ with the property

$$(\forall k < l)(\forall c,d \in K)\ [(\xi < e_{kc} < e_{ld}) \& (c < d \rightarrow e_{kc} < e_{kd})].$$

An existence of I is guaranteed by the fact that J is an unbounded σ-class. Put $M = M_{\xi \cup I}$.

We define $G_o: \xi \cup I \rightarrow \xi \cup I$ as follows:

0) $k \equiv 0 \pmod 3 \rightarrow G_o(e_{kc}) = e_{kc}$, $c \in K$,

1) $k \equiv 1 \pmod 3 \rightarrow G_o(e_{kc}) = e_{k,c+2}$, $c \in K$,

2) $k \equiv 2 \pmod 3 \rightarrow G_o(e_{kc}) = e_{k,c-2}$, $c \in K$,

3) $\alpha \in \xi \rightarrow G_o(\alpha) = \alpha$.

It is easy to see that G_o is an automorphism of $\langle \xi \cup I, < \rangle$. Let $G \supseteq G_o$ be an automorphism of $\mathbb{M}$. We can see as above that the following propositions hold:

(i) $k \equiv 1 \pmod 3 \rightarrow x \in [e_{ko}, e_{k1}] \cap M \rightarrow F_{1j}(x) < G(x)$, $k,j \in FN$,

(ii) $k \equiv 2 \pmod 3 \rightarrow x \in [e_{ko}, e_{k1}] \cap M \rightarrow F_{2j}(x) > G(x)$, $k,j \in FN$.

We deduce, using Lemma 2, that the assertion

(o) $F_{oj}(e_{ko}) < e_{k1}$, $k,j \in FN$

holds, too. The class I is unbounded in M. We conclude from this and from 0), (o),(i),(ii), and 3) that $\gamma_1 = 0$, $\mathbb{M}$ and G have the required properties.

R e f e r e n c e s

[1] P. VOPĚNKA: Mathematics in the alternative set theory, Teubner Texte, Leipzig 1979.

[2] A. SOCHOR, A. VENCOVSKÁ: Indiscernibles in the alternative set theory, Comment.Math.Univ.Carolinae 22(1981), 785-798.

[4] A. SOCHOR and P. VOPĚNKA: Revealments, Comment. Math. Univ. Carolinae 21(1980), 97-118.

Mathematical Institute, Charles University, Sokolovská 83, 18600 Praha 8, Czechoslovakia

(Oblatum 13.12. 1984)