THE THEOREM OF MATIJASEVIC IS PROVABLE IN PEANO'S ARITHMETIC BY FINITELY MANY AXIOMS

Hans Georg CARSTENS

1. The unsolvability of Hilbert's tenth problem was established by Matijasevic's theorem: «Enumerable sets are diophantine». The following equivalent form is provable in the first order version of Peano's arithmetic (PA):
For all Σ^{o}_{1}-formulas A there are diophantine formulas B with the same free variables such that PA $\vdash$ A $\leftrightarrow$ B.
We show that finitely many axioms are sufficient to prove this schema. This could be done by a very careful inspection of the original proof, we will give, however, a short and simple argument from the «outside».
In 3. we indicate some consequences of the result.

2. Peano's arithmetic is the theory dealt with in Chapter 8 of [2]. We give inductive definitions of $\overset{\delta}{\exists}_1$-formulas, i.e. diophantine formulas, and Σ^{o}_{1}-formulas.

(1) $\overset{\delta}{\exists}_1$-formulas:

a) $Sx = y$, $x + y = z$, $x \cdot y = z$, $\neg Sx = y$, $\neg x + y = z$, $\neg x \cdot y = z$ are diophantine.

b) If A, B are diophantine formulas then $A \vee B$, $A \& B$ are diophantine.

c) If A is diophantine then $\exists x A$ is diophantine.

(2) Σ^{o}_{1}-formulas:

a) The formulas of (1)a) and $x < y$, $\neg x < y$ are Σ^{o}_{1}.

b) Exactly as in (1)b).

c) If A is a Σ^{o}_{1}-formula and $x \not\equiv y$ then $\exists x A$, $\forall x (x < y \rightarrow A)$ are Σ^{o}_{1}.

Theorem.

There is a finite set Γ of axioms of PA s.t. for all Σ^o_1-formulas A there are $\overset{\delta}{\exists}_1$-formulas B with the same free variables and

$$\Gamma \vdash A \leftrightarrow B.$$

Proof.

Let P, L, R be a pairing function and decoding functions resp., $P : \mathbb{N} \rightarrow \mathbb{N} \setminus 13$.

$$\mathrm{Sub}\,(l, m, n) := \begin{cases} P(O, e) & \text{if } m = P(O, n) \\ n & \text{if } m = P(O, k)\ \&\ k \neq m \\ P(i,\ \mathrm{Sub}(l, n, k)) & \text{if } 1 \leqslant i \leqslant 12\ \&\ m = P(i, k) \\ P(\mathrm{Sub}(l, n, i),\ \mathrm{Sub}(l, n, k)) & \\ & \text{if } i > 12\ \&\ m = P(i, k) \end{cases}$$

We extend PA by definitions of P, L, R, Sub.
Consider the following formulas:

(1) $B(P1v) \leftrightarrow SRLv = RRv$
(2) $B(P2v) \leftrightarrow \neg\, SRLv = RRv$
(3)
... analoguously for $+\,,\ .\,,\ <$
(8)
(9) $B(P9v) \leftrightarrow (B(Lv) \vee B(Rv))$
(10) similar for &
(11) $B(P11v) \leftrightarrow \forall n < RLLvB(\mathrm{Sub}(n, RRLv, Rv))$
(12) $B(P12v) \leftrightarrow \exists n\ B(\mathrm{Sub}(n, RLv, Rv))$

Interpret (1) ... (12) as a definition of B in $\mathbb{N}$. Hence B is a recursively enumerable set. By the representatiblity theorem and Lemma 1 [2, p. 128] there is a Σ^o_1-formula A such that

$$\forall n\ B(n) \Leftrightarrow PA \vdash A(n)$$

By the theorem of Matijasevič we have a $\overset{\delta}{\exists}_1$-formula B such that

$$PA \vdash A \leftrightarrow B$$

Therefore we assume that B in (1) ... (12) is a $\overset{\delta}{\exists}_1$-formula.
The following is derivable in our extension of PA:

(13) $LPxy = x,\ RPxy = y$
(14) $Sub(x, y, POy) = POx$
(15) $Sub(x, y, POv) = POv;\ y \neq v$
(16) $Sub(x, y, Piv) = PiSub(x, y, v) \qquad 1 \leqslant i \leqslant 12$
(17) $Sub(x, y, Pnv) = PSub(x, y, n)$
$\quad Sub(x, y, v) \leftarrow n > 12$
(18) $n = Pvw \rightarrow n > 12$

Let Γ^* be the set of the formulas (1) ... (18). We show:
$\forall A\ \Sigma^o_1$-formula, $\exists$ a term with exactly the same free variables as in A such that

$$\Gamma^* \vdash B(a) \leftrightarrow A$$

The proof is by induction on the definition of Σ^o_1-formulas.

a) $A \equiv Sx = y$. We put $a = P1PPOxPOy$.
Now the following holds by Γ^*:
$$B(a) \leftrightarrow B(P1PPOxPOy) \underset{(1)}{\leftrightarrow} SRLPPOxPOy = RRPPOxPOy$$
$$\underset{(13)}{\leftrightarrow} Sx = y \leftrightarrow A$$
The rest of a) is analoguously.

b) Let a_o, a_1 be terms inductively defined such that
$\Gamma^* \vdash A_o \leftrightarrow B(a_o)$, $B(a_1) \leftrightarrow A_1$. $A \equiv A_o \vee A_1$.
We put $a \equiv P9Pa_oa_1$. Now the following holds by Γ^*:
$$B(a) \leftrightarrow B(P9Pa_oa_1) \underset{(9)}{\leftrightarrow} B(LPa_oa_1) \vee B(RPa_oa_1)$$

$\underset{(13)}{\leftrightarrow} B(a_0) \vee B(a_1) \leftrightarrow A_0 \vee A_1 \leftrightarrow A.$

Similar for &.

c) $A \equiv \forall x\,(x < y \rightarrow A_0)$. Let a_0 be s.t. $\Gamma^* \vdash B(a_0) \leftrightarrow A_0$ and put $a \equiv \text{P11PPPOyPOz}\, a_0 \; {}_x[z]$ where z is new.

Now the following holds by Γ^*:

$B(a) \leftrightarrow B(\text{P11PPPOyPOz}\, a_0 \; {}_x[z])$

$\underset{(11)}{\leftrightarrow} \forall x\,(x < \text{RLLPPPOyPOz}\, a_0 \; {}_x[z]$

$\rightarrow B(\text{Sub}(x, \text{RRLPPPOyPOz}\, a_0 \; {}_x[z], \text{RPPPOyPOz}$

$a_0 \; {}_x[z]))$

$\underset{(13)}{\leftrightarrow} \forall x\,(x < y \rightarrow B(\text{Sub}(x, z, a_0 \; {}_x[z]))$

$\underset{(*)}{\leftrightarrow} \forall x\,(x < y \rightarrow B(a_0)) \leftrightarrow \forall x\,(x < y \rightarrow A_0) \leftrightarrow A.$

Similar for $\exists x A_0$. We need the following fact:

(*) $\Gamma^* \vdash \text{Sub}(x, z, a_0 \; {}_x[z]) = a_0$

But this is trivial by the construction of the terms and (14) ... (18).

Now we shall give axioms without P, L, R, Sub.

By the representability theorem and the theorem of Matijasevič there are $\overset{\delta}{\exists}_1$-formulas D_P, D_L, D_R, D_{Sub} representing P, L, R, Sub in PA.

We apply the operation * of [2, p. 59] to formulas of our extended language and get formulas without P, L, R, Sub.

Let Γ be the set of the following formulas:

(1)* ... (18)* and in addition the existence and uniqueness conditions for P, L, R, Sub. Γ is finite.

Let Γ' be the extension of Γ by definitions of P, L, R, Sub. By [2, p. 59] the following holds:

(a) $\Gamma' \vdash A \leftrightarrow A^*$

(b) $A \in L(\Gamma) \Rightarrow (\Gamma' \vdash A \Rightarrow \Gamma \vdash A)$

Hence

$\Gamma' \vdash (1) \dots (18)$ and therefore

$\forall$ A Σ°_1-formula $\exists$ a term with exactly the same free variables as in A such that

$$\text{and} \quad \begin{array}{l} \Gamma' \vdash (B(a) \leftrightarrow A \\ \Gamma \vdash (B(a))^* \leftrightarrow A \end{array}$$

But $(B(a))^*$ is $\overset{\delta}{\exists}_1$. This concludes the proof.

3. Now we indicate some consequences of the result in 2.

Let N be the set of axioms given in [2, p. 22]. We call a structure $\mathcal{A}$ for the language of PA diophantine if $\mathcal{A} \models N +$ Matijasevič's theorem.

Corollary.

The class of diophantine structures is elementary.

Theorem.

Let $\mathcal{A}$ be a non-standard model of PA. For all finite subsets $N \subseteq \Gamma \subseteq PA \cap \Pi^\circ_3$ which imply the theorem of Matijasevič there is a diophantine substructure $\mathcal{L} \subseteq \mathcal{A}$ such that (1) $\mathcal{L} \models \Gamma$ and (2) $\mathcal{L}$ is not cofinal in $\mathcal{A}$.

Proof.

Let A be the conjuction of Γ. By contraciton of quantifiers we have:

$$A \equiv \forall x \, \exists y \, \forall z \, (B(x, y, z); \; B \in \overset{\delta}{\exists}_1.$$

Let C be the following formula:

$$\forall z \; B(x, y, z) \;\; \& \;\; \forall y_1 < y \; \neg B(x, y_1, z)$$

$$\& \ \forall y \neg \forall z \ B(x, y, z) \rightarrow y = 0)$$

and D(z, x, y):

$$(z)_0 = x \ \& \ \mathrm{Seq}(z) \ \& \ \forall i < \mathrm{lh}(z) \ C((z)_i, (z)_{i+1}) \ \& \ y = (z)_{\mathrm{lh}(z)}.$$

We have to show that the iteration of the function defined by C is simultaneously bounded in $\mathcal{A}$.
Suppose not. Hence

$$\exists a \in |\mathcal{A}| \quad \forall b \in |\mathcal{A}| \ \exists c \in |\mathcal{A}|$$

(1) $c \underset{\mathcal{A}}{\geqslant} b$

(2) $\exists n \in \mathbb{N} \ \mathcal{A} \models D(n, a, c)$

Let α be a non-standard number of $\mathcal{A}$. The following holds:

$$\mathcal{A} \models \exists x \ \forall y \ \exists z \geqslant y \quad \exists n < \alpha \, D(n, x, z)$$

By the least number principle:

$$\exists n \in \mathbb{N} \ \mathcal{A} \models \exists x \ \forall y \quad \exists z \geqslant y \ \exists n < n \, D(n, x, z)$$

This is a contradiction.

Corolloray.

PA is not finitely axiomatizable.

Universität Hannover Hans Georg Carstens

REFERENCES

[1] MATIJASEVIČ. V.: Enumerable sets are diophantine, *Soviet mathematics*, vol. 11 (1970).

[2] SHOENFIELD, J.R.: *Mathematical logic*, Reading (Mass.) 1967.