Undecidability of intuitionistic theories formulated with the apartness relation

by

Dov M. Gabbay (Ramat-Gan)

Abstract. Many theories of intuitionistic mathematics are formulated in Heyting's predicate logic. This paper proves the undecidability of certain versions of linear order, linearly ordered abelian groups and of algebraically closed fields formulated in Heyting's predicate logic in a language with the apartness relation. The method is to obtain a faithful interpretation of the classically undecidable theory of a reflexive and symmetric relation into those intuitionistic theories.

0. Introduction. In [1], [2], [3] we dealt with the decision problem of several intuitionistic theories formulated in a language with possibly a symbol $=$ for equality but without the apartness relation $\#$. In this note we extend our methods to obtain undecidability results for several intuitionistic theories formulated with $\#$.

In Section 1 we treat a version of linearly ordered abelian groups. This is the first time any version of this theory (with or without $\#$) is dealt with. In Section 2 we turn to versions of algebraically closed fields. Other versions of algebraically and real closed fields (without $\#$) were treated in [2]. In Section 3 we treat some theories of linear order. Some of the undecidability results obtained here (i.e., for the pure theory of $\#$ and a version of dense linear order) were obtained in Smoryński [6] by a related but different method. Further discussion and comparisons are given in each section.

We assume no previous knowledge of [1]-[3] and [6], but we do assume knowledge of the Kripke semantics for Heyting's predicate calculus (HPC). See [5]. The Kripke structures are denoted by $(S, R, o, \underline{D}_t)$ where S is the set of possible worlds, R is the accessibility relation $o \in S$ is the actual world, and for each $t \in S$, $\underline{D}_t$ is the classical model associated with t. We denote the truth value of a formula A at a world t by $[A]_t$.

1. Linearly ordered abelian groups. In this section we prove that the intuitionistic version T_1 of linearly ordered abelian groups formulated below is not decidable. (We also look at other versions.) We prove undecidability by showing that the classically undecidable theory of a reflexive and symmetric relation is faithfully interpretable in T_1. No version of linearly ordered abelian groups (with or without $\#$) was ever treated before.

The language of T_1 contains 0, +, #, =, and < (actually it will follow from the axioms that = can be defined from # by $(x = y \leftrightarrow \neg x \# y)$. T_1 has the following axioms:

Group E. Axioms for quality.

E1: $x = x$,

E2: $x = y \to y = x$,

E3: $x = y \to (y = z \to x = z)$,

E4: $x = y \to (A(x) \to A(y))$, A is any formula of the language.

Group S. Axioms for apartness.

S1: $\neg(x \# x)$,

S2: $x \# y \to y \# x$,

S3: $\neg(x \# y) \to x = y$,

S4: $x \# y \to x \# z \vee y \# z$,

S5: $\neg(x \# y) \vee \neg\neg(x \# y)$.

Group A. Axioms for addition.

A1: $x+y = y+x$,

A2: $x+(y+z) = (x+y)+z$,

A3: $x+o = x$,

A4: $\forall x \exists y (x+y = o)$,

A5: $x \# y \to x+z \# y+z$.

Group O. Axioms for order.

O1: $x<y \wedge y<z \to x<z$,

O2: $x = y \vee x<y \vee y<x$,

O3: $\neg(x<x)$,

O4: $x<y \to x+z<y+z$.

From the above axioms it follows that

O5: $x \# y \to x<y \vee y<x$,

E5: $x = y \leftrightarrow \neg(x \# y)$,

The following does not follow from the axioms:

S6: $x<y \to x \# y$.

In fact, if we let T_1^* be the theory with the axioms below, then we do not know whether T_1^* is decidable. (In T_1^*, $x \# y$ is $x<y \vee y<x$).

Axioms for T_1^*: E1-E4; S1-S4; A1-A5; O1, O3, O4, O5, S6 and O6, where:

O6: $x<y \to x<z \vee z<y$.

THEOREM A. *The theory T_1 of linearly ordered abelian groups is undecidable.*

Towards the proof of Theorem A we need some constructions.

Let (M, P) be countably infinite classical model of a reflexive and symmetrical relation P. We can assume that M is the set of natural numbers. We now construct a Kripke model $(S, R, o, \underline{D}_t)$, called the Kripke model associated with (M, P). Let I be the linearly ordered abelian group of the integers. Let

(1) $S = \{M\} \cup \{\{m, n\} \subseteq M \mid mPn\} \cup \{\infty\}$,

(2) $R = \{M\} \times S \cup \{(s, s) \mid s \in S\} \cup S \times \{\infty\}$,

(3) $o = \{M\}$.

To define $\underline{D}_t$, $t \in S$, let the domain of $\underline{D}_t$ be I^M.

(4) Define = on the domain as identity.

(5) Define + on the domain pointwise, and let $\bar{o}$ be $(o \ldots o)$.

(6) For $f, g \in I^M$, let $k(f, g)$ be the first coordinate k, in the ordering of M (= set of natural numbers) such that $f(k) \neq g(k)$. Then define $f<g$ iff $f(k)<g(k)$, where $k = k(f, g)$. This means that < is the lexicographic ordering on I^M.

(7) Define # on $\underline{D}_t$ as follows (this is the first time that the definition depends on t):

(7a) $[f \# g]_0 = o$, for all f, g,

(7b) $[f \# g]_{\{m,n\}} = 1$ iff for some $k \notin \{m, n\}$, $f(k) \neq g(k)$,

(7c) $[f \# g]_\infty = 1$ iff $f = g$.

We have thus defined a Kripke model for the language of T_1.

LEMMA 8. *All axioms of T_1 hold in the above model.*

Proof. We check each group of axioms.

Group E. Equality was defined as identity.

Group S. S1-S3 are clear, S3 follows from (7c) and the definition of R. S4 follows from (7) and S5 from the definition of R.

Group A. + was defined pointwise, A5 follows from (6).

Group O. Follows from (6).

We now turn to give some more definitions.

(8) Let E be defined as: $E = \exists x(x \# \bar{o})$.

(9) Let $B(x)$ be: $x \neq \bar{o} \wedge E \to x \# \bar{o}$.

(10) Let $D(x)$ be $\forall y(B(y) \vee [(y \# \bar{o} \to x \# \bar{o}) \to (x \# \bar{o} \to y \# \bar{o}) \vee E)]) \to E \vee B(x)$.

(11) Let $x \equiv y$ be $(x \# \bar{o} \leftrightarrow y \# \bar{o})$.

(12) Let xPy be $E \to x \# \bar{o} \vee y \# \bar{o}$.

LEMMA 13. *In the Kripke model defined we have that*

(14) $[E]_t = 1$ *iff* $t \neq o$.

(15) $[B(x)]_0 = 0$ *iff* $x \neq \bar{o}$ *and for some* $m, n \in M$ *we have that* $x(k) = o$, *for all* $k \notin \{m, n\}$.

(16) $[D(x)]_0 = 0$ *iff* $x \neq \bar{o}$ *and for some* $m \in M$ *we have that for all* k, $x(k) \neq o$ *iff* $k = m$.

(17) *For* x, y *such that* $[x \equiv y]_0 = 1$ *and* $[D(x) \vee D(y)]_0 = o$ *we have that* $x(k) \neq o$ *iff* $y(k) \neq o$ *for all* $k \in M$.

(18) *For x, y such that $[D(x)\vee D(y)]_0 = o$ we have that $[xPy]_0 = o$ iff $M \models a(x)Pa(y)$, where $a(x)$ is defined as the $m \in M$ such that for all k $(x(k) \neq o$ iff $k = m)$.* (See (16).)

Proof. (14) Follows from the definition of $\#$ in (7a).

(15) Is clear from the fact that $x = y \vee x \neq y$ holds, and from (14).

(16) Assume that for some m we have that $x(k) = o$ iff $k \neq m$; for all k. We want to show that $[D(x)]_0 = o$.

Clearly $[E \vee B(x)]_0 = o$. We will show that the antecedent of $D(x)$ holds at o. Let y be such that $[B(y)]_0 = o$, then we must show that

$$(*) \qquad [(y\#\bar{o} \to x\#\bar{o}) \to (x\#\bar{o} \to y\#\bar{o})\vee E]_0 = 1\,.$$

Since $[B(y)]_0 = o$, then for some $n, n^1 \in M$ we have $y(k) = o$ for all $k \notin \{n, n^1\}$. Now if it were the case that $(*)$ is false, then in view of (14) we must have that

$$[y\#\bar{o} \to x\#\bar{o}]_0 = 1\,, \qquad [x\#\bar{o} \to y\#\bar{o}]_0 = o\,.$$

So $[y\#\bar{o} \to x\#\bar{o}]_{\{m\}} = 1$, since $[x\#\bar{o}]_{\{m\}} = o$, we must have $[y\#\bar{o}]_{\{m\}} = o$, i.e., $\{m\}\supseteq\{n, n^1\}$. But this means $m = n = n^1$ ($\{n, n^1\}$ must be nonempty since $y \neq \bar{o}$) and so $[x\#\bar{o} \to y\#\bar{o}]_0 = 1$, a contradiction.

To show the other direction, let $[D(x)]_0 = 0$, then clearly (by (14)), $[B(x)]_0 = 0$, and the antecedent of $D(x)$ holds at o. Assume that $m, n \in M$ are such that for all k, $k \in \{m, n\} \to x(k) \neq o$. We claim that $m = n$. Otherwise let y be such that $y(k) = x(k)$ for $k \neq n$ and $y(n) = 0$. Clearly $[B(y)]_0 = o$ and so we must have that $(*)$ holds for this y and this x. Now clearly for any t, $[y\#\bar{o}]_t = 1$ implies $t = \infty$ or $m \notin t$, and so $[x\#\bar{o}]_t = 1$ must also hold. However, for $t = \{m\}$, $[x\#\bar{o}]_{\{m\}} = 1$ but $[y\#\bar{o}]_{\{m\}} = o$. Thus we contradicted $(*)$ and therefore $m = n$. This proves the other direction of (16).

(17) Let x, y be such that $[D(x)\vee D(y)]_0 = o$ and $[x \equiv y]_0 = 1$. Assume that $x(k) = o \wedge y(k) \neq o$, for some $k \in M$. Then for $t = \{k\}$, $[y\#\bar{o}]_t = 0$, since by (16) there could be only one point $k \in M$ such that $y(k) \neq o$. On the other hand $[x\#o]_t = 1$ since, again by (16), there must be another point $k^1 \neq k$ such that $x(k^1) \neq 0$.

(18) Suppose $m, n \in M$ are such $M \not\models mPn$, then $\{m, n\} \notin S$, we claim that $[E \to x\#\bar{o} \vee y\#\bar{o}]_0 = 1$ for x, y such that for all k,

$$x(k) \neq o \quad \text{iff} \quad k \neq m\,,$$
$$y(k) \neq o \quad \text{iff} \quad k \neq n\,.$$

This is clear since for all $t \in S$, $t \neq \infty, o$; $\{m, n\} \not\subseteq t$. Now assume that $M \models mPn$, then for $t = \{m, n\} \in S$ and x, y defined as above, $[E]_t = 1$ and $[x\#\bar{o} \vee y\#\bar{o}]_t = o$. Thus (18) is proved.

(19) Observe that from (17) and (18) it follows that the relation $[x \equiv y]_0 = 1$ is an equivalence relation on $\{x|\ [D(x)]_0 = o\}$ and that it is a congruence relation with respect to $[xPy]_0 = o$.

(20) Thus from (17), (18) and (19) it follows that the model (M, P) is isomorphic to the model $(\bar{M}, \bar{P})$ where $\bar{M}$ is the set of $\equiv$ equivalence classes of $\{x|\ [D(x)]_0 = o\}$ and $\bar{P}$ is defined by $x/\equiv \bar{P} y/\equiv$ iff $[xPy]_0 = o$.

We are now in a position to define a faithful translation from the classical theory RS of a reflexive and symmetric relation into the theory T_1 of this section. If φ is translated into φ^*, then we shall have

$$T_1 \vdash \varphi^* \quad \text{iff} \quad \mathrm{RS} \vdash \neg\varphi\,.$$

To obtain the translation, we need some more definitions.

(21) Define the following:

(a) Let the quantifiers $\forall^*$, $\exists^*$ be defined by

$$\forall^* y\varphi \quad \text{iff} \quad (\forall y)(D(y)\vee\varphi)\,,$$
$$\exists^* y\varphi \quad \text{iff} \quad (\exists y)((D(y)\to E)\wedge\varphi)\,.$$

(b) Let φ be a sentence of *RS*. Write φ in the form $(Q\ldots)\wedge(\bigwedge x_iPy_i \to \bigvee u_jPv_j)$, where Q is a string of quantifiers and P is the symbol for the relation in the language of *RS*. Let the translation φ^* of φ, in the language of T_1 be the following sentence

$$\forall u[Q^*\ldots)\wedge(\bigwedge u_jPv_j \to \bigvee x_iPy_i \vee E) \to E\vee D(u)]\,.$$

Where Q^* is the same string of quantifiers as Q except that $\forall$ and $\exists$ are replaced by $\forall^*$ and $\exists^*$ of (21) (a), and D, P and E are as defined in (8), (10) and (12).

LEMMA 22. *For φ, φ^* of* (21) *we have*: $T_1 \vdash \varphi^*$ *iff* $\mathrm{RS} \vdash \neg\varphi$.

Proof. We show that T_1 not $\vdash \varphi^*$ iff RS not $\vdash \neg\varphi$.

Assume that there exists a model (M, P) in which φ holds. We will show a Kripke model of T_1 in which φ^* does not hold. Let $(S, R, o, \underline{D}_t)$ be the model associated with (M, P) as constructed in the beginning of this section. We want to show that $[\varphi^*]_0 = o$. To show this, let u be any element such that $[D(u)]_0 = o$, and let us show (since $[E]_0 = o$) that

$$[(Q^*\ldots)\wedge(\bigwedge u_jPv_j \to \bigvee x_iPy_i \vee E)]_0 = 1\,.$$

To prove this remember that by (20), $(\bar{M}, \bar{P})$ is isomorphic to (M, P). We use this to proceed and show by induction on the length of $(Q^*\ldots)$, that for any substitution of elements f_i such that $[D(f_i)]_0 = 0$, and any string of quantifiers Q_1 we have:

$$(**) \qquad [(Q_1^*\ldots)\psi^*(f_i)]_0 = 1 \quad \text{iff} \quad M \models (Q_1\ldots)\psi(a(f_i))$$

where $a(f_i)$ is as in (17) and

$$\psi = \bigwedge(\bigwedge x_i P y_i \to \bigvee u_j P v_j),$$
$$\psi^* = \bigwedge(\bigwedge u_j P v_j \to \bigvee x_i P y_i \bigvee E).$$

For the proof observe that the empty string of quantifiers (**) follows from (14), (18) and (20). The induction cases follow from the definitions of $\forall^*$, $\exists^*$ and (14). The definition of $\forall^*$, $\exists^*$ ensures that $\forall^*$, $\exists^*$ are $\forall$ and $\exists$ relativized to $\{x| \ [D(x)]_0 = 0\}$.

Now for the other direction, let $(S, R, o, \underline{D}_t)$ be a model of T_1 where φ^* is false. Then for some $t \in S$, $u \in D_t$ we have

(23) $\quad [(Q^* \dots) \wedge (\bigwedge u_j P v_j \to \bigvee x_i P y_i \vee E)]_t = 1 \quad$ and $\quad [D(u) \vee E]_t = o$.

Let $\overline{M} = \{x \in D_t| \ [D(x)]_t = o\}/\equiv$ (i.e., equivalence classes over $\equiv$ of (11)). Clearly $\overline{M}$ is nonempty. Let for $x/\equiv$, $y/\equiv \in \overline{M}$, $x/\equiv \overline{P} y/\equiv$ iff $[xPy]_t = o$. By (12) and (11) this definition is okay. We now have to show that $\overline{P}$ is reflexive and symmetric on $\overline{M}$. (12) shows that $\overline{P}$ is symmetrical. For the reflexivity observe that by (10) if $x/\equiv \in \overline{M}$ then $[B(x)]_t = o$ and so by (9) and (12), $[xPx]_t = o$.

So $(\overline{M}, \overline{P})$ is a model of RS. We want to show now that $(\overline{M}, \overline{P}) \vDash \varphi$. To show this we observe that $[E]_t = o$ and use (23) and the same argument we used in the proof of (**) of (Lemma 22).

Thus the proof that T_1 is undecidable is completed.

Remarks. Note that in the translation $\varphi \mapsto \varphi^*$ of RS in T_1 we have not used the ordering $<$. Also note that the model $(S, R, o, \underline{D}_t)$ that was constructed is a model of constant domains (i.e., a model CD = HPC + schema

$$\forall x(A \vee B(x) \to A \vee \forall x B(x)).$$

Thus we get that the theory of linearly ordered abelian group in the logic CD is undecidable. Also since $<$ was not in the translation, the proof presented works for the theory T_1^* of abelian groups with axioms E1-E4, S1-S5 and A1-A5. Now for the case of HPC, the undecidability of the theory of abelian groups with decidable equality (and hence $x \# y$ can be taken as $x \neq y$!) was proved in [1]. However, as remarked in [2], the theory of abelian group with decidable equality with CD as the underlying logic is decidable. We see here, in comparison, that if we formulate the theory of abelian groups with $\#$ and decidable equality (S5), then the CD theory is undecidable. To summarize

THEOREM B. *In the logic* CD, *the theory of abelian group formulated without* $\#$ *(but with decidable equality) is decidable, but when formulated with* $\#$ *is undecidable.*

2. Algebraic closed fields. The language of these theories contains $+$, o, $=$, $\#$, 0, 1. (As before, $=$ is definable from $\#$.) The axioms are taken from [4] and are the following:

Axioms for the theory T_2 of algebraically closed fields are E1-E4, S1-S4, A1-A5, and the following:

Group M.
M1: $x \cdot y = y \cdot x$,
M2: $x \cdot 1 = x$,
M3: $x(y+z) = x \cdot y + x \cdot z$,
M4: $x \# o \to \exists y(x \cdot y = 1)$,
M5: $x \# y \wedge z \# o \to xz \# yz$.
Add. S7 to Group S.
S7: $0 \# 1$.
Group AC.
AC1. $(\forall x_1, \dots, x_n) \neg\neg \exists y(y^{n+1} + \sum x_1 \cdot y^i = o)$ (this is a schema; $n \in \omega$).

THEOREM C. *The theory* T_2 *of algebraically closed fields is undecidable.*

The decidability of the theory with the more natural axiom schema.

AC2: $(\forall x_1, \dots, x_n) \exists y(y^{n+1} + \sum x_i y^i = o)$ is still open.

We now turn to prove that T_2 is undecidable; we use similar constructions as before. Let (M, P) be an infinite model of a classical reflexive and symmetric relation P. We construct a Kripke model $(S, R, o, \underline{D}_t)$ of the theory T_2, called the Kripke model associated with (M, P) as follows:

(24) Let S be the same as in (1).

(25) Let $R \subseteq S \times S$ be the reflexive and transitive closure of the following relation:

$$\{M\} \times S \cup \{(\{m, n\}, \{m\})| \ \{m, n\} \in S\} \cup \{(\{m, n\}, \infty)| \ \{m, n\} \in S, \ m \neq n\}.$$

(26) Let $o = \{M\}$.

For each $t \in S$, we must define the classical models $\underline{D}_t$. These are going to be certain rings. To describe these rings we need more definitions.

(27) Let K be an algebraically closed field. Let Y be a set of indeterminates over K. We want to define a ring $K\{Y\}$ as follows. The elements of $K\{Y\}$ are all finite sums of elements from $\bigcup_{y \in Y} K[y]$, where $K[y]$ is the ring of polynomials in y over k. So if $q \in K\{Y\}$, then q has the form $\sum q_i(y_i)$, $q_i(y_i) \in K[y_i]$. Define addition on $K\{Y\}$ as addition of sums, i.e.,

$$q + q^1 = \sum q_i(y_i) + \sum q_j^1(y_j').$$

Define multiplication on $K\{Y\}$ by extending the following multiplication table to all the elements of $K\{Y\}$ through the distributive and associative laws:

$$y \cdot y^1 = \begin{cases} y^2 & \text{if} \quad y = y^1, \\ o & \text{if} \quad y \neq y^1 \end{cases} \quad \text{for} \quad y, y^1 \in Y.$$

Let $y, y^1 \in K\{Y\}$, we can define a homomorphism $h_K(y, y^1)$: $K\{Y\} \to K\{\{y, y^1\}\}$ by letting, for $q = \sum q_i(y_i)$, $h(y, y^1)(q)$ = result of substituting o in q for all $x \in Y - \{y, y^1\}$. Let $h_K(\infty)$: $K\{Y\} \to K$ be defined by the substitution of o for all the $y \in Y$. Let $\overline{K}\{Y\}$ be the set of all elements of the form $r = q/q^1$ (i.e., rational functions) with $q, q^1 \in K\{Y\}$ and q^1 is nonzero, i.e., $h_K(\infty)(q^1) \neq o$. Extend the definitions of multiplication and addition to $\overline{K}\{Y\}$ in the natural way. We can also extend $h_K(\infty)$ and $h_K(y, y^1)$ in a natural way.

We are now in a position to define the domains and models for D_t.

(28) Proceed as follows:
(a) Let $D_0 = D_{\{m,n\}} m \neq n = D_\infty = \overline{K}\{Y\}$, where Y is a set of transcendentals of the form $Y = \{\overline{m} |\ m \in M\}$.
(b) Let $D_{\{m\}} = \overline{K(m)}\{Y - \{\overline{m}\}\}$, where $K(m)$ is the algebraic closure of $K[\overline{m}]$.

Let us define the extensions of $+$, o, $\#$, $=$, 0, 1 in $\underline{D}_t$.

(29) Let $+$ and o, 0, 1 be as defined for the ring $K\{Y\}$ in (27).

(30) To define $\#$, let r, r^1 be elements of the domain; let
(a) $[r \# r^1]_t = 1$ iff $h_K(\infty)(r) \neq h_K(\infty)(r^1)$ for $t = \infty, 0, \{m, n\}$, $m \neq n$,
(b) $[r \# r^1]_{\{m\}} = 1$ iff $h_{K(m)}(\infty)(r) \neq h_{K(m)}(\infty)(r^1)$.

(31) To define $=$ on D_t let
(a) $[r = r^1]_0 = 1$ iff r, r^1 are identical,
(b) $[r = r^1]_\infty = 1$ iff $h_K(\infty)(r) = h_K(\infty)(r^1)$,
(c) $[r = r^1]_{\{m,n\}} = 1$, for $m \neq n$, iff $h_K(\overline{m}, \overline{n})(r) = h_K(\overline{m}, \overline{n})(r^1)$,
(d) $[r = r^1]_{\{m\}} = 1$ iff $k_{K(m)}(\infty)(r) = h_{K(m)}(\infty)(r^1)$.

Thus the definition of $(S, R, o, \underline{D}_t)$ is completed.

LEMMA 32. *The Kripke model thus defined is a model of the theory T_2 of algebraically closed fields.*

Proof. We check each axiom.
(a) E1-E4 follow from the fact that h is homomorphism. S1-S2 are simple to check. For S3, notice that if $\sum g_i(\overline{n}_i) \neq \sum g_i^1(\overline{n}_i)$ then for some i, $g_i \neq g_i^1$ and so $[g_i = g_i^1]_{\{\overline{n}_i\}} = o$. Equality art is defined in such a way that it amounts to substituting 0 for some of the indeterminates, e.g., $\underline{D}_{\{m\}}$ is nothing but $\overline{K}(m)$. S4 also holds because h is a homomorphism. A1-A5 clearly hold. So do M1-M3. To check M4, note that $x \# o$ iff $h(x) \neq o$ and then $1/x$ is also present, by construction. M5 and S7 are also easy to verify. AC1 holds because $D_{\{m\}}$ is isomorphic with $K(\overline{m})$ which is algebraically closed and D_∞ is isomorphic with K. Thus Lemma 32 is proved.

To proceed with the translation we need more definitions:

(33) Let E be

$$(\forall x_1, x_2, x_3)\Big(\bigwedge_{i\neq j} x_i x_j = 0 \rightarrow \bigvee_j (x_j = o \vee x_j \# o)\Big).$$

(34) Let $B(x)$ be

$$\forall u, v\,[u \# o \vee v \# o \vee (u+v = x \wedge u\cdot v = 0 \rightarrow u = o \vee v = o \vee E] \rightarrow x \# o \vee E.$$

(35) Let $x \equiv y$ be

$$\exists z (z \# o \wedge x = yz).$$

(36) Let $D(x)$ be

$$\forall y[(y \# o \leftrightarrow x \# o) \rightarrow E \vee \exists z (y = zx)] \rightarrow B(x) \vee E.$$

(37) Let xPy be

$$(E \rightarrow x \# o \vee y \# o \vee \forall x (x = o \vee x \# o)) \wedge (x \equiv y \rightarrow E).$$

LEMMA 38. *In the above model:*
(a) $[E]_t = o$ *iff* $t = o$.
(b) $[B(x)]_0 = 0$ *iff x has the form $\overline{m}q(\overline{m})/r$ with $\overline{m} \in Y$ and $q(\overline{m})$ a polynomial in $\overline{m}$.*
(c) $[D(x)]_0 = o$ *iff* $x = \overline{m}a$, $\overline{m} \in Y$, $a \# o$.
(d) *For $\overline{m}, \overline{n} \in Y$ if $a \# o$, $b \# o$ then $[a\overline{m}Pb\overline{n}]_0 = o$ iff $M \models mPn$.*

Proof. (a) For $t = o$, let $\overline{m}_i$, $i = 1-3$ be three distinct transcendentals; (We assumed M was infinite.) Then clearly the antecedent of E holds at 0 but the consequent does not. Now assume that $t \neq 0$ and $[\bigwedge_{i\neq j} x_i \cdot x_j = 0]_t = 1$. Then for $t = \{k\}$ or $t = \infty$, clearly $[\bigvee_j x_j = 0]_t = 1$, since $\underline{D}_t$ is a field. In the case of $t = \{n, n^1\}$, $n \neq n^1$, observe that the only elements X that are not 0 are of the form $(q(\overline{n}) + q^1(\overline{n}^1))/r$. Since $[(q(\overline{n}) + q^1(\overline{n}^1))/r \# o]_t = 0$ we must have that $q = \overline{n}p$, $q^1 = n^1 p^1$, with p, p^1 polynomials in $\overline{n}, \overline{n}^1$ respectively. Now if $x_i = (\overline{n}p_i + \overline{n}^1 p_i^1)/r_i$, then

$$x_1 \circ x_2 = (\overline{n}^2 p_1 p_2 + (\overline{n}^1)^2 p_1^1 p_2^1)/r_i r_2$$

so $p_1 p_2 = 0$, $p_1^1 \cdot p_2^1 = 0$. Also,

$$p_2 \cdot p_3 = p_2^1 p_3^1 = p_1 p_3 = p_1^1 p_3^1 = 0.$$

This clearly implies that at least one of the x_i's is 0.

(b) First, if x has the form $\overline{m}q(\overline{m})/r$, then $[x \# o \vee E]_0 = 0$. Now if u, v are such that $(u \# o \vee v \# o]_0 = 0$, then

$$u = \sum \overline{n} \cdot q(\overline{n}_i)/r \quad \text{and} \quad v = \sum \overline{n}_i^1 q^1(\overline{n}_i)/r^1.$$

We want to show that

$$[u+v = x \wedge u\cdot v = o \rightarrow u = o \vee v = o \vee E]_0 = 1.$$

So assume $[u+v = x \wedge u \cdot v = o]_0 = 1$. Since $(u \cdot v = 0]_0 = 1$ we must have that $n_i \neq n_j^1$ for all i, j. But then since $[u+v = x]_0 = 1$, either $u = x$ or $v = x$, i.e., $u = o$ or $v = o$. At any $t \neq o$, $[E]_t = 1$ and so $[u = o \vee v = o \vee E]_t = 1$. For the other direction, let x be such that $[B(x)]_0 = o$. By Lemma 38 (a) we must have that $[x \# o]_0 = o$ and [consequent of $B]_0 = 1$. So x must have the form $\sum \bar{n}_i q(\bar{n}_i)/r$. If there is more than one $\bar{n}_i$ present let

$$u = \bar{n}_1 q(\bar{n}_1)/r\,, \quad v = \sum_{i \geq 2} \bar{n}_i q(\bar{n}_i)/r$$

then clearly

$$[u \# o \vee v \# o]_0 = o\,, \quad [u+v = x]_0 = 1\,, \quad [u \cdot v = o]_0 = 1$$

and

$$[u = o \vee v = o \vee E]_0 = o\,.$$

So the antecedent of B does not hold at o. Thus x must have the form $\bar{n}_1 q(\bar{n}_1)/r$.

(c) First observe that if x is of the form $\bar{m}q(\bar{m})/r$ and at o, $y \# o \leftrightarrow x \# o$, then y must be of the form $\bar{m}q_1(\bar{m})/r$. Now assume that $[D(x)]_0 = o$, then we show that $x \equiv \bar{m}$, for some $\bar{m}$. Now since $[D(x)]_0 = o$, we get that $[B(x)]_0 = o$ and therefore $x = \bar{m}^{-i}q(\bar{m})/r$ with $q(\bar{m}) \# o$ and $i \geq 1$. If $i = 1$, we are finished. Otherwise let $y = \bar{m}^{i-1}q/r$. Clearly $y \# o \leftrightarrow x \# o$, so we must have that either $x \equiv y$, which is impossible, or that for some Z, $\bar{m}^{i-1}q/r = Z\bar{m}q/r$, which again is impossible.

Now assume that $x \equiv \bar{m}$. Then certainly $[E \vee B(x)]_0 = o$. To show that the antecedent of $D(\bar{m})$ holds at o, assume $[y \# o \leftrightarrow x \# o]_0 = 1$. Then y must be of the form $\bar{m}q(\bar{m})/r$ and therefore $\exists z(y = xz)$.

(d) First assume that $M \models mPn$. We distinguish two cases.

(1) $m = n$, then $[\bar{m}aP\bar{m}b]_0 = 0$ since $[\bar{m}\bar{a} \equiv \bar{m}b]_0 = 1$.

(2) If $m \neq n$, then we have $[E]_{\{m,n\}} = 1$ and $[\bar{m}a \# o \vee \bar{m}b \# o]_{\{m,n\}} = 0$, and $[\forall x(x = o \vee x \# o)]_{\{m,n\}} = 0$. So again, $[\bar{m}aP\bar{n}b]_0 = 0$.

Now assume that $[\bar{m}aP\bar{n}b]_0 = 0$. If $[\bar{m}a \equiv \bar{n}b \to E]_0 = 0$, then we must have $[\bar{m}a \equiv \bar{n}b]_0 = 1$, which can hold only if $m = n$ and so mPn. If $[E \to \bar{m}a \# o \vee \vee \bar{n}b \# o]_0 = o$, then for some $t \neq o$, $(\bar{m}a \# o]_t = 0$, $[\bar{n}b \# o]_t = 0$, $[\forall x(x = o \vee \vee x \# o)]_t = 0$. Since $[\forall x(x = o \vee x \# o)]_t = o$, $t \neq \infty$, and $t \neq \{n^1\}$. So $t = \{m^1, n^1\}$, $m^1 \neq n^1$. But then $[\bar{m}a \# o]_t = 0$ implies $m \in \{m^1, n^1\}$ and similarly $n \in \{m^1, n^1\}$ and so mPn must hold in M. Thus Lemma 38 is proved.

(39) Now observe that from Lemma 38 (d) it follows that if $x \equiv y$, $x^1 \equiv y^1$ then xPy iff x^1Py^1. Thus if $\bar{M} = \{x | \; [D(x)]_0 = 0\}/\equiv$ and $\bar{P}$ is defined by $x/\equiv \bar{P}y/\equiv$ iff $[xPy]_0 = 0$, we get that (M, P) is isomorphic to $(\bar{M}, \bar{P})$.

(40) As we did in (21) (for the theory T_1 of linearly ordered abelian groups), we define $\forall^*$ and $\exists^*$ by

$$(\forall^* y)\varphi = \forall y(D(y)) \vee \varphi)\,,$$
$$(\exists^* y\varphi) = \exists y((D(y) \to E) \wedge \varphi)\,.$$

The translation $\varphi \mapsto \varphi^*$ is defined exactly as in (21), i.e., if φ is a formula of RS of the form $(Q\ldots) \wedge (\bigwedge x_i P y_i \to \bigvee u_j P v_j)$ then φ^* is the following formula of T_2:

$$\forall u[(Q^*\ldots) \wedge (\bigwedge u_j P v_j \to \bigvee x_i P v_i \vee E) \to E \vee D(u)]$$

where P, D, E are those defined in this section (§ 2). We have:

LEMMA 41. *$T_2 \vdash \varphi^*$ iff* $\mathrm{RS} \vdash \neg\varphi$.

Proof. First assume that $\mathrm{RS} \vdash \neg\varphi$; so φ has a model (M, P). We may assume that M is infinite because RS contains no equality. Construct the model $(S, R, o, \underline{D}_t)$ associated with (M, P). Observe, by following the lines of argument of the proof of (22) that $[\varphi^*]_0 = o$. The proof of (22) used (14), (18) and (20). Our proof now will use (38)-(39), which were defined for the same purpose.

For the other direction, let (S, R, o, D_t) be a model in which φ^* is false. Obtain a model of φ by following the line of the proof following (23). The reflexivity and symmetry of $\bar{P}$ follows from (37). Thus Theorem C is proved.

We turn now to the theory T_3 of real closed fields. The language of T_3 contains the symbols $+$, $'$, $=$, $\#$, 0, 1 and $>$. The axioms are the following:

Axioms for the theoty T_3 of real closed fields are E1-E4, S1-S4, A1-A5, M1-M5, S7 and Groups P and RC.

P1: $x \# o \to x > 0 \vee (-x) > 0$,
P2: $x > 0 \wedge y > 0 \to x + y > 0$,
P3: $x > 0 \wedge y > 0 \to x \cdot y > 0$,
P4: $\neg(0 > 0)$,
RC1: $x \# o \to \neg\neg\exists y(x = y^2 \vee -x = y^2)$,
RC2: $(\forall x_0, \ldots, x_{2n})\neg\neg\exists y(y^{2n+1} + \sum x_i y^i = o)$.

We do not know whether T_3 is decidable or not. Neither do we know whether the theory with RC3 and RC4 is undecidable. Where

RC3: $x \# o \to \exists y(x = y^2 \vee -x = y^2)$,
RC4: $(\forall x_0, \ldots, x_{2n})\exists y(y^{2n+1} + \sum x_i y^i = 0)$.

3. Linear order. We begin with the theory T_4 of dense linear ordering. This theory was first proved undecidable by Snoryński [6] by interpreting in it the intuitionistic theory of one monadic letter. In [1] we show that the theory of decidable linear ordering is undecidable (here $\#$ can be defined from $<$).

The language of T_4 contains $<$, $\#$, $=$, and the following axioms:
E1-E4, S1-S5, O1, O3, O5, O6, S6 and O7, O8, O9 below:

O7: $\exists y(x < y)$,
O8: $\exists y(y < x)$,
O9: $\exists y(x < z \to x < y \wedge y < z)$.

THEOREM D. *T_4 is undecidable.*

We sketch the proof; we use the same method we used before.

Let (M, P) be a countably infinite model of a reflexive and symmetric relation. We can assume that M is the set of rational numbers. We construct a Kripke model $(S, R, o, \underline{D}_t)$ called the Kripke model associated with (M, P) as follows:

(42) $S = \{M\} \cup \{\infty\} \cup \{\{x, y\} | \; xPy\}$, let $o = \{M\}$.

(43) $R = \{M\} \times S \cup S \times \{\infty\} \cup \{(t, t) | \; t \in S\}$.

Let K be the rational numbers. Let $D_t = K \times M$. We have to define $<$, $\#$, $=$ on D_t, $t \in S$. We proceed as follows:

(44) $[(r, m) = (r^1, m^1)]_t = 1$ iff $r = r^1$, $m = m^1$.

(45) $[(r, m) < (r^1, m^1)]_0 = 1$ iff $m < m^1$.

(46) $[(r, m) < (r^1, m^1)] = 1$ iff $m < m^1$ or if $m = m^1$ then $r < r^1$.

(47) $[(r, m) < (r^1, m^1)]_{\{n, n^1\}} = 1$ iff $m < m^1$ or if $m = m^1 \in \{n, n^1\}$ then $r < r^1$.

Let $x \# y$ mean $x < y \vee y < x$.

LEMMA 48. *All axioms of T_4 hold in the model.*

LEMMA 49. *$[x \# y]_0 = o$ is an equivalence relation in the model.*

Proof. Transitivity follows from S4.

LEMMA 50. *Let E be the sentence $\exists x \forall y(x = y \vee x \# y)$, then $[E]_t = o$ iff $t = o$.*

LEMMA 51. *If xPy is defined as $E \to (\forall z(z = x \vee z \# x) \leftrightarrow \forall z(z = y \vee z \# y))$ then $[(r, m)P(r^1, m^1)]_0 = o$ iff mPm^1.*

LEMMA 52. *The relation $x \equiv y$ defined below is an equivalence relation on D_0 and furthermore, $x \equiv x^1 \wedge y \equiv y^1 \wedge xPy \to x^1Py^1$, where $x \equiv y$ is $\forall z(z \# x \leftrightarrow z \# y)$. In fact, the set $\overline{M}$ of equivalence classes with the relation $\overline{P}$ (induced by $[xPy]_0 = o$) is isomorphic to (M, P).*

Now let φ be a sentence of RS in the form $(Q...) \wedge (\bigwedge x_i P y_i \to \bigvee u_j P v_j)$. Let φ^* be

$$(Q...) \wedge (\bigwedge u_j P v_j \to \bigvee x_i P y_i \vee E) \to E.$$

We claim that

$$T_4 \vdash \varphi^* \quad \text{iff} \quad \mathrm{RS} \vdash \neg \varphi.$$

Remark. This translation and construction shows that the apartness relation itself (E1-E4, S1-S5) is undecidable (Smoryński [6]). Simply take the same constructions for a language without $<$.

References

[1] D. M. Gabbay, *Sufficient conditions for the undecidability of intuitionistic theories*, J. Symbolic Logic 37 (1972), pp. 375–384.

[2] — *The undecidability of the intuitionistic theories of algebraic and real closed fields* 38 (1973), pp. 86–92.

[3] D. M. Gabbay, *Decidability of some intuitionistic predicate theories*, ibid. 37 (1972), pp. 579–588.

[4] A. Heyting, *Intuitionism*, North Holland 1956.

[5] S. Kripke, *Semantical Analysis for Intuitionistic Logic* 1, *Formal Systems and Recursive Functions*, North Holland 1965, pp. 92–131.

[6] C. Smoryński, *Some recent results on elementary intuitionistic theories*, J. Symbolic Logic 38 (1973), pp. 102–135.

BAR-ILAN UNIVERSITY
Ramat-Gan, Israel

Accepté par la Rédaction 17. 3. 1975