

Table des matières du tome LXXXII, fascicule 3

	Pages
K. Hauschild, Rekursive Unentscheidbarkeit der Theorie der pythagoräischen Körper	191-197
H. Barendregt, Combinatory logic and the ω -rule	199-215
C. E. M. Yates, Prioric games and minimal degrees below $0^{(1)}$	217-237
J. Bělý and L. Bukovský, On expansions of β -models	239-244
C. P. Когаловский, Некоторые простые следствия аксиомы конструктивности	245-267
R. Vaught, Invariant sets in topology and logic	269-293

Rekursive Unentscheidbarkeit der Theorie
der pythagoräischen Körper

von

Kurt Hauschild* (Berlin)

Abstract. By interpreting the theory of graphs within the theory of pythagorean fields the latter is shown to be undecidable.

Es sei P die Klasse der formal reellen pythagoräischen Körper. Wir zeigen, daß sich jeder abzählbare Graph $\langle G, R \rangle$ ($\text{card } G \leq \aleph_0$, R binäre irreflexiv-symmetrische Relation in G) in ein $K \in P$ auf kanonisch definierbare Weise einbetten läßt. Daraus folgt die Universalität von P bezüglich Modellinterpretierbarkeit, d.h. jede abzählbare Struktur ist in einem $K \in P$ definierbar (vgl. [1]); speziell gilt dies für die arithmetische Struktur $\langle \omega, +, \cdot \rangle$. Damit ist die Theorie $\text{Th}K$ der 1. Stufe jeder Klasse $K \supset P$ rekursiv unentscheidbar, und, falls $\text{Th}K$ rekursiv axiomatisierbar ist, vom höchsten rekursiv aufzählbaren Grad. Speziell gilt dies auch für die Klasse der geordneten pythagoräischen Körper, die in der Geometrie eine besondere Rolle spielen. P kann in obigen Bemerkungen durch die engere Klasse der archimedisch anordnungsfähigen Körper ersetzt werden mit weiteren einschränkenden Bedingungen.

Die Beweismethode besteht darin, die Punkte des vorgegebenen Graphen als Transzendenzbasis des Körpers zu wählen und die Kantenrelation durch Radikaladjunktionen zu charakterisieren. Damit wird ein Verfahren gegeben, um das Entscheidungsproblem für unendliche algebraische Erweiterungen von P zu behandeln (vgl. [2]).

Die Rangeinführung (§ 1) ist algebraisch mit der Einführung von Bewertungen gleichwertig (vgl. [3], S. 28 ff.). Die nicht ausgeführten Beweisdetails können ohne Schwierigkeiten nachvollzogen werden.

Die Übertragung der Ergebnisse auf den euklidischen Fall wird am Schluß des Artikels angedeutet.

* Die Priorität an den Ergebnissen dieser Arbeit teile ich mit W. Rautenberg; siehe auch [1].

Les FUNDAMENTA MATHEMATICAE publient, en langues des congrès internationaux, des travaux consacrés à la *Théorie des Ensembles, Topologie, Fondements de Mathématiques, Fonctions Réelles, Algèbre Abstraite*. Ce volume paraît en 4 fascicules

Adresse de la Rédaction et de l'Échange:

FUNDAMENTA MATHEMATICAE, Śniadeckich 8, 00-950 Warszawa (Pologne)

Tous les volumes sont à obtenir par l'intermédiaire de

ARS POLONA-RUCH, Krakowskie Przedmieście 7, 00-068 Warszawa (Pologne)

Correspondence concerning editorial work and manuscripts should be addressed to: FUNDAMENTA MATHEMATICAE, Śniadeckich 8, 00-950 Warszawa (Poland)

Correspondence concerning exchange should be addressed to:

INSTITUTE OF MATHEMATICS, POLISH ACADEMY OF SCIENCES, Exchange Śniadeckich 8, 00-950 Warszawa (Poland)

The Fundamenta Mathematicae are available at your bookseller or at

ARS POLONA-RUCH, Krakowskie Przedmieście 7, 00-068 Warszawa (Poland)

§ 1. Es sei P der Körper der rationalen Zahlen und G ein über P irreduzibles transzendentes endliches oder abzählbares System von Elementen. Weiter sei $W = W_G$ der kleinste Körper mit den Eigenschaften

- (1) $P(G) \subseteq W$;
- (2) für jedes $f \in W$ und jede Primzahl $p \neq 2$ existiert ein $g \in W$ mit $g^p = f$;
- (3) für $f, g \in W$ ist $\sqrt{f^2 + g^2} \in W$.

W ist (archimedisch) anordnungsfähig. Für eine ungerade natürliche Zahl n und für $f \in W$ hat damit der Term $\sqrt[n]{f}$ — oder in anderer Bezeichnung $f^{1/n}$ — einen eindeutig bestimmten Sinn. Faßt man die Elemente von W als algebraische Funktionen in den Elementen von G als reellen Variablen auf, so kann man sagen:

- (4) die Funktionen aus W haben an allen definierten Stellen reelle Werte.

Achtung. Die Funktionen $f = \sqrt[3]{y+2}$ und $g = \sqrt{x+2}$ sind nur dann dieselben, wenn $x = y$ (in G).

Ist $f \in W, x \in G$, dann bedeutet die Redeweise f sei für $x = 0$ definiert, daß ein $g \in W_{G \setminus \{x\}}$ mit $g = f|_{x=0}$ existiert; Bezeichnung $g = f_x$. Eine rationale Zahl r heißt Rang von f bezüglich x (in Zeichen $r = Rg_x f$), wenn $(f x^{-r})_x$ definiert und von Null verschieden ist. $Rg_x f$ ist für $f \neq 0$ eindeutig bestimmt. Wir zeigen als nächstes, daß $Rg_x f$ für alle $f \in W (f \neq 0)$ und $x \in G$ existiert.

Es sei ein $x \in G$ gegeben. Man denke sich die Elemente von W als reelle Funktionen in der ausgezeichneten Variablen x , die übrigen Variablen werden vorübergehend als reelle transzendente Konstanten angesehen. Damit ergibt sich die Rangexistenz unmittelbar aus dem folgenden

LEMMA 1. Jedes $f \in W \setminus \{0\}$ ist als Funktion von x in einer gewissen Umgebung von 0 als eine unendliche Reihe

$$(5) \quad L_x f = x^{m/k} \sum_{i=0}^{\infty} a_i x^{i/k} \quad (a_0 \neq 0, m \in I, k \in 2\omega + 1)$$

darstellbar, wobei die a_i alle in einem endlich erzeugten Körper $K \subseteq W$ über $P(G')$ ($G' \subseteq G, x \notin G'$) liegen.

Beweis. Durch Reihenentwicklung ist für $f \in P(G)$ die Behauptung klar ($k = 1$). Es genügt, Induktion über Summe, Produkt und p -te Wurzel zu führen, da sich jedes $f \in W$ mittels dieser Operationen aus $P(G)$ erzeugen läßt. Aus Darstellungen (5) für f, g ergeben sich solche für $f+g$ bzw fg (die Reihen für f und g sind vorher mit einheitlichem k zu

schreiben). Nach bekannten Regeln der Reihenentwicklung folgt mit einer Reihe (5) für f :

$$L_x f^{1/p} = (L_x f)^{1/p} = x^{m/pk} \sum_{i=0}^{\infty} b_i x^{i/k}$$

mit $b_0 = a_0^{1/p}, b_1 = \frac{1}{p} a_1 a_0^{(1-p)/p}, \dots$. Wenn die a_i alle in einem Körper K liegen, so liegen die b_i in $K(a_0^{1/p})$. Da in W nur Quadratwurzeln aus Summen von Quadraten zu adjungieren sind, bleibt k im Induktionsschritt ungerade. Aus demselben Grund liegen die Koeffizienten a_i alle in W . Q.E.D.

(5) möge im folgenden die Laurentreihe von f nach x mit den Laurentkoeffizienten a_i genannt werden. Der Quotient m/k (der Rang von f), sowie die Teilfolge der von Null verschiedenen Laurentkoeffizienten sind für gegebenes $f \in W$ eindeutig bestimmt. Im folgenden verwenden wir ohne besonderen Hinweis häufig die folgenden leicht beweisbaren Formeln

$$(6) \quad Rg_x(f+g) \geq \min\{Rg_x f, Rg_x g\};$$

$$(7) \quad Rg_x f g = Rg_x f + Rg_x g;$$

$$(8) \quad Rg_x f^r = r Rg_x f \quad (r \in P).$$

Der Fall $\min\{Rg_x f, Rg_x g\} < Rg_x(f+g)$ kann höchstens im Falle $Rg_x f = Rg_x g$ eintreten. Mit (4) folgt ferner leicht

$$(9) \quad Rg_x(f^2 + g^2) = \min\{Rg_x f^2, Rg_x g^2\} = 2 \min\{Rg_x f, Rg_x g\}.$$

Es sei E das System der endlich erzeugten Körper $K \subseteq W$, genauer, das kleinste System F von Körpern mit den folgenden Eigenschaften:

(I) $P(G') \in F$ falls $G' \subseteq G$;

(II) Ist $K \in F, f \in K$, so ist $K(\sqrt[p]{f}) \in F$, wobei, im Falle $p = 2, f$ eine Summe von zwei Quadraten von Elementen aus K ist. Jedes $K \in E$ wird durch eine Körperkette $(K_i)_{i < n}$ mit $K_{n-1} = K$ und $K_{i+1} = K_i(\sqrt[p]{f_i})$, $f_i \in K_i, \sqrt[p]{f_i} \notin K_i, K_0 = P(G'), G' \subseteq G$ erzeugt, ist also endliche algebraische Erweiterung von K_0 . Den Grad von K über K_0 nennen wir kurz den Grad von K .

Die Funktionen aus W lassen sich durch Terme darstellen, die aus 0, 1 und Zeichen für die Elemente aus G mit Hilfe von +, ·, − (minus), − (Bruchstrich) und $\sqrt[p]{}$ ($n \in N$) zusammengesetzt sind. Zwei Terme stellen genau dann dieselbe Funktion dar, wenn sie durch Umformungen auseinander hervorgehen, die den Rechengesetzen für die Grundrechen-

arten und denen für die Radizierung entsprechen (Beweis etwa induktiv über die Erzeugungsprinzipien für W).

Es sei $H \subseteq G$, $f \in W$ und $t = t_1 + \dots + t_n$ ($n > 1$) eine Termdarstellung für f . t möge H -gut heißen, wenn für genau eines der t_i ($i = 1, \dots, n$) $\sum_{x \in H} \text{Rg}_x t_i$ minimal ist (gemeint sind natürlich die Ränge der entsprechenden Funktion). Z. B. ist $u^5 + v^5$ nicht $\{u, v\}$ -gut; dagegen ist $1 + f^5$ (in geeigneter Darstellung) $\{u, v\}$ -gut für jedes f mit $\text{Rg}_x f \neq 0$ für ein $x \notin \{u, v\}$ (im Falle $\sum_{x \in H} \text{Rg}_x f = 0$ ist zu einer Transzendenzbasis überzugehen, in der die Elemente von $G \setminus \{u, v\}$ durch geeignete Potenzen ihrer selbst ersetzt sind). Offenbar gilt:

(10) Sind $t = t_1 + \dots + t_n$ und $s = s_1 + \dots + s_m$ H -gut, so ist $\sum_{\substack{i \leq n \\ j \leq m}} t_i s_j$ H -gut.

(11) Ist $t = t_1 \cdot t' + \dots + t_n \cdot t'$ H -gut, so ist $t_1 + \dots + t_n$ H -gut.

Unter Verwendung von (10) und (11) beweist man, daß die Wurzelumformungen $t_1 \sqrt[p]{t_2} \Leftrightarrow \sqrt[p]{t_1^p \cdot t_2}$ bzw. $\sqrt[p]{t_1} \cdot \sqrt[p]{t_2} \Leftrightarrow \sqrt[p]{t_1 \cdot t_2^p}$ die Eigenschaft der Radikanden, H -gut zu sein, invariant lassen.

LEMMA 2. Ist $K \subseteq E$, $H \subseteq G$, $\sqrt[p]{g} \notin P(H)$ und $g \in P(H)$, und sind alle p -ten Wurzeln in einer K darstellenden Erzeugungskette von der Gestalt $\sqrt[p]{1+f^5}$, wo $\text{Rg}_x f \neq 0$ für ein $x \notin H$, so ist $\sqrt[p]{g} \notin K$.

Beweis (Skizze). Andernfalls besitzt $\sqrt[p]{g}$ eine Termdarstellung, in der alle Radikanden unter p -ten Wurzeln H -gut sind (auf Grund des Gradsatzes muß mindestens eine p -te Wurzel vorkommen); der ggf. nötige Wechsel der Transzendenzbasis kann in simultaner Weise erfolgen. Nach dem Vorangegangenen überlegt man sich leicht, daß dann auch (jede bezüglich der Länge minimale Darstellung von) g H -gut sein müßte. Das ist aber offenbar nicht der Fall.

Schließlich benötigen wir

LEMMA 3 (Kummer). Es sei K ein formal reeller Körper, $f, g \in K$ und p eine Primzahl. Dann ist $K(\sqrt[p]{f}) = K(\sqrt[p]{g})$ genau dann, wenn $f = a^p g^m$ mit $a \in K$ und $1 \leq m < p$.

§ 2. Wir konstruieren nun den Einbettungskörper $K = K_G$ für einen Graphen $\langle G, R \rangle$ mit $\text{card } G \leq \aleph_0$. Die Elemente von G erscheinen in K als gewisse definierbare Kongruenzklassen bezüglich einer definierbaren binären Relation R' in K , so daß das R' -Redukt von K , faktorisiert nach der genannten Kongruenz, eine zu $\langle G, R \rangle$ isomorphe Struktur ist.

Es sei K der kleinste Körper, der den folgenden Bedingungen genügt:

(a) $P(G) \subseteq K \subseteq W$;

(b) K ist pythagoräisch;

(c) Ist $f \in K$ und $\xi \text{Rg}_x f \equiv 0 \pmod{3}$ für alle $x \in G$, so ist $\sqrt[3]{f} \in K$;

(d) Ist $\langle x, y \rangle \in R$, $f, g \in K$ und $K(\sqrt[3]{f}) = K(\sqrt[3]{x})$, $K(\sqrt[3]{g}) = K(\sqrt[3]{y})$, so ist $\sqrt[3]{f^5 + g^5} \in K$;

(e) Ist $n \not\equiv 0 \pmod{2, 3, 5}$ und $f \in K$, so ist $\sqrt[n]{f} \in K$.

Dabei bezeichnet, für eine rationale Zahl r , ξr den Zähler von r in gekürzter Darstellung ($\xi \neq 0$), νr den Nenner von r ($\nu r > 0$, $\nu \neq 0$).

LEMMA 4. $\nu \text{Rg}_x f \not\equiv 0 \pmod{p}$ für $p = 2, 3$, $f \in K$, $x \in G$.

Beweis. Die Behauptung ergibt sich leicht aus (6)-(8), (a)-(e) und der Minimalitätseigenschaft von K . Q.E.D.

Für rationale Zahlen r, s , deren Nenner nicht durch 3 teilbar sind, sei $r \equiv s \pmod{3}$, wenn $\xi r \cdot \nu s \equiv \xi s \cdot \nu r \pmod{3}$. Es gelten die üblichen Rechengesetze. Es sei

$$\bar{f} =: \{x \in G : \text{Rg}_x f \not\equiv 0 \pmod{3}\}.$$

Aus der Bedingung (c) ergibt sich

$$\bar{f} = \emptyset \Leftrightarrow \sqrt[3]{f} \in K \quad \text{für alle } f \in K,$$

folglich ist die Relation $\bar{f} = \emptyset$ elementar charakterisierbar. Die Elemente $f \in K$, für die \bar{f} Einermenge ist, heißen *Atome*. Für Elemente $f, g \in K$ bedeute $f \equiv g$, daß $K(\sqrt[3]{f}) = K(\sqrt[3]{g})$. Die Relation \equiv ist aufgrund von Lemma 3 elementar definierbar.

LEMMA 5. Ist $f \equiv g$, so ist $\bar{f} = \bar{g}$. Ist f Atom und $\bar{f} = \bar{g}$, so ist $f \equiv g$.

Beweis. Aus $f \equiv g$ folgt, nach Lemma 3, $f = h^3 g^i$ ($i \in \{1, 2\}$) $h \in K$. Folglich ist $\text{Rg}_x f = 3 \text{Rg}_x h + i \text{Rg}_x g$, also $\text{Rg}_x f \equiv 0 \pmod{3}$ genau dann, wenn $\text{Rg}_x g \equiv 0 \pmod{3}$ für alle $x \in G$. Daher ist $\bar{f} = \bar{g}$. Sei $\bar{f} = \{x\}$, $f = x^r f'$ und damit $g = x^s g'$ mit $r, s \not\equiv 0 \pmod{3}$ und $\bar{f}', \bar{g}' = \emptyset$. Folglich ist, nach Lemma 4, $\sqrt[3]{f'} \in K$, also $f = x^r$, $g = x^s$. Ist $r \equiv s \pmod{3}$, so ist $x^r/x^s = x^t$ mit $t \equiv 0 \pmod{3}$, also $\sqrt[3]{x^t} \in K$ (Bedingungen (c) und (e)) und damit, nach Lemma 3, $x^r \equiv x^s$. Ist $r \not\equiv s \pmod{3}$, dann ist $r \equiv 2s \pmod{3}$, also $x^r = x^{2s} = x^s$. Q.E.D.

LEMMA 6. f Atom $\Leftrightarrow (\forall g, h \in K)(\bar{g}, \bar{h} \neq \emptyset \ \& \ f \equiv gh \rightarrow \overline{g^2 + h^2} \neq \emptyset)$.

Beweis. Sei f Atom, $\bar{f} = \{x\}$, wobei $\text{Rg}_x f \not\equiv 0 \pmod{3}$. Im Falle $\bar{g} = \bar{h} = \{x\}$ ist $\text{Rg}_x (g^2 + h^2) = 2 \min\{\text{Rg}_x g, \text{Rg}_x h\} \not\equiv 0 \pmod{3}$ (siehe (9)), also $\overline{g^2 + h^2} \neq \emptyset$. Andernfalls existiert ein $y \neq x$, $\text{Rg}_y g \not\equiv 0 \pmod{3}$. Wäre $\text{Rg}_y h \equiv 0 \pmod{3}$, so wäre $\text{Rg}_y gh \not\equiv 0 \pmod{3}$, wegen $f \equiv gh$ nach Lemma 5 also auch $\text{Rg}_y f \equiv 0 \pmod{3}$ im Widerspruch zur Voraussetzung. Also ist auch $\text{Rg}_y h \not\equiv 0 \pmod{3}$ und damit $\text{Rg}_y (f^2 + g^2) \not\equiv 0 \pmod{3}$, d.h. $y \in \overline{f^2 + g^2}$.

f sei kein Atom. Wir wählen zunächst ein $f' \equiv f$ mit $\text{Rg}_x f' \geq 0$ für alle $x \in G$. Wegen $\bar{f} = \bar{f}'$ ist $f' = x_0^{r_0} \dots x_n^{r_n} f''$ mit $n \geq 1$, $r_i \not\equiv 0 \pmod{3}$, $r_i > 0$, $\text{Rg}_x f'' \equiv 0 \pmod{3}$ ($x \in G$). Man setze $g = x_0^{r_0}$, $h = x_1^{r_1} \dots x_n^{r_n}$. Dann

ist $\bar{g}, \bar{h} \neq \emptyset$, $f \equiv gh$, aber offenbar $\text{Rg}_z(g^2+h^2) = 0$ für alle $z \in G$, d.h. $g^2+h^2 = \emptyset$. Q.E.D.

Die Elemente $x \in G$ werden in K durch die ihnen zugeordneten Klassen $\{f \in K: f \equiv x\}$ repräsentiert. Diese Klassen sind aufgrund von Lemma 6 elementar definierbar. Entscheidend für die elementare Charakterisierung der Relation R ist das folgende

LEMMA 7. Ist $u, v \in G$, $\langle u, v \rangle \notin R$, so ist $\sqrt[5]{u^5+v^5} \notin K$.

Beweis. Es genügt zu zeigen, daß $\sqrt[5]{u^5+v^5}$ in keinem Teilkörper $F \in E$ von K liegt. Nun haben die Radikale 5-ten Grades in der F erzeugenden Körperkette die Gestalt $\sqrt[5]{f^5+g^5}$ mit $f \equiv x$, $g \equiv y$ für gewisse $x, y \in G$, $\langle x, y \rangle \in R$. Diese Radikale können gleichwertig durch $\sqrt[5]{1+h^5}$ mit $h = f/g$ ersetzt werden. Wegen $\langle x, y \rangle \in R$, $\langle u, v \rangle \notin R$ ist o.B.d.A. $x \neq u$, v . Ferner ist $\text{Rg}_x f \neq 0$. Daraus folgt die Behauptung unmittelbar aus Lemma 2. Q.E.D.

Wegen Lemma 7 ist die Relation R' , definiert durch

$$R'fg \Leftrightarrow f, g \text{ Atome} \ \& \ (\forall f_1, g_1 \in K)[f_1 \equiv f \ \& \ g_1 \equiv g \rightarrow \exists h (h^5 = f_1^5 + g_1^5)]$$

faktorisiert nach \equiv auf der Menge der Atome isomorph zu R . Die Gleichheit von $\langle G, R \rangle$ wird mit Hilfe von Lemma 5 elementar definiert. Somit ist $\langle G, R \rangle$ auf kanonische Weise elementar in K definiert.

Dieser Beweis läßt sich im wesentlichen auf den euklidischen Fall übertragen. Wir geben eine Skizze. Anstelle von W wird ein kleinster über $P(G)$ euklidischer Körper betrachtet, der der Bedingung (2) genügt. Die Rangtheorie wird auf diesen Körper ausgedehnt. Dabei geht die Allgemeingültigkeit der Beziehung (9) verloren. Diese Beziehung wird nur im Beweis von Lemma 6 ausgenutzt (Charakterisierung der Atome). An die Stelle von Lemma 6 tritt

LEMMA 6'.

$$f \text{ Atom} \Leftrightarrow (\forall g, h \in K)[\bar{g}, \bar{h} \neq \emptyset \ \& \ f \equiv gh \rightarrow (f+g \neq \emptyset \vee f-g \neq \emptyset)].$$

Lemma 6' wird bewiesen mit Hilfe der leicht zu verifizierenden Beziehung

$$(9') \quad \text{Für } f, g \neq 0, 0 \text{ ist } \text{Rg}_x(f+g) = \min\{\text{Rg}_x f, \text{Rg}_x g\} \text{ oder } \text{Rg}_x(f-g) = \min\{\text{Rg}_x f, \text{Rg}_x g\}.$$

Abschließend folgende Bemerkungen. Es dürfte keine besonderen Schwierigkeiten bereiten, den Beweis auf den Fall auszudehnen, daß die Bedingung (e) in der Konstruktion von K durch

(e') Jedes Polynom n -ten Grades ($n \not\equiv 0 \pmod{2, 3, 5}$) hat eine Nullstelle

ersetzt wird. Dies könnte durch Erweiterung der Rangtheorie geschehen. Eine andere Aufgabe besteht darin, anstelle zweier ungerader Primzahlen in obigem Beweis nur eine zu verwenden. Damit könnte sehr wahrscheinlich ein altes Problem (Tarski, Mostowski) endgültig gelöst werden: zu zeigen, daß ein Teilsystem des Tarskischen Schemas für die Arithmetik der reellen Zahlen, welches durch Weglassen eines der Axiome über die Existenz von Nullstellen von Polynomen ungeraden Grades entsteht, eine rekursiv unentscheidbare Theorie darstellt.

Literatur

- [1] W. Rautenberg, *Lecture Notes on Decidability*, Warszawa 1973.
- [2] J. Robinson, *The decision problem for fields, in Model Theory*, 1965.
- [3] Van der Waerden, *Moderne Algebra I*.

Reçu par la Rédaction le 16. 8. 1973.