

THE UNDECIDABILITY OF ALGEBRAIC RINGS AND FIELDS

JULIA ROBINSON

1. **Introduction.** Our main result is the solution of the decision problem for algebraic fields of finite degree over the rationals. We will give a definition of the natural numbers within the arithmetic of any such field, thereby showing that the field is undecidable.

By the *arithmetic* of a field F , we mean the mathematical theory whose statements are constructed from the logical symbols \wedge (and), \vee (or), \neg (not), \rightarrow (if \dots then \dots), \leftrightarrow (if and only if), \wedge (for every), \vee (there exists), and $=$ (equals); the mathematical symbols $+$ and \cdot ; and variables whose range is F . Similarly, the arithmetic of a ring R or of the natural numbers N is defined by restricting the variables either to R or to N .

An *arithmetical definition* of an n -ary relation ρ within a particular mathematical theory is an equivalence with $\rho(u_1, \dots, u_n)$ on the left and with an expression of the theory, having u_1, \dots, u_n as its only free variables, on the right.

We say a mathematical theory is *decidable* if there is an effective method of determining the validity of each statement of the theory. If there is no such method, the theory is *undecidable*. It is clear that if there is a mechanical way of transforming each statement of an undecidable theory into an equivalent statement of another theory, the second theory is also undecidable. This principle, together with the fact that the arithmetic of natural numbers is undecidable, enables us to solve the decision problem for fields of finite degree over the rationals.¹

The relation $n \in N$ can be defined arithmetically in the ring I of rational integers as follows:

$$n \in N \leftrightarrow \bigvee_{x,y,z,w} n = x^2 + y^2 + z^2 + w^2.$$

Hence it is possible to transform routinely any statement of the arithmetic of N into an equivalent statement of the arithmetic of I .

Presented to the Society, January 22, 1959; received by the editors January 29, 1959.

¹ For a complete account of much more powerful arguments to deduce the undecidability of one theory from that of another, see Tarski, Mostowski, and Robinson [9]. This monograph also contains a proof of the fundamental theorem that the arithmetic of the natural numbers is undecidable. This was first proved by Rosser extending the work of Church and Gödel.

Applying the principle stated above, we see that the ring of rational integers is undecidable. In §2, we give a definition of the natural numbers within the arithmetic of the ring \mathbf{R} of the algebraic integers of a field of finite degree over the rationals. As before, it follows that \mathbf{R} is undecidable.²

Let \mathbf{R} be any integral domain and \mathbf{F} its quotient field. Every statement of the arithmetic of \mathbf{F} can be transformed into an equivalent statement of the arithmetic of \mathbf{R} by replacing each variable whose range is \mathbf{F} by the ratio of two variables with range \mathbf{R} and adjoining the condition that the denominator is not 0, then clearing the resulting equations of fractions. The undecidability of \mathbf{F} thus implies the undecidability of \mathbf{R} . It is not known whether the converse always holds. If \mathbf{R} can be defined arithmetically in \mathbf{F} , we can transform mechanically any sentence of the arithmetic of \mathbf{R} into an equivalent sentence of the arithmetic of \mathbf{F} . Hence in this case the converse holds.

The first field shown to be undecidable was the rational field [6]. This was done by using the theory of ternary quadratic forms to define the ring of integers arithmetically in the rational field, and thus reducing the decision problem for the rational field to that of the ring of integers, which was known to be undecidable. In §3, we apply a similar method to fields of finite degree over the rationals. We no longer obtain an arithmetical definition of the rational integers but instead an arithmetical definition of the algebraic integers of the field. Combining the results of §§2 and 3, we see that the natural numbers can be defined arithmetically in any field of finite degree over the rationals, and therefore such a field is undecidable.

2. The definability of the natural numbers in \mathbf{R} . In this section, we will define arithmetically the relation $n \in \mathbf{N}$, i.e. n is a natural number, in the ring \mathbf{R} of the algebraic integers of a field of finite degree over the rationals.

LEMMA 1. *There are only finitely many numbers a of \mathbf{R} such that*

$$a + 1 \mid f \wedge \dots \wedge a + l \mid f$$

where l is the degree of \mathbf{R} and f is any number of \mathbf{R} different from 0.

PROOF. For any a in \mathbf{R} , put $P_a(x) = (x + a^{(1)}) \cdot \dots \cdot (x + a^{(l)})$ where $a^{(1)}, \dots, a^{(l)}$ are the l conjugates of a . If k is a rational integer, the

² I first proved the undecidability of \mathbf{R} by an entirely different method. The definition of the natural numbers given here was discovered jointly with R. M. Robinson. He had shown earlier that the ring of the algebraic integers of a field of finite degree over the rationals which has at most one fundamental unit is undecidable [7].

norm $N(a+k)$ is given by $P_a(k)$. Since $N(f)$ is not 0, it has only a finite number of rational integer divisors. If a satisfies the conditions of the lemma, $N(a+k)$ divides $N(f)$ for $k=1, \dots, l$. Only a finite number of values can be assumed by $N(a+k)=P_a(k)$ for those a 's which satisfy the lemma. Since P_a is of degree l and has leading coefficient 1, it is determined uniquely by $P_a(1), \dots, P_a(l)$. There can be only a finite number of such polynomials and, since $P_a(-a)=0$, only a finite number of a 's satisfying the conditions of the lemma.

THEOREM. *Let \mathbf{R} be the ring of the algebraic integers of a field of degree l over the rationals. The set \mathbf{N} of natural numbers is arithmetically definable in \mathbf{R} , and hence \mathbf{R} is undecidable. In fact, if we let*

$$\tau(a, f, g, h) \leftrightarrow f \neq 0 \wedge a + 1 \mid f \wedge \dots \wedge a + l \mid f \wedge 1 + ag \mid h,$$

then

$$n \in \mathbf{N} \leftrightarrow$$

$$\bigvee_{f, g, h} \left\{ \tau(0, f, g, h) \wedge \bigwedge_a [\tau(a, f, g, h) \rightarrow a = n \vee \tau(a + 1, f, g, h)] \right\}.$$

PROOF. Suppose $f, g,$ and h satisfy the right side of the equivalence for some n . By Lemma 1, there are only finitely many numbers a in \mathbf{R} such that $\tau(a, f, g, h)$. The inductive form of the definition insures that $\tau(0, f, g, h), \tau(1, f, g, h), \dots$, terminating only for $a=n$. Therefore, n must be a natural number.

Conversely, suppose that n is a natural number. We must show that $f, g,$ and h exist which satisfy the condition on the right side of the definition. It will be sufficient to find $f, g,$ and h so that

$$\tau(a, f, g, h) \leftrightarrow a = 0 \vee a = 1 \vee \dots \vee a = n.$$

First put $f = (n + l)!$ and define the set \mathbf{S} by

$$a \in \mathbf{S} \leftrightarrow a + 1 \mid f \wedge \dots \wedge a + l \mid f.$$

By Lemma 1, \mathbf{S} is finite. Now choose g a positive integer such that

$$a \in \mathbf{S} \wedge b \in \mathbf{S} \wedge a \neq b \rightarrow a - b \mid g$$

and

$$a \in \mathbf{S} \wedge a \neq 0 \rightarrow 1 + ag \nmid 1.$$

Clearly, we can choose g satisfying both conditions since the first condition holds if g is a multiple of all the rational integers $N(a-b)$ with a and b in \mathbf{S} and $a \neq b$, and the second condition holds if g is so large a natural number that all the conjugates of $1+ag$ lie outside

the unit circle. (Since $|N(1+ag)| > 1$, then $1+ag$ is not a unit.)

For this particular choice of f and g , the numbers $1+ag$ and $1+bg$ for a and b in \mathbf{S} and $a \neq b$ are relatively prime. Suppose this were not the case. If a prime ideal \mathfrak{p} divided both $1+ag$ and $1+bg$, \mathfrak{p} would divide the difference $(a-b)g$ and would also divide g . But \mathfrak{p} cannot divide both g and $1+ag$.

Finally, put $h = (1+g)(1+2g) \cdots (1+ng)$. By our choice of f , g , and h , the relation $\tau(a, f, g, h)$ is satisfied for $a=0, \dots, n$. If a is in \mathbf{S} and not equal to $0, 1, \dots, n$, then $1+ag$ is not a unit and is prime to h . Therefore, $1+ag \nmid h$ and $\tau(a, f, g, h)$ does not hold.

3. The arithmetical definability of \mathbf{R} in \mathbf{F} . In this section, we give a definition of the ring \mathbf{R} within the arithmetic of \mathbf{F} . Here, as before, \mathbf{R} is the ring of the algebraic integers of a given field \mathbf{F} of finite degree over the rationals.

Let \mathfrak{p} be a valuation of \mathbf{F} and $\mathbf{F}_{\mathfrak{p}}$ be the completion of \mathbf{F} with respect to \mathfrak{p} . Since non-Archimedean valuations of \mathbf{F} are \mathfrak{p} -adic valuations with respect to some prime ideal \mathfrak{p} of \mathbf{F} , we will use the same letter \mathfrak{p} for both the valuation and the prime ideal.

Two nonzero numbers a and b of \mathbf{F} are said to be in the same \mathfrak{p} -adic class if a/b is the square of a number in $\mathbf{F}_{\mathfrak{p}}$. There are only a finite number of \mathfrak{p} -adic classes for any valuation \mathfrak{p} . For an Archimedean valuation \mathfrak{p} , $\mathbf{F}_{\mathfrak{p}}$ is either the field of complex numbers, which consists of just one \mathfrak{p} -adic class, or the field of real numbers, which consists of two \mathfrak{p} -adic classes. Corresponding to a prime ideal \mathfrak{p} which does not divide 2, there are four \mathfrak{p} -adic classes. In the case of a prime ideal \mathfrak{p} which divides 2, the number of classes is even—the exact number depending on the power to which \mathfrak{p} divides 2.

We will use the Hilbert symbol $(a, b)_{\mathfrak{p}}$, which is defined for all nonzero numbers a and b in \mathbf{F} and any valuation \mathfrak{p} as follows:

$$(a, b)_{\mathfrak{p}} = \begin{cases} +1 & \text{if } ax^2 + by^2 = 1 \text{ is solvable in } \mathbf{F}_{\mathfrak{p}}, \\ -1 & \text{otherwise.} \end{cases}$$

LEMMA 2. *Let a and b belong to \mathbf{R} , \mathfrak{p} be a prime ideal, and m be a positive integer such that $\mathfrak{p}^m \nmid 2$. If $a \not\equiv 0 \pmod{\mathfrak{p}^2}$ and $a \equiv b \pmod{\mathfrak{p}^{2m}}$, then a and b are in the same \mathfrak{p} -adic class.*

This lemma follows easily from Hensel's lemma as given by Artin [1, pp. 44–51].

It is clear that $(a, b)_{\mathfrak{p}}$ depends only on the \mathfrak{p} -adic classes to which a and b belong. Hasse [3; 4] gives formulas for evaluating the Hilbert symbol. Although we will not use these directly, we will need the following two lemmas which are immediate consequences of them.

LEMMA 3. If a and b are nonzero numbers of \mathbf{R} , then $(a, b)_{\mathfrak{p}} = -1$ implies that either \mathfrak{p} is an Archimedean valuation or the prime ideal \mathfrak{p} divides $2ab$; hence, there are only a finite number of valuations \mathfrak{p} for which $(a, b)_{\mathfrak{p}} = -1$.

LEMMA 4. If a belongs to \mathbf{R} and contains \mathfrak{p} to exactly the first power, then there exists a number b in \mathbf{R} with $\mathfrak{p} \nmid b$ such that $(a, b)_{\mathfrak{p}} = -1$.

Our next lemma was first proved by Furtwängler [2, p. 427].

LEMMA 5. If a and b are nonzero numbers of \mathbf{F} , then $(a, b)_{\mathfrak{p}} = -1$ for an even number of valuations.

Both Lemma 6 and Lemma 7 are special cases of a theorem given by Hasse [5, p. 32].

LEMMA 6. There are infinitely many prime ideals in every ideal class.

LEMMA 7. If a is a number of \mathbf{R} which is prime to an ideal \mathfrak{m} , there are infinitely many totally positive prime numbers p in \mathbf{R} such that $p \equiv a \pmod{\mathfrak{m}}$.

The next lemma is due to Hasse [4, p. 127]. Another proof is given by Witt [10, pp. 41–42].

LEMMA 8. A nonzero number h of \mathbf{F} can be represented by the ternary quadratic form $x^2 - ay^2 - bz^2$ in \mathbf{F} if and only if h does not belong to the same \mathfrak{p} -adic class as $-ab$ for any valuation \mathfrak{p} with $(a, b)_{\mathfrak{p}} = -1$.

LEMMA 9. Given any prime ideal \mathfrak{p}_1 , there exist relatively prime numbers a and b in \mathbf{R} such that $(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_{2k}$, where $\mathfrak{p}_1, \dots, \mathfrak{p}_{2k}$ are distinct prime ideals which include every prime ideal which divides 2, and b is a totally positive prime number such that $(a, b)_{\mathfrak{p}} = -1$ if and only if $\mathfrak{p} \mid a$.

PROOF. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_{2k-1}$ be a set of distinct prime ideals which includes every prime ideal dividing 2. Let A be the ideal class which contains the product $\mathfrak{p}_1 \cdots \mathfrak{p}_{2k-1}$. By Lemma 6, we can choose a prime ideal \mathfrak{p}_{2k} in the ideal class A^{-1} with $\mathfrak{p}_{2k} \neq \mathfrak{p}_i$ for $i = 1, \dots, 2k-1$. Then $\mathfrak{p}_1 \cdots \mathfrak{p}_{2k}$ will be a principal ideal and we can take a so that $(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_{2k}$.

For $i = 1, \dots, 2k$, by Lemma 4 we can choose b_i in \mathbf{R} and prime to \mathfrak{p}_i so that $(a, b_i)_{\mathfrak{p}_i} = -1$. Let m be a positive integer so that $\mathfrak{p}^m \nmid 2$ for every prime ideal \mathfrak{p} . By Lemma 2, if

$$x \equiv b_i \pmod{\mathfrak{p}_i^{2m}} \quad \text{for } i = 1, \dots, 2k,$$

then $(a, x)_{\mathfrak{p}_i} = -1$ for $i = 1, \dots, 2k$. By the analog of the Chinese Remainder Theorem, we can replace these $2k$ congruences by a single congruence:

$$x \equiv c \pmod{\mathfrak{p}_1^{2m} \cdots \mathfrak{p}_{2k}^{2m}}$$

where c is prime to the modulus. By Lemma 7, we can find a totally positive prime number b satisfying this congruence. Since c is prime to a , b will also be prime to a .

By our construction $(a, b)_{\mathfrak{p}_i} = -1$ for $i=1, \dots, 2k$. Since b is totally positive b is a square in $F_{\mathfrak{p}}$ for all Archimedean valuations \mathfrak{p} , and hence $(a, b)_{\mathfrak{p}} = +1$ for all Archimedean valuations. By Lemma 3, the only other valuation for which $(a, b)_{\mathfrak{p}} = -1$ could hold would be $\mathfrak{p} = (b)$; but, by Lemma 5, there are an even number of valuations \mathfrak{p} such that $(a, b)_{\mathfrak{p}} = -1$. Therefore, in our case $(a, b)_{\mathfrak{p}} = -1$ if and only if $\mathfrak{p} = \mathfrak{p}_i$ for $i=1, \dots, \text{ or } 2k$.

LEMMA 10. *If a and b satisfy Lemma 9 and m is a positive integer such that $\mathfrak{p}^m \nmid 2$ for all prime ideals \mathfrak{p} , then there exist $x, y,$ and z in F such that $1 - abc^{2m} = x^2 - ay^2 - bz^2$ if and only if c is a \mathfrak{p} -adic integer for every prime ideal \mathfrak{p} dividing a .*

PROOF. We can express $c = u/v$ with u and v in R and with no \mathfrak{p}_i dividing both u and v . We then need to show that if u and v ($v \neq 0$) are in R and no \mathfrak{p}_i divides both u and v , $v^{2m} - abu^{2m} = x^2 - ay^2 - bz^2$ is solvable for $x, y,$ and z in F if and only if v is prime to a .

Let $h = v^{2m} - abu^{2m}$. By Lemma 8, h can be represented by $x^2 - ay^2 - bz^2$ if and only if h does not lie in the same \mathfrak{p}_i -adic class as $-ab$ for $i=1, \dots, 2k$.

CASE I. Suppose $\mathfrak{p}_i \mid v$. Since \mathfrak{p}_i does not divide u or b , $h \not\equiv 0 \pmod{\mathfrak{p}_i^2}$ and $h \equiv -abu^{2m} \pmod{\mathfrak{p}_i^{2m}}$. By Lemma 2, h is in the same \mathfrak{p}_i -adic class as $-abu^{2m}$. But this class is the same as the class of $-ab$; therefore, h cannot be represented by $x^2 - ay^2 - bz^2$.

CASE II. Suppose v is prime to a . Then h is prime to a and cannot be in the same \mathfrak{p}_i -adic class as $-ab$ for any \mathfrak{p}_i , since \mathfrak{p}_i divides ab to exactly the first power. Therefore h can be represented by $x^2 - ay^2 - bz^2$ and the lemma follows.

THEOREM. *Let m be a positive integer such that $\mathfrak{p}^m \nmid 2$ for every prime ideal \mathfrak{p} and let $\phi(a, b, c)$ be defined by the equivalence,*

$$\phi(a, b, c) \leftrightarrow \bigvee_{x,y,z} 1 - abc^{2m} = x^2 - ay^2 - bz^2.$$

If $\psi(t)$ is defined by

$$\psi(t) \leftrightarrow \bigwedge_{a,b} \left\{ \bigwedge_c [\phi(a, b, c) \rightarrow \phi(a, b, c + 1)] \rightarrow \phi(a, b, t) \right\},$$

then $t \in I \rightarrow \psi(t)$ and $\psi(t) \rightarrow t \in R$.

PROOF. Since $\phi(a, b, 0)$ holds for every a and b , the inductive form of ψ insures that every natural number satisfies ψ . Since $\phi(a, b, c) \leftrightarrow \phi(a, b, -c)$, we see that every rational integer also satisfies ψ .

Suppose that t does not belong to \mathbf{R} . Then there is some prime ideal \mathfrak{p}_1 such that t is not a \mathfrak{p}_1 -adic integer. We choose a and b by Lemma 9. By Lemma 10, $\phi(a, b, c)$ holds if and only if c is a \mathfrak{p} -adic integer for every prime ideal \mathfrak{p} which divides a . Clearly, for this a and b , $\phi(a, b, c) \rightarrow \phi(a, b, c+1)$; but $\phi(a, b, t)$ does not hold. Thus, if t is not in \mathbf{R} , $\psi(t)$ does not hold.

It is not known whether $\psi(t) \rightarrow t \in I$; however, we can give an arithmetical definition of \mathbf{R} with the help of ψ . Let a_1, \dots, a_l be an integral basis for \mathbf{R} . (Here l is the degree of F over the rationals.) Then,

$$t \in \mathbf{R} \leftrightarrow \bigvee_{x_1, \dots, x_l} [t = a_1x_1 + \dots + a_lx_l \wedge \psi(x_1) \wedge \dots \wedge \psi(x_l)].$$

It would be sufficient for the x_i to range over I ; but if the x_i range over \mathbf{R} , no additional values of t are introduced. However, in general, a_1, \dots, a_l will not themselves be arithmetically definable.³

Let P_i be a polynomial with integer coefficients and leading coefficient equal to 1 such that $P_i(a_i) = 0$. Since every root of $P_i = 0$ which is in F is also in \mathbf{R} , we obtain

$$t \in \mathbf{R} \leftrightarrow \bigvee_{x_1, \dots, x_l; y_1, \dots, y_l} [t = x_1y_1 + \dots + x_ly_l \wedge P_1(y_1) = 0 \wedge \dots \wedge P_l(y_l) = 0 \wedge \psi(x_1) \wedge \dots \wedge \psi(x_l)].$$

Since this formula gives a suitable arithmetical definition of \mathbf{R} within the arithmetic of F , we have proved the following:

THEOREM. *If \mathbf{R} is the ring of the algebraic integers of a field F of finite degree over the rationals, then \mathbf{R} is arithmetically definable in F .*

This theorem with the final theorem of §2 gives us:

THEOREM. *If F is an algebraic field of finite degree over the rationals, the natural numbers are arithmetically definable in F and hence F is undecidable.*

REFERENCES

1. Emil Artin, *Lectures on modern higher algebra*, Part III, mimeographed notes, New York University, 1948.
2. Ph. Furtwängler, *Die Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern*, III, Math. Ann. vol. 74 (1913) pp. 413-429.
3. Helmut Hasse, *Zur Theorie des quadratischen Hilbertschen Normenrestsymbols in algebraischen Körpern*, J. Reine Angew. Math. vol. 153 (1923) pp. 76-93.
4. ———, *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper*, J. Reine Angew. Math. vol. 153 (1923) pp. 113-130.

³ For a description of numbers arithmetically definable in an algebraic field, see R. M. Robinson [8].

5. ———, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil I, Jahresbericht der Deutschen Mathematiker-Vereinigung vol. 35 (1926) pp. 1–55.
6. Julia Robinson, *Definability and decision problems in arithmetic*, J. Symb. Logic vol. 14 (1949) pp. 98–114.
7. R. M. Robinson, *Undecidable rings*, Trans. Amer. Math. Soc. vol. 70 (1951) pp. 137–159.
8. ———, *Arithmetical definability of field elements*, J. Symb. Logic vol. 16 (1951) pp. 125–126.
9. A. Tarski, A. Mostowski, and R. M. Robinson, *Undecidable theories*, Amsterdam, North-Holland Publishing Company, 1953.
10. Ernst Witt, *Theorie der quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. vol. 176 (1936) pp. 31–44.

CONTRA COSTA COUNTY, CALIFORNIA

CONCERNING LOCAL SEPARABILITY IN LOCALLY PERIPHERALLY SEPARABLE SPACES

L. B. TREYBIG

Alexandroff [1] has shown that a connected metric space is completely separable if it is locally completely separable. In the previous statement “completely separable” may be replaced with “separable,” since these are equivalent conditions in a metric space. In his dissertation (Texas, 1958) the author has shown an example of a connected, locally peripherally separable [2], metric space which is not separable, but which has the property that the set of all points at which it is not locally separable is separable. The purpose of this paper is to give a further result in this direction.

THEOREM. *If Σ is any connected, locally peripherally separable, metric space which is not separable, then the set of all points at which Σ is not locally separable is uncountable.*

PROOF. On the contrary, suppose that there exists such a space Σ where the set M of all points at which Σ is not locally separable is countable. Let M be denoted by $P_1 + P_2 + P_3 + \dots$, where, if $i \neq j$, $P_i \neq P_j$. For each positive integer n let G_n be the collection of all locally peripherally separable domains having diameter less than $1/n$. Let d denote a positive integer and g_1, g_2, g_3, \dots denote a sequence such that for each n , P_n and g_n are elements of G_n and G_{n+d} , respectively. Let H be a collection to which x belongs if and only if x is g_i for some i . For each positive integer n , let G'_n be the collection of all