TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 262, Number 1, November 1980

UNDECIDABILITY AND DEFINABILITY FOR THE THEORY OF GLOBAL FIELDS

BY

R. S. RUMELY[1]

ABSTRACT. We prove that the theory of global fields is essentially undecidable, using predicates based on Hasse's Norm Theorem to define valuations. Polynomial rings or the natural numbers are uniformly defined in all global fields, as well as Gödel functions encoding finite sequences of elements.

We will prove that the elementary theory of global fields is essentially undecidable. While this is a negative logical result, our proofs have the positive consequence that a great variety of number-theoretic objects, from rings of integers and valuations, to zeta-functions and adele rings, can be discussed in the theory of global fields. It is our hope that the theory may eventually be a vehicle for applying logical methods in number theory.

Our main theorems are as follows.

I. *There is a finite collection of predicates which define every valuation, archimedean and nonarchimedean, of every global field, in terms of parameters.*

II. *There is a sentence which distinguishes number fields from function fields.*

III. *Given a global field K*:

If K is a number field, the theory of number fields defines its algebraic integers, the rational integers, and the natural numbers.

If K is a function field, the theory of function fields defines its field of constants $\mathbf{F}$, *and for an arbitrary nonconstant* $x \in K$, *defines the polynomial ring* $\mathbf{F}[x]$ *and a model of* $\mathbf{N}$ *given by the powers of* x.

Gödel functions encoding all finite sequences of elements of K exist for each of these models of $\mathbf{N}$.

This investigation was motivated by the papers of Julia Robinson [9], [10] and Ershov [4], who used the Hasse-Minkowski theorem on quadratic forms to prove the undecidability of a given number field, or field of rational functions over a finite field of odd characteristic. Its original goal was to show the remaining algebraic function fields were undecidable, completing the parallel between number fields and function fields. Then Simon Kochen observed that the proof showed

Received by the editors February 26, 1979 and, in revised form, June 25, 1979.

AMS (MOS) subject classifications (1970). Primary 02G05; Secondary 10L05, 12N05.

Key words and phrases. Undecidability, definability, global fields, function fields, number fields, Hasse Principle, valuations.

[1]Work done at Princeton University.

0002-9947/80/0000-0506/$06.75

the theory of algebraic function fields was essentially undecidable, and the question became one of determining the strength of the theory of global fields.

Our predicates have the same basic structure as Robinson's and Ershov's, and we begin with fundamentally the same number-theoretic data as they do, but our thrust differs from theirs. We focus on the completions, first obtaining a class of predicates which define valuation rings. Our main innovation is replacing quadratic forms with norm forms, and the Hasse-Minkowski theorem with the Hasse Principle ("X is true globally if and only if X is true locally everywhere") which holds for norms from cyclic extensions. This avoids trouble with function fields of characteristic 2, and with ramification at primes above 2 in number fields.[2] The valuation rings easily yield rings of algebraic integers, and they, in turn, the rational integers and polynomial rings. We treat archimedean valuations at the end, making use of the natural numbers, which are by then available.

1. Number-theoretic preliminaries. Throughout this paper K will be a global field, that is, a number field: a finite algebraic extension of the rationals $\mathbf{Q}$, or a function field: a finite algebraic extension of some field of rational functions $\mathbf{F}(x)$, where $\mathbf{F}$ is finite. The reader is assumed to be familiar with the basic theorems of algebraic number theory involving local and global fields, but not necessarily with class field theory. This material is covered, for example, in [1], [3] and [5]. We will introduce deeper arithmetical facts as they are needed, in a series of lettered propositions; the main theorems we cite are the theorems on primes in generalized arithmetic progressions, Hasse's Norm Theorem, and Artin's Reciprocity Law.

Notations are standard. We use additive valuations; if $\mathfrak{p}$ is a prime of K, we normalize $\mathrm{ord}_{\mathfrak{p}}(x)$ so that the ord of a prime element is 1. We use the same letter $\mathfrak{p}$ to refer to a prime ideal in a maximal order of K, the prime spot it induces in K, or any of the valuations in it. We regard K as canonically embedded in its completion $K_{\mathfrak{p}}$; $U_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}} | \mathrm{ord}_{\mathfrak{p}}(x) = 0\}$ is the group of units in the ring of integers of $K_{\mathfrak{p}}$. Subrings of K itself are distinguished by script type: $\mathcal{O}_{\mathfrak{p}} = \{x \in K | \mathrm{ord}_{\mathfrak{p}}(x) \geq 0\}$ is the valuation ring at $\mathfrak{p}$. A bar ($\bar{}$) will be used for the residue class map; $\bar{K}_{\mathfrak{p}}$ denotes the residue class field of K at $\mathfrak{p}$. For any ring R, $R^{\times}$ is its group of invertible elements, and (r) is the principal ideal generated by r. If K is a function field, $\mathbf{F}$ denotes its exact field of constants; $\mathbf{F}_q$ means the finite field with q elements. The characteristic of K is abbreviated $\chi(K)$. If L/K is a finite extension, the notation $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ carries an implicit assertion that $\mathfrak{P}$ is a prime of L over $\mathfrak{p}$. Finally, we sometimes shorten the names of the norm maps $N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ and $N_{L/K}$ to just N.

If K is a number field, let I be the group of fractional ideals of its maximal order, and P its subgroup of principal fractional ideals. Consider the free abelian group on all valuations of K; its elements are called cycles. If one has

$$\mathfrak{f} = \left(\prod_{\text{arch}} \mathfrak{p}_{\infty}^{m_{\infty}}\right) \cdot \left(\prod_{\text{finite}} \mathfrak{p}_i^{m_i}\right)$$

[2]Jan Denef has pointed out that Penzin [7] earlier established the undecidability of the rational function fields in characteristic 2. His predicates, like ours, are based on Hasse's Norm Theorem, but he uses it differently than we do. The author also thanks Denef for pointing out the results of Julia Robinson in [8].

then $I(\mathfrak{f})$ means the group of fractional ideals prime to the finite part of $\mathfrak{f}$, and $P_{\mathfrak{f}}$ means the subgroup of principal fractional ideals with a generator congruent to 1 modulo the ideal corresponding to the finite part of $\mathfrak{f}$, and positive at the real archimedean primes occurring in $\mathfrak{f}$. Then, $I(\mathfrak{f})/P_{\mathfrak{f}}$ is called a generalized ideal class group, and it is finite (see [5, p. 127]). Its elements are the generalized ideal classes. The following well-known theorem is proved in [5, p. 166].

PROPOSITION A (NUMBER FIELD CASE). *Let $\mathfrak{f}$ be a cycle. Then, every generalized ideal class in $I(\mathfrak{f})/P_{\mathfrak{f}}$ contains infinitely many prime ideals.*

The analogue of this for function fields is a folk theorem, but there does not seem to be a reference for it. If K is a function field, choose some prime spot of K and designate it $\mathfrak{p}_\infty$; then the ring

$$\mathcal{R}_{\mathfrak{p}_\infty} = \bigcap_{\mathfrak{p} \neq \mathfrak{p}_\infty} \mathcal{O}_{\mathfrak{p}}$$

is a Dedekind domain and it has an ideal theory. Just as with number fields, one has the groups I, P and their quotient ideal class group I/P. For any ideal $\mathfrak{f}$ of $R_{\mathfrak{p}_\infty}$ one has $I(\mathfrak{f})$ and $P_{\mathfrak{f}}$. The extension to include the "infinite" prime $\mathfrak{p}_\infty$ in this schema goes as follows. Let H be any open subgroup of $K_{\mathfrak{p}_\infty}^{\times}$ with finite index, and define $P_{\mathfrak{f},H}$ to be the group of principal fractional ideals of $\mathcal{R}_{\mathfrak{p}_\infty}$ which have a generator congruent to 1 mod $\mathfrak{f}$, and lying in H at $\mathfrak{p}_\infty$. We will only be interested in the case $H = (K_{\mathfrak{p}_\infty}^{\times})^m$, where $(m, \chi(K)) = 1$, so we can write $P_{\mathfrak{f},m}$ rather than $P_{\mathfrak{f},H}$.

PROPOSITION A (FUNCTION FIELD CASE). *$\mathcal{R}_{\mathfrak{p}_\infty}$ is a Dedekind domain, and its units are just the constants in $\mathbf{F}^{\times}$. The generalized ideal class groups $I(\mathfrak{f})/P_{\mathfrak{f},m}$ are finite if $\chi(K) \nmid m$, and every generalized ideal class contains infinitely many prime ideals of $\mathcal{R}_{\mathfrak{p}_\infty}$.*

SKETCH OF PROOF. It is shown in part I of [6] that $\mathcal{R}_{\mathfrak{p}_\infty}$ is a Dedekind domain, as are indeed all rings $\mathcal{R}_S = \bigcap_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}}$ where S is a nonempty finite set of primes. Furthermore, it is shown that the group of units of $\mathcal{R}_S$ has rank $\#(S) - 1$, and the ideal class groups I/P are finite. Given that I/P is finite, one finds easily by means of a diagram similar to the one in [5, p. 126], that $I(\mathfrak{f})/P_{\mathfrak{f},m}$ is finite.

The last part of the theorem is proved using L-functions. Each character ψ of $I(\mathfrak{f})/P_{\mathfrak{f},m}$ gives rise to an idele class character. Hence the L-series,

$$L(s, \psi) = \prod_{\mathfrak{p} \nmid \mathfrak{f}} (1 - \psi(\mathfrak{p}) N_{\mathfrak{p}}^{-s})^{-1},$$

which converges for $\mathrm{Re}(s) > 1$ can be meromorphically continued to the entire complex plane. A unified treatment of L-functions for number fields and function fields is given in [15, Chapter 10], where it is shown that if ψ is nontrivial, then $L(1, \psi) \neq 0, \infty$, while if ψ is trivial then $L(s, \psi)$ has a pole of order 1 at $s = 1$. (See especially [15, Corollaries 1 and 2, p. 124, the remark at the bottom of p. 125 and Theorem 11, p. 288].) With this, the proof of the theorem for number fields given in [5, p. 166], carries over.

2. Definability of valuation rings. Let $\mathfrak{p}$ be a finite prime of K. The goal of this section is to find a predicate, as independent of $\mathfrak{p}$ and K as possible, which, for a proper choice of its parameters, is satisfied by precisely the valuation ring $\mathcal{O}_\mathfrak{p}$. A standard trick reduces the problem as follows: suppose $l \geqslant 2$ is a positive integer, and suppose we can find a predicate $R(t, \vec{c})$ with a choice of $\vec{c}$ so that R is satisfied by exactly those t for which $\mathrm{ord}_\mathfrak{p}(t) \equiv 0 \bmod l$. Then, choosing g to be a prime element at $\mathfrak{p}$, $\mathcal{O}_\mathfrak{p}$ is the set of all x satisfying

$$\exists t(1 + gx^l = t \& R(t, \vec{c})).$$

Namely, if $\mathrm{ord}_\mathfrak{p}(x) \geqslant 0$ then $\mathrm{ord}_\mathfrak{p}(1 + gx^l) = 0$, while if $\mathrm{ord}_\mathfrak{p}(x) < 0$ then

$$\mathrm{ord}_\mathfrak{p}(1 + gx^l) \equiv 1 \bmod l.$$

Our plan is to construct $R(t, \vec{c})$ by using norm forms from cyclic Kummer extensions of K. The first task, therefore, is to describe the representation properties of norm forms. Hasse's Norm Theorem says that an element is a "global" norm from a cyclic extension if and only if it is a "local" norm at all the completions. If l is a prime number, not equal to the characteristic $\chi(K)$, and if K contains the lth roots of 1, then all extensions of the kind $K(b^{1/l})/K$ are cyclic. In this special situation we can give a very precise description of the local extensions and local norm groups. For it, we will need some facts about local fields, proved in [3, pp. 142–143].

PROPOSITION B (LOCAL NORM INDICES). *Let $L_\mathfrak{P}/K_\mathfrak{p}$ be an abelian extension of local fields. Then*

(1) $[K_\mathfrak{p}^\times : NL_\mathfrak{P}^\times] = [L_\mathfrak{P} : K_\mathfrak{p}]$, *the degree of the extension,*

(2) $[U_\mathfrak{p} : NU_\mathfrak{P}] = e_\mathfrak{p}$, *the ramification index.*

We now have

LEMMA 1. *Let l be a prime number, and assume K contains the $2l$th roots of 1. Suppose $\mathfrak{p}$ is a prime of K such that the characteristic of the residue class field $\overline{K}_\mathfrak{p}$ is not l. We have*

(1) *If $\mathrm{ord}_\mathfrak{p}(b) \not\equiv 0 \bmod l$, then $L_\mathfrak{P}/K_\mathfrak{p}$ is totally ramified and of degree l, and $N(L_\mathfrak{P}^\times)$ is generated by b and $(K_\mathfrak{p}^\times)^l$.*

(2) *If $\mathrm{ord}_\mathfrak{p}(b) \equiv 0 \bmod l$ but $b \notin (K_\mathfrak{p}^\times)^l$, then $L_\mathfrak{P}/K_\mathfrak{p}$ is unramified and of degree l, and $N(L_\mathfrak{P}^\times) = \{x \in K_\mathfrak{p}^\times | \mathrm{ord}_\mathfrak{p}(x) \equiv 0 \bmod l\}$.*

(3) *If $b \in (K_\mathfrak{p}^\times)^l$, then $L_\mathfrak{P}/K_\mathfrak{p}$ is trivial and $N(L_\mathfrak{P}^\times) = K_\mathfrak{p}^\times$.*

PROOF. Since l is a prime, $\mathfrak{p}$ can be extended to L in only three ways, each of which corresponds to a case above.

(1) If $l \nmid \mathrm{ord}_\mathfrak{p}(b)$, the value group of $L_\mathfrak{P} = K_\mathfrak{p}(b^{1/l})$ will gain elements, so $L_\mathfrak{P}/K_\mathfrak{p}$ must be totally ramified and of degree l. $(K_\mathfrak{p}^\times)^l$ and b are certainly norms; since $(\mathrm{ord}_\mathfrak{p}(b), l) = 1$, the group generated by them contains elements with all ord values.[3] Thus any norm can be multiplied by an element of our group to make it a

[3] ADDED IN PROOF. In Lemma 1, when $l = 2$, b is in general a norm from $K_\mathfrak{p}(b^{1/2})$ only if $\sqrt{-1} \in K$; so we assume this throughout §2. With $\sqrt{-1} \in K$, the conditions "is totally positive" in Lemma 3 are vacuous. The requirement that $\sqrt{-1} \in K$ can be removed in §3 by forming a predicate $\vec{S}_2(x, 0; \vec{c})$ for the extension $K(\sqrt{-1})$, similar to $\vec{S}_3(x, 0; \vec{c})$ for $K(\omega)$.

unit. We claim $NU_{\mathfrak{P}} = (U_{\mathfrak{p}})^l$. To verify this, compare indices: because $\chi(\bar{K}_{\mathfrak{p}}) \neq l$, Hensel's Lemma applied to $x^l - u = 0$ shows that $u \in (U_{\mathfrak{p}})^l$ iff $\bar{u} \in (\bar{K}_{\mathfrak{p}}^{\times})^l$. Then, since $\bar{K}_{\mathfrak{p}}^{\times}$ is cyclic and contains the lth roots of 1, $[U_{\mathfrak{p}}: U_{\mathfrak{p}}^l] = [\bar{K}_{\mathfrak{p}}^{\times}: (\bar{K}_{\mathfrak{p}}^{\times})^l] = l$, and by Proposition B(2), $[U_{\mathfrak{p}}: NU_{\mathfrak{P}}] = l$. As $U_{\mathfrak{p}}^l \subset NU_{\mathfrak{P}}$, we are done.

(2) If $\mathrm{ord}_{\mathfrak{p}}(b) \equiv 0 \bmod l$, we can assume, after adjusting by an lth power if necessary, that $\mathrm{ord}_{\mathfrak{p}}(b) = 0$, b is not an lth power in $U_{\mathfrak{p}}$, so neither is $\bar{b}$ one in $\bar{K}_{\mathfrak{p}}^{\times}$. $f_{\mathfrak{p}} = [\bar{K}_{\mathfrak{p}}(\bar{b}^{1/l}): \bar{K}_{\mathfrak{p}}] = l$ since l is prime. Therefore $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is unramified of degree l, and it follows from Proposition B, (1) and (2), that the norm group is as stated.

(3) This is the only remaining case, and the assertions are clear. □

For the remainder of this section fix the prime $\mathfrak{p}$, and whenever we deal with an l assume that $2l$th roots of 1 are in K. If an extension $L = K(b^{1/l})$ is nontrivial, it gives rise to a norm form

$$N_l(b, \vec{a}) = N_{L/K}(a_0 + a_1 b^{1/l} + a_2 b^{2/l} + \cdots + a_{l-1} b^{(l-1)/l}).$$

Note that $N_l(b, \vec{a})$ can be explicitly calculated and has integer coefficients by the theorem on symmetric functions. For example,

$$N_2(b, a_0, a_1) = a_0^2 - a_1^2 b,$$

$$N_3(b, a_0, a_1, a_2) = a_0^3 + a_1^3 b + a_2^3 b^2 - 3a_0 a_1 a_2 b.$$

Experimentation suggests that no finite number of norm forms, with variables independent of each other, can produce a predicate R. However, several norm forms parametrizing each other, in effect giving an infinite number of forms, can. Define

$$R_l(t; c, d) \Leftrightarrow \exists \vec{a}_1 \exists \vec{a}_2 \exists \vec{a}_3 \exists w (w = N_l(d, \vec{a}_1) \& cw = N_l(cd, \vec{a}_2) \& t = N_l(w, \vec{a}_3)).$$

The next lemma shows that if $\mathfrak{q}$ is a prime of K, the first two conditions are a device for saying "$K(w^{1/l})/K$ is unramified at $\mathfrak{q}$".

LEMMA 2. *Suppose $l \neq \chi(\bar{K}_{\mathfrak{q}})$ is a prime number and $K_{\mathfrak{q}}$ contains the $2l$th roots of 1. If d is a non-lth power unit at $\mathfrak{q}$ and $\mathrm{ord}_{\mathfrak{q}}(c) = 1$, then $R_l(t; c, d)$ is satisfied only by $t \in K$ such that $\mathrm{ord}_{\mathfrak{q}}(t) \equiv 0 \bmod l$.*

PROOF. It is enough to look at the situation locally at $\mathfrak{q}$. By the first hypothesis, $K_{\mathfrak{q}}(d^{1/l})/K_{\mathfrak{q}}$ is unramified of degree l, and by the second, $K_{\mathfrak{q}}((cd))^{1/l}/K_{\mathfrak{q}}$ is totally ramified. From the description of the norm groups given in Lemma 1, and the fact that in $K_{\mathfrak{q}}$, c is a prime element, we obtain

$$w = u \cdot c^{nl}, \qquad cw = v^l (cd)^m, \quad \text{for some } m, n,$$

where u and v are in $U_{\mathfrak{q}}$ (but note that $w, c, d \in K$). Now multiply the first equation by c and take $\mathrm{ord}_{\mathfrak{q}}$ of both. Equating, we get $nl + 1 = \mathrm{ord}_{\mathfrak{q}}(cw) = m$. This leads to $w = d \cdot (vc^n d^n)^l$, so $K_{\mathfrak{q}}(w^{1/l}) = K_{\mathfrak{q}}(d^{1/l})$ is unramified of degree l, so by Lemma 1 again, $\mathrm{ord}_{\mathfrak{q}}(t) \equiv 0 \bmod l$. □

If we could choose c and d such that $R_l(t; c, d)$ were satisfied by *exactly* those $t \in K$ for which $\mathrm{ord}_{\mathfrak{p}}(t) \equiv 0 \bmod l$, we would be done. Unfortunately, I do not know whether such c and d exist. However, c and d can be chosen which impose conditions at only one other prime besides $\mathfrak{p}$, and we will see that this is enough.

Lemma 2 can be regarded as providing a sufficient condition for an element to be in $\mathcal{O}_\mathfrak{p}$; to prove a necessary condition we will need some facts from class field theory. Recall that if L/K is a finite algebraic extension and $\mathfrak{q}$ is a prime of K, then $\mathrm{Gal}(L_\mathfrak{Q}/K_\mathfrak{q})$ is canonically isomorphic to the decomposition group $\{\sigma \in \mathrm{Gal}(L/K) | \sigma(\mathfrak{Q}) = \mathfrak{Q}\}$. We will regard the groups $\mathrm{Gal}(L_\mathfrak{Q}/K_\mathfrak{q})$ as being embedded in $\mathrm{Gal}(L/K)$. Furthermore, if L/K is abelian, then the local norm groups $N_{L_\mathfrak{Q}/K_\mathfrak{q}}(L_\mathfrak{Q}^\times)$ and the galois groups $\mathrm{Gal}(L_\mathfrak{Q}/K_\mathfrak{q})$ (embedded in $\mathrm{Gal}(L/K)$ as just discussed) depend only on $\mathfrak{q}$, and not on the prime $\mathfrak{Q}$ extending it. However, the local norm groups for different $\mathfrak{q}$ are not entirely independent. The relationship between them is given by Artin's Reciprocity Law.

PROPOSITION C (HASSE'S NORM THEOREM). *Let L/K be a cyclic extension of global fields. Then, for $a \in K$, $a \in N_{L/K}(L)$ iff $a \in N_{L_\mathfrak{Q}/K_\mathfrak{q}}(L_\mathfrak{Q})$ for all primes $\mathfrak{q}$ of K (including archmimedean ones).*

PROPOSITION D. *Let L/K be a finite abelian extension of global fields. Then for each prime $\mathfrak{q}$, archimedean or nonarchimedean, there is a surjective homomorphism*

$$(\ ,\ L/K)_\mathfrak{q}\colon K_\mathfrak{q}^\times \to \mathrm{Gal}(L_\mathfrak{Q}/K_\mathfrak{q}) \subset \mathrm{Gal}(L/K),$$

called the norm residue symbol at $\mathfrak{q}$, such that $(x, L/K)_\mathfrak{q} = 1$ iff $x \in N_{L_\mathfrak{Q}/K_\mathfrak{q}}(L_\mathfrak{Q}^\times)$. Especially if $L_\mathfrak{Q}/K_\mathfrak{q}$ is unramified and $\mathrm{ord}_\mathfrak{q}(x) = 0$, then $(x, L/K)_\mathfrak{q} = 1$. Collectively they satisfy Artin's Reciprocity Law:

$$\textit{If } a \in K^\times, \textit{ then } \prod_\mathfrak{q} (a, L/K)_\mathfrak{q} = 1.$$

Note that the product above is actually finite, since $(a, L/K)_\mathfrak{q} = 1$ for almost all $\mathfrak{q}$. The norm residue symbol is discussed in [2] and [3]; Hasse's Norm Theorem is proved in [3, p. 185].

The construction of c and d differs slightly for number fields and function fields, owing to the presence of archimedean primes in number fields. Let us treat the number field case first. We are assuming $\mathfrak{p} \nmid l$ and, as always, that K contains the $2l$th roots of 1.

To construct c, first choose a number m so large that for all $\mathfrak{q}|l$, if $a \equiv 1 \bmod \mathfrak{q}^m$, then $a \in (K_\mathfrak{q}^\times)^l$, and define a cycle $\mathfrak{f}$ by $\mathfrak{f} = (\prod \mathfrak{p}_\infty) \cdot (\prod_{\mathfrak{q}|l} \mathfrak{q}^m)$ where the product over $\mathfrak{p}_\infty$ includes all archimedean primes. Let Ω be the class of $\mathfrak{p}$ in the generalized ideal class group $I(\mathfrak{f})/P_\mathfrak{f}$. Using Proposition A, choose a prime $\mathfrak{p}_1$ in Ω^{-1}. (If $\Omega = \Omega^{-1}$ we require also that $\mathfrak{p}_1 \neq \mathfrak{p}$.) We emphasize for future reference that there are infinitely many possible choices for $\mathfrak{p}_1$. Thus, $\mathfrak{p}\mathfrak{p}_1$ is a principal ideal with a generator c such that

$$c \equiv 1 \bmod \mathfrak{q}^m \text{ for all } \mathfrak{q}|l, \qquad c \text{ is totally positive.}$$

Consider $L = K(c^{1/l})$. $\mathfrak{p}$ and $\mathfrak{p}_1$ are the only primes of K which ramify in L/K. (Locally at the archimedean primes and at the $\mathfrak{q}|l$, the extension has been forced to be trivial; at all other primes, Lemma 1 applies.) Letting $\mathfrak{P}$ and $\mathfrak{P}_1$ be the (unique) primes of L above $\mathfrak{p}$ and $\mathfrak{p}_1$ respectively, we see that $[L_\mathfrak{P}\colon K_\mathfrak{p}] = [L_{\mathfrak{P}_1}\colon K_{\mathfrak{p}_1}] = l$, and by Proposition B(2), $[U_\mathfrak{p}\colon NU_\mathfrak{P}] = [U_{\mathfrak{p}_1}\colon NU_{\mathfrak{P}_1}] = l$. Pick a non-$l$th power unit $\xi_\mathfrak{p} \in U_\mathfrak{p}$: then since $NU_\mathfrak{P} = (U_\mathfrak{p})^l$, $(\xi_\mathfrak{p}, L/K)_\mathfrak{p} = \sigma \neq 1$. Also, $(\ ,\ L/K)_{\mathfrak{p}_1}$ maps $U_{\mathfrak{p}_1}$

surjectively onto $\mathrm{Gal}(L/K)$, so there is a non-lth power unit $\xi_{\mathfrak{p}_1}$ such that $(\xi_{\mathfrak{p}_1}, L/K)_{\mathfrak{p}_1} = \sigma^{-1}$.

To construct d, by the approximation theorem, there is an element b of K for which

$$b \equiv 1 \bmod \mathfrak{f} \quad (\text{so } b \text{ is totally positive, and } b \in \left(K_{\mathfrak{q}}^{\times}\right)^{l} \text{ if } \mathfrak{q} \mid l),$$
$$b \equiv \xi_{\mathfrak{p}} \bmod \mathfrak{p}, \quad b \equiv \xi_{\mathfrak{p}_1} \bmod \mathfrak{p}_1.$$

Consider the class Ω' of (b) in $I(\mathfrak{f}\mathfrak{p}\mathfrak{p}_1)/P_{\mathfrak{f}\mathfrak{p}\mathfrak{p}_1}$: every ideal in it is principal, and it contains infinitely many prime ideals. Pick one, and call it $\mathfrak{d}$. Now $\mathfrak{d} \cdot (b^{-1}) \in P_{\mathfrak{f}\mathfrak{p}\mathfrak{p}_1}$ is an ideal with a totally positive generator e, such that $e \equiv 1 \bmod \mathfrak{f}\mathfrak{p}\mathfrak{p}_1$. So, defining $d = be$, we have a generator d for the prime ideal $\mathfrak{d}$, satisfying

$$d \in \left(K_{\mathfrak{q}}^{\times}\right)^{l} \text{ for all } \mathfrak{q} \mid l, \quad d \text{ is totally positive},$$
$$d \equiv \xi_{\mathfrak{p}} \bmod \mathfrak{p}, \quad d \equiv \xi_{\mathfrak{p}_1} \bmod \mathfrak{p}_1.$$

We claim, moreover, that $c \in (K_{\mathfrak{d}}^{\times})^{l}$. For, $(d, L/K)_{\mathfrak{q}}$ can be different from 1 only if $\mathfrak{q}$ is $\mathfrak{p}$, $\mathfrak{p}_1$, or $\mathfrak{d}$ itself: at archimedean primes $(d, L/K)_{\mathfrak{q}} = 1$ because d is totally positive; for $\mathfrak{q} \mid l$, $(d, L/K)_{\mathfrak{q}} = 1$ because $d \in (K_{\mathfrak{q}}^{\times})^{l}$; and for all other finite primes $\mathfrak{q}$ besides $\mathfrak{p}$, $\mathfrak{p}_1$ and $\mathfrak{d}$, $(d, L/K)_{\mathfrak{q}} = 1$ because $L_{\mathfrak{Q}}/K_{\mathfrak{q}}$ is unramified and $\mathrm{ord}_{\mathfrak{q}}(d) = 0$. Furthermore d differs from $\xi_{\mathfrak{p}}$ by an lth power in $K_{\mathfrak{p}}$ since $\mathfrak{p} \nmid l$, and similarly for $\xi_{\mathfrak{p}_1}$. By Artin's Reciprocity Law,

$$1 = \prod_{\mathfrak{q}} (d, L/K)_{\mathfrak{q}} = (d, L/K)_{\mathfrak{p}} \cdot (d, L/K)_{\mathfrak{p}_1} \cdot (d, L/K)_{\mathfrak{d}} = \sigma \cdot \sigma^{-1} \cdot (d, L/K)_{\mathfrak{d}},$$

so $(d, L/K)_{\mathfrak{d}} = 1$, meaning d is a norm from the extension $L_{\mathfrak{D}}/K_{\mathfrak{d}}$. But L/K is unramified at $\mathfrak{d}$, and d is a prime element at $\mathfrak{d}$, so $L_{\mathfrak{D}}/K_{\mathfrak{d}}$ must be trivial. Since $L = K(c^{1/l})$ this means $c \in (K_{\mathfrak{d}}^{\times})^{l}$.

As a final remark, note that we could have imposed additional conditions of the form

$$d \equiv 1 \bmod \mathfrak{q}_1,$$
$$\vdots$$
$$d \equiv 1 \bmod \mathfrak{q}_s$$

where $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ are primes distinct from $\mathfrak{p}$ and $\mathfrak{p}_1$, by imposing the same conditions on b and working in the generalized ideal class group $I(\mathfrak{f}\mathfrak{p}\mathfrak{p}_1\mathfrak{q}_1 \ldots \mathfrak{q}_s)/P_{\mathfrak{f}\mathfrak{p}\mathfrak{p}_1\mathfrak{q}_1 \ldots \mathfrak{q}_s}$.

In the function field case we are assuming $\chi(K) \neq l$ and that K contains the lth roots of 1. Choose some prime of K distinct from $\mathfrak{p}$, and designate it $\mathfrak{p}_\infty$. Form the ring

$$\mathfrak{R}_{\mathfrak{p}_\infty} = \bigcap_{\mathfrak{q} \neq \mathfrak{p}_\infty} \mathfrak{O}_{\mathfrak{q}}.$$

Let Ω be the class of $\mathfrak{p}$ in the generalized ideal class group $I/P_{(1),l}$, and using Proposition A, choose a prime $\mathfrak{p}_1 \neq \mathfrak{p}$ in the class Ω^{-1}. The remainder of the construction of c and d is the same as with number fields, but with $\mathfrak{p}_\infty$ replacing the

archimedean primes and the phrase "is in $(K_{\mathfrak{p}_\infty}^\times)^l$" substituted for "is totally positive". We need no longer worry about primes $\mathfrak{q}$ dividing l.

LEMMA 3. *Let all notations and assumptions be as above; then $R_l(t;\ c, d)$ is satisfied by precisely those t for which $\operatorname{ord}_{\mathfrak{p}}(t) = 0 \bmod l$ and $\operatorname{ord}_{\mathfrak{p}_1}(t) \equiv 0 \bmod l$.*

PROOF. Lemma 2 shows that only t of this form can satisfy $R_l(t;\ c, d)$. We will prove the converse only for number fields, as the proof in the function field case is analogous. Assuming t satisfies the conditions of the lemma, we must find a w such that

$$\exists \vec{a}_1 \exists \vec{a}_2 \exists \vec{a}_3 (w = N_l(d, \vec{a}_1) \& cw = N_l(cd, \vec{a}_2) \& t = N_l(w, \vec{a}_3)).$$

In fact, w can be taken to be a prime element of $\mathcal{O}_K$: suppose $(t) = \mathfrak{p}^{nl}\mathfrak{p}_1^{n_1 l}\mathfrak{q}_1^{k_1} \dots \mathfrak{q}_s^{k_s}$. By the remark, we can find a prime ideal $\mathfrak{w}$ with a generator w such that

$$\begin{aligned}
&w \text{ is totally positive,}^4\\
&w \equiv 1 \bmod \mathfrak{q}^m \text{ for all } \mathfrak{q}|l, \text{ so } w \in \left(K_{\mathfrak{q}}^\times\right)^l,\\
&w \equiv \xi_{\mathfrak{p}} \bmod \mathfrak{p},\\
&w \equiv \xi_{\mathfrak{p}_1} \bmod \mathfrak{p}_1,\\
&w \equiv 1 \bmod \mathfrak{d},\\
&w \equiv 1 \bmod \mathfrak{q}_i \text{ for } i = 1, \dots, s.
\end{aligned}$$

(Note that these conditions are all compatible.) For such a w:

(1) w is a norm from $K(d^{1/l})$.

By Hasse's Norm Theorem it is enough to verify this locally at every prime.

At archimedean primes:	$K_\infty(d^{1/l})/K_\infty$ is trivial.
At $\mathfrak{q}\|l$:	$K_{\mathfrak{q}}(d^{1/l})/K_{\mathfrak{q}}$ is trivial.
At $\mathfrak{d}$:	$w \equiv 1 \bmod \mathfrak{d}$, so $w \in (K_{\mathfrak{d}}^\times)^l$ is a norm ($\mathfrak{d} \nmid l$ so Hensel's Lemma applies to $x^l - \bar{w} = \bar{0}$).
At all other primes $\mathfrak{q}$ besides $\mathfrak{w}$ itself:	$\operatorname{ord}_{\mathfrak{q}}(w) = 0$ and $K(d^{1/l})/K$ is unramified at $\mathfrak{q}$, so w is a norm.

Hence by Artin's Reciprocity Law w is a norm at $\mathfrak{w}$ also.

(2) cw is a norm from $K((cd)^{1/l})$.

Locally:

At archimedean primes:	cd is totally positive since c and d are; therefore $K_\infty((cd)^{1/l})/K_\infty$ is trivial.
At $\mathfrak{q}\|l$:	$cd \in (K_{\mathfrak{q}}^\times)^l$ since c and d are, and again the extension is trivial.

[4] See footnote 3.

At $\mathfrak{p}$:	$w \equiv \xi_{\mathfrak{p}} \equiv d \bmod \mathfrak{p}$, so $w/d \equiv 1 \bmod \mathfrak{p}$ is a norm (since $\mathfrak{p} \nmid l$). But cd is a norm from $K_{\mathfrak{p}}((cd)^{1/l})/K_{\mathfrak{p}}$ so $cw = (cd)(w/d)$ is also.
At $\mathfrak{p}_1$:	similarly.
At $\mathfrak{d}$:	$w \equiv 1 \bmod \mathfrak{d}$, so $w \in (K_{\mathfrak{d}}^{\times})^l$ since $\mathfrak{d} \nmid l$. We showed that $c \in (K_{\mathfrak{d}}^{\times})^l$, so cw is an lth power and a norm.
At all other primes $\mathfrak{q}$ besides $\mathfrak{w}$:	$\operatorname{ord}_{\mathfrak{q}}(cw) = 0$ and $K((cd)^{1/l})$ is unramified, so cw is a norm.

And so, Artin's Reciprocity Law says cw is a norm at $\mathfrak{w}$.

(3) t is a norm from $K(w^{1/l})$.

Locally:

At archimedean primes:	w is a totally positive.
At $\mathfrak{q} \mid l$:	$w \in (K_{\mathfrak{q}}^{\times})^l$.
At $\mathfrak{p}$:	$w \equiv \xi_{\mathfrak{p}} \bmod \mathfrak{p}$, so w is a non-lth power unit in $K_{\mathfrak{p}}$, and $K_{\mathfrak{p}}(w^{1/l})/K_{\mathfrak{p}}$ is unramified of degree l. By Lemma 1 and the assumptions on t, t is a norm.
At $\mathfrak{p}_1$:	similarly.
At $\mathfrak{q}_1, \ldots, \mathfrak{q}_s \nmid l$:	$w \equiv 1 \bmod \mathfrak{q}_i$, so $w \in (K_{\mathfrak{q}_i}^{\times})^l$
At all other primes $\mathfrak{q}$ besides $\mathfrak{w}$:	$\operatorname{ord}_{\mathfrak{q}}(t) = 0$ and $K(w^{1/l})/K$ is unramified.

This only leaves $\mathfrak{w}$, so t is a norm there too. □

Recall now the remark made in constructing c that there were infinitely many choices for $\mathfrak{p}_1$. Carry out the construction of c and d for two different choices of $\mathfrak{p}_1$, obtaining c_1, d_1 and c_2, d_2, say. Then every $t \in K$ with $\operatorname{ord}_{\mathfrak{p}}(t) \equiv 0 \bmod l$ is a product of an element t_1 satisfying $R_l(t_1; c_1, d_1)$ and a t_2 satisfying $R_l(t_2; c_2, d_2)$. Hence (note that c_1 is a prime element for $\mathfrak{p}$), $\mathcal{O}_{\mathfrak{p}}$ is the set of x satisfying

$$S_l(x; c_1, d_1, c_2, d_2) \Leftrightarrow \exists t_1 \exists t_2 \big(1 + c_1 x^l = t_1 t_2 \& R_l(t_1; c_1, d_1) \& R_l(t_2; c_2, d_2)\big).$$

3. Rings of algebraic integers. Now we remove the special assumptions on K and $\mathfrak{p}$.

If K is a function field and $\chi(K) \neq 2$, then since ± 1 are always in K, the predicate $S_2(x; c_1, c_2, c_3, c_4)$ picks out each valuation ring of K, for an appropriate choice of $\vec{c}$. If $\chi(K) = 2$, we can take $l = 3$. Then, if $\omega^2 + \omega + 1 = 0$ has a root in K, $S_3(x; c_1, c_2, c_3, c_4)$ picks out the valuation rings. However, if there is no root, form the extension $K(\omega)$. Regarding $K(\omega)$ as a vector space over K with basis

$\{1, \omega\}$, we can write out $\vec{S}_3(\vec{x}; \vec{c}_1, \vec{c}_2, \vec{c}_3, \vec{c}_4)$ for $K(\omega)$, with $\vec{x} = (x, y)$ representing $x + y\omega$. Moreover, every valuation ring $\mathcal{O}_\mathfrak{p}$ of K is of the form $\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{P} \cap K$, where $\mathcal{O}_\mathfrak{P}$ is a valuation ring of $K(\omega)$ lying above $\mathcal{O}_\mathfrak{p}$, so $x \in \mathcal{O}_\mathfrak{p}$ iff $\vec{S}_3(x, 0; \vec{c}_1, \vec{c}_2, \vec{c}_3, \vec{c}_4)$ for a proper choice of the eight parameters.

If K is a number field and $\mathfrak{p} \nmid 2$, then $\mathcal{O}_\mathfrak{p}$ is picked out by $S_2(x; c_1, c_2, c_3, c_4)$. If $\mathfrak{p}|2$ and K contains the cube roots of 1, then $S_3(x; c_1, c_2, c_3, c_4)$ works, while if not, we can form $K(\omega)$ as above and $\mathcal{O}_\mathfrak{p}$ will be picked out by $\vec{S}_3(x, 0; \vec{c})$.[5]

Thus we have a collection of predicates which, for good choices of their parameters, define every valuation ring of every global field. We can control what happens with bad choices by using the well-known characterization of valuation rings:

THEOREM 1. *There is a finite collection of predicates such that*

(1) *For every valuation ring of every global field, there is some predicate and some choice of its parameters for which the predicate defines the valuation ring.*

(2) *For every choice of its parameters, each of the predicates is satisfied either by a valuation ring or the entire field.*

PROOF. Let $S(x; \vec{c})$ be any of the predicates discussed above. Suppressing its parameters, put

$$V(x; \vec{c}) \Leftrightarrow [\forall y \forall z((S(y) \& S(z)) \rightarrow (S(-y) \& S(y + z) \& S(yz))) \\ \& \forall y(y \neq 0 \rightarrow (S(y) \vee S(1/y)))] \rightarrow S(x).$$

The first clause of the hypothesis states that $S(x; \vec{c})$ is satisfied by a ring; the second requires the ring to be a valuation ring or all of K. If the hypothesis fails, $V(x; \vec{c})$ is of course satisfied by all of K. □

Call $\mathrm{Val}_2(x; \vec{c})$, $\mathrm{Val}_3(x; \vec{c})$, and $\overrightarrow{\mathrm{Val}}_3(x; \vec{c})$ the predicates produced from

$$S_2(x; \vec{c}), \quad S_3(x; \vec{c}) \quad \text{and} \quad \vec{S}_3(x; \vec{c}).$$

Further, define $\mathrm{Val}_F(x; c_1, \ldots, c_8)$ to be the exclusive disjunction of Val_2, Val_3, and $\overrightarrow{\mathrm{Val}}_3$ over the cases in the first paragraph of this section. Then, Val_F parametrizes all valuation rings of all algebraic function fields.

COROLLARY 1. *The exact constant field* $\mathbf{F}$ *of an algebraic function field* K *is definable by a predicate independent of* K.

PROOF. We can use $\mathrm{Const}(t) \Leftrightarrow \forall \vec{c} \mathrm{Val}_F(t; \vec{c})$ because $\mathbf{F} = \bigcap_\mathfrak{p} \mathcal{O}_\mathfrak{p}$. □

If K is a function field and $x \in K$ is not a constant, we will call the integral closure of $\mathbf{F}[x]$ in K an algebraic function ring, $\mathcal{O}_x$.

COROLLARY 2. *Every algebraic function ring* $\mathcal{O}_x$ *in a function field* K *is arithmetically definable in terms of* x.

PROOF. Consider the predicate

$$\mathrm{Ring}(t; x) \Leftrightarrow \forall \vec{c}(\mathrm{Val}_F(x; \vec{c}) \rightarrow \mathrm{Val}_F(t; \vec{c})).$$

[5] See footnote 3.

The integral closure of any ring in any field is the intersection of all the valuation rings containing it. □

In symbols this is $\mathcal{O}_x = \bigcap_{\mathrm{ord}_\mathfrak{p}(x)\geqslant 0} \mathcal{O}_\mathfrak{p} = R_S$ in the notation of §1, where $S = \{\mathfrak{p} | x \notin \mathcal{O}_\mathfrak{p}\}$ is finite. We remark that conversely every R_S for a finite nonempty S is of the form $\mathcal{O}_x$ for some x.

COROLLARY 3. *When K is a number field, its ring of integers $\mathcal{O}_K$ is arithmetically definable by a predicate independent of K.*

PROOF. Since $\mathcal{O}_K = \bigcap_\mathfrak{p} \mathcal{O}_\mathfrak{p}$, define

$$\mathrm{Int}(t) \Leftrightarrow \forall \vec{c}\,\mathrm{Val}_2(t; \vec{c}) \& \forall \vec{c}\,\mathrm{Val}_3(t; \vec{c}) \& \forall \vec{c}\,\overrightarrow{\mathrm{Val}_3}(t; \vec{c}). \quad \square$$

COROLLARY 4. *There is a sentence which is true in all function fields and false in all number fields.*

PROOF. The predicate $\forall \vec{c}\,\mathrm{Val}_2(t; \vec{c})$ defines the field of constants for any function field of characteristic not 2. On the other hand, when it is interpreted in a number field, it is satisfied by some ring $\mathcal{R}$ for which $\bigcap_{\mathfrak{p}|2} \mathcal{O}_\mathfrak{p} \subseteq \mathcal{R} \subseteq \mathcal{O}_K$. Especially, 3 is not a unit in $\mathcal{R}$. So, the statement

$$2 = 0 \vee 3 = 0 \vee \exists t(\forall \vec{c}\,\mathrm{Val}_2(t; \vec{c}) \& 3 \cdot t = 1)$$

will serve our purpose. □

4. The undecidability of global fields. For a function field we will show how, given a nonconstant $x \in K$, to define the polynomial ring $\mathbf{F}[x]$ in K. This means K is undecidable, by a result of Raphael Robinson in [**11**]; in our case his proof even yields a specific model for the natural numbers, given by the powers of x. For a number field, we show how to separate $\mathbf{N}$ from K.

It will be convenient to abbreviate the division predicates for function fields and number fields, respectively, as

$$k_1|_{F,x}k_2 \Leftrightarrow \exists h(\mathrm{Ring}(h; x) \& k_1 h = k_2)$$

and

$$k_1|_N k_2 \Leftrightarrow \exists h(\mathrm{Int}(h) \& k_1 h = k_2).$$

Note that k_1, k_2 need not be in the rings of integers, but if k_1 is, and the division predicate is true, then k_2 is also.

First consider the case when K is a function field; throughout, x will denote a fixed nonconstant element of K. The predicate we use is an adaptation of the one given by Julia Robinson in [**10**]. The idea is to find a predicate satisfied by arbitrary finite subsets of K, and then by means of an inductive definition to describe $\mathbf{F}[x]$ as those elements lying on the "edges" of certain finite subsets.

LEMMA 4. *The predicate*

$$D(t; g_1, g_2) \Leftrightarrow \forall \vec{c}\left(\mathrm{Val}_F\left(tg_1^{-1}; \vec{c}\right) \vee \mathrm{Val}_F\left(tg_2^{-1}; \vec{c}\right)\right)$$

is satisfied by a finite subset of K for every nonzero choice of g_1, g_2; and g_1, g_2 can be chosen so that any given finite subset is contained in the set of elements satisfying it.

PROOF. This is really a statement about the adele ring of K. Since $\mathbf{F}$ is finite, the adele ring $K_{\mathbf{A}}$ is locally compact, that is, if $\mathfrak{a}$ is a given adele, the set $D(\mathfrak{a}) = \{\mathfrak{b} \in K_{\mathbf{A}} | \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}_{\mathfrak{p}}) \geqslant \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}_{\mathfrak{p}})$ for all $\mathfrak{p}\}$ is compact. On the other hand, K is discrete in $K_{\mathbf{A}}$, so $K \cap D(\mathfrak{a})$ is finite. These facts about adele rings are proved in [**15**, Chapter 4].

Here we are using $\mathfrak{a}$ defined by

$$\mathfrak{a}_{\mathfrak{p}} = \begin{cases} g_1 & \text{if } \mathrm{ord}_{\mathfrak{p}}(g_1) \leqslant \mathrm{ord}_{\mathfrak{p}}(g_2), \\ g_2 & \text{if } \mathrm{ord}_{\mathfrak{p}}(g_1) > \mathrm{ord}_{\mathfrak{p}}(g_2). \end{cases}$$

If a finite subset $\{b_1, b_2, \ldots, b_n\}$ of K is given, first choose g_1 so that $\mathrm{ord}_{\mathfrak{p}}(g_1) \leqslant \min\{\mathrm{ord}_{\mathfrak{p}}(b_i)\}$ at all $\mathfrak{p}$ where any $\mathrm{ord}_{\mathfrak{p}}(b_i) < 0$, and then choose g_2 so that $\mathrm{ord}_{\mathfrak{p}}(g_2) = 0$ at all $\mathfrak{p}$ where $\mathrm{ord}_{\mathfrak{p}}(g_1) > 0$. □

LEMMA 5. *There is a predicate* $\mathrm{Set}_F(t; \vec{g}; x)$ *which quantifies over finite subsets of function fields.*

PROOF. We mean that for all values of its parameters Set_F is satisfied by some finite set of t's, and for every finite set there is a choice of the parameters which yields that set. Let B be a nonempty finite subset of K. The claim is that there are $g_1, \ldots, g_5$ in K such that

$$\mathrm{Set}_F(t; \vec{g}; x) \Leftrightarrow D(t; g_1, g_2) \& (1 + (t - g_3)g_4|_{F,x}g_5)$$

is satisfied by exactly the $t \in B$. g_3 merely translates B; taking $g_3 \in B$, we can ignore it in the predicate, and assume $0 \in B$.

Choose g_1, g_2 as in Lemma 4 for this new B, and let C be the set of all $t \in K$ satisfying $D(t; g_1, g_2)$; C is a finite subset of K containing B. The second condition in the predicate is designed to separate B from C. We want to choose g_4 so that:

(1) $tg_4 \in \mathcal{O}_x$ for all $t \in C$.

(2) The quantities $1 + tg_4$ for all $t \in C$ are pairwise relatively prime elements of $\mathcal{O}_x$.

(3) The only $t \in C$ for which $1 + tg_4$ is a unit of $\mathcal{O}_x$, is $t = 0$.

The first two conditions will be satisfied by any $g_4 \in \mathcal{O}_x$ divisible to a sufficiently high power by all primes of $\mathcal{O}_x$ occurring in the factorizations of the nonzero fractional ideals (t) and $(t_i - t_j)$ for $t, t_i, t_j \in C$. For if s is such an element, and some prime $\mathfrak{p}$ of $\mathcal{O}_x$ divides $1 + st_i$ and $1 + st_j$, then $\mathfrak{p}|s(t_i - t_j)$, so $\mathfrak{p}|st_i$ by construction, so $\mathfrak{p}|1$, a contradiction.

Fix such a nonzero s. We will take $g_4 = sr$ for a suitably chosen r. Now, $1 + tsr$ is a unit in $\mathcal{O}_x$ iff its norm to $\mathbf{F}[x]$ is a unit, and the only units in $\mathbf{F}[x]$ are the constants in $\mathbf{F}^{\times}$. Because $\mathbf{F}(x)$ is the ground field, the product

$$P(r) = \prod_{\substack{t \in C \\ t \neq 0}} \prod_{f \in \mathbf{F}} (N_{K/\mathbf{F}(x)}(1 + tsr) - f), \quad \text{for } r \in \mathbf{F}[x],$$

is a polynomial in r, and it is clearly not the zero polynomial. Moreover, $P(r) = 0$ iff for some nonzero $t \in C$, $1 + tsr$ is either 0 or a unit of $\mathcal{O}_x$. Since $\mathbf{F}[x]$ is an infinite ring, there is an r in it for which $P(r) \neq 0$. Set $g_4 = sr$, and put

$$g_5 = \prod_{t \in B} (1 + tg_4). \quad \square$$

THEOREM 2. *Let K be an algebraic function field, $\mathbf{F}$ its exact field of constants, and x a nonconstant element of K. Then, the polynomial ring $\mathbf{F}[x]$ is arithmetically definable in terms of x by a predicate independent of K.*

PROOF. Specifically, suppressing the parameters $\vec{g}$ and x of Set_F,

$$t \in \mathbf{F}[x] \text{ iff } \mathrm{Poly}(t; x)$$

$$\Leftrightarrow t = 0 \vee \big[\mathrm{Ring}(t; x) \& \exists \vec{g}\{ g_1 \neq 0 \& g_2 \neq 0 \& \mathrm{Set}_F$$

$$\& \forall a\big[\mathrm{Set}_F(a) \rightarrow (\mathrm{Set}_F(xa) \vee \exists d(\mathrm{Const}(d) \& \mathrm{Set}_F(xa - dxt)))\big]\}\big]. \tag{1}$$

First suppose $t \in \mathbf{F}[x]$, $t \neq 0$. Let B be the set of all polynomials in $\mathbf{F}[x]$ with degree less than or equal to $\deg(t)$. If g_1, g_2, g_3, g_4, g_5 are chosen for this B as in Lemma 5, one checks easily that the right side is satisfied.

Conversely, suppose the right side is satisfied by some nonzero t, for a particular $\vec{g}$, so $t \in \mathcal{O}_x$. Let B be the set of all b satisfying $\mathrm{Set}_F(b; \vec{g}, x)$. From Lemma 4, B is a finite set, and the hypotheses require $1 \in B$. For each nonzero $b \in B$ there is an $m > 0$ and a constant $d \neq 0$ such that $\neg \mathrm{Set}_F(x^m b; \vec{g}, x)$ but $\mathrm{Set}_F(x^m b - dxt; \vec{g}, x)$. Define the least such m to be $m(b)$ and let a corresponding d be $d(b)$. Then, recursively, put

$$\begin{aligned} b_0 &= 1 && = 1 + (0)t \\ b_1 &= b_0 x^{m(b_0)} - d(b_0)xt && = q_1(x) + r_1(x)t \\ &\vdots \\ b_i &= b_{i-1} x^{m(b_{i-1})} - d(b_{i-1})xt && = q_i(x) + r_i(x)t \end{aligned}$$

stopping only if some $b_i = 0$. Inductively $q_i(x)$ and $r_i(x)$ are polynomials in x, with

$$\deg(q_i(x)) = \sum_{v=0}^{i-1} m(b_v) \quad \text{and} \quad \deg(r_i(x)) = 1 + \sum_{v=1}^{i-1} m(b_v)$$

for $i \geqslant 1$. This means, if $i > j$, then $r_i(x) - r_j(x) \neq 0$. If some $b_i = 0$, then $t = -q_i(x)/r_i(x)$; otherwise, since B is finite there will be two indices $i > j$ with $b_i = b_j$. Solving for t, one obtains $t = -(q_i(x) - q_j(x))/(r_i(x) - r_j(x))$.

If $r_i(x) | q_i(x)$ or if $(r_i(x) - r_j(x)) | (q_i(x) - q_j(x))$, then t is a polynomial. But if not, then t would have some irreducible polynomial of $\mathbf{F}[x]$ in its denominator, and so could not lie in $\mathcal{O}_x$, a contradiction. □

For the convenience of the reader, and for our own future use, we recall Raphael Robinson's construction of a model of $\mathbf{N}$ in $\mathbf{F}[x]$ using the powers of x. He observes first, that a polynomial in a constant multiple of a power of x if and only if x is the only irreducible polynomial dividing it, and second, for a constant d, $x - 1 | dx^n - 1$ if and only if $d = 1$. Thus we have

$$\mathrm{Mtple}(t; x) \Leftrightarrow \mathrm{Poly}(t; x) \& t \neq 0 \& \forall y((\mathrm{Poly}(y; x) \& y | t) \rightarrow (y | 1 \vee x | y)),$$

$$\mathrm{Power}(t; x) \Leftrightarrow \mathrm{Mtple}(t; x) \& (x - 1) | (t - 1)$$

and $t \in \{1, x, x^2, \dots\}$ iff Power(t; x). Addition in the model comes from multiplication in K; to define multiplication in the model, use the fact that multiplication in the natural numbers can be described in terms of addition and divisibility by the formulas

$$n = r(r+1) \Leftrightarrow \forall m(n|m \leftrightarrow (r|m \& r+1|m)),$$
$$n = rs \Leftrightarrow (r+s)(r+s+1) = r(r+1) + s(s+1) + n + n.$$

For divisibility in the model, note that $x^m - 1 | x^n - 1$ iff $m|n$.

Now suppose K is a number field. If the archimedean valuations of K were available as well as the nonarchimedean ones, we could define a predicate quantifying over finite subsets of K in the same way as in Lemmas 4 and 5, and in turn define **N**. For totally real fields this can actually be done (see §6).

However, in any case Julia Robinson has shown [**8**] that there is a uniform way of defining the natural numbers in the ring of integers of a number field. Her results may be formulated as follows.

LEMMA 6. *There is a predicate,* $\mathrm{Set}_N(t, g_1, \dots, g_5)$, *which quantifies over finite subsets of number fields.*

PROOF. We can take

$$\begin{aligned}\mathrm{Set}_N(t; \vec{g}) \Leftrightarrow & \left[g_2 \neq 0 \& \mathrm{Int}((t - g_1)g_2) \& \mathrm{Int}(g_4) \right] \\ & \& \left[g_3 \neq 0 \& (t - g_1)g_2((t - g_1)g_2 + 1) |_N g_3 \right] \\ & \& \left[(1 + (t - g_1)g_2 g_4) |_N g_5 \right].\end{aligned}$$

The fact that for a given choice of $\vec{g}$ only finitely many t can satisfy $\mathrm{Set}_N(t, \vec{g})$, is based on a result of Siegel [**16**, pp. 204–205]: "Let t be a positive number. Given a polynomial $f(x)$ with coefficients in $\mathcal{O}_K$ and at least two distinct roots, then there are only finitely many $x \in \mathcal{O}_K$ such that $|N_{K/\mathbf{Q}}(f(x))| < t$." Here $f(x) = x(x+1)$, and we have replaced x by $(t - g_1)g_2$; $f(x)|_N y$ is equivalent to $|N_{K/\mathbf{Q}}(f(x))| < |N_{K/\mathbf{Q}}(y)|$. On the other hand, given a finite set B in K, g_1, g_2, and g_3 can be chosen so that B is contained in the finite set satisfying the first two clauses, and then g_4 and g_5 chosen to separate B from the remainder of this set, as in Lemma 5. □

THEOREM 3. *Let K be a number field. Then* **N** *can be arithmetically defined in K by a predicate independent of K.*

PROOF. Let

$$\mathrm{Nat}(n) \Leftrightarrow \exists \vec{g} \left\{ \mathrm{Set}_N(0, \vec{g}) \& \forall t \left[\mathrm{Set}_N(t, \vec{g}) \rightarrow (t = n \vee \mathrm{Set}_N(t+1, \vec{g})) \right] \right\}.$$

We find that every $n \in \mathbf{N}$ satisfies Nat(n) by choosing $\vec{g}$ so that exactly $\{0, 1, \dots, n\}$ satisfies $\mathrm{Set}_N(t, \vec{g})$; on the other hand, the inductive form of the definition implies that only elements of **N** can satisfy it. □

Combining Theorems 2 and 3 and Corollary 4, we see that any statement about natural numbers can be formulated in the theory of global fields.

THEOREM 4. *The elementary theory of global fields is essentially undecidable.*

5. Gödel functions. Given the preceding results, it is natural to ask which functions and predicates are arithmetically definable in the theory of global fields. It will soon become evident that the theory is very strong, and almost any object of number-theoretic interest can be defined. The reason for this is of course the coding power of the natural numbers.

For number fields we will be interested in defining functions and predicates of the type $f(v_1, \ldots, v_k; n_1, \ldots, n_l)$ where the v_i range over K and the n_i range over $\mathbf{N}$. In function fields there is no uniquely determined model of $\mathbf{N}$ but rather a collection of equivalent ones, so our functions and predicates must be specified in the form $f(v_1, \ldots, v_k; x^{n_1}, \ldots, x^{n_l}; x)$ where the last x indicates that $\{1, x, x^2, \ldots\}$ is the model of $\mathbf{N}$ under consideration. For convenience of notation we will write $f(v_1, \ldots, v_k; n_1, \ldots, n_l)$ for both, it being understood that there are always two separate cases, and the n_i are in the model of $\mathbf{N}$ at hand.

LEMMA 7. *There is a function, $F(\vec{g}; n)$, arithmetically definable in the theory of number fields (respectively, $F(\vec{g}; x^n; x)$ in the theory of function fields) such that for all $\vec{g}$, $F(\vec{g}; 0) = m$ for some $m \in \mathbf{N}$, and for any finite sequence $k_1, \ldots, k_n$ of elements of K there is some $\vec{g}$ such that*

$$F(\vec{g}; 0) = n \quad \text{and} \quad F(\vec{g}; i) = k_i$$

for $i = 1, \ldots, n$.

PROOF. Let $\beta(a, i)$ be a standard Gödel function as defined, for example, in Shoenfield [**14**, p. 115], so that for all finite sequences $m_1, m_2, \ldots, m_n$ there is some a such that

$$\beta(a, 0) = n \quad \text{and} \quad \beta(a, i) = m_i$$

for $i = 1, \ldots, n$. The idea is to sharpen the arguments in Lemmas 5 and 6 so that not only finite sets, but finite sequences, can be distinguished, and then parametrize them with the standard Gödel function.

Case I. Function fields. Let $\mathrm{Set}_F(t; g_1, \ldots, g_5, x)$ be the predicate of Lemma 5, and choose g as in that lemma for the set $\{k_j\}$. We may assume $0 \notin \{k_j\}$ after translating it by a suitable element g_6 of K which will appear as one of the parameters of F. Our intention is to show that there are $h_1, \ldots, h_n$ of the form $x^{2m_i} - x^{m_i}$ such that:

(1) The quantities $1 + h_i k_j$ are all in $\mathcal{O}_x$.

(2) For all i_1, i_2 and for distinct k_{j_1}, k_{j_2} the $1 + h_{i_1} k_{j_1}$, $1 + h_{i_2} k_{j_2}$ are pairwise relatively prime.

(3) No $1 + h_i k_j$ is a unit of $\mathcal{O}_x$.

Each of the h_i will depend on the preceding ones; we first construct h_1. As in the proof of Lemma 5, if s is any element of $\mathcal{O}_x$ which is sufficiently divisible by all primes of $\mathcal{O}_x$ occurring in the factorizations of the ideals (k_i) and $(k_i - k_j)$ then the $1 + sk_j$ will be in $\mathcal{O}_x$ and will be pairwise relatively prime. Since every prime of $\mathcal{O}_x$ overlies one of $\mathbf{F}_p[x]$, s can be chosen to be in $\mathbf{F}_p[x]$. (Here $p = \chi(K)$.)

But every polynomial in $\mathbf{F}_p[x]$ divides infinitely many polynomials of the form $x^{2m} - x^m$. To see this, note first that if d is a common divisor of the degrees of the

irreducible polynomials $r_1(x), \ldots, r_v(x)$ then $r_1(x), \ldots, r_v(x) | x^{p^d} - x$. And second, if $q(x)$ is any polynomial in $\mathbf{F}_p[x]$, then $q(x^{p^e}) = (q(x))^{p^e}$.

It remains to show that we can choose h_1 of the form $x^{2m} - x^m$ so that the $1 + h_1 k_j$ are nonunits as well as being pairwise relatively prime. Examining the proof of Lemma 5, we must find r, $s \in \mathbf{F}_p[x]$ and an m such that $rs = x^{2m} - x^m$ and $P(r) \neq 0$. But this is clearly possible since $P(r)$ has only finitely many roots. Picking such an r, with its corresponding m, set $m_1 = m$ and $h_1 = x^{2m_1} - x^{m_1}$.

In choosing h_2 we want the $1 + h_2 k_j$ to be pairwise relatively prime, and also pairwise relatively prime with all the $1 + h_1 k_j$. This will be the case when h_2 is sufficiently divisible by all the primes appearing in (h_1), the (k_i), and the $(k_i - k_j)$. Thus, we can recursively find $h_2 = x^{2m_2} - x^{m_2}$, $h_3 = x^{2m_3} - x^{m_3}$, and so on.

Finally, let $g_7 = \prod_{i=1}^{n}(1 + h_i k_i)$. An element k of K satisfies

$$\mathrm{Set}_F(k; g_1, \ldots, g_5, x) \& 1 + h_i k \mid g_7$$

iff $k = k_i$. Note that in this case, $\beta(a, i) = m_i$ is an abbreviation for $\beta(x^a, x^i, x) = x^{m_i}$. Then,

$$F(g_1, \ldots, g_8; i) = \begin{cases} \beta(a, 0) & \text{if } g_8 = x^a \text{ for some } a, \text{ and } i = 0, \\ k & \text{if } g_8 = x^a \text{ for some } a,\ i > 0, \\ & \text{and there is exactly one } k \in K \\ & \text{satisfying } \mathrm{Set}_F(k; g_1, \ldots, g_5, x) \& \\ & \left[1 + (k - g_6)\left(\beta(a, i)^2 - \beta(a, i)\right)\right]\big|_{F, x g_7} \\ 0 & \text{otherwise,} \end{cases}$$

will be the Gödel function we want.

Case II. Number fields. The construction here is based on the predicate $\mathrm{Set}_N(t; g_1, \ldots, g_5)$ of Lemma 6. It is similar to, and simpler than, the one in the function field case, with the polynomials $x^{2m} - x^m$ replaced by elements of $\mathbf{N}$. □

One consequence of this lemma is that inductive definitions are possible: for example,

$$\omega^i = H(\omega; i) = \begin{cases} 1 & \text{if } i = 0, \\ v & \text{if } i > 0 \text{ and } \exists \vec{g}\big[F(\vec{g}; 1) = \omega \& F(\vec{g}; i) = v \\ & \quad \& \ \forall k(1 < k \leqslant i) \to F(\vec{g}; k) = \omega \cdot F(\vec{g}; k - 1)\big]. \end{cases}$$

Rather than prove a general theorem, we give further examples. Suppose K is a number field. Then, the definability of each of the following is a consequence of that of its predecessors:

(1) the function $P(\vec{g}, \omega; m) = \sum_{i=0}^{m} F(\vec{g}; i + 1)\omega^i$,

(2) the degree and coefficients of the minimal polynomial for ω over $\mathbf{Q}$,

(3) the degree of the extension $K/\mathbf{Q}$,

(4) the different and discriminant of $K/\mathbf{Q}$,

(5) the statement that p is a prime of $\mathbf{Q}$ ramified in K.

For function fields note that there is a natural surjective map $M(x^n; x)$ from $\{1, x, x^2, \ldots\}$ onto $\mathbf{F}_p[x]$, such that $1 = x^0$ goes to 0, and if $n = \prod_{i=1}^{m} p_i^{n_i}$ where p_i is the ith prime number, then $x^n \to \sum_{i=0}^{m-1} n_{i+1} x^i$ for $n > 0$. The definability of this map is left as an exercise.

With the Gödel functions of Lemma 7, different parameters $\vec{g}$ *from* K are required to encode each finite sequence of elements of K. In some situations it is desirable to have a function which codes sequences in K using only parameters of $\mathbf{N}$. Now in general, if F is a subfield of K it is not possible to code elements of K using parameters from F, because K may have nontrivial autmorphisms over F. (Indeed, a theorem of Raphael Robinson in [12] asserts that an element of K is definable using parameters of F if and only if it is invariant under $\mathrm{Gal}(K/F)$.) However, this is the only limitation:

COROLLARY 5 (STRONG GÖDEL FUNCTIONS). *There is a function* $G(\omega; m, n)$ *such that for any number field* K *and any* $\omega \in K$, $G(\omega; m, n)$ *encodes all finite sequences of* $\mathbf{Q}(\omega)$. *Similarly, for function fields there is a function* $G(\omega; x^m, x^n; x)$ *which encodes all finite sequences of* $\mathbf{F}_p(x, \omega)$.

The proof is an easy exercise in Gödel coding. In the number field case the idea is to construct a surjective map from $\mathbf{N}$ to $\mathbf{Q}(\omega)$, and compose it with a standard Gödel function. The map from $\mathbf{N}$ to $\mathbf{Q}(\omega)$ can be formed by first encoding a map of $\mathbf{N}$ onto $\mathbf{Q}$, and then encoding finite sums $\sum_{i=0}^{n} b_i \omega^i$ using the Gödel function of Lemma 7. The function field case is similar, and uses the mapping $M(x^n, x)$ discussed above. If x is such that K is separable over $\mathbf{F}_p(x)$, then there will be an ω with $K = \mathbf{F}_p(x, \omega)$; and there always exists such x.

6. Archimedean valuations. In this section we provide arithmetic definitions for the archimedean valuations of a number field. The method we used previously to define the nonarchimedean valuations can be extended to give the real archimedean ones, but in the case of complex valuations it fails, essentially because there are no nontrivial extensions of $\mathbf{C}$ from which to take norms. The definition we do give for the complex valuations depends heavily on the fact that the rational numbers are already available. It would be desirable to have an independent definition, for using it we could obtain a predicate quantifying over finite subsets of number fields similar to the one in function fields, and define $\mathbf{N}$ without using the result of Siegel.

By a definition of an archimedean valuation of K (or of an embedding of K into $\mathbf{R}$ or $\mathbf{C}$ which induces it) we mean a predicate which is satisfied by precisely the closed unit ball of that valuation. Such a predicate evidently enables us to compare magnitudes of elements.

The unit ball and the ordering induced on K under a real embedding can easily be defined in terms of each other, and the set of nonnegative elements under any real embedding can be obtained directly, using

PROPOSITION E (HASSE-MINKOWSKI). *A quadratic form with coefficients in a number field K represents* 0 *in K iff it represents* 0 *in all completions of K.*[6] *Moreover*

(1) *Every quadratic form in five or more variables represents* 0 *in a nonarchimedean completion.*

(2) *Every quadratic form in two or more variables represents* 0 *in* $\mathbf{C}$.

(3) *A quadratic form represents* 0 *in* $\mathbf{R}$ *iff it is indefinite.*

Proof is given in [**6**, §66].

Fix a real embedding of K, and pick any $a \in K$ which is positive under that embedding and negative under all the other real embeddings. Then the predicate

$$R_\infty(x; a) \Leftrightarrow \exists v_1 \ldots \exists v_5 (0 = av_1^2 + v_2^2 + v_3^2 + v_4^2 - xv_5^2)$$

is satisfied by precisely those $x \in K$ which are nonnegative under our chosen embedding: the quadratic form on the right automatically represents 0 in nonarchimedean and complex archimedean completions of K, and by our choice of a it is indefinite at all real completions except the fixed one. It is indefinite there if and only if x is positive; and when $x = 0$ of course $R_\infty(x; a)$ is also trivially satisfied.

For general a, $R_\infty(x; a)$ is satisfied by 0 and by those x which are positive at real embeddings where a is positive. So the predicate

$$\mathrm{Re}(x; a) \Leftrightarrow [\forall y (R_\infty(y; a) \vee R_\infty(-y; a)) \to R_\infty(x; a)]$$

is satisfied either by all of K or by the set of nonnegative elements under some embedding of K into $\mathbf{R}$.

Now we turn to the complex archimedean valuations of K. We may assume that $\sqrt{-1} \in K$; if not, it can be adjoined and the complex embeddings of K will be obtained as restrictions of those of $K(\sqrt{-1})$. In this situation K is totally complex, so $K \otimes_{\mathbf{Q}} \mathbf{R}$ is isomorphic as an algebra to $\mathbf{C}^{r_2}$, where $2r_2 = [K\colon \mathbf{Q}]$. Fixing an isomorphism between them, we obtain a dense embedding

$$\Phi\colon K \to K \otimes 1 \to K \otimes \mathbf{R} \xrightarrow{\theta} \mathbf{C}^{r_2}.$$

Thus, $\Phi(k) = (\varphi_1(k), \varphi_2(k), \ldots, \varphi_{r_2}(k))$ where the φ_j and their complex conjugates give all embeddings of K into $\mathbf{C}$. Fix a square root of -1 in K and designate it i; we can assume θ has been chosen so that $\mathrm{Im}(\varphi_j(i)) > 0$ for $j = 1, \ldots, r_2$.

Our procedure for defining the complex valuations has three steps. First we prove a geometric lemma showing how a certain type of cone contained in an "upper half-space" of $\mathbf{C}^{r_2}$ can be manipulated to give the closed unit ball of a valuation. Then we generate these cones and many others using the recursive coding of §5. Finally, we characterize those sets which are the closed unit ball of an archimedean valuation.

To begin, for each $j = 1, \ldots, r_2$, define

$$H_j = \{\vec{z} \in \mathbf{C}^{r_2} | \mathrm{Im}(z_j) > 0\},$$

$$B_j = \{\vec{z} \in \mathbf{C}^{r_2} | \, |z_j| \leqslant 1\},$$

$$\partial B_j = \{\vec{z} \in \mathbf{C}^{r_2} | \, |z_j| = 1\},$$

[6] A form $\sum c_{ij} x_i x_j$ is said to represent 0 in a field if there are numbers b_i, $i = 1, \ldots, n$, in the field, *not all* 0, such that $\sum c_{ij} b_i b_j = 0$.

and for $\zeta \in \mathbf{C}$ with $|\zeta| = 1$, put

$$\partial B_j(\zeta) = \{\vec{z} \in \mathbf{C}^{r_2} | z_j = \zeta\}.$$

H_j is what was referred to above as an upper half-space; $\Phi^{-1}(\Phi(K) \cap B_j)$ is the closed unit ball of the embedding φ_j. Further, when $d, h > 0$ define a "strip" $\mathrm{Str}_j(d, h)$ by

$$\mathrm{Str}_j(d, h) = \{\vec{z} \in \mathbf{C}^{r_2} | \ |z_k| < d \text{ if } k \neq j;\ |\mathrm{Re}(z_j)| < d,\ \mathrm{Im}(z_j) > h\},$$

and for $a > 0$ define $C_j(a)$ to be the cone spanned by $\mathrm{Str}_j(a, 1)$, that is,

$$C_j(a) = \{r \cdot \vec{z} | r \in \mathbf{R}, r > 0, \vec{z} \in \mathrm{Str}_j(a, 1)\}$$

$$= \bigcup_{r>0} \mathrm{Str}_j(ra, r). \tag{1}$$

LEMMA 8. *Suppose that for some $a > 1$, a subset S_j of K can be defined such that*

$$C_j(a) \cap \Phi(K) \subset \Phi(S_j) \subset H_j \cap \Phi(K).$$

Then the closed unit ball of the embedding φ_j: $K \to \mathbf{C}$ can also be defined.

PROOF. The proof consists of applying linear fractional transformations and taking unions of sets constructed from S_j. A linear fractional transformation T on K gives rise in a natural way to a mapping $\vec{T}$: $\mathbf{C}^{r_2} \to \mathbf{C}^{r_2}$. In terms of coordinates, if $T(k) = (ak + b)/(ck + d)$ with $a, b, c, d \in K$, put

$$T_j(z_j) = (\varphi_j(a)z_j + \varphi_j(b))/(\varphi_j(c)z_j + \varphi_j(d));$$

then

$$\vec{T}(\vec{z}) = (T_1(z_1), \ldots, T_{r_2}(z_{r_2})). \tag{2}$$

(The domains of T and $\vec{T}$ are taken to be the points where they are defined.) For $k \in K$, $\Phi(T(k)) = \vec{T}(\Phi(k))$. But more importantly, since T is a linear fractional transformation, if V is any subset of $\mathbf{C}^{r_2}$ then $\vec{T}(V \cap \Phi(K)) = \vec{T}(V) \cap \Phi(K)$. Similarly for unions: if $\{V_\alpha\}$ is a collection of subsets of $\mathbf{C}^{r_2}$, then $\bigcup(V_\alpha \cap \Phi(K)) = (\bigcup V_\alpha) \cap \Phi(K)$. Hence we can view our operations as acting either in K or in $\mathbf{C}^{r_2}$. We are really interested in them on K, but their interpretation comes best from the picture in $\mathbf{C}^{r_2}$.

We assert the following predicates lead from S_j to the closed unit ball:

$$P_1(z) \Leftrightarrow \exists w(w \in S_j \& (w + i)z = -iw - 1),$$

$$P_2(z) \Leftrightarrow \exists u \exists q(P_1(u) \& q \in \mathbf{Q} \& (1 + qi)u = (1 - qi)z),$$

$$P_3(z) \Leftrightarrow \exists u \exists q(P_2(u) \& q \in \mathbf{Q} \& 0 \leqslant q \leqslant 1 \& z = qu),$$

$$\mathrm{Ball}(z) \Leftrightarrow \forall k(k \neq 2 \to \exists r \exists s(P_3(r) \& P_3(s) \& z + kr = s)).$$

By hypothesis, S_j can be defined, and $\sqrt{-1} \in K$. Since $a > 1$, i is distinguished from $-i$ as being the unique square root of -1 in S_j. $\mathbf{Q}$ and its ordering $\leqslant$ can be defined by earlier results. Hence these predicates can be expressed formally. Their interpretation is as follows: consider the linear fractional transformation

$$T(w) = -(iw + 1)/(w + i).$$

Because of our normalization of θ, each $T_j(w_j)$ interchanges the upper half-plane and the unit disc. Thus $\vec{T}(H_j) \subset B_j$, and especially $\vec{T}(\Phi(S)) \subset B_j$.

A strip $\mathrm{Str}_j(ra, r)$ is a product of sets shown on the left side of Figure 1, so by formula (2) its image under $\vec{T}$ will be a product of sets on the right side, a wedge touching $-i$ in the jth coordinate and the exterior of a disc containing $-i$ at the other coordinates. For large r the radii of the omitted discs shrink to 0. In addition, $\vec{T}$ is an open map, so the image of $\mathrm{Str}_j(ra, r)$ is open.

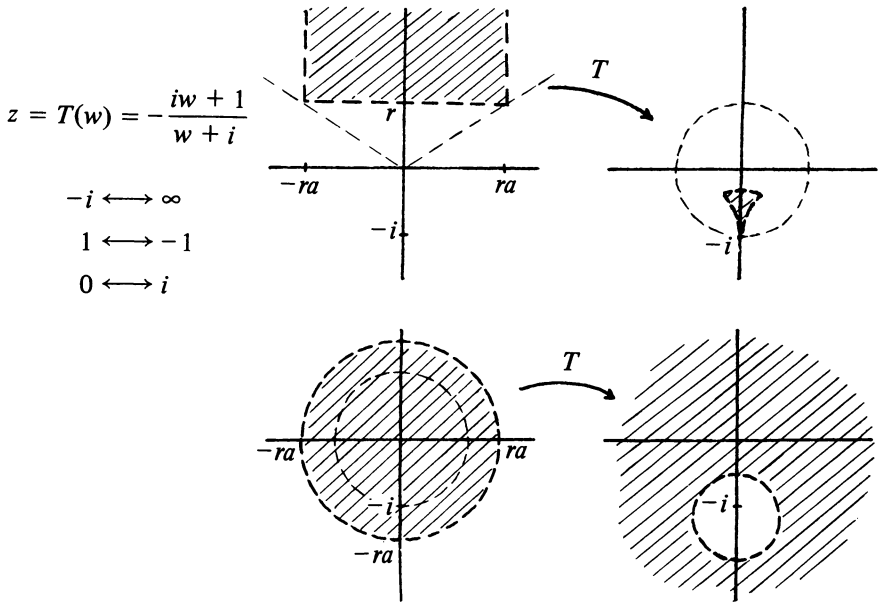

FIGURE 1

Let

$$\tilde{P}_1 = \vec{T}(C_j(a)).$$

By formula (1), $\tilde{P}_1$ is an open set contained in B_j with $\partial B_j(-i)$ in its closure. The numbers $(1 + qi)/(1 - qi)$ for $q \in \mathbf{Q}$ are dense in the unit circle for each embedding of K into $\mathbf{C}$, so

$$\tilde{P}_2 = \bigcup_{q \in \mathbf{Q}} \Phi\left(\frac{1 + qi}{1 - qi}\right) \cdot \tilde{P}_1$$

is an open set contained in B_j with the entire boundary ∂B_j in its closure. Finally, the points of B_j with nonzero jth coordinate are dense in B_j, and each of them generates a ray from the origin which intersects ∂B_j. $\tilde{P}_2$ contains points arbitrarily close to this intersection. Therefore,

$$\tilde{P}_3 = \{r \cdot u | r \in \mathbf{R}, 0 < r < 1, u \in \tilde{P}_2\} = \bigcup_{\substack{0 < q < 1 \\ q \in \mathbf{Q}}} q\tilde{P}_2$$

is open and dense in B_j.

When carried out in K, these steps yield a set whose image under Φ is dense in B_j, and is open in the relative topology induced on $\Phi(K)$ from $\mathbf{C}^{r_2}$. Ball(z) effects the closure operation. □

If S_j is only defined in terms of parameters, the lemma leads to a definition of the closed unit ball relative to those parameters. Such a set S_{r_2} will be given, for example, by the convex hull of $2r_2$ elements of K whose images under Φ approximate closely enough the vectors

$$\vec{v}_1 = \left(1, 0, 0, \ldots, \frac{i}{4r_2a}\right) \qquad \vec{w}_1 = \left(i, 0, \ldots, 0, \frac{i}{4r_2a}\right)$$

$$\vdots \qquad\qquad \vdots$$

$$\vec{v}_{r_2-1} = \left(0, 0, \ldots, 1, \frac{i}{4r_2a}\right) \qquad \vec{w}_{r_2-1} = \left(0, 0, \ldots, i, \frac{i}{4r_2a}\right)$$

$$\vec{v}_{r_2} = \left(0, \ldots, 0, 1 + \frac{i}{4r_2a}\right), \qquad \vec{w}_{r_2} = \left(-1 + i, \ldots, -1 + i, -1 + \frac{i}{4r_2a}\right).$$

It is clear from §5 that the predicate $S(s; \omega, m, n)$, which is to be satisfied by

$$\left\{ x = \sum_{j=1}^{n} q_j\omega_j | q_j \in \mathbf{Q}, q_j > 0, \omega_j = G(\omega; m, j) \text{ for } j = 1, \ldots, n \right\},$$

where $G(\omega; m, n)$ is the strong Gödel function of Corollary 5, can be defined. As ω, m, n run through all possible values it is satisfied by cones which give rise to all closed unit balls.

It remains to characterize closed unit balls among all subsets of K. In the following, we use multiplicative valuations.

THEOREM 5. *Suppose K is a number field and B is a subset of K. Then, B is the closed unit ball for some archimedean valuation λ of K (that is, $B(x)$ iff $x \in \{k \in K | \lambda(k) \leqslant 1\}$) if and only if*

(1) $\forall x \forall y[(B(x) \& B(y)) \rightarrow (B((x + y)/2) \& B(xy))]$,

(2) $\forall x[x = 0 \vee B(x) \vee B(1/x)]$,

(3) $\neg B(2) \& \forall x[\neg B(x) \rightarrow \neg B(1 + 2x)]$,

(4) $\forall x\{\forall r[r \neq 0 \rightarrow \exists y(B(y) \& B(x + ry))] \rightarrow B(x)\}$.

REMARKS. Axioms (1) and (2) are satisfied by all valuation rings of K above primes of $\mathbf{Q}$ other than $p = 2$. Axiom (3) ensures we have an archimedean valuation. Any set satisfying (1), (2) and (3) lies between an open and a closed unit ball; Axiom (4) gives closure.

PROOF. Clearly the closed unit ball of an archimedean valuation satisfies (1)–(4). Conversely, given a set B as in the theorem we must construct the valuation λ. Notice that all the axioms remain true when restricted to $\mathbf{Q}$. We first prove the theorem when $K = \mathbf{Q}$, and then do the general case.

We will need a lemma, easily established by induction on n.

LEMMA 9. *Let D be a subset of $\{0, 1, 2, \ldots, n\}$ containing 0, 1, and n, and such that if $r, s \in D$ and $r + s$ is even, then $(r + s)/2 \in D$. Then, $D = \{0, 1, 2, \ldots, n\}$.*

For the case $K = \mathbf{Q}$:

(A) By (2), since $1 = 1/1$ and $-1 = 1/(-1)$ these are both in B. By (1), their average $0 = (1 + (-1))/2 \in B$, and $1/2 \in B$. At this point we remark also that by (1), $b \in B$ iff $-b \in B$.

(B) Next we show $n \notin B$ for integers $n \geqslant 2$; the proof is by induction. From (3), $2 \notin B$. Therefore, by (3) and (A), $3 = -(1 + 2(-2)) \notin B$. Suppose we know $n \notin B$ for $n \in \{2, 3, \ldots, 2m + 1\}$, where $m \geqslant 1$. Then, $2m + 2 \notin B$, since otherwise $m + 1 = (2m + 2)/2$ would give $m + 1 \in B$. Also $2m + 3 = 1 + 2(m + 1)$ implies $2m + 3 \notin B$.

(C) Therefore, by (2), $\{(1/n) | n \in \mathbf{N}\} \subset B$. Fix n, and consider the set $\{0/n, 1/n, 2/n, \ldots, n/n\}$. Axiom (1) enables us to apply Lemma 9 to the numerators of these fractions, so the entire set is contained in B. Using the remark at the end of (A) we see that $\{q \in \mathbf{Q} | \, |q| \leqslant 1\} \subseteq B$.

(D) Now suppose $q \in B$ and $|q| > 1$. By the multiplicative closure of B, $q^n \in B$ for $n = 1, 2, \ldots$. For large enough n, $|q^n| > 2$, so $(2/q^n) \in B$. But then $2 = q^n(2/q^n) \in B$, a contradiction.

This completes the proof in this case; now let K be an arbitrary number field. From the case just treated, $\{q \in \mathbf{Q} | \, |q| \leqslant 1\} \subset B$.

Consider an embedding,

$$K \to K \otimes 1 \to K \underset{\mathbf{Q}}{\otimes} \mathbf{R} \cong \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$$

where $[K\colon \mathbf{Q}] = r_1 + 2r_2$. With some abuse of notation, our eventual goal is to show $B = K \cap \{\vec{z} \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} | \, |z_j| \leqslant 1\}$ for some j. As a first step we show that B contains an open ball B_1 about 0 in the topology induced on K by $K \hookrightarrow K \otimes \mathbf{R}$. Let ω be a primitive element for K, so $K = \mathbf{Q}(\omega)$; then also $K = \mathbf{Q}(1/\omega)$ so we can assume $\omega \in B$. It is easy to verify, using Axiom (1) and induction, that we can take

$$B_1 = \left\{ \sum_{i=0}^{n-1} a_i \omega^i \, | \, |a_i| < \left(\frac{1}{2}\right)^{n-1}, a_i \in \mathbf{Q} \right\}, \qquad n = [K\colon \mathbf{Q}].$$

Now define a function $\lambda\colon K \to \mathbf{R}$ by

$$\lambda(x) = \inf_{q \in \mathbf{Q}} \{|q| \, | \, x/q \in B\}.$$

We claim λ is a valuation:

(E) The set $\{q \in \mathbf{Q} | x/q \in B\}$ is not empty, because as we have just shown, for large enough q, x/q is in the ball $B_1 \subset B$. Thus λ is well-defined; clearly $\lambda(x) \geqslant 0$ for all x, and $\lambda(q) = |q|$ for $q \in \mathbf{Q}$.

For the remainder of the proof, p, q and r will denote elements of $\mathbf{Q}$. If $|q| > \lambda(x)$, then by definition there is some r with $|q| > r \geqslant \lambda(x)$ and $x/r \in B$, so also $x/q = (x/r) \cdot (r/q) \in B$. If $|q| < \lambda(x)$, then $x/q \notin B$, so $q/x \in B$.

(F) $\lambda(x) = 0$ iff $x = 0$: ($\Leftarrow$) is obvious. ($\Rightarrow$) means that for all $q \neq 0$, $x/q \in B$. Therefore, for all q, $qx \in B$. Suppose $x \neq 0$. Using the ball B_1 exhibited above, we see that $K = (\mathbf{Q}x)B_1 \subset B$. This contradicts $2 \notin B$.

(G) If $x, y \in K$ with $y \neq 0$, then $\lambda(x) \leqslant \lambda(y)$ iff $x/y \in B$: ($\Leftarrow$) If $x/y \in B$, then having $y/q \in B$ implies $x/q = (x/y) \cdot (y/q) \in B$. ($\Rightarrow$) Here we use the

closure of B. Given $\lambda(x) \leqslant \lambda(y)$, if $x/y \notin B$, then $y/x \in B$, so by the direction ($\Leftarrow$) just proved, $\lambda(y) \leqslant \lambda(x)$. Hence $\lambda(x) = \lambda(y)$. Since $y \neq 0$, by (F) there are p, q such that $p > \lambda(x) = \lambda(y) > q > 0$. For any such p, q we have $x/p, q/y \in B$ by (E), hence $(x/y)/(p/q) = (x/p) \cdot (q/y) \in B$. Taking p/q arbitrarily close to 1 we see that x/y is in the closure of B with respect to the topology induced on K from $K \otimes \mathbf{R}$. In view of Axiom (4) and the fact that B contains a ball about 0 with respect to this topology, we obtain $x/y \in B$, contradicting our assumption.

In particular $\lambda(x) \leqslant 1$ iff $x \in B$.

(H) $\lambda(xy) = \lambda(x)\lambda(y)$: $\lambda(xy) \leqslant \lambda(x)\lambda(y)$ because if $x/p, y/q \in B$, then $(xy)/(pq) \in B$. Assume $\lambda(xy) < r < \lambda(x)\lambda(y)$; then $xy/r \in B$ but $r/xy \notin B$. Choose p, q with $|p| < \lambda(x)$, $|q| < \lambda(y)$, $r < |pq| < \lambda(x)\lambda(y)$. Then, $r/pq \in B$ and $p/x, q/y \in B$, so $r/xy = (r/pq)(p/x)(q/y) \in B$, a contradiction.

(I) $\lambda(x + y) \leqslant 2 \max(\lambda(x), \lambda(y))$: Suppose $\lambda(x) \geqslant \lambda(y)$; we can assume $\lambda(x) \neq 0$ for otherwise $x = y = 0$. Then, by (G), $y/x \in B$, so by Axiom (1), $(x + y)/(2x) = (1 + y/x)/2 \in B$. Hence, by (G) again, $\lambda(x + y) \leqslant \lambda(2x) = 2 \cdot \lambda(x)$.

Thus by [**1**, Chapter 1], λ is a valuation of K and we have described B as its closed unit ball. □

Combining Lemma 9 and Theorem 5, we have

THEOREM 6. *There is a predicate which for every choice of its parameters is satisfied either by all of K or by the closed unit ball of some archimedean valuation of K, and every such ball is obtained for some choice of the parameters.*

REFERENCES

1. E. Artin, *Algebraic numbers and algebraic functions*, Gordon and Breach, New York, 1967.
2. E. Artin and J. Tate, *Class field theory*, Benjamin, New York, 1967.
3. J. W. S. Cassels and A. Frohlich (eds.), *Algebraic number theory*, Thompson, Washington, D. C., 1967.
4. Ju. L. Ershov, *The undecidability of certain fields*, Dokl. Akad. Nauk SSSR **161** (1965), 27–29.
5. S. Lang, *Algebraic number theory*, Addison-Wesley, New York, 1970.
6. O. T. O'Meara, *Introduction to quadratic forms*, 2nd ed., Die Grundelhren der math. Wissenschaften, Band. 117, Academic Press, New York, 1963; Springer-Verlag, Berlin and New York, 1971.
7. Y. Penzin, *The undecidability of fields of rational functions over fields of characteristic* 2, Algebra i Logika **12** (1973), 205–210.
8. J. Robinson, *On the decision problem for algebraic rings*, Studies in Mathematical Analysis and Related Topics, no. 42, Stanford Univ. Press, Stanford, Calif., 1962, pp. 297–304.
9. _____, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114.
10. _____, *The undecidability of algebraic rings and fields*, Proc. Amer. Math. Soc. **10** (1959), 950–957.
11. R. M. Robinson, *Undecidable rings*, Trans. Amer. Math. Soc. **70** (1951), 137–159.
12. _____, *Arithmetical definability of field elements*, J. Symbolic Logic **16** (1951), 125–126.
13. _____, *The undecidability of pure transcendental extensions of real fields*, Z. Math. Logik Grundlagen Math. **10** (1964), 275–282.
14. J. Shoenfield, *Mathematical logic*, Addison-Wesley, Reading, Mass., 1967.
15. A. Weil, *Basic number theory*, 3rd ed., Die Grundlehren der math. Wissenschaften, Band 144, Springer-Verlag, Berlin and New York, 1974.
16. C. L. Siegel, *Approximation algebraischer Zahlen*, Math. Z. **10** (1921), 173–213.

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MASSACHUSETTS 02139