ISRAEL JOURNAL OF MATHEMATICS 101 (1997), 229–254

THE LOGIC OF PSEUDO-S-INTEGERS

BY

ALEXANDRA SHLAPENTOKH*

Department of Mathematics, East Carolina University
Greenville, NC 27858, USA
e-mail: mashlape@ecuvax.cis.ecu.edu

ABSTRACT

Let $\{n_i\}$ be a sequence of natural numbers and let $\{p_i\}$ be a listing of rational primes. Then an abelian group $G = \{x \in \mathbb{Q} | \ \mathrm{ord}_{p_i} x \geq -n_i\}$ is called a group of pseudo-integers. We investigate the logical properties of such groups of pseudo-integers and the counterparts of such groups in global fields in the case the number of primes allowed to appear in the denominator is infinite. We show that, while the addition problem of any recursive group of pseudo-integers is decidable, the Diophantine problem for some recursive groups of pseudo-integers with infinite number of primes allowed in the denominator, is not decidable. More precisely, there exist recursive groups of pseudo-integers, where infinite number of primes are allowed to appear in the denominator, such that there is no uniform algorithm to decide whether a polynomial equation over $\mathbb{Z}$ in several variables has solutions in the group. This result is obtained by giving a Diophantine definition of $\mathbb{Z}$ over these groups. The proof is based on the strong Hasse norm principal.

1. Introduction

The notion of pseudo-integers was first introduced by Hilton in [H] and further investigated in group-theoretic context by Ries and Militello (see [R1], [R2] and [M-R]). Groups of pseudo-integers are additive subgroups of rational numbers and are defined below.

* The research for this paper has been partially supported by NSA grant MDA904-96-1-0019.
Received July 30, 1995

Definition 1.1: Rational pseudo-integers. Let $\{n_i\}$ be a sequence of natural numbers and let $\{p_i\}$ be a listing of rational primes. Then a group of pseudo-integers G is defined to be the following set:

$$G = \{x \in \mathbb{Q} | \ \mathrm{ord}_{p_i} x \geq -n_i\}.$$

In the papers mentioned above it is shown that in many aspects these additive groups are similar to $\mathbb{Z}$ (thus the name pseudo-integers). The notion of pseudo-integers has natural extensions. Before we can state the generalized definition we need to define the notion of S-integers.

Definition 1.2: S-integers. Let K be a global field, i.e. a number field or an algebraic function field over a finite field of constants. Let S be a finite collection of its non-archimedean valuations. Then the ring $O_{K,S} = \{x \in K | \ \mathrm{ord}_{\mathfrak{p}} x \geq 0 \text{ for } \mathfrak{p} \notin S\}$ is called the ring of S-integers.

Definition 1.3: Pseudo S-integers. Let K be a global field, let S be a finite non-empty set consisting of all archimedean and some non-archimedean primes of K, let $\{n_i\}$ be a sequence of natural numbers, let $\{\mathfrak{p}_i\}$ be a listing of non-archimedean primes of K and let M be the following $O_{K,S}$-module: $M = \{x \in K | \ \mathrm{ord}_{\mathfrak{p}_i} x \geq -n_i \text{ for } \mathfrak{p}_i \notin S\}$. Then M is called a module of pseudo-S-integers.

We will say that a module M of pseudo-S-integers is **uniformly bounded** by n, if there exists $n \in \mathbb{N}$ such that for all $i, n_i \leq n$.

We will also say that a set T of non-archimedean primes of K is the set of **denominator primes** of a module of pseudo-S-integers M if $T = \{\mathfrak{p}_i | \ n_i > 0\}$.

In the future $M_{n,T,S}$ will denote a module of pseudo-S-integers uniformly bounded by n and with a set of denominator primes T.

We will show that if M and the function $\mathfrak{p}_i \to n_i$ are recursive in the sense which will be made precise below, there is an effective procedure which can decide whether a linear system $A \cdot X = C$, where A is a matrix over $O_{K,S}$ and C is a vector of elements of M, has solutions in M. We will also prove the following theorem.

THEOREM: *Let K be an algebraic number field or an algebraic function field over a finite field of constants. Let $p > 2$ be distinct from the characteristic of the field, and let T be a collection of non-archimedean primes of K such that for*

some $a \in K$, for all but finitely many $\mathfrak{p} \in T$, the polynomial $x^{\mathfrak{p}} - a$ is irreducible modulo $\mathfrak{p}$. Let S be a finite collection of non-archimedean primes of K and let $n < p$.

Then $O_{K,S}$ has a Diophantine definition over $M_{n,T,S}$.

Thus, if the Diophantine problem of $O_{K,S}$ is undecidable (and it is known in all cases for function fields and in some cases for number fields (see [Da], [Da-Mat-Ro], [D1], [D2], [D4], [D5], [D-L], [Ph1], [Ph2], [Sha-Sh], [S1]–[S6])), the Diophantine problem of $M_{n,T,S}$ is also undecidable. (Of course the undecidability result in the function field case is not particularly interesting, since we have the undecidability result for the field itself. For more details see [D3], [K-R1]–[K-R3], [Ph2], [S7], [V].) The result above can be made a bit stronger in the following sense.

THEOREM: *Let T be an arbitrary set of non-archimedean primes of a global field K. Let n be any natural number. Then for any $\delta > 0$ there exists a module of pseudo-integers $M_{n,T_\delta,S}$ such that $T_\delta \in T$, the Dirichlet density of some set containing $T - T_\delta$ is less than δ, and S-integers are polynomially definable over $M_{n,T_\delta,S}$.*

Arguably, the most interesting open questions in the area of Diophantine definability and decidability are two questions pertaining to $\mathbb{Q}$. Is the Diophantine problem of $\mathbb{Q}$ decidable and do rational integers have a Diophantine definition over $\mathbb{Q}$? A conjecture of Barry Mazur implies that there is no Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$. (For more details see [M1].) Since these questions seem completely intractable at this moment, one could try a gradual approach, i.e. considering holomorphy rings of $\mathbb{Q}$ (and other number fields). Holomorphy rings of global fields are defined in the same fashion as the rings of S-integers with the difference being that S is now allowed to be infinite. For more systematic development of this approach see [M2] and [S5]. Unfortunately, even these intermediate problems seem at the moment very hard for infinite S. Even over the function fields of positive characteristic, where the progress has been much more rapid than over number fields, so far there is no Diophantine definition of polynomials over a rational function field or over a holomorphy ring with infinite S. And that's where pseudo-S-integers come into the picture. They offer yet another approach to the field and, judging from these results, pseudo-integers might be easier to handle than holomorphy rings.

The main method used in this paper, which is based on the strong Hasse norm principal (see, for example, Theorem 4.5, page 56 of [J] or p. 195 of [L] and Propositions 10, 11, pp. 182–183, Theorem 2, p. 206 of [W]), was first introduced by Kim and Roush in [K-R1], where they used it to give a Diophantine definition of integrality at one fixed prime over the rational function fields of positive characteristic over the constant fields not containing the algebraic closure of a finite field. We extend this method so that when the poles of elements under consideration are bounded, we can give a Diophantine definition of integrality at infinitely many primes.

We will start with showing that the addition problem for any recursive module of pseudo-S-integers is solvable. This result, which is not hard to prove, is really a consequence of the Strong Approximation Theorem (for example, see [O], p. 77).

2. Decidability of the addition problem of pseudo-S-integers

The main technical difficulty associated with the proof of decidability concerns methods of presenting primes in the finite extensions of rational fields. Before we proceed we need to settle on a presentation of the global fields over which we will do our work. A finite extension of $\mathbb{Q}$ or a rational function field over a finite field of constants will be presented by specifying the monic irreducible polynomial of its generator, and all the other field elements will be presented as linear combinations of powers of the generator over the underlying rational field. Under such a presentation, given an element of the field we can effectively construct its minimal polynomial over the corresponding rational field.

LEMMA 2.1: *Let K be a finite separable extension of a rational field R which is either $\mathbb{Q}$ or a rational function field over a finite field of constants. Let $\mathfrak{p}$ be a prime of R. Let $\{\omega_1, \ldots, \omega_n\}$ be either an integral basis with respect to $\mathbb{Z}$ or a polynomial ring in R such that $\mathfrak{p}$ is not the infinite valuation of that polynomial ring. (We know such a basis exists since both rings are PID's.) Let $A = \{\sum_{i=1}^{n} a_{ij}\omega_i\}$, where a_{ij} is either a rational integer or a polynomial of the above described polynomial ring of R, and $(a_{1j}, \ldots, a_{nj})$ independently run through all the residue classes modulo $\mathfrak{p}^2$. Assume $\mathfrak{p} = \prod_{i=1}^{k} \beta_i^{e_i}$ is the factorization of $\mathfrak{p}$ in K. Let $(b_1, \ldots, b_k)$ be any k-tuple of representatives of residue classes modulo $\beta_1^2, \ldots, \beta_k^2$ respectively. Then A contains an element α such that $\alpha \cong b_i$ modulo β_i^2.*

Proof: By the strong approximation theorem, K contains an algebraic integer or an integral function γ (an algebraic function integral over the polynomial ring chosen above) such that $\gamma \cong b_i$ modulo β_i^2. Since $\{\omega_i\}$ constitute an integral basis, $\gamma = \sum_{i=1}^{n} c_i\omega_i$, where c_i are either rational integers or polynomials. By assumption on A, it contains an element $\alpha = \sum_{i=1}^{n} a_i\omega_i$ such that $a_i \cong c_i$ modulo $\mathfrak{p}^2$. Therefore, $\gamma \cong \alpha$ modulo $\mathfrak{p}^2$ and therefore $\gamma \cong \alpha$ modulo β_i^2 for all i.

COROLLARY 2.2: *Let $A, \mathfrak{p}, K, \beta_1, \ldots, \beta_k$ be as above. Then A contains elements $\{\alpha_1, \ldots, \alpha_k\}$ such that $\mathrm{ord}_{\beta_i}\alpha_i = 1$, for all $i \neq j$, $\mathrm{ord}_{\beta_i}\alpha_j = 0$, and for any pair (α_i, α_j) such that $i \neq j$ there exist $\tau_{ij} \in A$ such that $\alpha_i + \tau_{ij}\alpha_j$ is a unit at all the factors of $\mathfrak{p}$.*

Proof: By Lemma 2.1, there exists an element α_i such that $\mathrm{ord}_{\beta_i}\alpha_i = 1$ and $\alpha_i \cong 1$ modulo β_r^2 for all $r \neq i$. Let α_j be defined correspondingly for β_j. By the strong approximation theorem, there exists an algebraic integer or an integral function τ such that $\mathrm{ord}_{\beta_i}\tau = 0$, $\mathrm{ord}_{\beta_j}\tau = 0$, $\mathrm{ord}_{\beta_r}\tau = 1$ for all $r \neq i, j$. As in the argument above, A contains an element $\tau_{ij} \cong \tau$ modulo $\mathfrak{p}^2$. Thus, $\alpha_i + \tau_{ij}\alpha_i$ will be a unit at all the factors of $\mathfrak{p}$.

LEMMA 2.3: *Let K be a finite separable extension of a rational field R, where R is as above. Let $\mathfrak{p}$ be a prime of R. Then assuming K is given by the monic irreducible polynomial of its generator, the following statements are true.*

1. *There is an algorithm to determine factorization of $\mathfrak{p}$ in K, i.e. there is an algorithm to determine the number of factors $\mathfrak{p}$ has in K and their relative and ramification degrees.*
2. *If $\mathfrak{p}$ has m factors $\beta_1, \ldots, \beta_m$ in K, then there is an algorithm to construct $\alpha_1, \ldots, \alpha_m \in K$ such that $\mathrm{ord}_{\beta_i}\alpha_i = 1$ and for $i \neq j$, $\mathrm{ord}_{\beta_j}\alpha_i = 0$.*

Proof: First of all, we note that both in cases of the rational function field and $\mathbb{Q}$, one can construct integral bases for the polynomial ring and the ring of rational integers respectively in K. (In the case of the function field we would have to treat separately the infinite valuation of the polynomial ring.) For a description of algorithms for such a construction see [Po] or [Sei]. Next, assuming we have constructed an integral basis, and have been given a rational prime $\mathfrak{p}$, let A be as in the preceding lemma and corollary.

Then we can use the following procedure:

1. Select the element $\alpha_1 \in A$ such that its norm has the smallest possible positive order at $\mathfrak{p}$ (amongst the elements of A). (To make this selection pro-

cess completely deterministic, given a natural ordering on $\mathbb{Z}$ and some effective ordering of the polynomial ring, extend this ordering to the algebraic integers or integral functions of K by using the lexicographical ordering with coefficient of ω_1 having the highest weight and the coefficient of ω_n having the lowest weight. Given several elements satisfying the selection criteria, we will now pick the first one under our ordering.) Then there exists a factor β_1 of $\mathfrak{p}$ such that $\mathrm{ord}_{\beta_1}\alpha_1 = 1$, and $f(\beta_1/\mathfrak{p}) = \mathrm{ord}_{\mathfrak{p}}\mathbb{N}_{K/R}(\alpha_1)$.

2. Assume $\alpha_1, \ldots, \alpha_r$ have been selected already. Then let

$$B_r = \{x \in A |\ N_{K/R}(x) \cong 0 \text{ modulo } \mathfrak{p},$$
$$\forall i = 1, \ldots, r\ \exists y \in A\ \mathbb{N}_{K/R}(\alpha_i - yx) \ncong 0 \text{ modulo } \mathfrak{p}\}.$$

Choose an element of B_r with the norm whose order at $\mathfrak{p}$ is as small as possible (amongst the elements of B_r) and let α_{r+1} be equal to this element. (Again we make the selection process deterministic by using the ordering described above.)

Repeat steps 1 and 2 until at some iteration k, B_k is empty. At this point we can conclude that $\mathfrak{p}$ has k factors $\beta_1, \ldots, \beta_k$ and $f(\beta_i/\mathfrak{p}) = \mathrm{ord}_{\mathfrak{p}}\mathbb{N}_{K/R}(\alpha_i)$.

3. Find an n-tuple $(e_1, \ldots, e_k)$ of natural numbers such that $\prod_{i=1}^{k}\alpha_i^{e_i} \cong 0$ modulo $\mathfrak{p}$, but the congruence is no longer true if any of the exponents is reduced by one. (We can establish whether $\prod_{i=1}^{k}\alpha_i^{e_i} \cong 0$ modulo $\mathfrak{p}$ by determining whether $(\prod_{i=1}^{k}\alpha_i^{e_i})/\mathfrak{p}$ is integral at $\mathfrak{p}$. The last step can be accomplished by examining the coordinates of $(\prod_{i=1}^{k}\alpha_i^{e_i})/\mathfrak{p}$ with respect to an integral basis.) Conclude, $\{e_i\}$ are the ramification degrees.

LEMMA 2.4: *Let K be a global field. Then given an element $\gamma \in K$, we can effectively construct its divisor in K.*

Proof: First of all, by looking at the denominators of the coordinates of γ with respect to an integral basis, we can determine at which rational primes γ is not integral and produce a bound on the order of poles of γ. Then, using a procedure similar to the one used in part 3 of the lemma above, we can determine the exact order of the poles. By repeating this procedure for γ^{-1} we can take care of zeros of γ.

THEOREM 2.5: *Let K be a finite separable extension of a rational field R, where R is either $\mathbb{Q}$ or a field of rational functions over a finite field of constants. Let S be a finite set of non-archimedean primes of K. Let M be a module of pseudo-S-integers such that given a prime there is a recursive procedure to determine*

the minimal order any element of M may have at this prime. Then the addition problem of M is decidable, i.e. given a linear system $A \cdot X = C$, where A is a matrix over K, and C is a vector of elements of K, one can determine effectively whether this system has solutions in M.

Proof: First of all, if the system is inconsistent or has a unique solution (and both cases can be identified effectively) there is nothing to do. So the problem reduces to the case of a system of the form

$$\{y_j = \sum_{i=1}^{u} a_{ij}x_i + a_j \mid j = 1, \ldots, k\}, \tag{2.5.1}$$

where the coefficients are arbitrary elements of K and which has to be solved over M in variables x_i and y_i. By the preceding lemma, we can determine what primes occur as poles of the coefficients of any of the equations. Let $(\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m)$ be the list of primes occurring as poles of coefficients. Let $\prod_r$ be a local uniformizing parameter for $\mathfrak{p}_r$, let $-m_r \in \mathbb{Z}^-$ be the smallest order an element of M may have at $\mathfrak{p}_r$, and let $-n_{ij} \in \mathbb{Z}^-$ be the smallest order any of $\{a_j, a_{1j}, \ldots, a_{uj}\}$ has at $\mathfrak{p}_r$. Then we claim that the system (2.5.1) will have solutions in M if and only if for every $r = 1, \ldots, m$ the following system has solutions $z_{11}, \ldots, z_{um}$ in the residue ring of $\mathfrak{p}_r^{n_r}$, where $n_r = \max\{n_{jr}\}$:

$$\left\{ \sum_{i=1}^{u} a_{ij}\pi_r^{n_{jr}} z_{ir} \cong -a_j \pi_r^{n_{jr}+m_r} \text{ modulo } \mathfrak{p}_r^{n_{jr}} \mid j = 1, \ldots, k \right\}. \tag{2.5.2}$$

Indeed, suppose (2.5.1) has solutions in M. Then for each j and each r, $\mathrm{ord}_{\mathfrak{p}_r}([\sum_{i=1}^{u} a_{ij}x_i] - a_j) \geq -m_r$, and consequently

$$\mathrm{ord}_{\mathfrak{p}_r}\left(\left[\sum_{i=1}^{u} a_{ij}\pi_r^{n_{jr}}\pi_r^{m_r}x_i \right] + a_j\pi_r^{n_{jr}+m_r} \right) \geq n_{jr},$$

$$\mathrm{ord}_{\mathfrak{p}_r}\left(\left[\sum_{i=1}^{u} a_{ij}\pi_r^{n_{jr}} z_{ir} \right] + a_j\pi_r^{n_{jr}+m_r} \right) \geq n_{jr},$$

where $z_{ir} = \pi_r^{m_r}x_i$ is integral at $\mathfrak{p}_r$ and hence a representative of a residue class modulo $\mathfrak{p}_r^{n_r}$.

Conversely, suppose for every r, (2.5.2) has solutions $(z_{1r}, \ldots, z_{ur})$. By the Strong Approximation Theorem for each i, there exists an element x_i such that

$\pi_r^{m_r} x_i \cong z_{ir}$ modulo $\mathfrak{p}_r^{n_r+1}$, $r = 1, \ldots, m$, and all the other poles of x_i are among valuations of S. Then for all $i, x_i \in M$, and

$$\begin{aligned}
\mathrm{ord}_{\mathfrak{p}_r} y_j =& \mathrm{ord}_{\mathfrak{p}_r} \left(\sum_{i=1}^{u} a_{ij} x_i + a_j \right) \\
=& -m_r - n_{jr} + \mathrm{ord}_{\mathfrak{p}_r} \left(\left[\sum_{i=1}^{u} a_{ij} \pi_r^{n_{jr}} \pi_r^{m_r} x_i \right] + a_j \pi_r^{n_{jr}+m_r} \right) \\
& -m_r - n_{jr} + \mathrm{ord}_{\mathfrak{p}_r} \left(\left[\sum_{i=1}^{u} a_{ij} \pi_r^{n_{jr}} (\pi_r^{m_r} x_i = z_{ir}) \right] \right. \\
& \qquad \left. + \sum_{i=1}^{u} a_{ij} \pi_r^{n_{jr}} z_{ir} + a_j \pi_r^{n_{jr}+m_r} \right) \\
\geq& -m_r - n_{jr} + \min(n_r + 1, n_{jr}) = -m_r - n_{jr} + n_{jr} = -m_r.
\end{aligned}$$

On the other hand, if $\mathfrak{q} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ is any other non-archimedean prime of K not in S, then $\mathrm{ord}_{\mathfrak{q}}(\sum_{i=1}^{u} a_{ij} x_i + a_j) \geq 0$ by assumption on the coefficients and by construction of x_i. Thus, $y_j \in M$.

Finally, since the residue ring of $\mathfrak{p}_r^{n_r}$ is finite, we can decide effectively whether (2.5.2) has solutions in this residue ring.

In the next section we will construct a Diophantine definition of S-integers over some modules of pseudo-S-integers with infinite sets of denominator primes.

3. A Diophantine defintion of S-integers over some modules of pseudo-S-integers

LEMMA 3.1: *Let K be an algebraic number field or an algebraic function field over a finite field of constants. Let $\mathfrak{p}$ be a non-archimedean prime of K, let p be a rational prime relatively prime to $\mathfrak{p}$ and not divisible by the characteristic of K, and let L be a cyclic extension of K of degree p such that $\mathfrak{p}$ remains prime in the extension. (That is the ideal $\mathfrak{p}R_{L,\mathfrak{p}}$, where $R_{L,\mathfrak{p}}$ is the ring of elements of L integral at $\mathfrak{p}$, is a prime ideal.) Let $z \in K$ be an element such that $\mathrm{ord}_{\mathfrak{p}} z \not\equiv 0 \bmod p$. Then the equation $\mathbf{N}_{L/K}(x) = z$ has no solutions in L.*

Proof: Let $\mathcal{P}$ be the prime above $\mathfrak{p}$ in L. Since $\mathbf{N}_{L/K}(x) = z$, we must conclude that $\mathrm{ord}_{\mathfrak{p}} \mathbf{N}_{L/K}(x) \neq 0$, $\mathrm{ord}_{\mathcal{P}} x \neq 0$ and for any $\sigma \in \mathrm{Gal}(L/K)$, $\mathrm{ord}_{\mathcal{P}} \sigma(x) = \mathrm{ord}_{P} x$. Thus, $\mathrm{ord}_{\mathfrak{p}} \mathbf{N}_{L/K}(x) \cong 0 \bmod p$ and we have a contradiction.

LEMMA 3.2 (Hensel's Lemma): *Let $K_\mathfrak{p}$ be a local field with a prime $\mathfrak{p}$ and a finite residue field and let $f(X)$ be a polynomial over the ring of integers of K. Let α_0 be an integer of $K_\mathfrak{p}$ such that $\mathrm{ord}_\mathfrak{p} f(\alpha_0) > 2\mathrm{ord}_\mathfrak{p} f'(\alpha_0)$. Then $f(X)$ has a root α in $K_\mathfrak{p}$.* (See, for example, [L], Proposition 2, page 42.)

LEMMA 3.3: *Let $K_\mathfrak{p}$ be a local field with a finite residue field and the prime $\mathfrak{p}$, let p be a positive rational integer relatively prime to the characteristic of the residue field of $K_\mathfrak{p}$, let a $K_\mathfrak{p}$ unit a be a pth power in the residue field of $\mathfrak{p}$. Then a is a pth power in $K_\mathfrak{p}$.*

Proof: Consider the polynomial $X^p - a$ which is separable and has a root modulo $\mathfrak{p}$. Thus by Hensel's lemma, this polynomial has a root in $K_\mathfrak{p}$.

LEMMA 3.4: *Let $K_\mathfrak{p}$ be a local field of characteristic 0 with a prime $\mathfrak{p}$ and the residue field of characteristic $p > 0$, such that $\mathfrak{p}$ is a factor of p, let a be a unit of $K_\mathfrak{p}$ such that $a \cong \epsilon^p$ modulo $\mathfrak{p}^{2e(\mathfrak{p}/p)+1}$ for some $\epsilon \in K_\mathfrak{p}$. Then a is a pth power in $K_\mathfrak{p}$.*

Proof: Consider the polynomial $f(X) = X^p - a$. Then $\mathrm{ord}_\mathfrak{p} f(\epsilon) = 2e(\mathfrak{p}/p) + 1$. On the other hand, $f'(\epsilon) = p\epsilon^{p-1}$, and $\mathrm{ord}_\mathfrak{p}(f'(\epsilon))^2 = 2\mathrm{ord}_\mathfrak{p} p = 2e(p/\mathfrak{p}) < \mathrm{ord}_\mathfrak{p} f(\epsilon)$. Thus, $f(X)$ has a root in $K_\mathfrak{p}$.

LEMMA 3.5: *Let $K_\mathfrak{p}$ be a local field with a prime $\mathfrak{p}$ and a finite residue field. Let p be a rational prime different from the characteristic of the residue field, let $x \in K_\mathfrak{p}$ and let $E_\mathcal{P} = K_\mathfrak{p}(x^{-1} - 1)^{1/p}$. Then if $\mathrm{ord}_\mathfrak{p}(x^{-1} - 1) > 0$ or if $\mathrm{ord}_\mathfrak{p} x > 0$, x is a pth power in $E_\mathcal{P}$.*

Proof: First suppose $\mathrm{ord}_\mathfrak{p}(x^{-1} - 1) > 0$ and let $w = (x^{-1} - 1)$. Then

$$x = \frac{1}{1+w} = (1 - w + w^2 + \cdots) \cong 1 \bmod \mathfrak{p},$$

and consequently, by a previous lemma, x is a pth power in $K_\mathfrak{p}$.

Suppose next $\mathrm{ord}_\mathfrak{p} x > 0$. Then $\frac{1-x}{x} = z^{-p}$ for some integer $z \in E_\mathcal{P}$. Therefore, $xz^{-p} = (1 - x) \Longrightarrow xz^{-p} \cong 1$ modulo $\mathcal{P}$, where $\mathcal{P}$ is the prime above $\mathfrak{p}$ in E. Again, by Lemma 3.3, xz^{-p} is a pth power in $E_\mathcal{P}$, and therefore x is a pth power in $E_\mathcal{P}$.

LEMMA 3.6: *Let L be a field and let E be a cyclic extension of L of prime degree $p > 2$. Let $x \in L$ be such that it is a pth power in E. Then x is a norm of an element in E.*

Proof: If x is a pth power in L, then it is clearly a norm. Suppose x is not a pth power in L. Let $y \in E$ be such that $y^p = x$. Then all the conjugates of y over L are of the form $\xi_p^i y$, where ξ_p is a primitive pth root of unity. Thus, $\mathbb{N}_{E/L}(y) = \xi_p^{(p(p-1))/2} x = x$, since p is odd.

LEMMA 3.7: *Let $K_\mathfrak{p}$, $E_\mathcal{P}$ be as in Lemma 3.5, and assume that the extension $E_\mathcal{P}/K_\mathfrak{p}$ is unramified. Let x be such that $\mathrm{ord}_\mathfrak{p} x \cong 0 \bmod p$. Then x is a norm of an element from $E_\mathcal{P}$.*

Proof: Let π be a local uniformizing parameter of $K_\mathfrak{p}$. Then for some r, $x = \pi^{rp}\epsilon$ where ϵ is a $\mathfrak{p}$-unit. Since the extension is not ramified, ϵ is a norm of some $\delta \in E_\mathcal{P}$ (see, for example, Proposition 3.11, page 153 of [J]). Thus x is the norm of $\pi^r \delta$.

LEMMA 3.8: *Let K be a number field or an algebraic function field over a finite field of constants. Let $a \in K$. Let p be a rational prime distinct from the characteristic of the field. Then a prime $\mathfrak{p}$ of K relatively prime to p ramifies in the extension $K(a^{1/p})/K$ if and only if $\mathrm{ord}_\mathfrak{p} a \not\cong 0 \bmod p$. (Here and below "$a^{1/p}$" will denote a p-th root of a.)*

Proof: If $\mathrm{ord}_\mathfrak{p} a \not\cong 0$ then $\mathfrak{p}$ will clearly ramify in the extension. Suppose now the residue field of $\mathfrak{p}$ is not of characteristic p and $\mathrm{ord}_\mathfrak{p} a \cong 0 \bmod p$. Since we can multiply or divide a by a pth power of some local uniformizing parameter without changing the extension, without loss of generality we can assume that $\mathrm{ord}_\mathfrak{p} a = 0$. But in this case the discriminant of the power basis of $a^{1/p}$ will be a unit at $\mathfrak{p}$, and thus $\mathfrak{p}$ will be unramified.

LEMMA 3.9: *Let K be an algebraic function field of positive characteristic. Let p be a rational prime distinct from the characteristic of the field. Let $\{\mathfrak{q}, \mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ be a set of primes of K, where $\mathfrak{q}$ is of degree 1, let $\{a, b_1, \ldots, b_m\}$ be a set of elements of K such that a is integral at $\mathfrak{q}$ and for each $i = 1, \ldots, m$, b_i is integral at $\mathfrak{p}_i$. Let $\{n, n_1, \ldots, n_m\}$ be a set of natural numbers and let π be of order 1 at $\mathfrak{q}$. Then there exists $y \in K$ satisfying the following requirements:*

1. $\mathrm{ord}_\mathfrak{q} y = -n - kp$, *for some* $k \in \mathbb{N}\backslash\{0\}$;
2. *y is integral at all the other primes of K;*
3. $\mathrm{ord}_{\mathfrak{p}_i}(y - b_i) > n_i$;
4. $\mathrm{ord}_\mathfrak{q}(y\pi^{n+kp} - a) > 0$.

Proof: By the Strong Approximation Theorem, there exists $c \in K$ such that $\mathrm{ord}_{\mathfrak{p}_i}(c - b_i) > n_i$, c has a pole at $\mathfrak{q}$ and is integral at all the other primes. Next

using the Strong Approximation Theorem twice, one can establish that there exists an element $w \in K$ whose divisor is of the form $\mathfrak{q}^{-n-kp}\prod \mathfrak{p}_i^{t_i}\mathcal{T}$, where $\mathcal{T}$ is an integral divisor, and for all $i, t_i > \mathrm{ord}_{\mathfrak{p}_i}(c - b_i)$, and $n + kp > |\mathrm{ord}_{\mathfrak{q}}c|$. Furthermore, by multiplying w by an appropriate constant if necessary, we can assume that $\pi^{n+kp}w \cong a$ modulo $\mathfrak{q}$. (Since we have assumed $\mathfrak{q}$ to be of degree 1, every residue class modulo $\mathfrak{q}$ contains a constant.) Next consider $z = w + c$. z is integral at all the primes except for $\mathfrak{q}$ at which it has a pole of the prescribed order. Furthermore, $z\pi^{n+kp} \cong \pi^{n+kp}w \cong a$ modulo $\mathfrak{q}$, $z \cong c \cong b_i$ modulo $\mathfrak{p}_i^{n_i}$, and hence we are done.

LEMMA 3.10: *Let F be a field, let p be a rational prime distinct from the characteristic of the field. Assume F has all the p-th roots of unity and let $a \in F$. Then either a is a pth power in F or $a^{1/p}$ is of degree p over F and the extension $F(a^{1/p})/F$ is cyclic.*

Proof: Suppose a is not a pth power and F contains pth roots of unity. Let α be a root of the polynomial $G(X) = X^p - a$ in the algebraic closure of F. $F(\alpha)$ also contains $\xi_p^i\alpha$, where ξ_p is a pth primitive root of unity and $i = 1, \ldots, p-1$. Therefore, $F(\alpha)$ contains all the roots of $G(X)$ and the extension is Galois. Finally consider an element $\sigma \in \mathrm{Gal}(F(\alpha)/F)$ sending α to $\xi_p\alpha$. It is clear that the order of σ is p, and thus the extension is of degree p and is cyclic.

LEMMA 3.11: *Let K be a number field or an algebraic function field over a finite field of constants. Let $p > 2$ be a rational prime different from the characteristic of the field. Assume K contains all the pth roots of unity. Let S be a finite collection of primes of K which in the case of a number field should contain all the archimedean primes and all the factors of p, and in the case of an algebraic function field should contain at least one valuation of degree 1. Let $S_f \subset S$ be a subset of S which in the number field case contains all the non-archimedean primes in S and in the function field case contains all but one element of S which will be assumed to be of degree 1. Let $\mathfrak{m}$ be the following integral divisor of K:*

$$\mathfrak{m} = \left(\prod_{(\mathfrak{p}\in S_f, \mathfrak{p}\nmid p)} \mathfrak{p}^p\right)\prod_{\mathfrak{p}\mid p}\mathfrak{p}^{p+2e(\mathfrak{p}/p)+2}.$$

Let $\{c_i\}$ be a collection of elements of K satisfying the following requirements:

1. *If K is a number field, all c_i's are algebraic integers.*

2. *If K is a function field and $\{\mathfrak{q}\} = S \backslash S_f$, then c_i's have a pole at valuation $\mathfrak{q}$ only.*
3. *Let $\alpha \in K$ be a representative of an equivalence class modulo $\mathfrak{m}$. Let r be an integer between 0 and p. Let β be a representative of an equivalence class modulo $\mathfrak{q}$. Let π be a local uniformizing parameter with respect to $\mathfrak{q}$ (in case K is a function field). Then for some i,*

$$c_i \cong \alpha \text{ modulo } \mathfrak{m},$$
$$\operatorname{ord}_{\mathfrak{q}} c_i \cong r \text{ modulo } p,$$
$$c_i \pi^{-\operatorname{ord}_{\mathfrak{q}} c_i} \cong \beta \text{ modulo } \mathfrak{q},$$

where the last two equivalencies apply in the function field case only. Let $W = S \cup \{\text{all the primes dividing } c_i\text{'s}\}$. Next, for some $x \in K$, let $\alpha_i = ((c_i x)^{-1} - 1)^{1/p}$, let $a \in O_{K,S}$ be an S-unit (i.e. all non-archimedean primes at which a has a pole or a zero are elements of S) such that it is not a pth power of K, and assume x does not have a pole at any prime $\mathfrak{t} \notin S$ such that a is a pth power modulo $\mathfrak{t}$, and at any prime $\mathfrak{t} \in W \backslash S$.

Consider the following equations:

$$\text{(3.11.1.}i\text{)} \qquad \mathbf{N}_{K(\alpha_i)/K}(y_1) = c_i x, \quad i = 0, \ldots, |\{c_i\}|,$$

$$\text{(3.11.2.}i\text{)} \qquad \mathbf{N}_{K(\alpha_i, a^{1/p})/K(\alpha_i)}(y_2) = (c_i x), \quad i = 0, 1, \ldots, |\{c_i\}|.$$

Then for some i both (3.11.1.i) and (3.11.2.i) have solutions $y_q \in K(\alpha_i)$ and $y_2 \in K(\alpha_i, a^{1/p})$ if and only if for every non-archimedean prime $\mathfrak{t}$ of K such that $\operatorname{ord}_{\mathfrak{t}} x < 0$, either $\operatorname{ord}_{\mathfrak{t}} x \cong 0 \bmod p$ or $\mathfrak{t} \in S$.

Proof: First of all, we note that the collection $\{c_i\}$ as described above exists in the function field case by Lemma 3.9, and by the Strong Approximation Theorem in the case of number fields. Next assume there exists a non-archimedean prime $\mathfrak{t}$ of K such that $\operatorname{ord}_{\mathfrak{t}} x < 0$, $\operatorname{ord}_{\mathfrak{t}} x \ncong 0 \bmod p$, and a is not a pth power in the residue field of $\mathfrak{t}$, $\mathfrak{t} \notin S$. First of all, consider $\mathbf{N}_{K(\alpha_i)/K}(y_1) = c_i x$ for some i. Since $\operatorname{ord}_{\mathfrak{t}} x < 0$, $\mathfrak{t} \notin W$, $\operatorname{ord}_{\mathfrak{t}}(c_i x)^{-1} > 0$ and $\operatorname{ord}_{\mathfrak{t}}((c_i x)^{-1} - 1) = 0$. Since $\mathfrak{t}$ is not a factor of p, $\mathfrak{t}$ is not ramified in the extension $K(\alpha_i)/K$. On the other hand, $\operatorname{ord}_{\mathfrak{t}} c_i x \ncong 0 \bmod p$, and thus unless $\mathfrak{t}$ splits into distinct factors in $K(\alpha_i)/K$, (3.11.1.i) will have no solutions by Lemma 3.1. So suppose $\mathfrak{t}$ splits completely in $K(\alpha_i)$, and let $\mathfrak{t}_1, \ldots, \mathfrak{t}_p$ be factors of $\mathfrak{t}$ in the extension. Then a is not a pth power modulo any of $\mathfrak{t}_j$, since their residue fields are the same as the residue field

of $\mathfrak{t}$. By the same argument as above, in the extension $K(\alpha_i, a^{1/p})/K(\alpha_i)$ no $\mathfrak{t}_j$ will be ramified, and since a is not a pth power in the residue field, no $\mathfrak{t}_j$ will split either. Thus, either the first or the second norm equation will have no solutions.

To prove the converse, we will show that if x does not have the prohibited poles, for some i both equations will have solutions locally at all primes of K and their factors in $K(\alpha_i)$. Then we will use the Hasse Norm Principal to assert the existence of a global solution. The proof will proceed by considering 5 different cases: $\mathfrak{t} \notin S$, $\mathrm{ord}_{\mathfrak{t}}(c_i x) = 0$ (under our assumptions this is equivalent to $\mathrm{ord}_{\mathfrak{t}} c_i = \mathrm{ord}_{\mathfrak{t}} x = 0$) and $\mathrm{ord}_{\mathfrak{t}}((c_i x)^{-1} - 1) > 0$; $\mathfrak{t} \notin S$, $\mathrm{ord}_{\mathfrak{t}}(c_i x) = 0$ and $\mathrm{ord}_{\mathfrak{t}}((c_i x)^{-1} - 1) = 0$; $\mathfrak{t} \notin S$, $\mathrm{ord}_{\mathfrak{t}} x < 0$ (under our assumptions this is equivalent to $\mathrm{ord}_{\mathfrak{t}}(c_i x) < 0$) and $p | \mathrm{ord}_{\mathfrak{t}} x$; $\mathfrak{t} \notin S$, $\mathrm{ord}_{\mathfrak{t}} x > 0$ (under our assumptions this is equivalent to $\mathrm{ord}_{\mathfrak{t}}(c_i x) > 0$); $\mathfrak{t} \in S$.

We will first fix i and show that assuming x has no forbidden poles, both equations (3.11.1.i) and (3.11.2.i) will have solutions locally at all the primes outside S. Then we will show that for some i for all $\mathfrak{t} \in S$ both equations will have local solutions.

CASE 1: $\mathfrak{t} \notin S$, $\mathrm{ord}_{\mathfrak{t}} x = 0 = \mathrm{ord}_{\mathfrak{t}} c_i = 0$ and $\mathrm{ord}_{\mathfrak{t}}((c_i x)^{-1} - 1) > 0$. Since $\mathrm{ord}_{\mathfrak{t}}((c_i x)^{-1} - 1) > 0$, by Lemma 3.5, $c_i x$ is a pth power in $K_{\mathfrak{t}}$ and thus in $K_{\mathfrak{t}}(\alpha_i)$, and hence, by Lemma 3.6, $(c_i x)$ is a norm in the extensions $K_{\mathfrak{t}}(\alpha_i)/K_{\mathfrak{t}}$ and $K_{\mathfrak{t}}(a^{1/p}, \alpha_i)/K_{\mathfrak{t}}(\alpha_i)$.

CASE 2: $\mathfrak{t} \notin S$, $\mathrm{ord}_{\mathfrak{t}} x = 0 = \mathrm{ord}_{\mathfrak{t}} c_i$ and $\mathrm{ord}_{\mathfrak{t}}((c_i x)^{-1} - 1) = 0$. In this case $\mathfrak{t}$ and its factors in $K(\alpha_i)$ are unramified in both extensions, and thus, since $c_i x$ is a unit at $\mathfrak{t}$, it is a local norm with respect to $\mathfrak{t}$ and its factors in both extensions, by Lemma 3.7.

CASE 3: $\mathfrak{t} \notin S$, $\mathrm{ord}_{\mathfrak{t}}(c_i x) < 0$ and $p | \mathrm{ord}_{\mathfrak{t}} x$ (under our assumption this is equivalent to the condition $p | \mathrm{ord}_{\mathfrak{t}}(c_i x)$). In this case, $\mathfrak{t}$ is again not ramified in either extension, and we can apply Lemma 3.7.

CASE 4: $\mathfrak{t} \notin S$, $\mathrm{ord}_{\mathfrak{t}} c_i x > 0$. By Lemma 3.5, $c_i x$ is a pth power in $K_{\mathfrak{t}}(\alpha_i)$. The rest of the argument proceeds as in case 1.

CASE 5: $\mathfrak{t} \in S$, $\mathfrak{t}$ is non-archimedean. By assumption on $\{c_i\}$, for any x there exists i such that for all $\mathfrak{t}$ in S, $c_i x$ is a pth power in $K_{\mathfrak{t}}$. Therefore, for this i, both equations will have solutions locally at all the primes of S and their factors in $K(\alpha_i)$.

Thus, we have shown that for $\mathfrak{t} \notin S$, both equations (3.11.1.i) and (3.11.2.i) have solutions locally at $\mathfrak{t}$ (and its factors) for any i, and we have shown that there exists i such that (3.11.1.i) and (3.11.2.i) have solutions locally for all non-archimedean $\mathfrak{t} \in S$. In case K is a number field we still have to consider archimedean valuations. Clearly, if the archimedean valuation is a complex one, both equations will have solutions. If the archimedean valuation is a real one, then since $p > 2$, $c_i x$ is a pth power in $\mathbb{R}$ and both equations have solutions.

Thus, for some i, both (3.11.1.i) and (3.11.2.i) will have solutions at all the primes and therefore, by the Hasse Norm Theorem, will have global solutions.

LEMMA 3.12: *Let K be as above and let S be any finite set of non-archimedean primes of K. Let M be any module of pseudo-S-integers. Then the set of non-zero elements of K has a Diophantine definition over M.*

Proof: The proof can proceed essentially along the same lines as the proof of Theorem 4.2 of [S5], the only difference being that after we select two primes $\mathfrak{p}$ and $\mathfrak{q}$ not in S we should let $a(\mathfrak{p})$ be such that $\mathrm{ord}_{\mathfrak{p}} a(\mathfrak{p})$ is greater than the allowable exponent of $\mathfrak{p}$ in the denominator of elements of M, so that $(a(\mathfrak{p}))^{-1} \notin M$. A similar requirement will apply to $a(\mathfrak{q})$.

LEMMA 3.13: *Let E be a global field and let $\mathfrak{p}$ be a non-archimedean prime. Then the set of elements of E integral at $\mathfrak{p}$ is Diophantine over E.*

Proof: If the field characteristic is different from 2 see [S5], §3. In the case the characteristic is 2, we cannot use norm forms from extensions of degree 2 as is done in the above reference. Let $\mathfrak{q} \neq \mathfrak{p}$ be another prime of E of prime degree $q > 2$. (Existence of such a prime can be derived from the proof of the Chebotarev density theorem.) Pick a rational prime $p > \max(3, h_E \,\mathrm{degree}(\mathfrak{p})\,\mathrm{degree}(\mathfrak{q}))$, where $h = h_E$ is the class number of E, and let x be an element whose divisor is of the form $(\mathfrak{p}^{\mathrm{degree}(\mathfrak{q})}/\mathfrak{q}^{\mathrm{degree}(\mathfrak{p})})^h$. Let $w = (xt^p + t^{-p})$. Then

$$\mathrm{ord}_{\mathfrak{p}} w \cong 0 \text{ modulo } p \Longleftrightarrow \mathrm{ord}_{\mathfrak{p}} t \geq 0.$$

Let $\{d_i\} \subset K = E(\xi_p)$, where ξ_p is a primitive pth root of unity, and assume $\{d_i\}$ satisfy the following conditions:

1. There exists a valuation $\mathfrak{t}$ of K such that every d_i is integral at all the primes except for $\mathfrak{t}$ and $\mathrm{ord}_{\mathfrak{t}} d_i \cong 0 \bmod p$.

2. For all i, $\mathrm{ord}_{\mathfrak{p}} d_i = 0$.

3. $\{\mathrm{ord}_{\mathfrak{q}} d_i\}$ runs through all the residue classes modulo p.

A finite set of such elements exists by Lemma 3.9. Let $\alpha_i = ((d_i w)^{-1} - 1)^{1/p}$, and let c be a constant such that $c \in K$ is not a pth power modulo $\mathfrak{p}$ in K. (Note that $\mathfrak{p}$ and $\mathfrak{q}$ might split in K. On the other hand, they do not ramify in this constant extension. So if $\mathfrak{p}_1$ ($\mathfrak{q}_1$) is a factor of $\mathfrak{p}$ ($\mathfrak{q}$) in K and $w \in E$, then $\mathrm{ord}_{\mathfrak{p}_1} w = \mathrm{ord}_{\mathfrak{p}} w$ ($\mathrm{ord}_{\mathfrak{q}_1} w = \mathrm{ord}_{\mathfrak{q}} w$). Thus, we will continue to treat $\mathfrak{p}$ and $\mathfrak{q}$ as if they remained prime in K with the understanding that a factor of $\mathfrak{p}$ or $\mathfrak{q}$ should be substituted for them, if $\mathfrak{p}$ or $\mathfrak{q}$ do not remain prime.) Next consider the following equations:

$$\mathbb{N}_{K(\alpha_i)/K}(y_1) = d_i w; \tag{3.13.1.i}$$

$$\mathbb{N}_{K(\alpha_i, c^{1/p})/K_i(\alpha)}(y_2) = d_i w. \tag{3.13.2.i}$$

First of all, we observe the following. If $\mathrm{ord}_{\mathfrak{p}} t < 0$ and consequently

$$\mathrm{ord}_{\mathfrak{p}} d_i w \not\cong 0 \text{ modulo } p,$$

as in the proof of Lemma 3.11, for all i, either (3.13.1.i) or (3.13.2.i) will have no solutions. So assume $\mathrm{ord}_{\mathfrak{p}} t \geq 0$ and thus $\mathrm{ord}_{\mathfrak{p}} w \cong 0 \,\mathrm{modulo}\, p$. Then, $\mathrm{ord}_{\mathfrak{p}} d_i w \cong 0 \,\mathrm{modulo}\, p$, and as in the proof of Lemma 3.10, for all i, both norm equations will have solutions locally with respect to $\mathfrak{p}$ and its factors in $K(\alpha_i)$.

Next let $\mathfrak{r}$ be a prime different from $\mathfrak{p}$ and $\mathfrak{q}$. Fix any i. Then if $\mathfrak{r} = \mathfrak{t}$ is a pole of $d_i w$, then in the extensions $K(\alpha_i)/K$ and $K(\alpha_i, c^{1/p})/K(\alpha_i)$, $\mathfrak{r}$ and its factors are not ramified since $d_i w$ has a pole of degree equivalent to 0 modulo p at $\mathfrak{r}$ and any of its factors in $K(\alpha_i)$. Thus, both norm equations will have solutions locally at such a prime $\mathfrak{r}$ and its factors in $K(\alpha_i)$. If $\mathfrak{r}$ is a zero of $d_i w$ or a zero of $(d_i w)^{-1} - 1$, then as in the argument in the proof of Lemma 3.11, $d_i w$ is a pth power locally at all the factors of $\mathfrak{r}$ in $K(\alpha_i)$ and $K(\alpha_i, c^{1/p})$ and therefore both norm equations will have solutions. Finally, if $\mathfrak{r}$ is not a zero or a pole of $d_i w$ or $(d_i w)^{-1} - 1$, then it is not ramified in either extension, and $d_i w$, as a unit at $\mathfrak{r}$, is a local norm again.

Thus, if $\mathrm{ord}_{\mathfrak{p}} t \geq 0$, for all i, both equations will have local solutions at all primes different from $\mathfrak{q}$. Furthermore, for some i, $\mathrm{ord}_{\mathfrak{q}} d_i w \cong 0$ modulo p, and thus for this i, both norm equations will have local solutions at $\mathfrak{q}$ and its factors in $K(\alpha_i)$. Therefore, again by the strong Hasse norm principal, for this i, we will have global solutions to both norm equations.

Since we can rewrite equation (3.13.1.i) and (3.13.2.i) as equivalent polynomial equations over E, we are done.

LEMMA 3.14: *Let E be a global field, let p be a rational prime different from the characteristic of the field, let $a \in E$, let T be a set of all primes $\mathfrak{q}$ of E such that $x^p - a$ is irreducible modulo $\mathfrak{q}$, let S be a finite set of non-archimedean primes of E, let $n \in \mathbb{N}$. Then $M_{n,T,S}$ is recursive.*

(Follows from the discussion in §2.)

LEMMA 3.15: *Let F be a finite field. Let $a \in F$ and let p be a rational prime distinct from the characteristic of the field. Then $G(X) = X^p - a \in F[X]$ is irreducible if and only if a is not a pth power in F and F contains pth roots of unity.*

Proof: Suppose a is not a pth power and F contains pth roots of unity. Then by Lemma 3.10, any pth root of a is of degree p over F and $G(X)$ is irreducible.

Conversely, suppose the polynomial is irreducible and let a be a root of $G(X)$. Then $[F(\alpha)\colon F] = p$. On the other hand, all extensions of finite fields are normal and consequently $F(\alpha)$ will contain roots of unity. But if pth roots of unity are not in F, the extension $F(\alpha)/F$ contains a non-trivial subextension of degree equal to or less than $p - 1$. Thus, we have a contradiction.

COROLLARY 3.16: *Let K be a global field, let p be a rational prime distinct from the characteristic of the field, let $\mathfrak{p}$ be a K-prime such that $\mathfrak{p}$ is not a factor of p, let $a \in K$ be a unit at $\mathfrak{p}$, let ξ_p be a primitive pth root of unity. Then a polynomial $G(X) = X^p - a$ is irreducible modulo $\mathfrak{p}$ if and only if the extension $K(\xi_p, a^{1/p})/K(\xi_p)$ is of degree p, and a factor of $\mathfrak{p}$ in $K(\xi_\mathfrak{p})$ remains prime in this extension.*

Proof: Suppose $G(X)$ is irreducible modulo $\mathfrak{p}$. Then $G(X)$ is irreducible over K, and $[K(a^{1/p})\colon K] = p$. Since $[K(\xi_p)\colon K] \leq p - 1$, $a^{1/p} \notin K(\xi_p)$ and thus by an argument similar to the one used in Lemma 3.10, $[K(\xi_p, a^{1/p})\colon K(\xi_p)] = p$. Furthermore, by Lemma 3.15, a is not a pth power modulo $\mathfrak{p}$ and the residue field modulo $\mathfrak{p}$ contains pth roots of unity. Therefore, either K contains pth roots of unity or $\mathfrak{p}$ splits completely in the extension $K(\xi_p)/K$. On the other hand, in either case, the residue field of any factor of $\mathfrak{p}$ in $K(\xi_p)$ is the same as the residue field of $\mathfrak{p}$. Thus, $G(X)$ is irreducible over the residue field of any factor of $\mathfrak{p}$ in $K(\xi_p)$, and hence these factors will not split in the extension $K(\xi_p, a^{1/p})/K(\xi_p)$.

Conversely, if one of the factors of $\mathfrak{p}$ in $K(\xi_p)$ did not split in the above extension which is of degree p, then $a^{1/p}$ must be of degree p over the residue field of this factor, but then $a^{1/p}$ must be of degree p over the residue field of $\mathfrak{p}$, and thus the polynomial $G(X)$ must be irreducible modulo $\mathfrak{p}$.

THEOREM 3.17: *Let E be an algebraic number field or an algebraic function field over a finite field of constants. Let $p > 2$ be distinct from the characteristic of the field, and let T be a collection of non-archimedean primes of E such that for some $a \in E$, for all $\mathfrak{p} \in T$, the polynomial $x^p - a$ is irreducible modulo $\mathfrak{p}$. Let $\overline{S}$ be a finite collection of non-archimedean primes of E and let $n < p$.*

Then $O_{E,\overline{S}}$ has a Diophantine definition over $M_{n,T,\overline{S}}$.

Proof: If E is a number field then let $K = E(\xi_p)$, where ξ_p is a primitive pth root of unity. If E is an algebraic function field, then let K be a field which is obtained from E by adjoining primitive pth root of unity and, if E does not have a prime of relative degree 1, by adjoining a constant of degree prime to p over E, so that the resulting field has a degree 1 prime. If such a prime of degree 1 is not in $\overline{S}$, then add this prime together with all the zeros and poles of a, and in the case of a number fields, together with all the factors of p, to $\overline{S}$, and call the resulting set S. The only primes which will ramify in the above described extension are factors of p (in the case of a number field). Therefore, if t lies above some prime of E which is not a factor of p, and $x \in E$, then x will have the same order at t as at a prime above it in K. Furthermore, by Lemma 3.16, a will be of degree p over the residue fields of all the primes above primes in T.

Next consider equations (3.11.1.i), (3.11.2.i) with the above described K and S. These equations can be rewritten as equivalent polynomial equations over K and $K(\alpha_i)$ respectively, which can then be rewritten as equivalent polynomial equations over E. Furthermore, since, as we have noted above, the set of non-zero elements of $M_{n,T,\overline{S}}$ has a Diophantine definition over $M_{n,T,\overline{S}}$, we can then rewrite all the polynomial equations over K as equivalent polynomial equations over $M_{n,T,\overline{S}}$.

Given $x \in M_{n,T,\overline{S}}$, using Lemma 3.13, we can write down a system of Diophantine equations assuring that x does not have poles at valuations of $W\backslash\overline{S} \cup S\backslash\overline{S}$, where W is as in the proof of Lemma 3.11. Finally, if $x \in M_{n,T,\overline{S}}$ and x does not have poles at $W\backslash\overline{S} \cup S\backslash\overline{S}$ then for some i, (3.11.1.i) and (3.11.2.i) have solutions in the corresponding fields if and only if $x \in O_{E,\overline{S}}$. ∎

For future reference denote the set of equations used to form the above described Diophantine definition by $DD(n, T, \bar{S}, p, a)$.

COROLLARY 3.18: *Let E be any number field where the Diophantine problem is undecidable over the ring of integers, let $M_{n,T,\bar{S}}$ be as above and let $P(x_1, \ldots, x_n) = 0$ be any polynomial equation over E. Then there is no algorithm to decide whether this equation has solutions in $M_{n,T,\bar{S}}$. (Note that the corresponding result concerning algebraic function fields over finite fields of constants has been known before, since it is implied by the Diophantine undecidability of the field.)*

We will next show that by combining several systems of the form $DD(n, T, S, p, a)$ for different p's and a's we can make the density of T arbitrarily large.

LEMMA 3.19: *Let K be a global field. Let R_1/K and R_2/K be two Galois extensions of K such that $[R_1R_2\colon R_1] = [R_2\colon K]$ and $[R_1R_2\colon R_2] = [R_1\colon K]$. Then the following statements are true:*

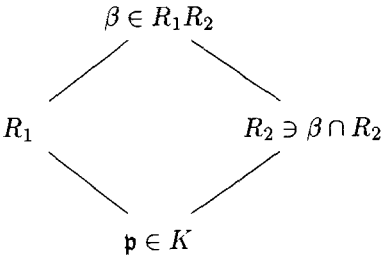
1. *R_1R_2/K is Galois, $\mathrm{Gal}(R_1R_2/K) \cong \mathrm{Gal}(R_1/K) \oplus \mathrm{Gal}(R_2/K)$, and for $i = 1, 2$, $i \neq j$, $\mathrm{Gal}(R_1R_2/R_i) \cong \mathrm{Gal}(R_j/K)$.*
2. *Let β be a prime of R_1R_2 and let $\mathfrak{p}$ be the prime below β in K. Then $\mathfrak{p}$ splits completely in R_2 if and only if the Frobenius automorphism of β is of the form (σ, identity), where $\sigma \in \mathrm{Gal}(R_1/K)$, and the second element of the pair is the identity element of the $\mathrm{Gal}(R_2/K)$.*

Proof: 1. Let α_i be the generator of R_i over K. Then α_i will retain the same conjugates over R_j, for $i \neq j$, $i, j = 1, 2$. Furthermore, each element of $\mathrm{Gal}(R_1R_2/K)$ will be determined by the images of α_1 and α_2, while each element of $\mathrm{Gal}(R_i/K)$ is determined by the image of α_i. Thus we have a one-to-one onto map between $\mathrm{Gal}(R_1R_2/K)$ and $\mathrm{Gal}(R_1/K) \oplus \mathrm{Gal}(R_2/K)$ as sets and it is easy to verify that it is an isomorphism. Finally, given the above argument it is clear that for $i, j = 1, 2$, $i \neq j$,

$$\mathrm{Gal}(R_1R_2/R_i) = \{(\sigma, \text{ identity}) | \ \sigma \in \mathrm{Gal}(R_j/K)\}.$$

2. Consider the following diagram:

(3.19.1)



and let β and $\mathfrak{p}$ be as described in the statement of the lemma. Let τ be the Frobenius automorphism of β over K. Then $\langle\tau\rangle$ is the decomposition group of β over K and $\langle\tau\rangle \cap \mathrm{Gal}(R_1R_2/R_2)$ is the decomposition group of β over R_2. Furthermore, the decomposition group of $\beta \cap R_2$ over K is isomorphic the quotient $\langle\tau\rangle/\langle\tau\rangle \cap \mathrm{Gal}(R_1R_2/R_2)$. But since $\mathfrak{p}$ splits completely in R_2, this quotient is trivial, and thus $\langle\tau\rangle \subseteq \mathrm{Gal}(R_1R_2/R_2)$. Hence, τ must be of the desired form. Conversely, suppose $\sigma \in \mathrm{Gal}(R_1/K)$, and consider $\tau = (\sigma,$ identity$) \in \mathrm{Gal}(R_1R_2/K)$. Let β be a prime whose Frobenius automorphism is τ. Then since $\tau \in \mathrm{Gal}(R_1R_2/R_2)$, $\langle\tau\rangle$ is the decomposition group of β over R_2, and thus the decomposition group of $\beta \cap R_2$ over K is trivial. Thus $\mathfrak{p}$ will split completely in R_2.

COROLLARY 3.20: *Let K be a global field; let $\{L_i\}$ be a sequence of Galois extensions of K satisfying the following requirements:*

1. *Let $T_{i_1\cdots i_k} = L_{i_1}\cdots L_{i_k}$. Then for any $i_{k+1} \in \mathbb{N}\backslash\{i_1,\ldots,i_k\}$,*

$$[T_{i_1\cdots i_{k+1}}\colon T_{i_1\cdots i_k}] = [L_{i_{k+1}}\colon K] \text{ and } [T_{i_1\cdots i_{k+1}}\colon L_{k+1}] = [T_{i_1\cdots i_k}\colon K].$$

2. *For any $\{i_1,\ldots,i_k\} \subset \mathbb{N}$, $T_{i_1\cdots i_k}$ is Galois over K.*

Let $E_{k+1} = L_1\cdots L_{k+1} = T_{1\cdots(k+1)}$, let $\tau_{k+1} \in \mathrm{Gal}(E_{k+1}/K)$.

Then either all K-primes $\mathfrak{p}$ with an E_{k+1}-factor whose Frobenius automorphism is τ_{k+1} split completely in some L_i, $i = 1,\ldots,k+1$, or none of them do.

Proof: Assume there exists a prime $\mathfrak{p}$ in K, such that $\mathfrak{p}$ splits completely in some L_i, $1 \le i \le k+1$ and $\mathfrak{p}$ has a factor β in E_{k+1} whose Frobenius automorphism is τ_{k+1}. We will prove that all the other primes $\mathfrak{q}$ of K with factors γ in E_{k+1} whose Frobenius automorphism is τ_{k+1} will split completely in this L_i.

First, we write $E_{k+1} = T_{1\cdots(i-1)(i-1)\cdots k}L_i$, and note that we can apply Lemma 3.19 with $R_1 = T_{1\cdots(i-1)(i+1)\cdots k}$ and $R_2 = L_i$. Thus, we conclude $\mathfrak{p}$ splits completely in L_i if and only if $\tau_{k+1} = (\sigma_{k+1},$ identity$)$, where $\sigma_{k+1} \in$

$\mathrm{Gal}(T_{1\cdots(i-1)(i+1)\cdots k}/K)$ and the second element is the identity of $\mathrm{Gal}(L_i/K)$. The last assertion, however, is true if and only if all $\mathfrak{q}$'s as described above will split completely in L_i.

LEMMA 3.21: *Let K be a global field; let $\{L_i\}$ be a sequence of Galois extensions of K satisfying the requirements 1 and 2 from Corollary 3.20 as well as the following requirements:*

3. $\sum_{i=1}^{\infty} \frac{1}{[L_i\colon K]} = \infty$.
4. *For all $i \in \mathbb{N}$, the extension L_i/K is abelian.*

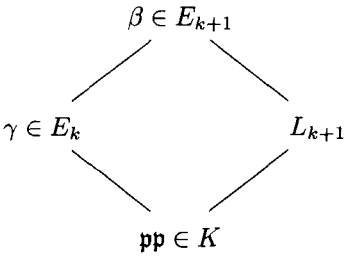
Let S_k be the density of the set of all the primes of K splitting completely in some L_i for $1 \leq i \leq k$. Then $\lim_{k\to\infty} S_k = 1$.

Proof: We will prove by induction that

$$S_{k+1} = S_k + \frac{1}{[E_{k+1}\colon K]}(1 - S_k).$$

Consider the primes in $S_{k+1}\backslash S_k$. Let $\mathfrak{p}$ be a prime in the above described set and apply Lemma 3.19 with $R_1 = E_k$ and $R_2 = L_{k+1}$ using the diagram below:

(3.21.1)



Then in E_{k+1}, $\mathfrak{p}$ has a factor β whose Frobenius automorphism is $\tau = (\sigma, \text{identity})$, where $\sigma \in \mathrm{Gal}(E_k/K)$ and the second element is the identity of $\mathrm{Gal}(L_{k+1}/K)$. Thus, $\tau_{|E_k} = \sigma$. Conversely, for each $\sigma \in \mathrm{Gal}(E_k/K)$, τ is a Frobenius automorphism of some E_{k+1}-prime β, such that $\mathfrak{p}$, the prime below it in K, splits completely in L_{k+1}. Let γ be the E_k-prime above $\mathfrak{p}$. Then γ splits completely in E_{k+1}. Therefore, the decomposition group of γ over $\mathfrak{p}$ is isomorphic to the decomposition group of β over $\mathfrak{p}$, and hence, σ is the Frobenius automorphism of γ over $\mathfrak{p}$.

By assumption, $\mathfrak{p}$ does not split completely in any L_i, $i = 1, \ldots, k$. Thus $\mathfrak{p}$ belongs to the set whose density is $1 - S_k$. Furthermore, from the previous corollary, all the primes in this set can be divided into non-intersecting classes

corresponding to the Frobenius automorphisms of their factors in E_k. Using the Chebotarev density theorem and the fact that all extensions are abelian, we can conclude the number of elements of $\mathrm{Gal}(E_k/K)$ which are Frobenius automorphisms of E_k-primes lying above primes of K which do not split in any L_i for $i = 1, \ldots, k$ is $(1 - S_k) \cdot [E_K\colon K]$. Therefore, we have $(1 - S_k) \cdot [E_K\colon K]$ elements of $\mathrm{Gal}(E_{k+1}/K)$ which are Frobenius automorphisms of the primes lying above the primes in $S_{k+1} \backslash S_k$. Therefore, the density of this prime set is

$$(1 - S_k) \cdot [E_K\colon K]/[E_{k+1}\colon K] = (1 - S_k) \cdot [L_{k+1}\colon K]^{-1}.$$

Suppose now $\lim_{k\to\infty} S_k \neq 1$. Since $\{S_k\}$ is a non-decreasing bounded sequence, it must have a limit. Suppose this limit $A < 1$. Then $1 - S_k \geq 1 - A$ for all k. But then

$$S_{k+1} > S_k + (1 - A) \cdot [L_{k+1}\colon K]^{-1},$$

$$S_{k+1} > (1 - A) \sum_{i=1}^{k+1} \frac{1}{[L_i\colon K]} \to \infty.$$

COROLLARY 3.22: *Let K be a number field, and let $\{p_i\}_{i\in\mathbb{N}}$ be the sequence of all rational primes which do not have ramified factors in K. For each $i \in \mathbb{N}$, let ξ_i be a p_ith primitive root of unity and let S_k be the density of the set of primes of K splitting completely in $K(\xi_i)$ for some $1 \leq i \leq k$. Then $\lim_{k\to\infty} S_k = 1$.*

Proof: We have to show that all the conditions of Lemma 3.21 are satisfied.

First of all, we will show that $[K(\xi_{i_1} \cdots \xi_{i_{k+1}})\colon K(\xi_{i_1} \cdots \xi_{i_k})] = [K(\xi_{k+1})\colon K]$. In the extension, $K(\xi_{i_1} \cdots \xi_{i_{k+1}})/\mathbb{Q}$, the ramification degree of a factor of $p_{i_{k+1}}$, is at least $p_{i_{k+1}} - 1$. On the other hand, by assumption $p_{i_{k+1}}$ does not have any ramified factors in the extension $K/\mathbb{Q}$ and no ramified factors in the extension $K(\xi_{i_1} \ldots \xi_{i_k})/K$. Thus,

$$[K(\xi_{i_1} \cdots \xi_{i_{k+1}})\colon K(\xi_{i_1} \cdots \xi_{i_i})] = [K(\xi_{k+1})\colon K] = p_{i_{k+1}} - 1.$$

All the extensions are clearly Galois and abelian by Lemma 3.19 and induction. Finally, $\sum_{i=1}^{\infty} \frac{1}{p_i - 1}$ diverges since we removed only finitely many primes.

COROLLARY 3.23: *Let K be an algebraic function field over a finite field of constants C of size q. Let $\{p_i\}_{i\in\mathbb{N}}$ be a sequence of all rational primes which does not include factors of q. For each $i \in \mathbb{N}$, let ξ_i be a primitive q_ith root of*

unity, where q_i is a rational prime, $q_i | \frac{q^{p_i}-1}{q-1}$ and $q_i \not| (q-1)$. Then the following statements are true:

1. *For each i the above described q_i exists.*
2. $[K(\xi_i)\colon K] = p_i$.
3. $q_i \neq q_j$, *for* $j \neq i$.
4. *Let S_k be the density of the set of primes of K splitting completely in $K(\xi_i)$ for some $1 \leq i \leq k$. Then* $\lim_{k\to\infty} S_k = 1$.

Proof: 1. Let t be a common divisor of $q-1$ and $\frac{q^{p_i}-1}{q-1} = q^{p_i-1} + \cdots + 1$. Then $t | p_i$, i.e. $t = p_i$.

2. Since $q_i \not| q-1$, q_ith primitive roots of unity are not elements of C. On the other hand, if C_i is the extension of degree p_i of C, then $\xi_i \in C_i$. Thus, $C(\xi_i) = C_i$ since the extension C_i/C is of prime degree and therefore has no subextensions. Thus, $[K(\xi_i)\colon K] = p_i$.

3. $\xi_i \notin C_j$, where C_j is the extension of degree $p_j \neq p_i$ of C, since the extension C_j/C does not have subextensions of degree p_i. Thus $q_i \neq q_j$ for $i \neq j$.

4. First of all, the equality $[K(\xi_{i_1} \cdots \xi_{i_{k+1}})\colon K(\xi_{i_1} \cdots \xi_{i_k})] = [K(\xi_{k+1})\colon K]$ follows from the fact that for each pair $i \neq j$, $([K(\xi_i)\colon K], [K(\xi_j)\colon K]) = 1$. Since we are talking about extensions of finite fields, all the extensions are Galois and abelian. Finally, as in the preceding corollary $\sum_{i=1}^{\infty} 1/p_i$ diverges.

LEMMA 3.24: *Let K be a global field, let p be a rational prime distinct from the characteristic of the field. Let ξ be a primitive pth root of unity. Let $a_1, \ldots, a_k \in K$ be such that there exists a set of distinct K-primes $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_k\}$ satisfying the following conditions:*

1. $\mathrm{ord}_{\mathfrak{q}_i} a_i = 1$.
2. $\mathrm{ord}_{\mathfrak{q}_i} a_j = 0$ *for* $i \neq j$.
3. *If K is a number field then, for all $i = 1, \ldots, k$, $\mathfrak{q}_i$ is not a factor of p.*

Then the density of the set of K-primes which split completely in $K(\xi)$ but whose factors do not remain prime in any of the extensions $K(a_i^{1/p}, \xi)/K(\xi)$ is

$$\frac{1}{[K(\xi, a_1^{1/p}, \ldots, a_k^{1/p})\colon K]} = \frac{1}{[K(\xi)\colon K]p^k}.$$

Proof: First of all, we note that $a_1, \ldots, a_k \in K$ exist by the Weak Approximation Theorem. Secondly, we note that for each $i = 1, \ldots, k$, by construction, $\mathfrak{q}_i$ does not ramify in the extension $K(\xi, a_1^{1/p}, \ldots, a_{i-1}^{1/p}, a_{i+1}^{1/p}, \ldots a_k^{1/p})/K$ but does have ramification degree p in the extension $K(\xi, a_1^{1/p}, \ldots, a_k^{1/p})/K$, so that

indeed $[K(\xi, a_1^{1/p}, \ldots, a_k^{1/p})\colon K] = [K(\xi)\colon K]p^k$. Furthermore, suppose $\mathfrak{p}$ splits completely in $K(\xi)$, but a factor β of $\mathfrak{p}$ does not remain prime in any of the extensions $K(\xi, a_i^{1/p})/K(\xi)$. Since all of these extensions are cyclic of degree p, this means β splits completely in all these extensions. On the other hand, let M be any finite extension of $K(\xi)$ and assume β splits completely in the extension $K(\xi, a_i^{1/p})/K(\xi)$. Then, assuming $M(\xi)$ does not contain $a_i^{1/p}$, all the factors of β will split completely in the extension $M(\xi, a_i^{1/p})/M(\xi)$. Thus, β will split completely in $K(\xi, a_1^{1/p}, \ldots, a_k^{1/p})/K(\xi)$. Therefore $\mathfrak{p}$ will split completely in $K(\xi, a_1^{1/p}, \ldots, a_k^{1/p})/K$. Consequently, the desired conclusion follows from the Chebotarev density theorem.

THEOREM 3.25: *Let T be an arbitrary set of non-archimedean primes of a global field K. Let n be any positive integer. Then for any $\delta > 0$ there exists a module of pseudo-integers $M_{n,T_\delta,S}$ such that $T_\delta \subset T$, the Dirichlet density of some set containing $T - T_\delta$ is less than δ, and S-integers are polynomially definable over $M_{n,T_\delta,S}$.*

Proof: Assume $\delta > 0$ is given. Let $\{p_i\}$ be a sequence of rational primes such that in the case of a number field, the primes in the sequence are greater than n and satisfy the requirement of Corollary 3.22. In the case of a function field, the sequence $\{p_i\}$ should be such that the corresponding sequence $\{q_i\}$, as defined in Corollary 3.23, contains only the primes which are greater than n.

Let k be large enough so that $|1 - S_k| < \delta/2$, where S_k is defined in Corollary 3.22 or 3.23, depending on the nature of the field. Next, for each $i = 1, \ldots, k$, select $a_{i1}, \ldots, a_{im}$ satisfying the requirements of Corollary 3.23 and assume that m is large enough so that in the case of a number field for all i, $1/(p_i - 1)p_i^m < \delta/2k$, and in the case of a function field $1/(p_i \cdot q_i^m) < \delta/2k$, where q_i is defined as in Corollary 3.23. Next consider equations $\bigcup_{i,j=1}^{k,m} DD(n, T_{ij}, S, p_i, a_{ij})$ for number fields, $\bigcup_{i,j=1}^{k,m} DD(n, T_{ij}, S, q_i, a_{ij})$ for function fields, where T_{ij} is the set of K primes whose factors in $K(\xi_i)$ remain prime in the extension $K(\xi_i, a_{ij}^{1/p_i})/K(\xi_i)$ or $K(\xi_i, a_{ij}^{1/q_i})/K(\xi_i)$ depending on the nature of the field. Let $T = \bigcup_{i,j=1}^{k,m} T_{ij}$. By Theorem 3.17 and Corollary 3.16, these equations will be a Diophantine definition of $O_{K,S}$ over $M_{n,T,S}$. Suppose a K-prime $\mathfrak{p} \notin T$. Then either $\mathfrak{p}$ does not split completely in any extension $K(\xi_i)/K$, or for some i, $\mathfrak{p}$ splits completely in some extension $K(\xi_i)/K$, but no factor of $\mathfrak{p}$ in $K(\xi_i)$ remains prime in any extension $K(\xi_i, a_{ij}^{1/p_i})/K(\xi_i)$ or $K(\xi_i, a_{ij}^{1/q_i})/K(\xi_i)$ depending on the nature of

the field. Thus, $\mathfrak{p}$ will belong to a set whose density is less than $\delta/2 + k\delta/2k = \delta$.

References

[Da] M. Davis, *Hilbert's tenth problem is unsolvable,* American Mathematical Monthly **80** (1973), 233–269.

[Da-Mat-Ro] M. Davis, Yu. Matijasevich and J. Robinson, *Positive aspects of a negative solution,* Proceedings of Symposia in Pure Mathematics, American Mathematical Society **28** (1976), 323–378.

[D1] J. Denef, *Hilbert's tenth problem for quadratic rings,* Proceedings of the American Mathematical Society **48** (1975), 214–220.

[D2] J. Denef, *Diophantine sets over* $\mathbb{Z}[T]$, Proceedings of the American Mathematical Society **69** (1978), 148–150.

[D3] J. Denef, *The Diophantine problem for polynomial rings and fields of rational functions,* Transactions of the American Mathematical Society **242** (1978), 391–399.

[D-L] J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers,* Journal of the London Mathematical Society (2) **18** (1978), 385–391.

[D4] J. Denef, *The Diophantine Problem for Polynomial Rings of Positive Characteristic,* Logic Colloquium 78 (M. Boffa, D. van Dalen and K. MacAloon, eds.), North-Holland, Amsterdam, 1979, pp. 131–145.

[D5] J. Denef, *Diophantine sets of algebraic integers. II,* Transactions of the American Mathematical Society **257** (1980), 227–236.

[H] P. Hilton, *On groups of pseudo-integers,* Archiv för Mathematik Sinica 4 **2** (1988), 189–192.

[J] G. Januz, *Algebraic Number Fields,* Academic Press, New York, 1973.

[K-R1] K. H. Kim and F. W. Roush, *Diophantine unsolvability for function fields over certain infinite fields of characteristic p,* Journal of Algebra **152** (1992), 230–239.

[K-R2] K. H. Kim and F. W. Roush, *Diophantine undecidability of* $\mathbb{C}(t_1, t_2)$, Journal of Algebra **150** (1992), 35–44.

[K-R3] K. H. Kim and F. W. Roush, *Diophantine unsolvability over p-adic function fields,* Journal of Algebra, to appear.

[L] S. Lang, *Algebraic Number Theory,* Addison-Wesley, Reading, MA, 1970.

[M1] B. Mazur, *The topology of rational points*, Experimental Mathematics **1** (1992), 35–45.

[M2] B. Mazur, *Questions of decidability and undecidability in number theory*, Journal of Symbolic Logic **59** (1994), 353–371.

[M-R] R. Militello and H. Ries, *On pseudofree groups and sequential representations*, New Zealand Journal of Mathematics **23** (1994), 137–146.

[O] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag, New York, 1973.

[Ph1] T. Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers*, Proceedings of the American Mathematical Society **104** (1988), 611–620.

[Ph2] T. Pheidas, *Hilbert's tenth problem for fields of rational functions over finite fields*, Inventiones Mathematicae **103** (1991), 1–8.

[Po] M. Pohst, *Computational Number Theory*, Birkhäuser Verlag, Basel, 1993.

[R1] H. Ries, *On extensions of pseudo-integers*, Publicacions Matemàtique **37** (1993), 387–401.

[R2] H. Ries, *On the calculation of a certain extension group*, Bulletin de la Société Mathématique de Belgique **45** (1993), 199–209.

[Sei] A. Seidenberg, *Constructions in algebra*, Transactions of the American Mathematical Society **197** (1974), 273–313.

[Sha-Sh] H. N. Shapiro and A. Shlapentokh, *Diophantine relations between algebraic number fields*, Communications on Pure and Applied Mathematics **47** (1989), 1113–1122.

[S1] A. Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields*, Communications on Pure and Applied Mathematics **42** (1989), 939–962.

[S2] A. Shlapentokh, *Hilbert's tenth problem for rings of algebraic functions of characteristic zero*, Journal of Number Theory **40** (1992), 218–236.

[S3] A. Shlapentokh, *Hilbert's tenth problem for rings of algebraic functions in one variable over fields of constants of positive characteristic*, Transactions of the American Mathematical Society **333** (1992), 275–298.

[S4] A. Shlapentokh, *A Diophantine definition of rational integers in some rings of algebraic numbers*, Notre Dame Journal of Formal Logic **33** (1992), 299–321.

[S5] A. Shlapentokh, *Diophantine classes of holomorphy rings of global fields*, Journal of Algebra **169** (1994), 139–175.

[S6] A. Shlapentokh, *Diophantine undecidability for some holomorphy rings of algebraic functions of characteristic* 0, Communications in Algebra **22** (1994), 4379–4404.

[S7] A. Shlapentokh, *Diophantine undecidability of algebraic function fields over finite fields of constants*, Journal of Number Theory, to appear.

[V] C. Videla, *Hilbert's tenth problem for rational function fields in characteristic 2*, Proceedings of the American Mathematical Society **120** (1994), 249–253.

[W] Andre Weil, *Basic Number Theory*, Springer-Verlag, New York, 1974.