Arithmetic over the ring of all algebraic integers

To the memory of Julia Robinson

By *Robert S. Rumely**) at Athens

In this note we will establish two theorems about diophantine equations over the ring of all algebraic integers. Let V be a geometrically irreducible affine variety defined over a number field K; let $\tilde{\mathcal{O}}$ denote the ring of all algebraic integers, and for each finite place v of K, let $\tilde{\mathcal{O}}_v$ be the ring of integers in the algebraic closure of K_v. The first theorem is a general local-global principle: V has points over $\tilde{\mathcal{O}}$ if and only if it has points over $\tilde{\mathcal{O}}_v$, for every v. The second is an application of the first: Hilbert's Tenth Problem has a positive solution over $\tilde{\mathcal{O}}$.

Both results had been conjectured by David Cantor, and proved by him and Roquette ([2]) for rationally parametrizable varieties. Our proof of the local-global principle follows the same lines as theirs, the main new ingredient being a Fekete-Szegö theorem on algebraic curves given by the author in ([11]). The local-global principle generalizes an old theorem of Skolem ([14]), which gave a criterion for a polynomial in several variables to represent units over $\tilde{\mathcal{O}}$. It also implies some of the results proved by Estes and Guralnick ([3], [5]) concerning equivalence of modules and similarity of matrices over $\tilde{\mathcal{O}}$. The solution to Hilbert's Tenth Problem is a consequence of the existence of a decision procedure for the first-order theory of valued, algebraically closed fields (Robinson [10], Weispfenning [18]), together with effective constructions in algebraic geometry (Seidenberg [12], van den Dries [15], [16]). These, combined with the local-global principle, yield an algorithm for determining when a system of diophantine equations and inequalities is solvable over $\tilde{\mathcal{O}}$. This was anticipated in ([2]).

Our notations are standard. In addition to those above, $\tilde{K}_v$ is the algebraic closure of the completion K_v, $\tilde{K}$ is the algebraic closure of K, and $\mathcal{O}_K$ is the ring of integers of K.

The author would like to thank Roy Smith and Robert Varley for their help with algebraic geometry, and Professors Cantor and Roquette for their encouragement and receptiveness. The publication of these results has been delayed, and several people have

*) Research supported in part by grants from the Alfred P. Sloan Foundation and the National Science Foundation.

suggested improvements. Especially, Jan Denef supplied the reference to Weispfenning's work, which makes the algorithm for Hilbert's problem primitive recursive. Robert Guralnick pointed out the applications noted above. Finally, Professor Roquette has obtained a self-contained proof of the local-global principle, which he will publish soon.

I. The idea for the local-global principle is simple. One direction is trivial. If V has points over $\tilde{\mathcal{O}}$, then clearly it has points over $\tilde{\mathcal{O}}_v$ for every v. Conversely, suppose V has points over $\tilde{\mathcal{O}}_v$ for all v. To produce a point over $\tilde{\mathcal{O}}$, we first reduce to the case of a curve, cutting V by hypersurfaces, using Bertini's theorem to maintain irreducibility. Then we apply the Fekete-Szegö theorem on the curve to prove that the global algebraic points are dense in the adelic points. Note that V need not be smooth.

Theorem 1 (Local-global principle for $\tilde{\mathcal{O}}$). *Let V be a geometrically irreducible affine variety defined over K. Then $V(\tilde{\mathcal{O}}) \neq \emptyset$ if and only if $V(\tilde{\mathcal{O}}_v) \neq \emptyset$, for all finite places v of K.*

For use with Hilbert's problem, it is useful to formulate a slightly more general version in algebraic guise.

Theorem 1′. *Let $F_i(\vec{x}, \vec{y}) \in K[x_1, \dots, x_m, y_1, \dots, y_n]$, $i = 1, \dots, r$, be polynomials which define a geometrically irreducible affine variety $V \subset \mathbb{A}^{m+n}$. Then V has points belonging to $\tilde{\mathcal{O}}^m \times \tilde{K}^n$ if and only if it has points belonging to $\tilde{\mathcal{O}}_v^m \times \tilde{K}_v^n$ for every finite place v of K.*

Both of these are immediate consequences of the following density theorem. Let V be an geometrically irreducible variety over K (not necessarily affine), and for each place v of K (finite or not), let B_v be a non-empty open subset of $V(\tilde{K}_v)$ in the v-topology. We suppose that each B_v is stable under $\mathrm{Gal}(\tilde{K}_v/K_v)$, and that $\prod_v B_v$ is large in the following sense: there is some affine open $W \subset V$ defined over K such that for all but finitely many v, $W(\tilde{\mathcal{O}}_v) \subset B_v$.

Proposition (Density theorem). *Fix a place v_0 of K. Then there exists a point $\zeta \in V(\tilde{K})$ such that for every $v \neq v_0$, all the conjugates of ζ over K belong to B_v.*

The condition that the conjugates belong to B_v is independent of the choice of embedding $\tilde{K} \hookrightarrow \tilde{K}_v$, since B_v is galois stable. By replacing V with W, and B_v with $B_v \cap W(\tilde{K}_v)$, it suffices to prove the proposition when V is affine. The next step is to reduce from V to a curve $C \subset V$. Some care is needed to insure that $C(\tilde{K}_v) \cap B_v$ is nonempty for every v, and that C is irreducible.

To do this, we first produce a finite, galois stable set of points in $V(\tilde{K})$, at least one of which belongs to B_v, for every v, and then arrange for C to pass through these points. Fix some $\alpha \in V(\tilde{K})$. There is a finite set S of places of K such that for every $v \notin S$, α or some conjugate of α over K belongs to $V(\tilde{\mathcal{O}}_v)$. By enlarging S, we can assume it contains all v such that B_v does not contain $V(\tilde{\mathcal{O}}_v)$, as well as all archimedean v. For each $v \in S$, choose $\alpha_v \in B_v$ so that α_v is algebraic over K. This is possible since $V(\tilde{K})$ is dense in $V(\tilde{K}_v)$ for any embedding $\tilde{K} \hookrightarrow \tilde{K}_v$. Let $\mathscr{A}$ be the set of conjugates of α and the α_v over K.

Suppose V is embedded in $\mathbb{A}^N$, and let $\hat{V}$ be its closure in $\mathbb{P}^N$. Let $\hat{Y}$ be the variety obtained by blowing up $\hat{V}$ at each of the points in $\mathscr{A}$. Since $\mathscr{A}$ is galois stable, $\hat{Y}$ is defined over K. It is also irreducible and projective. Let $p: \hat{Y} \to \hat{V}$ be the natural projection. Embed $\hat{Y}$ in $\mathbb{P}^M$ for an appropriate M; we can assume it is not contained in any hyperplane. By Bertini's theorem (see Fulton and Lazarsfeld ([4], Theorem 1. 1), for a version without extraneous hypotheses), if $\hat{V}$ has dimension $\geqq 2$, then a generic hyperplane section H of $\hat{Y}$ is irreducible. Here 'generic' means all hyperplanes in a nonempty Zariski-open subset, when the hyperplanes are parametrized by $\mathbb{P}^N$. Every such subset meets $\mathbb{P}^N(K)$ as K is an infinite field. Hence we may take H over K. Note that H intersects each of the exceptional divisors, as their dimension is $\geqq 1$. Hence $V' = p(H \cap \hat{Y}) \cap V$ is an irreducible proper subvariety of V, defined over K, which contains $\mathscr{A}$. Replace V by V', and each B_v by $B_v \cap V'(\tilde{K}_v)$. Repeating the process a finite number of times, we arrive at a curve C. Let $\mathscr{C}$ be the normalization of C, embedded in $\mathbb{P}^n$ for some n.

Now we apply the Fekete-Szegö theorem, which uses that $\mathscr{C}$ is smooth. $\mathscr{C}$ will be said to have good reduction at a place v of K (with respect to the given embedding in $\mathbb{P}^n$) if, when the equations defining $\mathscr{C}$ are reduced mod v, they define a smooth connected reduced curve over the residue field. It is known (see Shimura-Taniyama ([13], section 12)) that $\mathscr{C}$ has good reduction for almost all v. Let $\mathfrak{X} \subset \mathscr{C}(\tilde{K})$ be a finite set of points, stable under $\mathrm{Gal}(\tilde{K}/K)$. Call a subset of $\mathscr{C}(\tilde{K}_v)$ $\mathfrak{X}$-adequate if $\mathscr{C}$ has good reduction at V, if the points in $\mathfrak{X}$ reduce to distinct points (mod v), and if the subset contains all the points of $\mathscr{C}(\tilde{K}_v)$ which do not reduce to the same point as any $x \in \mathfrak{X}$ (mod v). (Such a set contains an $\mathfrak{X}$-trivial set, in the sense of [11].) For each v of K, let U_v be an open, $\mathrm{Gal}(\tilde{K}_v/K_v)$-stable subset of $\mathscr{C}(\tilde{K}_v)$, such that almost all of the U_v are $\mathfrak{X}$-adequate. Put $\mathbb{U} = \prod_v U_v \subset \prod_v \mathscr{C}(\tilde{K}_v)$. The following is a reformulation of the Fekete-Szegö theorem for curves ([11], Theorem 6. 2. 2):

Theorem. *There is a quantity $\gamma(\mathbb{U}, \mathfrak{X})$, called the capacity, such that if $\gamma(\mathbb{U}, \mathfrak{X}) > 1$, then $\mathbb{U}$ contains infinitely many K-conjugate sets of points of $\mathscr{C}(\tilde{K})$.*

(The capacity here is the sup of the capacities of closed sets contained in $\mathbb{U}$, as defined in [11].) The only fact one needs to know about capacity is that $\gamma(\mathbb{U}, \mathfrak{X})$ can be made arbitrarily large, with U_v fixed for $v \neq v_0$, by taking U_{v_0} to be the complement in $\mathscr{C}(\tilde{K}_{v_0})$ of sufficiently small discs about the points in $\mathfrak{X}$.

To prove the proposition, let $p: \mathscr{C} \to C$ be the natural projection. Let $\mathfrak{X}_0$ be the set of points at infinity on C, and put $\mathfrak{X} = p^{-1}(\mathfrak{X}_0)$. For each $v \neq v_0$ let $U_v = p^{-1}(B_v)$, and take U_{v_0} large enough that $\gamma(\mathbb{U}, \mathfrak{X}) > 1$, as explained above. Our hypotheses on the B_v guarantees that all but finitely many U_v are $\mathfrak{X}$-adequate. Hence there are infinitely many algebraic points, which, together with their conjugates over K, belong to $\mathbb{U}$. Choose such a point ξ, and let $\zeta = p(\xi)$. It is a point in $V(\tilde{K})$ whose conjugates lie in B_v, for all $v \neq v_0$.

It may be worth remarking that some irreducibility condition on V is needed for the theorems above, as the trivial example of the variety in $\mathbb{A}^2$ determined by $(2x-1)(3x-1)=0$ shows. This has the points $\left(\frac{1}{2}, 0\right)$, $\left(\frac{1}{3}, 0\right)$, at least one of which is integral for every p, but it has no points over $\tilde{\mathcal{O}}$. It is of course sufficient to assume that each irreducible component of V contains a point rational over $\tilde{\mathcal{O}}_v$, if V is not irreducible.

II. The solution to Hilbert's Tenth Problem follows rather formally from the local-global principle. Briefly, it is this: given an affine variety V/K, decompose it into geometrically irreducible components V_i (which may be defined over an extension field k/K). For each V_i, find some point $\zeta_i \in V_i(\tilde{k})$. This point will belong to $V_i(\tilde{\mathcal{O}}_w)$ for all but a finite set of places w of k. For each remaining nonarchimedean place w, apply the decision procedure for the valued algebraically closed field $\tilde{k}_w$. If $V_i(\tilde{\mathcal{O}}_w)$ is nonempty for every w, then by the local-global principle $V_i(\tilde{\mathcal{O}})$ is nonempty. Check this for each V_i: $V(\tilde{\mathcal{O}})$ is nonempty if and only if some $V_i(\tilde{\mathcal{O}})$ is nonempty.

Theorem 2. *There is a primitive recursive algorithm to solve Hilbert's Tenth Problem over the ring of all algebraic integers.*

In more detail, let $\vec{x}=(x_1, \dots, x_m)$ and consider the decidability of a statement of the type

$$(\exists \vec{x} \in \tilde{\mathcal{O}}^m)\,(f_1(\vec{x})=0 \wedge \cdots \wedge f_\ell(\vec{x})=0 \wedge g_1(\vec{x}) \neq 0 \wedge \cdots \wedge g_n(\vec{x}) \neq 0)$$

where the $f_i(\vec{x})$ and the $g_j(\vec{x})$ are polynomials with coefficients in K. By introducing auxiliary variables $y_1, \dots, y_n$ we can reduce this to the decidability of

$$(\exists \vec{x} \in \tilde{\mathcal{O}}^m)\,(\exists \vec{y} \in \tilde{K}^n)\,(f_1(\vec{x})=0 \wedge \cdots \wedge f_\ell(\vec{x})=0 \wedge y_1 g_1(\vec{x})=1 \wedge \cdots \wedge y_n g_n(\vec{x})=1)$$

in which only equalities occur. Let $\mathscr{I}$ be the ideal in $K[x_1, \dots, x_m, y_1, \dots, y_n]$ generated by the polynomials $f_i(\vec{x})$ and $y_j g_j(\vec{x})-1$, and let V be the variety in $\mathbb{A}^{m+n}$ that it determines.

In order to decompose V into irreducible components, one needs to know first that it is possible to compute in $\tilde{\mathbb{Q}}$: to carry out arithmetic operations, to determine when two elements are equal or unequal, and to factor polynomials in one variable into irreducible factors. This point will be dealt with in section III. Now results of Seidenberg ([12], sections 5, 19, 36, and 42) make it possible to effectively calculate generators for the minimal prime ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ associated to $\mathscr{I}$ in $\tilde{\mathbb{Q}}[\vec{x}, \vec{y}]$.

Let k be the field generated over K by the coefficients of generators for the $\mathfrak{P}_i$, and for each i let $V_i \subset \mathbb{A}^{m+n}$ be the variety determined by $\mathfrak{P}_i$. We wish to determine whether V_i has points belonging to $\tilde{\mathcal{O}}^m \times \tilde{k}^n$. By elimination theory (see van der Waerden, [17], pp. 116ff.), one can construct a point $\zeta_i \in V_i(\tilde{k})$ or else conclude that $V_i(\tilde{k})=\emptyset$. One can then compute a bound M_i so that ζ_i belongs to $V_i(\tilde{\mathcal{O}}_w)$ for all primes w of k with norm $>M_i$ (for example, by considering the leading coefficient of the minimal polynomials over $\mathbb{Z}$ of the coordinates of ζ_i). For each of the finitely many w with $Nw \leqq M_i$, apply Weispfenning's ([18]) decision procedure for the valued algebraically closed field $\tilde{k}_w$ to decide whether V_i has a point belonging to $\tilde{\mathcal{O}}_w^m \times \tilde{k}_w^n$. If the answer is yes for each w, then there is a point in $V_i(\tilde{\mathcal{O}}^m \times \tilde{k}^n)$; otherwise there is not. V has a point if and only if some V_i does.

There is one technical issue to deal with in applying the decision procedure for $\tilde{k}_w$: it is necessary to express the fact that the coefficients of the polynomials generating the $\mathfrak{P}_i$ are regarded as embedded in $\tilde{k}_w$. This can be done as follows. Let $\mathfrak{p}_w$ be the prime ideal of $\mathcal{O}_k$ determined by w. An appropriate high power $\mathfrak{p}_w^h$ is principal; let π be a generator. Also, let α be a primitive element for the extension $k/\mathbb{Q}$. (It is well known that h, π and α can be effectively computed; see for example Borevich and Shafarevich [1], pp. 119—123, 225—227 and 404.) The language of valued fields contains the valuation function w and the ordering relation $>$ on the value group. Write π and the coefficients of the generators for the $\mathfrak{P}_i$ as rational linear combinations of powers of α: then add the relations $w(\pi) > 0$ and $P_\alpha(\alpha) = 0$, where $P_\alpha(x)$ is the monic irreducible polynomial over $\mathbb{Q}$ satisfied by α. Because π is divisible only by the prime $\mathfrak{p}_w$, all other facts about the valuation w on elements of $k = \mathbb{Q}(\alpha)$ are determined.

Finally, we consider bounds in the algorithm above.

Seidenberg ([12]), correcting work of Herman (and himself corrected in minor ways by Lazard and Masser-Wüstholz; see [9]), gave effective algorithms for basic constructions in algebraic geometry. In this construction of the minimal prime ideals associated to an ideal $\mathscr{I}$, the number of prime ideals, the number of their generators, and the degrees of those generators are explicitly bounded in terms of the number of variables $m+n$ *and* the number and degrees of the generators for $\mathscr{I}$. Also, the number of arithmetic steps (additions, subtractions, multiplications, divisions, or comparisons) in the calculations are bounded in terms of the same quantities. As will be seen in section III, the number of basic steps (say, Turing machine cycles) needed to carry out an 'arithmetic step' is bounded in terms of the sizes of the operands. Hence constructions in algebraic geometry over $\tilde{\mathbb{Q}}$ are primitive recursive. We note that van den Dries ([15]) and van den Dries-Schmidt ([16]) have given much simpler proofs for the existence of effective bounds in geometrical constructions. Moreover, their bounds are field independent. Unfortunately, they do not seem to be primitive recursive, and so do not yield the sharpest results here.

Robinson ([10]) was the first to show that the first-order theory of a valued, algebraically closed field is decidable. His decision procedure was an enumeration of proofs, based on the fact that the theory is complete. However, recently Weispfenning ([18], corollary 3. 3 ii) has given a primitive recursive decision procedure using quantifier elimination.

Thus, as claimed, our algorithm is primitive recursive. It does not, however, explicitly construct an element belonging to $V(\tilde{\mathcal{O}})$ if there is one: the proof of the Fekete-Szegö theorem is not at present constructive, and consequently neither is application of the local-global principle.

III. It seems to be generally known that $\tilde{\mathbb{Q}}$ is a computable field. However, I am not aware of a reference. The representation indicated here has the merit that the operations are clearly primitive recursive.

We will show that $\tilde{\mathbb{Q}}$ is an 'explicitly given field' in the sense of Seidenberg. This means that one can effectively carry out the field operations and determine when two elements are equal. We will also see that $\tilde{\mathbb{Q}}$ satisfies Seidenberg's conditions (F) and (P): a field satisfies condition (F) if, given a polynomial in one variable $f(x) \in K[x]$, one can construct the complete factorization of $f(x)$ into irreducible factors over $K[x]$. It satisfies condition (P) if, given a finite system of linear homogeneous equations $\sum a_{ij} x_j = 0$ with the $a_{ij} \in K$, one can decide whether this system has a nontrivial solution in K^p, and if it does, find one (here p is the characteristic of K). This is, of course, trivial in characteristic 0.

It is well known that $\mathbb{Q}$ is explicitly given and satisfies (F) and (P). (The factorization can even be carried out in polynomial time; see ([8]).) Also, if K satisfies (F) and (P), then so does a finite extension $K(\alpha)$, where α is given as satisfying an explicit monic irreducible polynomial $f(x) \in K[x]$: see ([12], section 41).

The difficulty is that $\tilde{\mathbb{Q}}$ is not a simple extension of $\mathbb{Q}$. It is necessary to specify how elements of different subextensions are related to each other. One way to do this is to regard $\tilde{\mathbb{Q}}$ as embedded in $\mathbb{C}$, and represent each $\alpha \in \tilde{\mathbb{Q}}$ by a pair $(P_\alpha(x), a+bi)$, where $P_\alpha(x)$ is the monic irreducible polynomial over $\mathbb{Q}$ satisfied by α, and $a+bi$ is a sufficiently good finite decimal approximation to α to distinguish it from its conjugates. This approximation can be refined as needed, so that numbers can be added, subtracted, multiplied, divided, and compared.

How good an approximation is 'good enough'?

Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \tilde{\mathbb{Q}}[x]$, and put $\|f\| = 1 + \sum |a_i|$. It is trivial that every root α_i of $f(x)$ satisfies $|\alpha_i| \leqq \|f\|$. On the other hand, let $D(f)$ be the discriminant of f:

$$D(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{1}{2}n(n-1)} \cdot \text{Resultant}\,(f(x), f'(x)).$$

Put $B(f) = \left| \dfrac{D(f)}{(2\|f\|)^{n^2}} \right|$. Clearly, for any $i \neq j$ we have $|\alpha_i - \alpha_j| \geqq 2B(f)$. Hence if $|\alpha - (a+b^i)| < B(f)$, then $a+bi$ is close enough to α to distinguish it from its conjugates. Note also that the approximation may be refined as needed (see Henrici ([6], pp. 457—552) for several methods).

Clearly, given two pairs $\alpha = (f(x), a+bi)$ and $\beta = (g(x), u+vi)$, they represent the same algebraic number if and only if $f(x) = g(x)$ and $|(a+bi) - (u+vi)| < 2B(f)$. To perform an arithmetic operation on α and β, first factor $g(x)$ into irreducible factors over $\mathbb{Q}(\alpha)$:

$$g(x) = \prod g_i(x).$$

Let G be the maximum absolute value of any coefficient of $g(x)$, and G_i the corresponding quantity for each $g_i(x)$. By Lang ([7], Proposition 2, p. 47),

$$\max(G_i) \leqq 4^{(\deg g)} \cdot G.$$

Hence by refining $u+vi$ if need be, we can determine which factor $g_i(x)$ is satisfied by β. Then form $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)[x]/(g_i(x))$. Within $\mathbb{Q}(\alpha, \beta)$ we can compute $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ and $\dfrac{\alpha}{\beta}$. Let γ be one of these elements, and let M be the matrix over $\mathbb{Q}$ representing multiplication by γ relative to the basis $\alpha^i \beta^j$ of $\mathbb{Q}(\alpha, \beta)$. Compute $H(x) = \det(xI - M)$: this is a monic polynomial satisfied by γ. Factor it over $\mathbb{Q}$: the result will be a power of an irreducible polynomial $h(x)$, which is the minimal polynomial of γ. Also compute an approximation $w + \gamma i$ which is within $B(h)$ of γ, by using the approximations $a+bi$ and $u+vi$ to α and β (refining these if needed). We can represent γ by $(h(x), w+yi)$.

To factor a polynomial $f(x) \in \tilde{\mathbb{Q}}[x]$, first let L be the field generated over $\mathbb{Q}$ by the coefficients of $f(x)$, and factor $f(x)$ algebraically into irreducible factors $f_j(x)$ over L. For each j, form the extension $L[x]/(f_j(x))$, and determine the minimal polynomial of x $(\bmod f_j(x))$ over $\mathbb{Q}$ by the method of the preceding paragraph. Our representation of elements of L also includes specification of their embedding in $\mathbb{C}$. Determine analytically approximations $a_{jk} + b_{jk} i$ to the roots γ of $f_j(x)$. The roots of $f(x)$ in $\tilde{\mathbb{Q}}$ will be represented by the various pairs $(h_\gamma(x), a_{jk} + b_{jk} i)$, where $h_\gamma(x)$ is the minimal polynomial of γ over $\mathbb{Q}$.

References

[1] *Z. I. Borevich* and *I. R. Shafarevich*, Number Theory (tr. N. Greenleaf), New York 1974.

[2] *D. Cantor* and *P. Roquette*, On diophantine equations over the ring of all algebraic integers, J. Number Theory **18** (1984), 1—26.

[3] *D. Estes* and *R. Guralnick*, Module equivalences: local to global when primitive polynomials represent units, J. Algebra **77** (1982), 138—157.

[4] *W. Fulton* and *R. Lazarsfeld*, Connectivity and its applications in algebraic geometry, in Algebraic Geometry, LNM **862,** Berlin-Heidelberg-New York 1981, 26—92.

[5] *R. Guralnick*, Isomorphism of modules under ground ring extensions, J. Number Theory **14** (1982), 307—314.

[6] *P. Henrici*, Applied and Computational Complex Analysis. 1, New York 1974.

[7] *S. Lang*, Diophantine Geometry, Interscience Tracts in Pure and Applied Mathematics **11,** New York 1962.

[8] *H. W. Lenstra, Jr., A. K. Lenstra*, and *L. Lovasz*, Factoring polynomials with rational coefficients, Math. Ann. **261** (1982), 515—534.

[9] *D. W. Masser* and *G. Wüstholz*, Fields of large transcendence degree generated by values of elliptic functions, Inv. Math. **72** (1983), 407—464.

[10] *A. Robinson*, Complete Theories, Amsterdam 1956.

[11] *R. Rumely*, Capacity theory on algebraic curves, manuscript, to appear in LNM.

[12] *A. Seidenberg*, Constructions in algebra, Trans. AMS **197** (1974), 273—313.

[13] *G. Shimura* and *Y. Taniyama*, Complex Multiplication of Abelian Varieties and its application to Number Theory, Tokyo 1964.

[14] *T. Skolem*, Lösung gewisser Gleichungen in ganzen algebraischen Zahlen, insbesondre in Einheiten, Det Norske Videnskops — Akademi i Oslo, I. Math. Naturv. Klasse **10** (1934).

[15] *L. van den Dries*, Model Theory of Fields, thesis, Utrecht 1978.

[16] *L. van den Dries* and *K. Schmidt*, Bounds in the theory of polynomial rings over fields: a nonstandard approach, Inv. Math. **76** (1984), 77—91.

[17] *B. L. van der Waerden*, Einführung in die algebraische Geometrie, New York 1946.

[18] *V. Weispfenning*, Quantifier elimination and decision procedures for valued fields, in Models and Sets, LNM **1103,** Berlin-Heidelberg-New York 1984, 419—472.

Department of Mathematics, University of Georgia, Athens, Georgia 30602, USA

Eingegangen 10. Oktober 1985