stichting
mathematisch
centrum

MC

AFDELING INFORMATICA
(DEPARTMENT OF COMPUTER SCIENCE)

IW 106/79 JANUARI

V. STOLTENBERG-HANSEN & J.V. TUCKER

COMPUTING ROOTS OF UNITY IN FIELDS

Preprint

2e boerhaavestraat 49 amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O).

AMS(MOS) subject classification scheme (1970): 02F30, 02F47, G8A10

ACM-Computing Reviews-category: 5.27

Computing roots of unity in fields *

by

V. Stoltenberg-Hansen** & J.V. Tucker

ABSTRACT

The roots of unity, and torsion subgroups, of computable fields, and abelian groups, of complex numbers are shown to occur with arbitrary turing degree complexity.

KEY WORDS & PHRASES: *computable fields, computable groups, degrees of insolubility, roots of unity, torsion subgroups.*

---

* This paper is not for review; it is meant for publication elsewhere.

** Department of Mathematics, University of Uppsala, Sweden.

Introduction

Here we consider some simple decision problems to do with fields and abelian groups and show they are algorithmically insoluble and, indeed, that they can occur with arbitrary complexity:

THEOREM. *For any recursively enumerable set* A, *there exists a computable field* F *whose set of roots of unity* $U(F) = \{x \in F: \exists n.x^n = 1\}$ *is of the turing degree of* A.

COROLLARY. *For each r.e. turing degree there exists a computable abelian group* G *whose set of elements of finite order, or torsion subgroup, has that degree whilst, locally, the torsion subroup of each finitely generated subgroup is computable.*

The paper is in four sections. First we provide some necessary background to computing in fields, then follows a collection of algebraic lemmas. In section three we prove the theorem and in four append useful information on related decision problems. These theorems are straight-forward contributions to Computable Algebra, to work on fields and (non finitely presented!) groups, see sections one and four for references. Such arbitrary degree results are desirable for Recursion Theory since they establish that the turing degree, its natural classification of complexity with its notorious issue of complications, is relevant to algorithmic questions as they arise in Algebra. And since our fields and groups are systems within the complex numbers, $\underline{\subseteq}$, these particular insoluble decision problems are elementary in ways in which the word problem for a finitely presented group is not; for example, they can be quoted to students immature for the machinery of presentations.

We are happy to acknowledge the support of the Matematisk institutt, Universitetet i Oslo, and several convivial conversations with friends in its Algebra group; also the patronage of our present institutions at Uppsala and Amsterdam respectively.

1. Computable rings and fields

Algorithmic properties of fields make an appearance in van der Waerden's

Moderne algebra [11] but a more suitable starting point is A. Fröhlich and J.C. Shepherdson's [4] and M.O. Rabin's [9]. We assume the reader familiar with the ideas and results of these papers subsumed under the following basic definition of A.I. Mal'cev [8]; see also J.V. Tucker's [14]. A finitary algebraic system $A = (A;\sigma_1,\ldots,\sigma_k)$ is a *computable algebra* if there exists a recursive subset Ω of the natural numbers, ω, a surjection $\alpha\colon \Omega \to A$, and recursive functions $\bar{\sigma}_1,\ldots,\bar{\sigma}_k$ so that (i) the equality relation, defined for $n,m \in \Omega$ by $n \equiv_\alpha m$ iff $\alpha n = \alpha m$ in A is recursive, and (ii) if σ is an n-ary operation of A then $\bar{\sigma}$ recursively *tracks* σ in Ω in the sense that the following diagram commutes,

$$\begin{array}{ccc} A^n & \xrightarrow{\sigma} & A \\ {\scriptstyle \alpha^n}\uparrow & & \uparrow{\scriptstyle \alpha} \\ \Omega^n & \xrightarrow{\bar{\sigma}} & \Omega \end{array}$$

. Our recursion-theoretic and algebraic terminology and techniques are completely standard and can be found, for example, in the books of Rogers [10] and Lang [7].

The field construction in section three consists of factoring a polynomial ring by a prime ideal and taking the quotient field of the resulting entire ring; we need these simple facts.

Let R be a computable commutative ring with 1. Then the polynomial rings $R[X_1,\ldots,X_n]$ and $R[X_1,X_2,\ldots]$, sometimes jointly abbreviated by R[X], are computable. If $I \lhd R$ and I is a computable subset of R then the quotient ring R/I is computable. If R is an entire ring then its quotient field $\Sigma(R)$ is computable.

The reader should verify these results, using [4] or [9], with due attention to the following observations. In each construction one begins with a computable coordinatisation of R and must make up a computable numbering for the new structure which is *standard* relative to R: for polynomial rings this means that R and the $R[X_1,\ldots,X_n]$ are computable subrings of $R[X_1,X_2,\ldots]$, that one can computably enumerate codes for indeterminates, calculate degrees of polynomials, $\deg\colon R[X] \to \omega$, from their codes, and obtain codes for their coefficients. For $\Sigma(R)$ it means R is a computable subring and that one can compute codes for numerators and denominators from codes for the field elements and so on. The point is that all computations take place within ω, in terms of a chosen codification: not any computable ring or field numberings will do, in general there are manifold intrinsically distinct computable codifications of a computable algebra. For example,

$R[X_1,X_2,\ldots]$ has a continuum of distinct coordinatisations where the basic classification is Mal'cev's concept of recursive equivalence [8]. Now in each case it is easy to formalise what is required of the standard numberings and then show that the standard computable coordinatisations comprise an equivalence class under Mal'cev's classification. In what follows we are always choosing standard codings and what is computable *in an algebra* with respect to one is computable with respect to any other. Thus we may make special assumptions with impunity, such as taking a numbering to be bijective rather than surjective. On one occasion for the codings of the R[X] we assume that if $q \in R[X]$ contains an indeterminate X_n and $|q|$ denotes any code for q then $n \leq |X_n| \leq |q|$. These remarks are necessary because as far as possible, for reasons of brevity and elegance, we henceforth surpress the codings in our arguments informally manipulating algebra elements; so in saying the unity problem of the field F is of the turing degree of the r.e. set A we write $U(F) \equiv_T A$. For further elaboration of these technicalities see Mal'cev [8] or Tucker [13], [14].

First we must prove that the membership relation for finitely generated ideals in certain polynomial rings is decidable. This requires a short digression on Matrix Theory.

Let M(m,n,F) denote the set of all $m \times n$ matrices over the field F. If F is computable then M(m,n,F) is computable and can be shown to be so under a standard coordinatisation procedure uniform in m,n which allows a computable decomposition of the matrices into their entries and so on; once formalised this method can be proved unique up to recursive equivalence. In particular, with respect to a standard coordinatisation, the *rank function* ${}^{m,n}r: M(m,n,F) \to \omega$ defined ${}^{m,n}r(A)$ = rank of matrix A is computable uniformly in m,n.

1.1 LEMMA. *Let* F *be a computable field. Then the relation* ${}^{m,n}R \subset M(m,n,F) \times F^m$ *defined* ${}^{m,n}R(A,b) \equiv (\exists x \in F^n)(Ax = b)$ *is computable uniformly in* m,n.

Proof. This follows from a well-known theorem of Linear Algebra: given $A \in M(m,n,F)$ and $b \in F^m$ let [A,b] be A augmented by b as an (n+1)-th column. Then ${}^{m,n}R(A,b)$ iff ${}^{m,n}r(A) = {}^{m,n+1}r([A,b])$. Since matrix rank and $[,]: M(m,n,F) \times F^m \to M(m,n+1,F)$ are uniformly computable under the standard

coordinatising of matrices the relation is computable uniformly in m,n. Q.E.D.

If R is a commutative ring with 1 then the ideal in R generated by $a_1,\ldots,a_k \in R$ is $(a_1,\ldots,a_k) = Ra_1 +\ldots+ Ra_k = \{r_1a_1 +\ldots+ r_ka_k: r_i \in R\}$.

1.2 LEMMA. *Let* F *be a computable field. Then the membership relation for finitely generated ideals of* $F[X_1,\ldots,X_n]$, *defined*

$$^{n,k}M(q,p_1,\ldots,p_k) \equiv q \in (p_1,\ldots,p_k)$$

is computable uniformly in k,n.

Proof. From Statz 2 of Hermann's [5] one can obtain this theorem, *Hermann's Lemma. Let* F *be a computable field. Consider equations in* $F[X_1,\ldots,X_n]$ *of the form*

$$r_1p_1+\ldots+r_kp_k = q \qquad (*)$$

where $p_1,\ldots,p_k,q$ *are given and the* $r_1,\ldots,r_k$ *are to be found. There exists a recursive function* $f: \omega^3 \to \omega$ *such that if* (*) *has a solution in* $F[X_1,\ldots,X_n]$ *then it does so with* $\deg(r_i) \leq f(a,b,n)$ *where* $a = \deg(q)$ *and* $b = \max\{\deg(p_i): 1 \leq i \leq k\}$.

To decide $q \in (p_1,\ldots,p_k)$ is to decide whether or not equation (*) has a solution. Since F is computable, degree is computable and computing f(a,b,n) we can set up a system of linear equations over F to decide the relation as follows.

Construct formal polynomials $r_1,\ldots,r_k$ of degree $d = f(a,b,n)$ with coefficients treated as indeterminates over F, $r_i = \Sigma_{|j|\leq d}\, t_{ij}X^j$ where $j = (j_1,\ldots,j_n)$, $|j| = j_1 +\ldots+ j_n$ and $X = X_1^{j_1}\ldots X_n^{j_n}$. Substituting these into equation (*) produces a polynomial identity wherein the LHS has degree $\leq f(a,b,n) + b$ and the RHS has degree = a. Since F is a field we can compare coefficients and obtain a set of linear equations in the t_{ij} over F. Thus, $q \in (p_1,\ldots,p_k)$ iff this set of linear equations has a solution in F. But all these constructions are uniformly computable so lemma 1.1 can be applied to decide this relation. Q.E.D.

1.3 COROLLARY. *The membership relation for finitely generated ideals of* $F[X_1,X_2,\ldots]$ *is computable.*

Proof. We claim that $q \in (p_1,\ldots,p_k)$ in $F[X_1,X_2,\ldots]$ if, and only if, $q \in (p_1,\ldots,p_k)$ in $F[X_1,\ldots,X_m]$ where X_m is the highest indeterminate occuring in $q,p_1,\ldots,p_k$. From this 1.3 follows for one has only to calculate m from $q,p_1,\ldots,p_k$ and apply the algorithm ${}^{m,k}M$ from lemma 1.2.

One implication of the claim is obvious, so assume there exist $r_1,\ldots,r_k \in F[X_1,X_2,\ldots]$ such that $q = r_1p_1+\ldots+r_kp_k$. Since $F[X_1,X_2,\ldots]$ is a free F-algebra on its indeterminates, we can define an F-algebra homomorphism $\phi_m\colon F[X_1,X_2,\ldots] \to F[X_1,\ldots,X_m]$ by extending the map $X_i \to X_i$ if $i \leq m$ and $X_i \to 0$ otherwise. Now $\phi_m q = \phi_m(\Sigma r_i p_i) = \Sigma \phi_m r_i . \phi_m p_i$. By the construction of ϕ_m, in particular the choice of m, $\phi_m q = q$ and $\phi_m p_i = p_i$. Thus $q = \Sigma \phi_m r_i . p_i$ which implies $q \in (p_1,\ldots,p_k)$ in $F[X_1,\ldots,X_m]$. Q.E.D.

Secondly, here is a proposition about deciding the unity problem in simple number rings and fields. If R is a computable ring with 1 then the unity problem for R is decidable if the set $U(R) = \{x \in R: \exists n.x^n = 1\}$ is computable. A computable subring R of the field of complex numbers $\underline{\underline{C}}$ is said to have a *transcendence algorithm* if $T(R) = \{x \in R: x \text{ is a transcendental number}\}$ is computable.

1.4 LEMMA. *Let* R *be a computable subring of* $\underline{\underline{C}}$. *If* R *has a transcendence algorithm then its unity problem is decidable.*

Proof. Given $x \in R$ there are two cases which can be decided by hypothesis. First, x is transcendental in which case $x \notin U(R)$. Secondly, x is algebraic in which case we can computably search $\underline{\underline{Z}}[X]$, the ring of polynomials with integer coefficients, for a polynomial p having x as a zero. Now if x were a root of unity of order n then since the n-th cyclotomic polynomial $\Phi_n(X)$ is irreducible over $\underline{\underline{Z}}$ we would have Φ_n dividing p and $n-1 \leq \deg(p)$. This yields a bound as $x \in U(R)$ iff at least one of $x,x^2,\ldots,x^{\deg(p)+1}$ is 1. Q.E.D.

A set of examples of such rings, used in the next section, is the family of ring and field extensions of the rational numbers, $\underline{\underline{Q}}$, of the special forms $\underline{\underline{Q}}[\varepsilon_1,\ldots,\varepsilon_k,t_1,\ldots,t_{n-k}]$ and $\underline{\underline{Q}}(\varepsilon_1,\ldots,\varepsilon_k,t_1,\ldots,t_{n-k})$ where ε_i is a

primitive p_i-th root of unity and t_i are indeterminates. Having consulted Fröhlich and Shepherdson's [4], the reader will find it routine to prove these systems computable and that they possess transcendence algorithms uniform in n and $<p_1,\ldots,p_k>$.

2. Algebraic preliminaries

What follows are algebraic facts required by our construction in section three. We identify $F[X_1,\ldots,X_n]$ with $F[X_1,\ldots,X_{n-1}][X_n]$ and consequently write $f \in F[X_1,\ldots,X_n]$ in the form $f = \Sigma f_i X_n^i$ where $f_i \in F[X_1,\ldots,X_{n-1}]$. By $\deg_{X_n}(f)$ we mean the degree of f as a polynomial in X_n.

2.1 LEMMA. *Let* $q \notin I \lhd F[X]$. *Assume* X_n *does not appear in* some *set of generators for* I. *If* $p \in F[X_n]$ *and* $\deg(p) > \deg_{X_n}(q)$ *then* $q \notin I + (p)$.

Proof. Clearly it suffices to prove the lemma with $F[X_1,\ldots,X_n]$ in place of $F[X]$. Let $J = I \cap F[X_1,\ldots,X_{n-1}]$, the ideal in $F[X_1,\ldots,X_{n-1}]$ generated by the basis of I there, and $R = F[X_1,\ldots,X_{n-1}]/J$. Consider the following sequence of homomorphisms,

$$F[X_1,\ldots,X_n] \xrightarrow{\phi} R[X_n] \xrightarrow{v} R[X_n]/(p)$$

where $\phi(f) = \Sigma \bar{f}_i X_n^i$, $f_i = f_i \bmod J$, and v is the natural factoring homomorphism. Since $q \notin I$ it follows that $\phi q \neq 0$ in $R[X_n]$. Furthermore by the hypothesis on the degree of p and the fact that $\deg_{X_n}(q) \geq \deg_{X_n}(\phi q)$, $\phi q \notin (p) \lhd R[X_n]$. Thus, letting $\psi = v\phi$, $\psi q \neq 0$. On the other hand it is clear that $I + (p) \leq \ker\psi$ so $q \notin I + (p)$. Q.E.D.

Henceforth we work over the field $\underline{Q}$ with a view to building number fields.

Let $p_1,\ldots,p_n$ be distinct rational primes, not necessarily the first n primes, $\Phi_i \in \underline{Q}[X_i]$ denote the p_i-th cyclotomic polynomial, $\Phi_i = X_i^{p_i-1} + X_i^{p_i-2} + \ldots + q_1$; let ε_i denote a primitive p_i-th root of unity.

2.2 LEMMA. Φ_n *is irreducible in* $\underline{Q}(\varepsilon_1,\ldots,\varepsilon_{n-1})[X_n]$.

Proof. Since $p_1,\ldots,p_n$ are distinct primes $\varepsilon_1 \cdot \ldots \cdot \varepsilon_n$ is a primitive

$(p_1 \cdot \ldots \cdot p_n)$-th root of unity. Thence each $\varepsilon_i \in \underline{\underline{Q}}(\varepsilon_1 \cdot \ldots \cdot \varepsilon_n)$ so $\underline{\underline{Q}}(\varepsilon_1,\ldots,\varepsilon_n) = \underline{\underline{Q}}(\varepsilon_1 \cdot \ldots \cdot \varepsilon_n)$. Furthermore, $[\underline{\underline{Q}}(\varepsilon_1 \cdot \ldots \cdot \varepsilon_n):\underline{\underline{Q}}] = \phi(p_1 \cdot \ldots \cdot p_n)$ where ϕ is the Euler phi function. And $\phi(p_1 \cdot \ldots \cdot p_n) = (p_1-1) \cdot \ldots \cdot (p_n-1)$, again since the primes are distinct. Let f be the irreducible polynomial of ε_n over $\underline{\underline{Q}}(\varepsilon_1,\ldots,\varepsilon_{n-1})$. Then

$$\deg(f) = [\underline{\underline{Q}}(\varepsilon_1,\ldots,\varepsilon_n) : \underline{\underline{Q}}(\varepsilon_1,\ldots,\varepsilon_{n-1})] = \frac{[\underline{\underline{Q}}(\varepsilon_1,\ldots,\varepsilon_n) : \underline{\underline{Q}}]}{[\underline{\underline{Q}}(\varepsilon_1,\ldots,\varepsilon_{n-1}):\underline{\underline{Q}}]}$$

$$= \frac{(p_1-1) \cdot \ldots \cdot (p_n-1)}{(p_1-1) \cdot \ldots \cdot (p_{n-1}-1)} = p_n - 1 = \deg(\Phi_n).$$

It follows that $f = \Phi_n$. Q.E.D.

2.3 LEMMA. $\underline{\underline{Q}}[X_1,\ldots,X_n] / (\Phi_1,\ldots,\Phi_n) \tilde{=} \underline{\underline{Q}}[\varepsilon_1,\ldots,\varepsilon_n] = \underline{\underline{Q}}(\varepsilon_1,\ldots,\varepsilon_n)$.

Proof. The proof is by induction on n. The base step is obvious. So assume

$$R = \underline{\underline{Q}}[X_1,\ldots,X_{n-1}] / (\Phi_1,\ldots,\Phi_{n-1}) \overset{\phi_{n-1}}{\cong} \underline{\underline{Q}}[\varepsilon_1,\ldots,\varepsilon_{n-1}]$$

and

$$\phi_{n-1}(\bar{X}_i) = \varepsilon_i \quad \text{for } i = 1,\ldots,n-1 \text{ where } \bar{X}_i = X_i \bmod(\Phi_1,\ldots,\Phi_{n-1}).$$

Make $\underline{\underline{C}}$ into an R-algebra by defining for $r \in R$ and $z \in \underline{\underline{C}}$, $r \cdot z = \phi_{n-1}(r) \cdot z$. Let ϕ map X_n to ε_n and extend ϕ to an R-algebra homomorphism $\phi: R[X_n] \longrightarrow \underline{\underline{C}}$. Then $\mathrm{im}(\phi)$ = smallest R-subalgebra of $\underline{\underline{C}}$ containing ε_n, i.e. $\underline{\underline{Q}}[\varepsilon_1,\ldots,\varepsilon_n]$, and $R[X_n] / \ker\phi \cong \underline{\underline{Q}}[\varepsilon_1,\ldots,\varepsilon_n]$. Trivially, $(\Phi_n) \subset \ker\phi$. For the converse inclusion assume $\phi(f) = 0$ for $f \in R[X_n]$. Then $\phi_{n-1}f(\varepsilon_n) = 0$ so by 2.2 $\Phi_n \mid \phi_{n-1}f$ and thence $\Phi_n \mid f$. Thus $\ker\phi = (\Phi_n)$.

It remains to show $\underline{\underline{Q}}[X_1,\ldots,X_n] / I \cong R[X_n] / (\Phi_n)$ where $I = (\Phi_1,\ldots,\Phi_n)$. Let $J = \underline{\underline{Q}}[X_1,\ldots,X_{n-1}] \cap (\Phi_1,\ldots,\Phi_{n-1})$ and consider the following sequence of homomorphisms,

$$\underline{\underline{Q}}[X_1,\ldots,X_n] \xrightarrow{\psi_0} \underline{\underline{Q}}[\varepsilon_1,\ldots,\varepsilon_{n-1}][X_n] \xrightarrow{v} \underline{\underline{Q}}[\varepsilon_1,\ldots,\varepsilon_{n-1}][X_n] / (\Phi_n)$$

where $\psi_0 f = \Sigma(\phi_{n-1}\bar{f}_i)X_n^i$, $\bar{f}_i = f_i \bmod J$ and v is the natural factoring homomorphism. Let $\psi = v\psi_0$. Clearly $I \leq \ker\psi$. For the converse inclusion note that $\psi_0 X_i = \varepsilon_i$ for $i < n$ and $\psi_0 X_n = X_n$. Suppose $f \in \ker\psi$. Then $\psi_0(X_1,\ldots,X_n) = f(\psi_0 X_1,\ldots,\psi_0 X_n) = f(\varepsilon_1,\ldots,\varepsilon_{n-1},X_n) \in (\Phi_n)$. Hence there is an $r \in \underline{Q}[X_1,\ldots,X_n]$ so that $\psi_0 f = \psi_0 r\Phi_n$, i.e. $f - r\Phi_n \in \ker\psi_0$. This means that $f - r\Phi_n = \Sigma\, q_i X_n^i$ where $q_i \in J \leq I$ for each i. But then $f = \Sigma\, q_i X_n^i + r\Phi_n \in I$. Let ϕ_n: $\underline{Q}[X_1,\ldots,X_n] / (\Phi_1,\ldots,\Phi_n) \cong \underline{Q}[\varepsilon_1,\ldots,\varepsilon_n]$ be the isomorphism obtained. It is easily verified that $\phi_n(\bar{X}_i) = \varepsilon_i$ for $i = 1,\ldots,n$. Of course $\underline{Q}[\varepsilon_1,\ldots,\varepsilon_n] = \underline{Q}(\varepsilon_1,\ldots,\varepsilon_n)$ since $\varepsilon_1,\ldots,\varepsilon_n$ are algebraic over $\underline{Q}$. Q.E.D.

Let $\{t_i : i \in w\}$ be a sequence of mutually transcendental elements over the algebraic numbers and let $\Sigma(R)$ denote the quotient field of the entire ring R.

The following corollary is an immediate consequence of 2.3, remembering that Φ_i involves only the variable X_i.

2.4 COROLLARY. *The following isomorphisms hold where* $\bar{X}_i$ *is mapped to* ε_i for $i = 1,\ldots,k$ *and to* t_{i-k} *for* $i = k+1,\ldots,n$.

(i) $\underline{Q}[X_1,\ldots,X_n] / (\Phi_1,\ldots,\Phi_k) \cong \underline{Q}[\varepsilon_1,\ldots,\varepsilon_k,t_1,\ldots,t_{n-k}]$

(ii) $\Sigma(\underline{Q}[X_1,\ldots,X_n] / (\Phi_1,\ldots,\Phi_k)) \cong \underline{Q}(\varepsilon_1,\ldots,\varepsilon_k,t_1,\ldots,t_{n-k})$.

2.5 COROLLARY. U(R) *is decidable for* $R = \underline{Q}[X_1,\ldots,X_n] / (\Phi_1,\ldots,\Phi_k)$ *or its quotient field* $\Sigma(R)$ *uniformly in* n *and* $\langle p_1,\ldots,p_k\rangle$ *where* Φ_i *is the* p_i*-th cyclotomic polynomial.*

Proof. Given n and $\langle p_1,\ldots,p_k\rangle$ one can recursively build $\underline{Q}[\varepsilon_1,\ldots,\varepsilon_k,t_1,\ldots,t_{n-k}]$ and recursively construct the isomorphisms of 2.4. Now 2.5 follows because the unity problem is computable in $\underline{Q}[\varepsilon_1,\ldots,\varepsilon_k,t_1,\ldots,t_{n-k}]$ by Lemma 1.4, in particular, uniformly in n and $\langle p_1,\ldots,p_k\rangle$, and decidability is an invariant of computable isomorphisms. And similarly with an argument about $\underline{Q}(\varepsilon_1,\ldots,\varepsilon_k,t_1,\ldots,t_{n-k})$. Q.E.D.

3. Proof of the theorem

3.1 THEOREM. *Let* A *be an r.e. set. Then there is a computable entire*

ring R *such that* $U(R) \equiv_T A$.

Proof. Our constructed R will be $\underline{Q}[X]$ / I for some suitable prime ideal I. There are two kinds of requirements. The positive requirements are to code A into U(R); this is done by adding appropriate cyclotomic polynomials as generators for I. On the other hand, there is need for some restraint in order to obtain R computable or, equivalently, to make I into a computable ideal. The latter is achieved, using Lemma 2.1, by choosing the generators for I of sufficiently high degree. I is constructed in stages. At each stage the p-th cyclotomic polynomial Φ_p is added as a generator for I where the variable of Φ_p does not appear in the previously added generators and p is a prime larger than the degrees of those generators and sufficiently large to satisfy the negative condition.

Let $\lambda s.A^s$ be a recursive enumeration of A such that $A^s - A^{<s}$ contains precisely one element where $A^{<s} = \cup_{t<s} A^t$.

Construction at stage s: Let $I^{<s} = (\Phi_{p_1},\ldots,\Phi_{p_{s-1}})$ be that part of I constructed before stage s and assume $n \in A^s - A^{<s}$. Let p_s = least prime p greater than $p_1,\ldots,p_{s-1}$ such that for each $q \in \underline{Q}[X]$ if $|q| < s$ then $\deg_{X_n}(q) + 1 < p$. Put $I^s = I^{<s} + (\Phi_{p_s})$ where $\Phi_{p_s} \in \underline{Q}[X_n]$.

To complete the construction, let $I = \cup_{s\in\omega} I^s$.

3.2 LEMMA. R = Q[X] / I *is a computable entire ring.*

Proof. R is obviously commutative. If R contained zero divisors, then, for some n and $\Phi_1,\ldots,\Phi_k$ taken from the constructed generators of I, $\underline{Q}[X_1,\ldots,X_n]$ / $(\Phi_1,\ldots,\Phi_k)$ would contain zero divisors thus contradicting 2.4. Hence R is entire. To show R is computable we show that for each $q \in \underline{Q}[X]$, $q \in I$ iff $q \in I^{|q|}$, the latter ideal being computable uniformly in |q| by Lemma 1.3. To obtain a contradiction in the non-trivial direction assume $q \in I$ but $q \notin I^{|q|}$. Let s be least such that $q \in I^s$. Then $|q| < s$ and $q \in I^s - I^{<s}$. By construction $p_s > \deg_{X_n}(q) + 1$ where $n \in A^s - A^{<s}$. But then $\deg(\Phi_{p_s}) > \deg_{X_n}(q)$ and X_n does not appear in the previously constructed generators, so, by Lemma 2.1, $q \notin I^{<s} + (\Phi_{p_s}) = I^s$. Q.E.D.

3.3 LEMMA. $U(R) \equiv {}_{T}A$.

Proof. To prove $A \leq {}_{T}U(R)$ we show $n \in A$ iff X_n mod $I \in U(R)$, the latter being equivalent to $\exists m(X_n^m - 1 \in I)$. If $n \in A^s - A^{<s}$ then $\Phi_{p_s}(X_n)$ is put into I so $X_n^{p_s} - 1 = (X_n - 1)\Phi_{p_s}(X_n) \in I$. Suppose there is m such that $X_n^m - 1 \in I$. Then for some $\ell \geq n$ $X_n^m - 1 \in J = I \cap \underline{Q}[X_1,\ldots,X_\ell]$. Let $\Phi_1,\ldots,\Phi_k$ be all the constructed generators of I with variables among $X_1,\ldots,X_\ell$. By 2.4, $\underline{Q}[X_1,\ldots,X_\ell] / J = \underline{Q}[X_1,\ldots,X_\ell] / (\Phi_1,\ldots,\Phi_k) \cong \underline{Q}[\varepsilon_1,\ldots,\varepsilon_k,t_1,\ldots,t_{n-k}]$ where X_n mod$J$ is mapped either to an ε_i or t_i. Since, by our hypothesis, X_n mod$J$ is not transcedental it must be mapped to an ε_i and thence X_n must appear in I_i. So $n \in A$.

To prove $U(R) \leq {}_{T}A$ define, recursively in A, the function $b_A: \underline{Q}[X] \longrightarrow w$ by $b_A(q) = (\text{least } s)[\{n : n \leq |q|\} \cap A^s = \{n : n \leq |q|\} \cap A]$. Given $q \in \underline{Q}[X]$ we are to determine if $\exists m(q^m - 1 \in I)$. Our standard codification of $\underline{Q}[X]$ has the property that $n \leq |X_n| \leq |q|$ whenever X_n appears in q. It follows that $q \in Q[X_1,\ldots,X_{|q|}]$. Let $J = I \cap \underline{Q}[X_1,\ldots,X_{|q|}]$. Clearly for each m, $q^m - 1 \in I$ iff $q^m - 1 \in J$. But $J = I^{b_A(q)} \cap \underline{Q}[X_1,\ldots,X_{|q|}]$ so by reworking the constructions up to stage $b_A(q)$ we obtain generators $\Phi_i,\ldots,\Phi_k$ such that $J = (\Phi_1,\ldots,\Phi_k) \lhd \underline{Q}[X_1,\ldots,X_{|q|}]$. Thus by 2.5 we can decide if there is m such that $q^m - 1 \in J$ and hence if there is m such that $q^m - 1 \in I$. Q.E.D.

This completes the proof of the theorem:

3.4 THEOREM. *Let* A *be a r.e. set. Then there is a computable field* F *such that* $U(F) \equiv_T A$.

Proof. Let $F = \Sigma(R)$ where R is the entire ring constructed in the proof of theorem 3.1; we use the notation from that proof. F is computable and R is a computable subring of F. It follows that $A \leq_T U(F)$. To prove the converse reduction note that for $p,q \in Q[X]$; $p^m - q^m \in I$ iff $p^m - q^m \in J$ where $J = I^\ell \cap \underline{Q}[X_1,\ldots,X_n]$, $n = \max\{|p|,|q|\}$ and $\ell = \max\{b_A(p),b_A(q)\}$. It follows that p/q is a root of unity in F iff it is a root of unity in $\Sigma(\underline{Q}[X_1,\ldots,X_n] / J)$. Thus, just as in the proof of 3.3, we can, recursively in A, transform the problem to $\underline{Q}(\varepsilon_1,\ldots,\varepsilon_k,t_1,\ldots,t_{n-k})$ where it is dedicable by 2.5. Q.E.D.

4. Concluding remarks

The corollary follows directly from the theorem, one considers the multiplicative group structure of its field; the local computability of the order problem comes from the well-known structure theorem for finitely generated abelian groups. Notice that while the order problem is dedicable *individually* for the finitely presented abelian groups there can be no *uniform* algorithm and so the uniform order problem for that class must have degree 0'.

The order problem in groups was first observed insoluble in Baumslag, Boone and Neumann's [1], its turing degree complexity for finitely presented groups awaiting D.J. Collins' excellent study [3]. On the other hand, in [12], E.I. Timoshenko proves that the order problem is decidable in any finitely generated meta-abelian group (which is computable, of course). From Kopytov's work on number fields [6], it can be proved that, for any n, the order problem in GL(n,K) has the turing degree of the roots of unity problem in the field K. More recently, there have followed algebraic characterizations of the decidability of the order problem from Boone and Higman [2] and Sacerdote [11].

REFERENCES

1 G. BAUMSLAG, W.W. BOONE and B.H. NEUMANN, 'Some unsolvable problems about elements and subgroups of groups', Math. Scand., 7 (1959) 191-201.

2 W.W. BOONE and G. HIGMAN, 'An algebraic characterization of groups with soluble order problem', pp. 53-54 of H.E. ROSE and J.C. SHEPHERDSON (editors), *Logic Colloquium, '73,* (North-Holland, Amsterdam, 1975).

3 D.J. COLLINS, 'The word, power and order problems in finitely presented groups', pp. 401-420 of W.W. BOONE, F.B. CANNONITO and R.C. LYNDON (editors), *Word Problems,* (North-Holland, Amsterdam, 1973).

4 A. FROHLICH and J.C. SHEPHERDSON, 'Effective procedures in field theory', Phil. Trans. Royal Soc. London, (A) 248 (1956) 407-432.

5 G. HERMANN, 'Die Frage der endlich vielen Schritte in der Theorie der Polynomideale', Math. Ann., 95 (1926) 736-788.

6 V.M. KOPYTOV, 'Solvability of the problem of occurrence in finitely generated soluble groups of matrices over the field of algebraic numbers', Alg. & Logic, 7 (1968) 388-393.

7 S. LANG, *Algebra*, (Addison-Wesley, Reading, Massachusetts, 1965).

8 A.I. MAL'CEV, 'Constructive algebras, I', pp. 148-212 of A.I. MAL'CEV *The metamathematics of algebraic systems. Collected papers: 1936-1967*, (North-Holland, Amsterdam, 1971).

9 M.O. RABIN, 'Computable algebra, general theory and the theory of computable fields', Trans. Amer. Math. Soc., 95 (1960) 341-360.

10 H. ROGERS, *Theory of recursive functions and effective computability*, (McGraw-Hill, New York, 1967).

11 G. SACERDOTE, 'Subgroups of finitely presented groups', Proc. London Math. Soc., (3) 35 (1977) 193-212.

12 E.I. TIMOSHENKO, 'Algorithmic problems for metabelian groups', Alg. & Logic, 12 (1973) 132-137.

13 J.V. TUCKER, *Computability as an algebraic property*, Ph.D. Thesis, University of Bristol, Bristol, 1976.

14 _____ 'Computability and the algebra of fields: some affine constructions', to appear in J. Sym. Logic.

15 B.L. VAN DER WAERDEN, *Modern algebra*, (Ungar, New York, 1959),