ISRAEL JOURNAL OF MATHEMATICS, Vol. 27, Nos. 3-4, 1977

SETS OF DEGREES OF COMPUTABLE FIELDS†

BY
ELIE BIENENSTOCK

ABSTRACT

Given a Σ_2 (resp. Σ_1) degree of recursive unsolvability **a**, a computable field (resp. a computable field with a splitting algorithm) F is constructed in any given characteristic, such that the set of dimensions of all finite extensions of F has degree **a**.

§1. Preliminaries

Let k be a field, $\bar{k}$ its algebraic closure. We define the set of degrees of k as in [4]:

$$S(k) = \{n \in N: \text{ there exists a field } F, k \subseteq F \subseteq \bar{k}, [F:k] = n\}.$$

A set $S \subseteq N$ such that there exists a field k with $S = S(k)$ is called a degree set. Several partial results on the characterization of degree sets are presented in [4]. The present paper deals with the following question: What can be said about the degree of recursive unsolvability of $S(k)$, if k is a computable field?

We adopt the terminology of M. O. Rabin in [5]: $\langle F, +, \cdot \rangle$ is said to be a computable field if F is at most countable, and there is a one to one mapping $i: F \to N$ such that $i(F)$ is a recursive set of integers and i transforms the addition and multiplication operations of F into recursive functions of $i(F)^2$ into $i(F)$. Such a mapping i is called an admissible indexing of F. A computable field F is said to possess a splitting algorithm with respect to the admissible indexing i, if there exists an effective procedure for deciding for every polynomial $f(t) \in F(t)$, which is given as a sequence of the i-indices of its coefficients, whether or not $f(t)$ splits over F.

† This is part of an M.Sc. Thesis presented at The Hebrew University. The author wishes to express his indebtedness to his Supervisor Professor H. Gaifman for his constant guidance and encouragement. Thanks are also due to Professor G. Sabbagh (University of Paris VII) for several useful suggestions.

Received May 31, 1976

It is proved in [4] that $S(k)$ is the set of degrees of irreducible polynomials in $k[t]$. It follows that whenever k is computable, $S(k)$ is a Σ_2 set in the arithmetical hierarchy of sets of natural numbers. For, let i_0 be an admissible indexing of the ring $k[t]$, effective with respect to i, and such that i_0 maps $k[t]$ onto N. Then the relation $M \subseteq N^3$ defined by

$$(n_1, n_2, n_3) \in M \Leftrightarrow i_0^{-1}(n_1).\ i_0^{-1}(n_2) = i_0^{-1}(n_3)$$

is recursive, as well as the function $d : N \to N$ defined by

$$d(n) = \deg(i_0^{-1}(n)),$$

and we have:

$$n \in S(k) \Leftrightarrow \exists m\ \forall m_1 \forall m_2$$

$$[d(m) = n \wedge ((m_1, m_2, m) \in M \to (d(m_1) = d(m) \vee d(m_1) = 0))]$$

which shows that $S(k)$ is Σ_2.

Likewise, we see that if k possesses a splitting algorithm with respect to i (which amounts to say that the set $I = \{n \in N : i_0^{-1}(n)$ is irreducible over $k\}$ is recursive), then $S(k)$ is Σ_1 (r.e.) for in this case

$$n \in S(k) \Leftrightarrow \exists m\, [d(m) = n \wedge m \in I].$$

The principal theorems proved in the present paper are in some sense converses of the last two statements. Before we formulate these theorems we bring some more definitions and results of [4]:

A finite extension E/k is called cyclic if it is normal and the Galois group $G(E/k)$ is cyclic. A field k is called a C E field if all finite extensions E/k are cyclic. We denote by $\mathcal{P}$ the set of all prime positive integers. For any $P \subseteq \mathcal{P}$, let N_P be the set of all positive integers whose prime factors are all in P. The following results are proved in [4].

1) k is a C E field iff for each $n \in N$, k has at most one separable extension of degree n (in a fixed algebraic closure $\bar{k}$).

2) Every algebraic extension Δ of a C E field k is a C E field. Moreover, $S(\Delta) \subseteq S(k)$.

3) For any $P \subseteq \mathcal{P}$, there exists a C E field K of any prescribed characteristic χ, such that $S(K) = N_P$.

Our principal theorems are "computable" versions of statement 3:

THEOREM 1.1. *Let $P \subseteq \mathcal{P}$ be Σ_1, then there exists a C E field K of any prescribed characteristic χ, such that K is computable, possesses a splitting algorithm, and $S(K) = N_P$.*

(K possesses a splitting algorithm just means that there exists an admissible indexing i of K, such than K possesses a splitting algorithm with respect to i.)

THEOREM 1.2. *Let $P \subseteq \mathcal{P}$ be Σ_2, then there exists a C E field K of any prescribed characteristic χ, such that K is computable, and $S(K) = N_P$.*

As mentioned above, these two theorems can be considered as converses of the two first statements of this section. Indeed, let us denote by dg S the degree of recursive unsolvability of S, then it is clear that for any $P \subseteq \mathcal{P}$, $\mathrm{dg}\, P = \mathrm{dg}\, N_P$, and that for any degree $\boldsymbol{a}$, there exists a set $P \subseteq \mathcal{P}$ such that $\mathrm{dg}\,\mathrm{P} = \boldsymbol{a}$. We thus get the following corollaries:

COROLLARY. *Let $\boldsymbol{a}$ be a Σ_1 degree of recursive unsolvability. Then there exists a field K of any prescribed characteristic, such that K is computable, possesses a splitting algorithm, and $\mathrm{dg}\, S(K) = \boldsymbol{a}$.*

COROLLARY. *Let $\boldsymbol{a}$ be a Σ_2 degree of recursive unsolvability. Then there exists a field K of any prescribed characteristic, such that K is computable and $\mathrm{dg}\, S(K) = \boldsymbol{a}$.*

We thus have a complete characterization of $\mathrm{dg}\, S(K)$ for computable fields K, with or without splitting algorithms.

Theorems 1.1 and 1.2 will be obtained by the construction of appropriate algebraic extensions of computable quasi-finite fields. A field F is said to be quasi-finite [1] if F is perfect and possesses precisely one extension of each degree. Any finite field is of course quasi-finite, and any quasi-finite field is a C E field. Any finite extension of a quasi-finite field is obviously quasi-finite. It is shown in [1, beginning of §8] that quasi-finiteness can be characterized by a set of first-order sentences. It follows that any non-trivial ultraproduct of all prime finite fields is quasi-finite with characteristic 0.

§2. Recursively presentable quasi-finite fields

A structure $\mathcal{A} = \langle A, R_j \rangle_{j \in J}$ is said to be recursively presentable if A is at most countable, and there is an enumeration of $A: a_1, a_2, \ldots$, such that the complete diagram of $\langle \mathcal{A}, a_1, a_2, \ldots \rangle$ is decidable, that is

$$\{\langle \ulcorner \varphi \urcorner, i_1, \ldots, i_m \rangle : \mathcal{A} \models \varphi\,[a_{i_1}, \ldots, a_{i_m}]\} \text{ is recursive.}$$

It is a well known theorem that any decidable theory admits a recursively presentable model (see, for example, [3, theor. 1, p. 115]).

Obviously, any recursively presentable field is computable and possesses a splitting algorithm. We need the following result of J. Ax:

THEOREM (Ax). *The theory of statements true in all but a finite set of prime finite fields is decidable* [1, §11, theor. 13″].

Note that this theory contains the set of sentences which characterizes quasi-finite fields, as well as a set of sentences which says that the characteristic is 0, so we may conclude:

THEOREM 2.1. *There exists a recursively presentable quasi-finite field of any prescribed characteristic* χ.

PROOF. For $\chi = 0$, take a recursively presentable model of the theory of statements true in all but a finite set of prime finite fields. For χ = a prime p, take the prime field of characteristic p.

§3. Proof of the main theorems

We recall the following definitions and results of Rabin about computable fields: Let k_1 and k_2 be computable fields, i_1 and i_2 respective admissible indexings. An isomorphism φ of k_1 into k_2 is said to be computable with respect to i_1 and i_2 if $i_2 \circ \varphi \circ i_1^{-1}$ is a recursive function of $i_1(k_1)$ into N. If in addition $i_2(\varphi(k_1))$ is a recursive subset of $i_2(k_2)$, we say that φ is strongly computable with respect to i_1 and i_2.

THEOREM (Rabin). (I). *If k is a computable field and i an admissible indexing of k, then the algebraic closure $\bar{k}$ of k is computable, and there exists an admissible indexing i_1 of $\bar{k}$ such that the imbedding isomorphism φ of k into $\bar{k}$ is computable with respect to i and i_1* [5, theor. 7].

(II). *A necessary and sufficient condition for a computable field k to possess a splitting algorithm with respect to the admissible indexing i is the existence of an admissible indexing i_1 of $\bar{k}$ such that the imbedding isomorphism φ of k into $\bar{k}$ is strongly computable with respect to i and i_1* [5, *theor.* 8].

PROOF OF THEOREM 1.1. Let k be a quasi-finite computable field which possesses a splitting algorithm. Such a field exists in any prescribed characteristic by Theorem 2.1. By Rabin's theorem, there exists an admissible indexing i of $\bar{k}$ such that $i(k)$ is a recursive subset of $i(\bar{k})$, and we clearly can assume that $i(\bar{k}) = N$. Let $P \subseteq \mathcal{P}$ be recursively enumerable. We shall construct a field F, $k \subseteq F \subseteq \bar{k}$, $i(F)$ recursive, and $S(F) = N_P$. This will prove the theorem. (The recursiveness of $i(F)$ will imply that $i|_F$ is an admissible indexing of F, and that F possesses a splitting algorithm with respect to it. F will, of course, be a C E field as an algebraic extension of the C E field k.)

If $P = \emptyset$, then $N_P = \{1\}$, and $F = \bar{k}$.

Assume $P \neq \emptyset$. Then, P being r.e., there exists a recursive $\lambda : N \to N$ with

(3.1) $\forall p \in \mathcal{P}(p \in P \leftrightarrow \exists n \; p = p_{\lambda(n)})$, where p_n = the n^{th} prime.

We define an increasing sequence of fields $k = k_0 \subseteq k_1 \subseteq \cdots \subseteq \bar{k}$ as follows:

$$(3.2)_n \qquad \begin{cases} k_n = k_{n-1}(i^{-1}(n)) & \text{if } \forall m \leq n \; p_{\lambda(m)} \nmid [k_{n-1}(i^{-1}(n)) : k_{n-1}] \\ k_n = k_{n-1} & \text{otherwise.} \end{cases}$$

(It is assumed that $\forall n \; p_{\lambda(n)} \neq 1$.)

Let $F = \bigcup_{n<\omega} k_n$.

Proposition 1. *There exists an algorithm which decides, given any n, whether*

$$k_n = k_{n-1} \quad \textit{or} \quad k_n = k_{n-1}(i^{-1}(n)).$$

For the proof of Proposition 1, we need two more results about computable fields:

Lemma. *Let i be an admissible indexing of the algebraic closure $\bar{k}$ of a field k, such that the set $i(k)$ is recursive. Then the function $d : i(\bar{k}) \to N$ defined by $d(n) = [k(i^{-1}(n)):k]$ is recursive* [5, lemma 6].

Theorem. *Let i be an admissible indexing of the algebraic closure $\bar{k}$ of a perfect field k, such that the set $i(k)$ is recursive. Then the set $i(k(\alpha))$ is recursive for every $\alpha \in \bar{k}$. Moreover, the following relation is recursive:*

$$\{(m, \langle n_1, \ldots, n_l \rangle) : i^{-1}(m) \in k(i^{-1}(n_1), \ldots, i^{-1}(n_l))\}.$$

The first part of the theorem which in view of Rabin's theorem approximately says that any finite separable extension of a computable field possessing a splitting algorithm is itself computable and possesses a splitting algorithm, is a result of Van der Waerden [6, pp. 134–135], and a proof of it in terms of admissible indexings can be found in [5, theor. 9]. This proof is easily seen to imply in fact the stronger second part of the theorem.

Proof of Proposition 1. Let $n \geq 1$. To decide whether $k_n = k_{n-1}$ or $k_n = k_{n-1}(i^{-1}(n))$, proceed as follows: compute $d_1 = [k_0(i^{-1}(1)):k_0]$. This can be done effectively by the above lemma. Decide whether $k_1 = k_0$ or $k_1 = k_0(i^{-1}(1))$ according to condition $(3.2)_1$:

$$k_1 = k_0(i^{-1}(1)) \quad \text{iff} \quad p_{\lambda(1)} \nmid d_1 .$$

By the above theorem, $i(k_1)$ is recursive, and the lemma can again be applied to compute $d_2 = [k_1(i^{-1}(2)):k_1]$ and decide whether $k_2 = k_1$ or $k_2 = k_1(i^{-1}(2))$, according to condition $(3.2)_2$. The final answer for k_n is obtained after n similar steps. Note that this procedure is uniform in n.

PROPOSITION 2. *For all* n, $i^{-1}(n) \in F$ *iff* $i^{-1}(n) \in k_n$.

PROOF. Suppose there exists $n_1 < n_2$ with $i^{-1}(n_1) \in k_{n_2}$, $i^{-1}(n_1) \notin k_{n_1}$. By $(3.2)_{n_1}$, $(\exists m \leq n_1\, p_{\lambda(m)} \mid [k_{n_1-1}(i^{-1}(n_1)) : k_{n_1-1}])$. Since $i^{-1}(n_1) \in k_{n_2}$, $p_{\lambda(m)} \mid [k_{n_2}:k_{n_1-1}]$, but this is impossible for it follows from $(3.2)_n$ that for any element $i^{-1}(n)$ adjoined from the n_1th step onwards, the degree $[k_{n-1}(i^{-1}(n)):k_{n-1}]$ is not divisible by $p_{\lambda(m)}$.

It follows from Propositions 1 and 2 that the set $i(F)$ is recursive: for all n, $n \in i(F)$ iff $n \in i(k_n)$ iff $k_n = k_{n-1}(i^{-1}(n))$, and this is decidable.

It remains to be shown that $S(F) = N_P$:

PROPOSITION 3. $N_P \subseteq S(F)$.

PROOF. Let $m \in N_P$. By (3.1) there exists n_0 such that $\forall p \in \mathcal{P}$ $(p \mid m \rightarrow \exists n \leq n_0 : p = p_{\lambda(n)})$, which by $(3.2)_n$ for $n > n_0$ implies that $(m, [k_n : k_{n_0}]) = 1$ for all $n \geq n_0$.

Let $\Delta \subseteq \bar{k}$ be an extension of k_{n_0} satisfying $[\Delta : k_{n_0}] = m$ (k_{n_0} is quasi-finite as a finite extension of k). Then clearly $\Delta \cap F = k_{n_0}$. Now if N/K is Galois, E is an extension of K, and $L = E \cap N$, then E and N are linearly disjoint over L (see, for example, [2, §10, theor. 1]). In our case, since all the finite extensions considered are Galois and even cyclic, it follows that Δ and F are linearly disjoint over k_{n_0}, which is equivalent to $[\Delta F : F] = [\Delta : k_{n_0}] = m$. Hence $m \in S(F)$.

PROPOSITION 4. $S(F) \subseteq N_P$.

PROOF. Let $m \in S(F)$, $[\Delta : F] = m$, and let p be a prime divisor of m. Since Δ/F is cyclic, there exists a field Φ, $F \subseteq \Phi \subseteq \Delta$, $[\Phi : F] = p$. Let $\theta = i^{-1}(n_1) \in \bar{k}$ be a primitive element of the extension Φ/F, and let m_0 be such that all the coefficients of the minimal polynomial of θ are in k_{m_0}. Then

$$m \geq m_0 \Rightarrow [k_m(\theta) : k_m] = [F(\theta) : F] = p .$$

Since $\theta \notin F$, we have, by Proposition 2, $\theta \notin k_{n_1}$. Hence there is $n_2 \leq n_1$ with $p_{\lambda(n_2)} \mid [k_{n_1-1}(\theta) : k_{n_1-1}]$.

If $n_1 - 1 \geq m_0$, then $[k_{n_1-1}(\theta) : k_{n_1-1}] = p$, so $p = p_{\lambda(n_2)}$.

If $n_1 - 1 < m_0$, then $p_{\lambda(n_2)} \mid [k_{m_0}(\theta):k_{n_1-1}] = [k_{m_0}(\theta):k_{m_0}] \cdot [k_{m_0}:k_{n_1-1}]$. By our construction $p_{\lambda(n_2)} \nmid [k_n : k_{n-1}]$ for all $n \geq n_2$, implying $p_{\lambda(n_2)} \nmid [k_{m_0}:k_{n_1-1}]$. Hence $p_{\lambda(n_2)} \mid [k_{m_0}(\theta):k_{m_0}] = p$, so $p = p_{\lambda(n_2)}$. This shows that $p \in P$.

Proof of Theorem 1.2. Again, k is quasi-finite of a prescribed characteristic χ, and i is an admissible indexing of $\bar{k}$, such that the set $i(k)$ is recursive, and $i(\bar{k}) = N$. $P \subseteq \mathcal{P}$ is Σ_2. We shall construct a computable field F, $k \subseteq F \subseteq \bar{k}$, such that $S(F) = N_P$.

Lemma. *Let $S \subseteq N$ be Π_2. There exists a sequence of sets of integers $\{A_n\}_{n=1}^{\infty}$ such that*:

1) $S = \limsup A_n = \bigcap_{m=1}^{\infty} \bigcup_{n=m}^{\infty} A_n$.

2) *If χ_n is the characteristic function of the set A_n, then $\chi_n(m)$ is a recursive function of n and m.*

3) $A_n \neq \emptyset$ *for all n.*

Proof. Since S is Π_2, there exists a recursive $R \subseteq N^3$, such that

$$\forall s \in N(s \in S \leftrightarrow \forall m \exists n\, (m, n, s) \in R).$$

We define $f(n,s) = \max\{m : m \leq n \wedge \forall m' \leq m \exists n' \leq n\, (m', n', s) \in R\}$. Then f is clearly a recursive function, and for every fixed s_0, $f(n, s_0)$ is a non-decreasing function of n.

Define $A_n \subseteq N$ by:

$$s \in A_n \leftrightarrow s = n \vee f(n,s) > f(n-1,s).$$

From the definition of f, it follows that for every fixed s_0, the function $f(n, s_0)$ has an infinite number of jumps iff $\forall m \exists n\, (m, n, s_0) \in R$, i.e. iff $s_0 \in S$. This proves property (1).

(2) is clear since f is recursive, and (3) follows from the fact that $n \in A_n$ for all n.

Returning to the proof of Theorem 1.2, let $S = \mathcal{P} - P$. Since P is Σ_2, S is Π_2 and there exists for S a sequence $\{A_n\}_{n=1}^{\infty}$ as in the lemma. We clearly can assume that $A_n \subseteq \mathcal{P}$ and $1 \notin A_n$ for all n.

Let $k = k_0 \subseteq k_1 \subseteq \cdots \subseteq \bar{k}$ be the sequence of fields defined by $k_{n+1} = k_n(\theta_{n+1})$, where θ_{n+1} is the first element θ of $\bar{k}$ (in the enumeration $i^{-1}(1), i^{-1}(2), \ldots$) which satisfies $[k_n(\theta):k_n] \in A_n$. For each n, θ_{n+1} exists, for the finiteness of the extension k_n/k_0 implies that k_n is quasi-finite, and for any $p \in A_n$, there exists $\theta \in \bar{k}$ with $[k_n(\theta):k_n] = p$. Moreover, θ_{n+1} can be found effectively, i.e. the function $f(n) = i(\theta_n)$ is recursive.

Define $F = \bigcup_{n<\omega} k_n$.

LEMMA. *Let k be a computable field, i an admissible indexing of k, and A a subset of k such that $i(A)$ is recursively enumerable. Then the subfield of k generated by A is computable.*

A proof of the lemma for the case of computable groups may be found in [5, theor. 3]. The proof for computable fields is completely analogous.

It follows from the lemma that F is computable.

Finally we prove $S(F) = N_P$:

1) $N_P \subseteq S(F)$. Let $m \in N_P$. Since lim sup $A_n = \mathcal{P} - P$, there exists n_0 such that for all $n \geq n_0$ no member of A_n divides m. k_{n_0} being quasi-finite, there exists an extention Δ/k_{n_0}, $[\Delta : k_{n_0}] = m$, and as in the proof of Theorem 1.1 (Proposition 3), we see that Δ and F are linearly disjoint over k_{n_0}. Thus $[\Delta F : F] = m$, and $m \in S(F)$.

2) $S(F) \subseteq N_P$. Let $n \in S(F)$, and $p \in \mathcal{P}$, $p \mid n$. As in the proof of Theorem 1.1 (Proposition 4), we can find $\theta_0 \in \bar{k}$ and m_0 such that $m \geq m_0 \Rightarrow [k_m(\theta_0):k_m] = [F(\theta_0):F] = p$. Suppose that $p \notin P$. Then $p \in$ lim sup A_n, which means that there is a sequence $\{n_j\}_{j=1}^{\infty}$ such that, for every j, $p \in A_{n_j}$. Now θ_{n_j+1} is the first member θ of $\bar{k}$ such that $[k_{n_j}(\theta):k_{n_j}] \in A_{n_j}$. For all j such that $n_j \geq m_0$, θ_0 satisfies $[k_{n_j}(\theta_0):k_{n_j}] = p \in A_{n_j}$, hence it belongs to the set of candidates for adjunction at step n_j. It follows that θ_0 must indeed be adjoined in the construction of F at most at the $n_{j_0+i(\theta_0)}$ step, where j_0 is the least j such that $n_j \geq m_0$. This is a contradiction, which shows that $p \in P$.

§4. Concluding remark

As in [2], let $S^*(k) = \{n \in N$: there exists a normal extension $F/k, [F:k] = n\}$. The same questions we asked about $S(k)$ naturally arise for $S^*(k)$.

First, note that for any field k, k has a normal extension of degree n iff k has a normal simple extension of degree n. Now, it is not difficult to show that the proposition "k has a normal simple extension of degree n" can be formulated as a Σ_2 sentence about k, or as a Σ_1 sentence if we allow the use of a supplementary predicate $I(f)$, whose interpretation in $k[t]$ is: $f(t)$ is irreducible over k.

It follows that, as for $S(k)$, $S^*(k)$ is Σ_2 whenever k is computable, and it is Σ_1 if, in addition, k possesses a splitting algorithm.

Since all the fields whose existence was proved in this paper are CE fields, they satisfy $S^*(F) = S(F)$. We thus obtain for sets of normal degrees the same full characterization as for sets of degrees.

References

1. J. Ax, *The elementary theory of finite fields*, Ann. of Math. **88** (1968), 239–271.

2. N. Bourbaki, *Algèbre*, Chapitre V, Actualités Sci. Indust. No. 1102, Hermann, Paris, 1950.

3. Ju. L. Ershov, *Constructive models*, in *Selected Questions of Algebra and Logic*, Nauka, Novosibirsk, 1973, pp. 111–130 (Russian).

4. Basil Gordon and E. G. Straus, *On the degrees of the finite extensions of a field*, in Proc. Symp. Pure Math., Vol VIII, Amer. Math. Soc., Providence, R.I., 1965, pp. 56–65.

5. M. O. Rabin, *Computable algebra, general theory and theory of computable fields*, Trans. Amer. Math. Soc. **95** (1960), 341–360.

6. B. L. van der Waerden, *Modern Algebra*, Vol. I, New York, Ungar, 1949.

The Hebrew University of Jerusalem
Jerusalem, Israel