BULL. AUSTRAL. MATH. SOC. 12F15
VOL. 33 (1986), 219-226.

FIELDS COUNTABLY GENERATED OVER A PROPER SUBFIELD

JAMES K. DEVENEY AND JOE YANIK

For an arbitrary field K there are two related questions that can be asked:

(1) Is there a proper subfield, L, of K such that K is countably generated over L?

(2) Given a proper subfield M of K is there a proper subfield, L, of K containing M such that K is countably generated over L?

We give an affirmative answer to (1) in characteristic $p \neq 0$ and provide counterexamples to (2) for arbitrary characteristic $\neq 2$.

Let L be a field and let K be a proper subfield of L. If L is algebraically closed, then the only finite possibility for the dimension of L over K is 2, and this can occur if and only if K is real closed. In [1], it was shown that any algebraically closed field L has a proper subfield K of countable codimension, that is, $[L:K] \leq \aleph_0$. This leads naturally to the question of when an arbitrary field L has a subfield of countable codimension. If the characteristic of L is $p > 0$, then L must have a subfield of countable codimension (Theorem 1). The general question for fields of characteristic 0 is still open.

This paper also examines the more general question: If $L \supseteq K$, does L have a subfield of countable codimension which contains K. An example is constructed for any characteristic $p \neq 2$ of a separable algebraic field extension $L \supseteq K$ with no proper subfield of countable codimension

Received 6 June 1985.

containing K. This example is also used to gain information on the lattice of intermediate fields of a field extension.

I

THEOREM 1. *Let L be a non-prime field of characteristic $p \neq 0$. Then L has a subfield of countable codimension.*

Proof. Suppose L is not perfect, that is, $L \neq L^p$. Let B be a p-basis for L ([2], p. 180), and let $x \in B$. Then $[L:L^p(B \setminus \{x\})] = p$ and L has a subfield of finite codimension. Thus we may assume L is perfect. If L is algebraic over its prime subfield F, then L is countable and hence F is of countable codimension. Thus let $X \neq \emptyset$ be a transcendence basis for L over F and let $x \in X$. Let $L_1 = F(\{y_\alpha^{p^{-n}} \mid y_\alpha \in X \setminus \{x\}, n \in N\}, x)$. Then L is algebraic over L_1 and $[L_1 : L_1^p] = p$. Let L_2 be the separable algebraic closure of L_1 in L. Then $[L_2 : L_2^p] = p$ and L is purely inseparable over L_2. Thus $L = L_2(\{x^{p^{-n}} \mid n \in Z\})$ and L_2 is a subfield of countable codimension.

LEMMA 2. *Assume L is separable normal algebraic over K and G is the Galois group of L over K. Then L is countably generated over K if and only if G has countably many closed normal subgroups of finite index in G.*

Proof. Suppose L/K is countably generated, say $L = K(\{x_i \mid i \in N\})$. The set of finite subsets of N is countable and, for each finite subset S of N, the set of normal extensions of K contained in $K(\{x_i \mid i \in S\})$ is finite. Since each finite normal extension of K is contained in $K(\{x_i \mid i \in S\})$ for some finite $S \subseteq N$, the set of finite normal extensions of K in L is countable, and hence G has countably many closed normal subgroups of finite index in G.

Conversely, suppose there are countably many closed normal subgroups of finite index in G. Then there are countably many finite normal extensions of K in L, each generated by a finite number of elements.

https://doi.org/10.1017/S0004972700003087 Published online by Cambridge University Press

But every element of L is in some finite normal extension of K and hence L is countably generated over K.

It follows from Lemma 2 that any field L which has an automorphism σ and is algebraic over the fixed field of σ has a subfield of countable codimension.

COROLLARY 3. *Let* $L \subseteq K$ *be a separable algebraic field extension.* L *is countably generated over* K *if and only if there are at most a countable number of finite extensions of* K *in* L.

Proof. If L/K is countably generated, then the normal closure, $\hat{L}$, of L is countably generated over K. By Lemma 2, there are at most a countable number of finite extensions of K in $\hat{L}$, hence certainly of K in L. Conversely, let $\{\alpha_i \mid i \in N\}$ be a set of primitive elements for the finite extension of K in L. Then $L = K(\{a_i \mid i \in N\})$.

The following result is a generalization of some ideas in [1].

PROPOSITION 4. *Let* L *be an algebraic extension of* K. *If there is a countably generated separable algebraic extension* F *of* L *and a* K*-automorphism* σ *of* F *which does not leave* L *elementwise fixed, then* L *has a proper subfield of countable codimension which contains* K.

Proof. Let $F = L(\{x_i \mid i \in N\})$. By adjoining all the conjugates of $\{x_i \mid i \in N\}$ we may assume F is normal over L. Let G be the Galois group of F over K and let H_1 be the Galois group of F over L. The fixed field of H_1 is L and the fixed field of G, F^G, is a proper subfield of L which contains K. If L is normal over F^G, let θ be an F^G-automorphism of L with $\theta \neq id$. If H is the group generated by θ, Lemma 2 shows L is countably generated over L^H.

If L/F^G is not normal, then H_1 is not normal in G. Let H_2 be a conjugate of H_1 in G. By Lemma 2, H_1 and H_2 both have countably many closed normal subgroups of finite index. Let $H = \langle H_1 \cup H_2 \rangle$. We claim H has countably many closed normal subgroups of finite index. This follows since a closed normal subgroup of finite index corresponds to the kernel of a continuous homomorphism of H onto a finite group G_0.

https://doi.org/10.1017/S0004972700003087 Published online by Cambridge University Press

But a homomorphism is completely determined by its restriction to H_1 and H_2. Thus by Lemma 2 and Corollary 3, L is countably generated over F^H.

COROLLARY 5. *Let* $L \supseteq K$ *be fields with* L/K *not purely inseparable. If* $\bar{L}$, *the algebraic closure of* L, *is countably generated over* L *then* L *has a proper subfield of countable codimension which contains* K.

Proof. Since $L \supseteq K$, L has a proper subfield containing K over which L is algebraic. Thus we may assume L is algebraic over K. Thus there is an isomorphism $\sigma \neq id$ of L over K into $\bar{L}$. Since $\bar{L}$ is algebraically closed, σ can be extended to an automorphism of $\bar{L}$. Proposition 4 now gives the desired result.

II

In this section we construct an example of a field L with a proper subfield K such that, for any field M, $K \subseteq M \subseteq L$, the codimension of M in L is uncountable.

Let S be an uncountable set. For each positive integer j define $I_j = S \times S \times \ldots \times S$ the product taken j times. Let $I = \bigcup_{j=1}^{\infty} I_j$.

We define a map $I_j \xrightarrow{-} I_{j-1}$ by $\alpha = (\alpha_1, \ldots, \alpha_j) \to \bar{\alpha} = (\alpha_1, \ldots, \alpha_{j-1})$.

Let k be an arbitrary field with char $k \neq 2$.

Define $K = k(\{x_\alpha \mid \alpha \in I\})(z)$ where the x_α and z are algebraically independent.

We define recursively z_α for $\alpha \in I$ by

$$z_\alpha = x_\alpha + \sqrt{z} \quad \text{for} \quad \alpha \in I_1$$

$$= x_\alpha + \sqrt{z_{\bar{\alpha}}} \quad \text{for} \quad \alpha \in I_n \, , \quad n > 1 \, .$$

Let $L = K(\{z_\alpha \mid \alpha \in I\})$.

LEMMA 6. $L = k(\{w_\alpha \mid \alpha \in I\})(w)$ *where* $w_\alpha = \sqrt{z_\alpha}$, $w = \sqrt{z}$ *and the set* $(\{w_\alpha \mid \alpha \in I\} \cup \{w\}$ *is algebraically independent over* k. *(Hence*

https://doi.org/10.1017/S0004972700003087 Published online by Cambridge University Press

L is a pure transcendental extension of k *).*

Proof. Note that $x_\alpha = w_\alpha^2 - w_{\bar{\alpha}}$ where, if $\alpha \in I_1$, we make the convention that $w_{\bar{\alpha}} = w$. So clearly $L = k(\{w_\alpha \mid \alpha \in I\})(w)$. The fact that they are algebraically independent follows readily from the fact that the x_α's are algebraically independent.

Thus, L does have a subfield of countable codimension. In fact, $[L:M] = 2$ where $M = k(\{w_\alpha \mid \alpha \in I\})(w^2)$. However, $K \not\subseteq M$.

LEMMA 7. *Let* M *be a field with* $K \subseteq M \subseteq L$ *and suppose* $\sqrt{z_\alpha} \notin M$, *but* $z_\alpha \in M$. *Let* β *and* γ *be such that* $\bar{\beta} = \bar{\gamma} = \alpha$, *but* $\beta \neq \gamma$. *Then* $M(\sqrt{z_\beta}) \neq M(\sqrt{z_\gamma})$. *(Hence, there are uncountably many distinct finite extensions of* M *).*

Proof. Suppose $\sqrt{z_\beta} = \sqrt{x_\beta + \sqrt{z_\alpha}} \in M\left(\sqrt{x_\gamma + \sqrt{z_\alpha}}\right)$. Then

$$\sqrt{x_\beta + \sqrt{z_\alpha}} = a + b\sqrt{x_\gamma + \sqrt{z_\alpha}} \quad \text{for some } a,b \in M(\sqrt{z_\alpha})$$

so

$$x_\beta + \sqrt{z_\alpha} = a^2 + 2ab\sqrt{x_\gamma + \sqrt{z_\alpha}} + b^2(x_\gamma + \sqrt{z_\alpha}) .$$

If $ab \neq 0$, then $\sqrt{x_\gamma + \sqrt{z_\alpha}} \in M(\sqrt{z_\alpha}) \Rightarrow \sqrt{x_\beta + \sqrt{z_\alpha}} \in M(\sqrt{z_\alpha})$.

If $b = 0$ then $\sqrt{x_\beta + \sqrt{z_\alpha}} = a \in M(\sqrt{z_\alpha})$.

If $a = 0$ then $\sqrt{\dfrac{x_\beta + \sqrt{z_\alpha}}{x_\gamma + \sqrt{z_\alpha}}} \in M(\sqrt{z_\alpha})$.

So either $\sqrt{x_\gamma + \sqrt{z_\alpha}} \in M(\sqrt{z_\alpha})$ or $\sqrt{\dfrac{x_\beta + \sqrt{z_\alpha}}{x_\gamma + \sqrt{z_\alpha}}} \in M(\sqrt{z_\alpha})$.

We claim that both are impossible.

Suppose $\sqrt{x_\beta + \sqrt{z_\alpha}} = c + d\sqrt{z_\alpha}$ for some $c,d \in M$. Then

$$0 = 4c^4 - 4x_\beta c^2 + z_\alpha .$$

https://doi.org/10.1017/S0004972700003087 Published online by Cambridge University Press

Such a c could exist only if $\sqrt{16x_\beta^2 - 16z_\alpha} \in M$ (by the quadratic formula). Recall that $x_\beta = w_\beta^2 - w_\alpha$, $z_\alpha = w_\alpha^2$.

So $\sqrt{x_\beta^2 - z_\alpha} = \sqrt{w_\beta^4 - 2w_\beta^2 w_\alpha} \notin k(\{w_\delta | \delta \in I\})(w)$, hence is certainly not in M .

Now suppose that $\sqrt{\dfrac{x_\beta + \sqrt{z_\alpha}}{x_\gamma + \sqrt{z_\alpha}}} = c + d\sqrt{z_\alpha}$ for some $c, d \in M$. Then

$$x_\beta + \sqrt{z_\alpha} = (c^2 x_\gamma + dx_\gamma z_\alpha + 2cdz_\alpha) + (c^2 + d^2 z_\alpha + 2cdx_\gamma)\sqrt{z_\alpha}$$

or

$$x_\beta = c^2 x_\gamma + d^2 x_\gamma z_\alpha + 2cdz_\alpha$$

$$1 = c^2 + d^2 z_\alpha + 2cdx_\gamma$$

Solving simultaneously we get $d = \dfrac{x_\beta - x_\gamma}{2c(z_\alpha - x_\gamma^2)}$ which when substituted into the equation above yields, after simplifying,

$$0 = 4(z_\alpha - x_\gamma^2)^2 c^4 + 4[(x_\beta - x_\gamma)(z_\alpha - x_\gamma^2)x_\gamma - (z_\alpha - x_\gamma^2)^2]c^2 + (x_\beta - x_\gamma)^2 z_\alpha$$

As before, there could be a solution in M only if

$$4(z_\alpha - x_\gamma^2)\sqrt{[(x_\beta - x_\gamma)x_\gamma - (z_\alpha - x_\gamma^2)]^2 - (x_\beta - x_\gamma)^2 z_\alpha} \in M$$

Substituting $x_\beta = w_\beta^2 - w_\alpha$, $x_\gamma = w_\gamma^2 - w_\alpha$, $z_\alpha = w_\alpha^2$, and simplifying we get

$$\sqrt{[w_\beta^4 - w_\beta^2 w_\gamma^2 - w_\alpha^2 + w_\gamma^2 - w_\alpha][w_\beta^4 - w_\beta^2 w_\gamma^2 - w_\alpha^2 + w_\gamma^2 - w_\alpha - 2w_\alpha w_\beta^2 + 2w_\alpha w_\gamma^2}$$

But one can easily check that the term under the radical is not a square in L . (For example the first term is of degree 2 in w_α but is clearly not the square of a linear polynomial. Furthermore, the terms are relatively prime since their difference is $2w_\alpha(w_\beta^2 - w_\gamma^2)$ and neither

https://doi.org/10.1017/S0004972700003087 Published online by Cambridge University Press

ω_α , $\omega_\beta - \omega_\gamma$, or $\omega_\beta + \omega_\gamma$ are factors of either term).

Hence, there is no solution in M and $M(\sqrt{z_\beta}) \neq M(\sqrt{z_\gamma})$.

Note that, similarly, if $\sqrt{z} \notin M$ and $\beta, \gamma \in I_1$, with $\beta \neq \gamma$ then $M(\sqrt{z_\beta}) \neq M(\sqrt{z_\gamma})$. The proof is identical.

THEOREM 8. *Let* K *and* L *be as described above. Suppose* M *is a field with* $K \subseteq M \subsetneq L$. *Then the codimension of* M *in* L *is uncountable.*

Proof. Since $M \subsetneq L$, $\sqrt{z_\alpha} \notin M$ *for some* $\alpha \in I$. Let $n = \inf\{j \in N \mid \sqrt{z_\alpha} \notin M$ for some $\alpha \in I_j\}$ and let $\alpha \in I_n$ be such that $\sqrt{z_\alpha} \notin M$. Then, either $n = 1$ and $\sqrt{z} \notin M$ or $z_\alpha \in M$, by the minimality of n . By Lemma 7 or the remark after Lemma 7 there are uncountably many distinct finite extensions of M . By Corollary 3, the codimension is not countable.

III

The previous example is also interesting from the point of view of the lattice of intermediate fields. Let $L \supseteq K$ be an algebraic field extension. If there is a unique minimal intermediate field properly containing K , what can be said concerning the lattice of intermediate fields? Such fields naturally occur as follows. Let $\alpha \in L \setminus K$. By Zorn's Lemma there are subfields M of L containing K and maximal with respect to not containing α . Then L/M has a unique minimal intermediate field, namely $M(\alpha)$.

If L/K has a unique proper minimal intermediate field and L/K is separable algebraic normal, then the intermediate fields of L/K must be chained. To see this, one can first reduce to where L/K is finite dimensional normal. If $K(\alpha)$ is the unique minimal field, and $\sigma(\alpha) \neq \alpha$, then the fixed field of σ is a subfield of L which does not contain α , that is, is K . Then the Galois group is cyclic and the intermediate fields are chained. However, if L/K is not normal, the intermediate fields need not be chained. For example, let L and K be as in section 2 and let M be an intermediate field that contains z_α but that is maximal with respect to not containing $\sqrt{z_\alpha}$. Then L/M has a unique minimal subfield of dimension 2 over M, namely $M(\sqrt{z_\alpha})$, and yet there are uncountably many distinct subfields of dimension 4 over M.

References

[1] A. Bialynicki-Birula, "On subfields of countable codimension", *Proc. Amer. Math. Soc.* 35 (1972), 354-356.

[2] N. Jacobson, *Lectures in abstract algebra*, Vol. III. Theory of fields and Galois theory, (Von Nostrand, Princeton, N.J., 1964).

Department of Mathematical Sciences,
Virginia Commonwealth University,
Richmond, Virginia 23284.
U.S.A.

https://doi.org/10.1017/S0004972700003087 Published online by Cambridge University Press